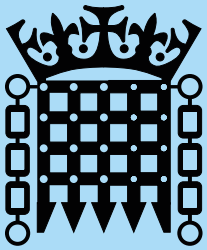


Intelligence and Security Committee of Parliament

China

Chairman:
The Rt Hon. Sir Julian Lewis MP

HC 1605

Intelligence and Security Committee of Parliament

China

Chairman:
The Rt Hon. Sir Julian Lewis MP

Presented to Parliament pursuant to sections 2 and 3
of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on
13 July 2023

HC 1605

Any enquiries regarding this publication should be sent to us via our webform at isc.independent.gov.uk/contact

This publication is also available on our website at: isc.independent.gov.uk

ISBN 978-1-5286-4302

E02938943 07/2023

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT*

The Rt Hon. Sir Julian Lewis MP (Chairman)

The Rt Hon. Maria Eagle MP
(from 10 February 2022)

The Rt Hon. Mark Pritchard MP
(until 22 January 2022)

The Rt Hon. Sir John Hayes CBE MP

Colonel The Rt Hon. Bob Stewart DSO MP

The Rt Hon. Stewart Hosie MP
(until 14 December 2022)

The Rt Hon. Theresa Villiers MP

The Rt Hon. Dame Diana Johnson DBE MP (until 14 January 2022)

Admiral The Rt Hon. Lord West of Spithead GCB DSC PC

The Rt Hon. Kevan Jones MP

The Rt Hon. Sir Jeremy Wright KC MP
(from 9 February 2022)

Owen Thompson MP
(from 7 February 2023)

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK Intelligence Community. The Committee was originally established by the Intelligence Services Act 1994 and was reformed, and its powers reinforced, by the Justice and Security Act 2013.

The Committee oversees the intelligence and security activities of the Agencies,** including the policies, expenditure, administration and operations of MI5 (the Security Service), MI6 (the Secret Intelligence Service or SIS) and GCHQ (the Government Communications Headquarters). The Committee also scrutinises the work of other parts of the Intelligence Community, including the Joint Intelligence Organisation (JIO) and the National Security Secretariat (NSS) in the Cabinet Office; Defence Intelligence (DI) in the Ministry of Defence; and Homeland Security Group† in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. Members are appointed by the Houses of Parliament, having been nominated by the Prime Minister in consultation with the Leader of the Opposition. The Chair of the Committee is elected by its Members.

* This Inquiry was commenced by the previous Committee, which sat from November 2017 to November 2019, and was completed by the current Committee. The Report is a compilation of the work undertaken by both Committees.

** Throughout the Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees; the term 'Agencies' refers to MI5, SIS and GCHQ as a collective; and the term 'Departments' refers to the intelligence and security parts of the Ministry of Defence, Cabinet Office and the Home Office (DI, JIO, the National Security Adviser (NSA), NSS and Homeland Security Group (HSG)) as a collective, unless specified otherwise.

† From 1 April 2021, the Home Office moved to a new structure and the work of the Office for Security and Counter-Terrorism (OSCT) is now carried out by Homeland Security Group. Therefore, OSCT is now referred to as Homeland Security Group.

The Members of the Committee are subject to section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties. The Committee sets its own agenda and work programme, taking evidence from Government Ministers, the Heads of the intelligence and security Agencies, senior officials, experts and academics as required. Its Inquiries tend to concentrate on current events and issues of concern, and therefore focus on operational[††] and policy matters, while its Annual Reports address administration and finance.

The Reports can contain highly classified material, which would damage the operational capabilities of the intelligence Agencies if it were published. There is therefore a well-established and lengthy process to prepare the Committee's Reports ready for publication. The Report is checked to ensure that it is factually correct (i.e. that the facts and figures are up to date in what can be a fast-changing environment). The Intelligence Community may then, on behalf of the Prime Minister, request redaction of material in the Report if they consider that its publication would damage their work – for example, by revealing their targets, methods, sources or operational capabilities. The Committee requires the Intelligence Community to demonstrate clearly how publication of the material in question would be damaging, since the Committee aims to ensure that only the minimum of text is redacted from a Report. Where the Committee rejects a request for material to be redacted, if the organisation considers that the material would cause serious damage to national security if published, then the Head of that organisation must appear before the Committee to argue the case. Once these stages have been completed, the Report is sent to the Prime Minister to consider. Under the Justice and Security Act 2013, the Committee can only lay its Reports before Parliament once the Prime Minister has confirmed that there is no material in them which would prejudice the discharge of the functions of the Agencies or – where the Prime Minister considers that there is such material in the Report – once the Prime Minister has consulted the Committee and it has then excluded the relevant material from the Report.

The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted: redactions are clearly indicated in the Report by ***. This means that the published Report is the same as the classified version sent to the Prime Minister (albeit with redactions).

[††] The Committee oversees operations subject to the criteria set out in section 2 of the Justice and Security Act 2013.

CONTENTS

OVERVIEW

> ***There is effectively a global values struggle going on in which China is determined to assert itself as a world power … China is increasingly thinking of a future in which it could be the world power and that means that – if you think of UK interests as being in favour of good governance and transparency and good economic management, which … serve our national interest because it helps with trade, investment, prosperity and stability and so forth – then I think that China represents a risk on a pretty wide scale.***
>
> – Chair of the Joint Intelligence Committee (JIC)

China's interest in the UK

1. China's national imperative continues to be the continuing dominance and governance of the Chinese Communist Party (CCP). However, it is its ambition at a global level – to become a technological and economic superpower, on which other countries are reliant – that represents the greatest risk to the UK.

2. The UK may not be the top priority for China when it comes to espionage and interference, but it is nevertheless of significant interest, mainly given our close relationship with the United States (US): China sees almost all of its global activity in the context of its struggle with the US. The UK is also of interest given its membership of international bodies of significance to China and the perception of the UK as an opinion-former – which plays into China's strategy to reshape international systems in its favour. These factors would appear to place the UK just below China's top priority targets, as it seeks to build support for its current 'core interests': to mute international criticism and to gain economically.

3. In respect of the latter, China sees the UK as a home for Chinese investment. This approach can be seen in relation to nuclear energy: Chinese interest lies in gaining UK regulatory approval for its reactor designs as it assesses that this will influence other countries to permit Chinese investment in their Civil Nuclear sectors. The same philosophy lay behind Huawei's interest in the UK's 5G telecommunications network.

The Inquiry

4. At the outset of this Inquiry, the Committee considered whether Huawei should be allowed to supply equipment for the UK's 5G telecommunications network: the key consideration, which lay at the heart of that issue, was the UK's over-reliance on Chinese technology. We urged that action be taken urgently to address this, cautioning: "*This will require us to take a long-term view – but we need to start now*."[1] China's aspirations are looking ahead to 2049, and the UK needs to be thinking in the same way.

5. Our Inquiry has continued since then, considering the nature of the threat more broadly (although evidence-taking concluded in 2021 – prior to the Russian invasion of Ukraine in

[1] 'ISC Statement on 5G suppliers', Intelligence and Security Committee website, 19 July 2019.

February 2022).[2] The Committee has taken evidence from a wide range of witnesses and considered a substantial volume of written evidence. We are grateful to those witnesses from outside the Intelligence Community – in particular John Gerson, Raffaello Pantucci, Charles Parton, Lord Patten, Dr Tim Stevens and Professor Steve Tsang – for kindly volunteering their very substantial expertise on China, as part of the Inquiry; we have benefitted greatly from their experience and knowledge.

6. This Report has been split into two parts. Part One considers the overall intelligence threat from China to the UK, and HMG's response to that threat. Part Two considers Case Studies on the threat to three specific areas – Academia, Industry and Technology, and Civil Nuclear energy – together with an annex considering China's response to, and use of, the Covid-19 pandemic.[3]

The 'whole-of-state' threat

7. It is clear that China has taken advantage of the policy of successive British Governments to boost economic ties between the UK and China, which has enabled it to advance its commercial, science and technology, and industrial goals in order to gain a strategic advantage. The fact that China is a strategic threat is not news. However, this Report explores the multifaceted nature of the intelligence threat posed by China.

8. China almost certainly maintains the largest state intelligence apparatus in the world – dwarfing the UK's Intelligence Community and presenting a challenge for our Agencies to cover. As a result, our Agencies' work has to be targeted on those aspects that are most damaging. However, the problem is compounded by China's 'whole-of-state' approach. In practice, this means that Chinese state-owned and non-state-owned companies, as well as academic and cultural establishments and ordinary Chinese citizens, are liable to be (willingly or unwillingly) co-opted into espionage and interference operations overseas: much of the impact that China has on national security is overt – through its economic might, its takeovers and mergers, its interaction with Academia and Industry – as opposed to covert activity carried out by its intelligence officers.

9. China's size, ambition and capability have enabled it to successfully penetrate every sector of the UK's economy, and – until the Covid-19 pandemic – Chinese money was readily accepted by HMG with few questions asked. China's commercial and industrial strategy is deliberately calibrated to establish China as an economic leader, a digital technology powerhouse and a global commercial power – on which the West is dependent. China has been buying up and seeking to control or influence the UK's Industry and Energy sectors: we have already mentioned China's interest in the UK's Civil Nuclear sector. China has been encouraged by decisions to allow the China General Nuclear Power Group into Hinkley Point C and promises of future investment in other sites. The Government has been

[2] The Committee began this Inquiry in 2019. Shortly afterwards followed: the dissolution of the Intelligence and Security Committee in November 2019 ahead of the General Election; a series of national lockdowns in 2020 and 2021 in the wake of the global Covid-19 pandemic; and the excessive delay in appointing a new Committee from December 2019 to July 2020. These events have impeded the conclusion of this Inquiry and the publication of our Report. Throughout this period, we continued to question, and take evidence from, the Intelligence Community on this important and timely Inquiry. (In preparing this Report, the Committee has considered evidence up to 2021.)

[3] The two Parts of the Report are designed to be read in conjunction.

so keen to take Chinese money that it has not been watching China's sleight of hand whilst it overtly penetrated the UK's Energy and Industry sectors: issues that are explored in Part Two of this Report.

10. China's ruthless targeting is not just economic: it is similarly aggressive in its interference activities, which it operates to advance its own interests, values and narrative at the expense of those of the West. While seeking to exert influence is a legitimate course of action, China oversteps the boundary, and crosses the line into interference in the pursuit of its interests and values at the expense of those of the UK. For example, China has been particularly effective at using its money and influence to penetrate or buy Academia in order to ensure that its international narrative is advanced and criticism of China supressed. This helps to reinforce the CCP's narrative and gives its international posture external credibility – helping it on its way to becoming a world power.

11. China's attempts to influence the international narrative can also be seen clearly in its response to the recent Covid-19 pandemic. Rather than being damaged by it, China has worked hard on disinformation. It has greatly exaggerated its work to counter the virus and develop vaccines, and has sown seeds of doubt about the origins of the virus, to make the world believe that China was not at fault. Further, it appears positioned to capitalise on the damage to world economies and may well emerge from the pandemic stronger than before – and certainly stronger relative to many other countries that have suffered from the pandemic. We also consider this issue in Part Two of the Report.

Protecting the UK

12. So what of the UK's response to this threat? As the world's second largest economy (and one of the fastest growing), with a military increasing in size and capability, considerable levels of diplomatic engagement and a large digital sector which acts as a force multiplier, China has a significant impact on global affairs. The balance between security and prosperity requires dexterity and we understand that there are a number of difficult trade-offs involved. The Government's policy on, and strategy towards, China must take this into account when considering how to tackle the threats China poses to the UK.

13. The Government says its response is "*robust*" and "*clear-eyed*".[4] The External Experts we spoke to were rather less complimentary. While we sought to examine whether the Government's strategy for dealing with such a large adversary was up to the task, they felt very strongly that HMG did not have any strategy on China, let alone an effective one, and that it was singularly failing to deploy a 'whole-of-government' approach when countering the threat from China – a damning appraisal indeed.

14. One of the factors involved is that, until recently, our Agencies did not even recognise that they had any responsibility for countering Chinese interference activity in the UK. Instead, they focused their efforts on China's 'covert' activity in the UK *** resources were diverted onto the acute counter-terrorism threat arising from Syria. Time and again resources have had to be diverted to tackling the terrorist threat, and it is clear that, historically, China did not receive as much attention as ***.

[4] Written evidence – HMG, 18 April 2019.

15. Yet the security community were at least aware of many of the issues we address in this Report several years ago and we were therefore surprised at how long it had taken for a process to be put in place to identify and protect UK assets, based on the UK's sovereign interests ***. The Government's lack of understanding contrasts with the approach of the US, which has already produced a national strategy on critical and emerging technologies, aimed at protecting its technological dominance, in which it lists what it considers to be its 20 priority technologies. The lack of action similarly to identify and protect UK assets from a known threat is a serious failure, and one that the UK may feel the consequences of for years to come. The global pandemic has brought into sharp relief the importance of the UK safeguarding its sovereign assets if we are to protect our domestic economic security.

16. As for who is in charge of countering Chinese interference, responsibility for mitigating the more overt aspects of the Chinese threat to the UK seems to rest with Whitehall policy departments. However, there is no evidence that those departments have the necessary resources, expertise or knowledge of the threat to investigate and counter China's approach. The nature of China's engagement, influence and interference activity in the UK is difficult to detect, but even more concerning is the fact that the Government may not previously have been looking for it. *** The UK is now playing catch-up – and the whole of the Government has its work cut out to understand and counter China's 'whole-of-state' threat.

17. A further radical change in approach is required in relation to planning. Even now, HMG's focus has been dominated by short-term or acute threats. It has consistently failed to think long term – unlike China – and China has historically been able to take advantage of this. The Government must adopt a longer-term planning cycle with regards to the future security of the UK if it is to face Chinese ambitions, which are not reset every political cycle. This will mean adopting cross-government policies which may well take years to stand up, and require multi-year spending commitments. This is something that will likely require Opposition support – but the danger posed by doing too little too late in this area is too significant to play politics with. For a long-term strategy on China – thinking ten, fifteen, twenty years ahead – the Government needs to plan for it and commit to it now: the UK is severely handicapped by the short-termist approach currently being taken.

18. If the Government is serious about tackling the threat from China, then it needs to ensure that it has its house in order such that security concerns are not constantly trumped by economic interest. Our predecessor Committee sounded the alarm, in relation to Russia, that oligarchs are now so embedded in society that too many politicians cannot even take a decision on an investment case because they have taken money from those concerned. We know that China invests in political influence, and we question whether – with high-profile cases such as David Cameron (UK–China Fund), Sir Danny Alexander (Asian Infrastructure Investment Bank), Lord Heseltine (The 48 Group Club) and HMG's former Chief Information Officer, John Suffolk (Huawei) – a similar situation might be arising in relation to China.

19. At present, it appears that the threat from China is primarily at a state, rather than an individual, level and it can exert that state power in every area because of its economic might. The Government has, finally, put in place legislation (the National Security and Investment (NSI) Act 2021) to factor in security when considering investment decisions – eight years after this Committee warned them to do so. Whilst this is a positive development, there is still no effective independent oversight of decisions made under the NSI Act.

Therefore, we cannot be confident that security is actually being taken into account or if, for Ministers drawn to the siren call of investment, that is still regarded as a trade-off.

20. During the course of this Inquiry, the Government argued that such decisions could be scrutinised effectively by the Chair of the Business, Energy and Industrial Strategy (BEIS) Select Committee[5] through a business lens, with the relevant supporting intelligence provided to the BEIS Select Committee Chair on an 'ad hoc basis'. We were told that the ISC should be satisfied by simply seeing the intelligence case that was fed into investment decisions. We considered this to be wholly unsatisfactory, as it means that no one oversight body will routinely have the full picture and be in a position to scrutinise the totality of the evidence before the Minister. Effective oversight is a key function of democracy and is particularly important in this case, given the length of time that Chinese investment in the UK has gone unchecked.

21. The fact that the Government does not want there to be any meaningful scrutiny of sensitive investment deals – and deliberately chose not to extend the ISC's oversight remit to cover this at the outset of the new legislation – is of serious concern. It is for this reason that we are still formally seeking to amend the Committee's Memorandum of Understanding (MoU) with the Prime Minister to include several relevant policy departments within the purview of the Committee's oversight remit. This is a small change which will have a significant impact on national security – and upon the trust placed by the public in Ministers who are charged with weighing up fundamental interests behind closed doors.[6]

[5] Now the Business and Trade Committee, as of 26 April 2023.

[6] On 7 February 2023, HMG announced a restructure of several government departments, including BEIS. This led to the creation of the Department for Energy Security and Net Zero, the Department for Business and Trade, and the Department for Science, Innovation and Technology, and the scaling back of the Department for Culture, Media and Sport (previously the Department for Digital, Culture, Media and Sport). Shortly afterwards, it was confirmed that the Investment Security Unit (ISU) – the body established to scrutinise investment decisions under the NSI Act – would be moved from BEIS to the Cabinet Office.
We presumed that this meant that the Government would confirm the ISC's responsibility for oversight of the ISU – in line with the Committee's MoU with the Government, which provides for ISC oversight over the National Security Secretariat in the Cabinet Office. However, on 21 March 2023, we received correspondence from the Minister of State for the Investment Security Unit advising that the ISU would still be overseen by the BEIS Select Committee – despite no longer sitting in the department which that Committee oversees. An MoU had been agreed between the BEIS Select Committee and the Chancellor of the Duchy of Lancaster (as the relevant Secretary of State now for the ISU) to this effect. The Deputy National Security Adviser wrote to this Committee on 23 March 2023 to clarify that HMG does not consider the ISC's remit under the current MoU to automatically extend to the activities of the Chancellor of the Duchy of Lancaster, as the Secretary of State now responsible for the ISU. This is a quite extraordinary decision. It is clear that the argument that the ISC's oversight does not extend to the activities of the Chancellor of the Duchy of Lancaster holds no weight (we note that the Chancellor of the Duchy of Lancaster is not overseen by the BEIS Select Committee either) and it is absurd that the ISC's oversight is being denied in this manner. The Committee will be pursuing this matter and reporting in due course.

PART ONE:
THREAT AND RESPONSE

THE NATIONAL SECURITY THREAT TO THE UK

I think the challenge of the rise of China absolutely raises huge questions for the future of the Western alliance … none of us can give a confident long-term answer to exactly how the balance of power plays out globally across the next few decades but it is clear for all of us that this is, I think, the central intelligence challenge for us across the next decade.

– Director General MI5, December 2020

CHINA: AIMS AND AMBITIONS

22. The Chinese state's prevailing aim is – very simply – to ensure that the Chinese Communist Party (CCP) remains in power. Everything else is subservient to that. Professor Steve Tsang, Director of the China Institute at the School of Oriental and African Studies (SOAS), explained, "[it is] *the single most important driving factor for Chinese politics since the post-Mao period*".[7] The UK Intelligence Community similarly referred to China's principal concern as being "*to ensure … the continuing dominance and governance of the Chinese Communist Party. Anything which subtracts or threatens to undermine that will immediately run into what China perceives as its key national interests*".[8]

23. This is familiar territory that has been covered in depth by others. However, the Intelligence Community added a second principal concern:

> *China also seeks to become … a global power by the middle of the century. 2049 … will be the 100th anniversary of the founding of the People's Republic of China and that is very much the timeframe in which China is looking at its global ambitions and its global activities.*[9]

24. Unlike Russia, China is not assessed to be "*fundamentally nihilistic*" in its attempt to once again be viewed as a "*great power*"[10] – it does not appear to intend to carry out a catastrophic attack. China wants to be a technological and economic superpower, with other countries reliant on its goodwill – that is its primary measure of sovereign success.[11] MI5 observed:

> *** *it is going after IP* [Intellectual Property]*, it is building itself as a power, it is positioning China in the world at the top of the tree* ***[12]

25. With these two overarching aims – remaining in power domestically and becoming a technological and economic superpower internationally – in mind, the UK Government considers China's supporting objectives as being:

- **Economic stability:** The CCP views economic prosperity as crucial to the legitimisation of the Party's rule. China's economic agenda focuses on ensuring the successful transition of its economy from a manufacturing base into an advanced high-tech economy that reflects and promotes modern China.
- **Geopolitical influence:** China seeks geopolitical influence in order to reshape international systems and values in line with its own interests and to be seen as a strong and dominant global power.
- **Domestic control:** The CCP looks to prevent internal dissent and ensure the survival of the Party.

[7] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[8] Oral evidence – MI5, *** July 2019.
[9] Oral evidence – JIO, *** July 2019.
[10] *Russia*, HC 632, 21 July 2020.
[11] Oral evidence – MI5, *** October 2020.
[12] Oral evidence – MI5, *** October 2020.

- **Foreign relations:** China prioritises the protection of its core interests (state sovereignty, national security, territorial integrity, national reunification, the political system and economic development).[13]

26. China's actions can be understood best when viewed through the lens of these overarching aims and supporting objectives since its approach to the rest of the world flows directly from them. The Foreign Affairs Committee's report on *China and the Rules-Based International System* stated that: "*China does not want a disrupted international order; it wants an international order that is more aligned with its interests and priorities*."[14] The Joint Intelligence Committee (JIC) said that Beijing *** is opportunistically trying to transform parts of the rules-based international system, through resistance to United Nations (UN) interference in states, development without human rights conditions, the elevation of economic rights above political rights, and internet regulation by states. Where rules and norms constrain China, under President Xi Jinping it has become increasingly selective in its compliance.[15]

27. The UK Intelligence Community told the Committee that there is *** between China and Russia, based on shared interests that include seeking to erode the established world order, for strategic advantage.[16] Although China and Russia will inevitably view each other as *** there is likely to be ***.[17]

28. Another shared interest that might result in material co-operation is around military capabilities. China is building global military capabilities to rival the US by 2049 and, as noted in our *Russia* Report, China and Russia have in recent years deepened defence and security co-operation, going so far as to conduct joint military exercises ***.[18]

China's positioning: The Belt and Road Initiative

The Belt and Road Initiative (BRI) – a 'belt' of overland connections to neighbouring countries (rail and road) and a maritime 'road' of shipping lanes to facilitate trade – is a clear example of President Xi Jinping's strategy to ensure that China is seen as a powerful force on the global stage, capable of shaping international norms and institutions for its own benefit.

Under the BRI, China is granting low-interest loans to countries in order to build infrastructure such as ports, roads and railways. By opening up numerous trade routes – more than 60 countries have signed up to the initiative – China seeks to develop new investment opportunities, cultivate export markets, and boost Chinese incomes and domestic consumption.

[13] Written evidence – HMG, 18 April 2019.
[14] House of Commons Foreign Affairs Committee, *China and the Rules-Based International System*, HC 612, 26 March 2019.
[15] Written evidence – JIO, 18 March 2019.
[16] Written evidence – HMG, 18 April 2019.
[17] Written evidence – HMG, 18 April 2019.
[18] Written evidence – JIO, 21 June 2019.

However, there are concerns that China will be able to use its leverage, over countries which owe it money, to extract strategic concessions (such as supporting China's territorial ambitions at the expense of their own, or agreeing to long-term contracts that might not be in their national interest): a practice known as 'debt-trap diplomacy'.[19]

The loans have, in some cases, included conditions such as a requirement to use Chinese contractors, which has inflated costs and reduced the benefit to the local economy. In other cases, there have been accusations that loans have been used to channel funds to companies owned by officials. In Sri Lanka, when the government asked to restructure repayments, China agreed – on the condition that it be given a 99-year lease on a strategically located port that it had funded.[20] GCHQ told us that the BRI was allowing China to change the rules in numerous multilateral fora:

> *So, the way in which China exerts its influence, we are seeing of course in Belt and Road, and that is a very physical thing but it is also a very virtual thing, it is the way in which technologies are being rolled out across the world ... we are not nearly ... fleet enough in thinking about how China is setting the standards for the world's technology ... it is dominating the block-votes in some of the key standard-setting bodies; ...* [and] *as part of its BRI diplomacy and its debt diplomacy, it is demanding the subservience of other countries to vote with them in these contexts. So they have a monopoly on a lot of the standard-setting bodies that we care about.*[21]

Professor Steve Tsang described the Chinese approach towards regional and international organisations as being "*instrumentalist*", adapting such organisations to better suit China's priorities.[22] The Council on Foreign Relations describes China as undermining United Nations human rights mechanisms by downplaying individual rights and instead emphasising the importance of state-led development, national sovereignty and non-intervention. China has also been accused of trying to ensure that it received a favourable review of its human rights record from the Human Rights Council by threatening consequences for countries – and in particular BRI countries – that supported a negative view.[23] While there is a question as to whether China's overseas lending constitutes a deliberate ploy to trap countries in unsustainable debt, in October 2020 the Joint Intelligence Committee noted that China can use loans and renegotiations as leverage to advance its policy objectives, and that developing countries have often been eager customers for Chinese lending, as China typically has competitive prices, can disburse loans quickly, can lend at a scale required for many large infrastructure projects and has been willing to fund prestige projects.[24]

[19] 'What is China's Belt and Road Initiative?', *The Guardian*, 30 July 2018; 'China's Massive Belt and Road Initiative', Council on Foreign Relations, 21 May 2019.
[20] 'China signs 99-year lease on Sri Lanka's Hambantota port', *Financial Times*, 11 December 2017.
[21] Oral evidence – GCHQ, *** July 2019.
[22] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[23] 'Is China undermining Human Rights at the UN?', Council on Foreign Relations, 9 July 2019.
[24] Written evidence – JIO, October 2020.

In November 2021, the Chief of SIS highlighted the risk of Chinese debt traps in his speech to the International Institute for Strategic Studies: "*we want other countries to be clear-eyed about the debt traps, data exposure and vulnerability to political coercion that arise from dependency on relationships where there is no recourse to an independent judiciary or free press*".[25]

We were also told that there had been several examples of the Chinese state-owned bank signing debt suspension agreements (***) and that China had also been taking advantage of gaps in international co-operation to expand its influence over international organisations such as the World Health Organization. Director GCHQ observed: "*yes, they have been opportunistic, not just in the commercial space but in the rules-based international system space too*".[26]

In the summer of 2020, 60% of BRI projects were facing significant challenges as a result of the pandemic, including:

- restrictions on cross-border movement of workers and logistics;
- the worldwide economic downturn increasing the financial burden on China; and
- rising anti-China sentiment across the world.

As a result, China has taken the decision to move away from infrastructure projects and instead focus on its Health Silk Road and its Digital Silk Road.

The Health Silk Road has been epitomised by so-called 'vaccine diplomacy' and 'mask diplomacy', donations of both intended to show that China is the superpower most able to defeat the virus globally. China has been very keen to promote its role in 'health diplomacy' – sometimes exaggerating its work to counter the virus and to develop vaccines – whilst also encouraging the spread of disinformation favourable to Chinese narratives. Disinformation also appears to have been used to sow seeds of doubt about the origin of the virus, including through fake news and conspiracy theories, to deny any fault and sway its domestic audience in particular.

The Digital Silk Road has seen developing countries being given the opportunity to upgrade their digital infrastructure – vital when combating a pandemic by utilising rapid test results and contact tracing – through the donation or subsidisation of Chinese technology. The success of the Digital Silk Road has resulted in China accounting for almost a quarter of global data flows (at the beginning of 2021), twice the amount that the United States accounts for.[27]

[25] Chief of SIS, speech to the International Institute for Strategic Studies, 30 November 2021.
[26] Oral evidence – GCHQ, *** October 2020.
[27] 'Coronavirus hasn't killed Belt and Road', *Foreign Policy*, January 2021; 'The Belt and Road Initiative after COVID: The Rise of the Health and Digital Silk Roads', Asian Institute for Policy Studies Issue Brief, March 2021.

What does China want from the UK?

29. The question for the UK is how China's global aims and ambitions affect the UK. The Intelligence Community have been clear that China's view of an ideal future – where it is a world power – would be antithetical to the UK's interests:

> *If you think of UK interests as being in favour of good governance and transparency and good economic management, which I think is fair, we regard those as things which are good in their own right but also serve our national interest because it helps with trade, investment, prosperity and stability and so forth, then I think that China represents a risk on a pretty wide scale.*[28]

30. The UK is unlikely to be the top priority for China when it comes to espionage and interference: the US, and perceived domestic threats to the CCP's rule (known as 'the Five Poisons' – Taiwanese independence, Tibetan independence, Xinjiang separatists, the Chinese democracy movement and the Falun Gong), are likely to receive the most attention from the Chinese Intelligence Services (ChIS). Nevertheless, the JIC Chair explained:

> *China sees almost all of its global activity in the context of what it sees as the struggle between the United States and China, and therefore it sees the United Kingdom fundamentally through that optic. China aspires to split off from the United States countries which it thinks might be detachable, and they sometimes have a sunnily optimistic view about which countries might be susceptible to that treatment. I would say that that was their single biggest issue with the United Kingdom.*[29]

31. In addition, the UK's membership of various international bodies of significance to China, and the perception of the UK as an international opinion-former, makes the UK of interest in the context of China's strategy to reshape international systems in its favour. The JIC Chair explained to the Committee:

> *China sees the United Kingdom as an important bellwether, an important country in guiding opinion on Chinese affairs within the European Union. It sees us as a global player, not of course of the same stature as the United States but nevertheless a country still of considerable influence.*[30]

GCHQ further observed: "*We are really important to them … where we are performing that international leadership role*."[31]

32. Linked to the UK's position as an opinion-former, the UK's unique historical role in China – particularly, but not exclusively, in relation to Hong Kong – is likely to make the UK a higher-profile target. In terms of Hong Kong, SIS recognised that:

> *activism around Hong Kong and the way in which Hong Kong has become a more pressing issue means that we have probably gone up the stack in terms of their interest.*[32]

[28] Oral evidence – JIO, *** October 2020.
[29] Oral evidence – JIO, *** July 2019.
[30] Oral evidence – JIO, *** July 2019.
[31] Oral evidence – GCHQ, *** July 2019.
[32] Oral evidence – SIS, *** October 2020.

33. This has been demonstrated over the past few years, with the Chinese government proving extremely sensitive to UK Government comments on the Hong Kong protests in 2019 – in a press conference in July 2019, the Chinese Ambassador to the UK said, "*I tell* [the UK Government]*: hands off Hong Kong and show respect. This colonial mind-set is still haunting the minds of some officials or politicians*"[33] – and threatening curtailment of Chinese investment in the UK following HMG's announcement of the British National (Overseas) visa scheme[34].[35] A number of our External Expert witnesses were clear that Hong Kong had become a personal project for President Xi and that he felt he had to be seen as victorious in the pursuit of his policy. Any move by the UK is viewed as interference in internal affairs and is responded to in an aggressive manner.[36]

34. These factors would appear to place the UK just below China's top priority targets, as it seeks to build support for its current 'core interests', to mute international criticism and to gain economically. In respect of the latter, China sees the UK as a home for Chinese investment. The JIC Chair told us:

> [China] *sees us as an important financial and commercial centre. It is no accident that of course the United Kingdom has been the major destination for Chinese investment in Europe since 2000, indeed I think by most estimates, if you add together investments in France, Germany and Italy, the United Kingdom still outstrips them. So there is a very strong commercial element.*[37]

35. China also values the UK in relation to both its technology industry and its education sector.[38] Lord Patten, Chancellor of the University of Oxford, observed:

> *I think they probably think we are not entirely reliable useful idiots … I think they do take us quite seriously, though not as seriously as once was the case, and I think they regard us as an economic opportunity and as an opportunity to, through elite capture, through the cultivation of useful idiots, through playing on things like the 'Golden Age' of British–China relations, getting us by and large corralled into doing the sort of things they would like us to do.*[39]

This approach can be seen in relation to Civil Nuclear energy: Chinese interest lies in gaining UK regulatory approval for its reactor designs as they assess that this will influence other countries to permit Chinese investment in their Civil Nuclear sectors. This is explored further in Part Two of this Report.

---

[33] A Chinese foreign ministry spokesman also said: "*The UK considers itself as a guardian* [of Hong Kong] *which is nothing but a delusion*." The Ambassador was summoned to the Foreign Office following these remarks. ('Britain summons Chinese Ambassador as he accuses Government of taking "wrong side" on Hong Kong', *The Telegraph*, 3 July 2019.)

[34] Under this scheme, an estimated 2.9m British National (Overseas) status holders were eligible to move to the UK with a further estimated 2.3m eligible dependants. ('Hong Kong BN(O) visa: UK government to honour historic commitment', www.gov.uk/government/news/hong-kong-bno-visa-uk-government-to-honour-historic-commitment, 29 January 2021.)

[35] 'China–UK relations grow more strained over Huawei and Hong Kong', *China Brief Jamestown*, 31 August 2020.

[36] Oral evidence – External Experts, 9 May 2019.

[37] Oral evidence – JIO, *** July 2019.

[38] Oral evidence – JIO, *** October 2020.

[39] Oral evidence – Lord Patten (University of Oxford), 9 May 2019.

36. As a result, while China poses the main state security threat to British interests,[40] at the same time China's targeting of the UK for strategic advantage will – in the short term at least – be tempered by its need to keep the diplomatic relationship afloat in order to retain economic ties with the UK and encourage wider UK support for China as a responsible global actor.[41]

37. However, as China's economic power develops, along with its capability to target foreign states covertly, China may be in a position to take a more aggressive stance against the UK. In addition, there is a realistic possibility that the UK's departure from the European Union (EU) will decrease the UK's attraction for China in terms of trade and investment, and that more assertive push-back from the UK and its Western allies may result in increasingly adverse retaliation from China.[42] In July 2020, following the UK Government's decision to prohibit the use of Huawei equipment in the UK telecommunications network, China's Ambassador Liu Xiaoming told the broadcaster Andrew Marr that it was "*a dark day for UK–China relations*".[43] There has been a definite cooling in the relationship, and it appears that the downwards trajectory is likely to continue. We were told:

> *China has reduced ministerial engagement and its media has threatened boycotts against UK pharmaceutical, financial and automotive companies.* ***[44]

Nevertheless, it is notable that the Huawei decision has not yet led to any direct action. Whilst we found that surprising, it may be because China still considers the decision to be reversible.

38. We questioned the UK Intelligence Community about the concerns raised by the Chair of the Foreign Affairs Committee that China may be targeting the Commonwealth, trying to undermine the alliance in order to gain the support of Commonwealth members who benefit from Chinese investment. The concerns were reported by *The Times* following the announcement that Barbados had taken the decision to remove the Queen as its Head of State – the article reported that Central Intelligence Agency (CIA) intelligence about Chinese activities in Barbados had been shared with the UK.[45] However, the JIC Chair ***.[46]

A. China's national imperative is to ensure that the Chinese Communist Party remains in power. Everything else is subservient to that.

B. However, it is its ambition at a global level – to become a technological and economic superpower, on which other countries are reliant – that poses a national security threat to the UK.

[40] Written evidence – JIO, 21 June 2019.
[41] Written evidence – HMG, April 2019.
[42] Written evidence – HMG, April 2019.
[43] 'China–UK relations grow more strained over Huawei and Hong Kong', *China Brief Jamestown*, 31 August 2020.
[44] Written evidence – JIO, 5 November 2020.
[45] 'China blamed for Barbados ditching Queen', *The Times*, 23 September 2020.
[46] Oral evidence – JIO, *** October 2020.

C. China views the UK through the optic of the struggle between the United States and China. When combined with the UK's membership of significant international bodies, and the perception of the UK as an international opinion-former, these factors would appear to place the UK just below China's top priority targets.

D. China views the UK as being of use in its efforts to mute international criticism and to gain economically: this, in the short term at least, will temper China's targeting of the UK.

WHAT IS CHINA SEEKING IN THE UK?

39. As noted previously, China's broad aims in relation to the UK are to mute criticism and build support for China as a partner, and to gain economically. More specifically, China's aims are:

- to encourage a divergence between US and UK policy goals on China;
- to shape the public narrative to mute criticism of the CCP and its actions (particularly in relation to Hong Kong, human rights, the South China Sea, Tibet, press freedom, Xinjiang etc.);
- to dissuade the UK from challenging any of China's territorial claims;
- to encourage the UK to endorse China as a reliable partner (and thereby boost its reputation on the global stage); and
- to ensure China can benefit economically from the UK (in particular by seeking UK endorsement of Chinese national champions and through the purchase of UK technology companies).[47]

40. In order to achieve these aims, China is seeking both political influence and economic advantage in relation to "*UK government departments, politicians, our academic institutions, non-government organisations, private companies with access to sensitive data and areas of emerging technology (e.g. artificial intelligence (AI), quantum, biotech)*".[48] This chapter provides an overview of the political influence and economic advantage that China is seeking: these are also expanded on in later chapters and Part Two of the Report.

Political influence

41. China is trying to create a world in which it is "*going to be increasingly hard to… swim against the tide of what China wants to happen in … global, economic, political* [and] *military settings*".[49] To this end, China seeks to influence elites and decision-makers in different walks of life.[50] HMG explained:

> *Distinct from China's legitimate lobbying and diplomacy efforts, China seeks to manipulate the perceptions of China and Chinese policy in line with* [its] *aims … We judge that China uses overt and covert methods in parallel in order to achieve its aims. Under President Xi, who is championing China's emergence as a global power, the appetite for using these methods is likely growing.*[51]

[47] Oral evidence – HMG, *** October 2020; Written evidence – HMG, April 2019; Written evidence – JIO, 5 November 2020.
[48] Written evidence – HMG, 18 April 2019.
[49] Oral evidence – MI5, *** July 2019. We also note that President Xi Jinping's speech to the CCP summit in October 2022 claimed: "*China's international influence, appeal and power to shape the world has significantly increased*."
[50] Oral evidence – JIO, *** July 2019.
[51] Written evidence – HMG, 18 April 2019.

42. China prioritises acquiring information on traditional targets of espionage – such as political decision-making and defence. In seeking to establish HMG's position, it casts its net widely. We were told that China hoovers up:

> *very large amounts of mostly not very damaging information in isolation. There is a big thing here about the aggregation of vast amounts of small insights, but alongside that you cannot be blind to the possibility of small amounts of very deep insights.*[52]

(China also uses its acquisition of large amounts of data to enable it to identify, and track, targets: this is covered in the Case Study on Industry and Technology in Part Two of the Report.)

43. ***[53] ***

44. In recent years, it appears that there has been a general rise in attempts to penetrate the Government or the UK Intelligence Community[54] ***.[55] UK students studying in China can also be targeted. ***.[56] *** both SIS and MI5 told us that the ChIS were most aggressive in ***.[57] ***

45. In terms of cultivating influence, HMG told us that the ChIS use the following methods:

- covert support for foreign political parties;
- covert funding and support of groups favourable to the CCP;
- using trade negotiations or investment activities as a platform to influence key decision-makers through bribery and corruption;
- co-opting academics, think-tank employees, former officials and former military figures;
- using cultural and friendship institutions to access key thinkers and decision-makers;
- obtaining and releasing materials to discredit individuals opposed to China's views;
- funding of universities, both to influence research direction towards Chinese priorities and to gain access to prominent individuals through philanthropy; and
- covert media manipulation to undermine support for policies and views deemed harmful to China.[58]

In terms of political parties, support groups, institutions, officials and the media, we consider these methods in more detail later, in the chapter on Interference.

---

[52] Oral evidence – MI5, *** July 2019.
[53] Written evidence – HMG, 18 April 2019.
[54] ***
[55] ***
[56] Oral evidence – SIS, *** July 2019.
[57] Oral evidence – SIS, MI5, *** July 2019.
[58] Written evidence – HMG, 18 April 2019.

46. In terms of Academia, this is the subject of a specific Case Study in Part Two of the Report. At this point, however, we note that Academia provides China with a key means of exerting influence: Chinese attempts to interfere with, and stifle debate, amongst the academic community in the UK are a significant problem, made possible by China's academic 'buying power'. Chinese students make up the largest overseas (non-EU) contingent in UK universities[59] and are responsible for generating almost £600m – a very significant proportion of universities' income. China is actively using this income as leverage to gain political influence and control and to direct the narrative.

47. However, China does not simply exert control and influence through student fees, it also provides direct investment to academic institutions so that it can guarantee input into academic programmes, direct research and ensure that UK students are taught an interpretation of China that reflects the CCP's interests.[60] In addition to seeking political influence at an institutional level, China also targets individual academics who study the country, seeking to ensure that they act in the CCP's best interests either through professional inducements or, if that doesn't work, by intimidation, including using Chinese visas as leverage. The threat of not allowing an academic to travel to China – when that is their area of expertise – is a very powerful threat. Our Case Study on Academia explores the scale of China's political influence in this area.

48. In terms of the use of investment activities as a platform, this can clearly be seen from the political influence China gains from its very significant investment in the UK's Civil Nuclear sector – seeking to ensure that the UK is economically reliant on China. In a bid to become a global supplier, China is looking to capitalise on the UK's international leadership and seeks to use UK regulatory approval for Chinese technology in this sector to enable the export of Chinese technology to other Western markets – thereby increasing China's political influence. We explore China's influence in this sector in our Case Study on Civil Nuclear energy.

Economic advantage

49. China is engaged in a battle for technological supremacy with the West – one which it appears to be winning. China's 'Made in China 2025' strategy is an initiative designed to help China become a manufacturing superpower through investing in, and then leveraging, foreign industries and foreign industry expertise in order to help China master complex design and manufacturing processes more quickly. China targets other countries' technology, Intellectual Property (IP) and data in order to "*bypass costly and time-consuming research, development and training*".[61] This approach means it can exploit foreign expertise, gaining economic and technological advantages and thereby achieving prosperity and growth more quickly – and at the expense of others.

50. Chinese dominance of technology has far-reaching consequences: a key issue in the 5G/Huawei decision was that there were few other options, such is the dominance of China

[59] Given the decline in EU applicants since 2019, the Chinese contingent has become even more important to UK universities. ('Chinese students now biggest foreign market for UK universities – but there's a reason why some experts are worried', *Daily Telegraph*, 14 July 2022.)
[60] The latter is primarily conducted through Confucius Institutes in the UK. This is explored in more detail in our Case Study on Academia.
[61] Written evidence – HMG, 1 May 2019.

in the market. In July 2019, our predecessor Committee published a statement reporting on the first aspect of this Inquiry, Chinese involvement in the UK telecommunications sector – and more specifically the then current issue of whether Huawei should be able to supply equipment to be used in the UK 5G telecommunications network. As this Committee warned in its 2019 statement, the problem is far bigger than the UK's 5G network: the West is over-reliant on Chinese technology generally and must act now to tackle China's technological dominance. The Committee warned that the Huawei decision was a geopolitical (rather than simply technological) issue and would require careful consideration. However, crucially, it also warned that action must be taken now to tackle the Chinese monopoly in technology generally:

> *one of the lessons the UK Government must learn from the current debate over 5G is that with the technology sector now monopolised by such a few key players, we are over-reliant on Chinese technology – and we are not alone in this, this is a global issue. We need to consider how we can create greater diversity in the market. This will require us to take a long-term view – but we need to start now.*[62]

This issue is not unique to telecommunications and we return to it in the Case Studies on Industry and Technology, and Civil Nuclear energy.

51. Chinese dominance of technology is driven and supported by the Chinese state. China uses regulation and state subsidies (***) to give its companies an advantage in the global marketplace, and uses its political weight to shape international standards to favour Chinese companies. China is aggressively acquiring technology and expertise through investment, and mergers and acquisitions, as well as by co-opting companies and Academia. Illicit acquisition of Intellectual Property also appears to be a major contributor to China's rapid progress. The JIC Chair confirmed that "[China] *is likely to want to access our science and technology base by legitimate and illegitimate means*".[63]

52. Academia provides China with a means of doing both. While it is the illegitimate means (such as the theft of IP) that may attract the headlines, China is also adept at making the most of overt routes (such as Foreign Direct Investment and joint ventures). Working in plain sight, China directs, funds and collaborates on academic research for its own ends, in particular seeking to benefit the Chinese military through targeted research on dual-use techniques and to secure economic advantage over the West. The vast number of Chinese students – especially post-graduates – in academic institutions in the UK provides a further opportunity.

53. China uses some students to operate as non-traditional collectors of IP – particularly those involved in cutting-edge research and development ***. In some cases, these students obscure their military affiliations, including through the use of misleading historical names for their institutions or even the use of non-existent institutions.[64] Once established in academic institutions in the UK, these students are in a position to identify and exfiltrate valuable IP and data. Once in China's hands, IP and data are used to build or short-cut

[62] 'ISC Statement on 5G suppliers', Intelligence and Security Committee website, 19 July 2019.
[63] Oral evidence – JIO, *** July 2019.
[64] 'Picking flowers, making honey – The Chinese military's collaboration with foreign universities', Australian Strategic Policy Institute, 26 October 2018.

Chinese expertise, giving China an economic advantage. (China's use of Academia to gain economic advantage is covered in more detail in a Case Study in Part Two of the Report.)

54. In terms of illicit acquisition, the Chinese target IP and data closely aligned with China's national strategies, including those industries identified as priorities in the 'Made in China 2025' strategy – such as IT, robotics, aerospace, ocean engineering equipment and ships, railways, energy-saving technology, vehicles, agriculture, new materials and medicine. (The last of these, medicine, has become particularly pertinent since the start of the Covid-19 pandemic.) HMG told us that the ChIS will have launched a systemic cyber effort, both increasing and diversifying its use of cyber attacks, to obtain IP, Personally Identifiable Information, ***.[65] This latter point is covered in more detail in the Case Study on Industry and Technology.

55. China has been accused of stealing IP and data from industries in the US, with the estimated cost of Chinese cyber-enabled theft alone thought to be around $320bn to the US economy in 2018. The danger posed by Chinese illicit acquisition of data and technology – and emerging technology in particular – is discussed further in the Case Study on Industry and Technology.

56. In the Energy sector, the Chinese government has a strategic imperative to acquire technology – through covert acquisition of IP – that will enable it to improve and increase domestic energy production. With severe pollution and environmental damage posing a possible threat to the CCP's popular support in China, there is a threat of economic espionage in the area of 'green' energy. These issues are explored in greater detail in our Case Study on Civil Nuclear energy.

57. China's attempts to achieve economic advantage pose a pervasive threat, but certain UK sectors would appear to be of particular interest:

- the Telecommunications sector (given that it provides access to information across other sectors);
- the Aerospace sector;
- key emerging technology sectors (e.g. artificial intelligence (AI), quantum and synthetic biology);
- traditional technology sectors (e.g. trains and ocean engineering);[66]
- Nuclear, Civil Nuclear and the wider Energy sector;[67] and
- the economy and Academia.[68]

(We consider these sectors in more detail later in our Case Studies on Academia, Industry and Technology, and Civil Nuclear energy.)

[65] Written evidence – ***, *** September 2020; 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking, 19 July 2021.
[66] Oral evidence – MI5, *** December 2020.
[67] Oral evidence – HMG, *** October 2020.
[68] Oral evidence – HMG, *** October 2020.

58. However, when we asked which specific aspects HMG prioritises for protection from China, the picture was startling. In December 2020, the Deputy National Security Adviser admitted:

> *I think in the past we have perhaps not had as rigorous a process at identifying across the board what needs to be protected based on our sovereign interest. We've had a very sophisticated process in some areas, so for example Critical National Infrastructure, which includes energy and so on. We've been weaker in other areas, for example emerging technology, potentially strategic suppliers and interdependences and data and telecoms infrastructure particularly.*[69]

We consider this later in the part of the Report dealing with the Government's response.

59. It is clear that China employs a range of overt and covert methods to gain political influence and economic advantage over the UK and that China's ambition and reach extends into a wide range of sectors in the UK, including Academia, Industry and Technology, and Civil Nuclear energy (each explored in the Case Studies in Part Two of this Report). China's activity is made possible by the nature and scale of its intelligence apparatus, which is explored in detail in the next chapter.

E. China is seeking both political influence and economic advantage in order to achieve its aims in relation to the UK. It seeks to acquire information and influence elites and decision-makers, and to acquire Intellectual Property using covert and overt methods to gain technological supremacy.

[69] Oral evidence – NSS, *** December 2020.

THE CHINESE INTELLIGENCE SERVICES

60. The nature and scale of the Chinese Intelligence Services (ChIS) are – like many aspects of China's government – hard to grasp for the outsider, due to the size of the bureaucracy,[70] the blurring of lines of accountability between party and state officials, a partially decentralised system, and a lack of verifiable information. ***[71]

Scale

61. President Xi's reform agenda has aimed to increase professionalisation of Chinese intelligence activities domestically and overseas.[72] Expenditure on the internal security apparatus has outpaced even China's recent dramatic military modernisation: by some estimates, China now spends almost 20% more on domestic security than on external defence,[73] and this appears to have led to an improvement in capability. MI5 told the Committee: ***[74]

62. According to UK Intelligence Community evidence, China almost certainly maintains the largest state intelligence apparatus in the world – in excess of *** personnel – which means that it is not necessarily straightforward to identify which parts of this enormous apparatus are targeted at the UK and our allies ***.[75] ***[76]

63. The ChIS are highly active, but the scope and scale of their activities vary widely – for instance, it has been reported that the Ministry of State Security (MSS) has a wide network of regional and municipal offices that exist under a federated structure.[77] This means that one area of domestic or foreign policy might be a priority for one office, but not for another; or alternatively, two offices will have the same priority but may not co-ordinate their efforts.[78]

64. With that said, the overarching priorities for the ChIS include ensuring that the CCP's message is delivered consistently and that subversive views are prevented from gaining traction amongst the population – thereby preserving the CCP's monopoly on power. According to open-source reporting, there are several CCP priorities supported by the ChIS's work:

---

[70] The Chief of SIS stated in July 2022 that the ChIS "*are extraordinarily well-resourced, I mean there are hundreds of thousands of civil intelligence officers, let alone their military capability*". (Fireside Chat with Richard Moore, Aspen Institute, 21 July 2022.)
[71] Oral evidence – SIS, *** July 2019.
[72] Written evidence – HMG, 18 April 2019.
[73] 'China Spends More on Domestic Security as Xi's Powers Grow', *Wall Street Journal*, 6 March 2018; 'China's Domestic Security Spending: An Analysis of Available Data', The Jamestown Foundation, 12 March 2018.
[74] Oral evidence – MI5, *** July 2019.
[75] Oral evidence – HMG, *** July 2019.
[76] Oral evidence – MI5, *** July 2019.
[77] For example, 'Everything We Know About China's Secretive State Security Bureau', *National Interest*, 9 July 2017.
[78] Written evidence – HMG, 18 April 2019. In 2019, the Committee was told ***. In 2022, the Committee was subsequently told that ***.

- suppressing threats to the CCP and its monopoly on state power – including international and domestic democracy advocates and minority groups, such as the Falun Gong and the Uighur Muslim population in Xinjiang;
- sovereignty – particularly with regard to Taiwan, Hong Kong, Macau and Tibet; and
- support to military operations – in addition to operations designed to ensure China's territorial integrity, this also includes monitoring US military movements in the Pacific and the military capabilities and capacity of adversaries.[79] Spying on other countries' defence industries would also fall under this category.[80]

65. The UK Intelligence Community broadly concurs, reiterating that China's prevailing priority is maintaining the power of the CCP and the Chinese state – but that this does not mean that the ChIS have a purely domestic focus, as their remit includes both seeking to suppress the 'Five Poisons'[81] (which are regarded as threats to China's national security) and advancing China's national interests by expanding its global reach and influence. There are public indications that, over the past decade, China has been placing greater emphasis on developing stronger foreign intelligence capabilities[82] – for example, the establishment of the People's Liberation Army Strategy Support Force (PLASSF) in 2015. SIS said that, while China "*are predominantly focused on internal threats*", nevertheless "*they have a potent external capability … they deploy globally*".[83]

66. It appears that President Xi's authority over the ChIS has grown since 2016, and that Beijing is using the ChIS as an increasingly important tool.[84] The ChIS target the UK and its interests prolifically and aggressively, with economic espionage a prominent motivation for the ChIS. We were told that there are up to *** ChIS officers usually stationed in the UK, as well as ***.[85] SIS noted that: ***[86]

[79] Hearing on China's Intelligence Services and Espionage Operations, US China Economic and Security Review Commission, 9 June 2016.
[80] For instance, ***.
[81] Taiwanese independence, Tibetan independence, Xinjiang separatists, the Falun Gong and the Chinese democracy movement.
[82] Written evidence – HMG, 18 April 2019.
[83] Oral evidence – SIS, *** July 2019.
[84] Written evidence – ***, *** December 2019.
[85] Written evidence – ***, *** December 2019.
[86] Oral evidence – SIS, *** July 2019.

The Chinese Intelligence Services

Ministry of State Security

- The main civilian intelligence service is answerable to the State Council and the Chinese Communist Party (CCP) Politburo Standing Committee, with a remit to operate both domestically and abroad. Unlike the UK intelligence Agencies, it has executive powers.
- SIS has told the Committee that it understands the strength of the Ministry of State Security (MSS) to be in the low hundreds of thousands.[87] In June 2018, a White House report examining the Chinese threat to technology and Intellectual Property cited open source reporting stating that the MSS deployed around 40,000 intelligence officers abroad and more than 50,000 in mainland China.[88]
- The vast majority of its work is spent on domestic security and the 'Five Poisons'. It divides its work along thematic lines, headed by individual bureaux.

The People's Liberation Army

- The People's Liberation Army (PLA, China's armed forces) has a significant intelligence collection role and answers to the Central Military Commission, which is chaired by President Xi Jinping.
- The Strategic Support Force ***, set up in 2016, is China's SIGINT (Signals Intelligence) agency and has responsibility for the PLA's previously disparate cyber and SIGINT capabilities (e.g. defensive cyber operations, disruptive and destructive cyber effects, cyber espionage, SIGINT collection and technology research).[89] It is a highly capable organisation: GCHQ cites China as being "*alongside Russia, the most capable cyber adversary we face and they put significant effort into it* ***."[90]
- *** the human intelligence arm of the PLA, persistently and aggressively targets government, military and commercial interests across the world, deploying *** covert tradecraft. ***[91] ***[92] ***[93]

[87] Oral evidence – SIS, *** October 2020. ***
[88] 'How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World', White House Office of Trade and Manufacturing Policy, June 2018.
[89] Written evidence – HMG, 18 April 2019.
[90] Oral evidence – GCHQ, *** July 2019.
[91] Written evidence – HMG, 18 April 2019.
[92] Written evidence – HMG, 18 April 2019.
[93] Written evidence – HMG, 18 April 2019.

The Ministry of Public Security

- The Ministry of Public Security is responsible for domestic law enforcement, counter-terrorism, counter-espionage operations and maintaining 'social order' – including the forced repatriation of Chinese nationals – although since 2015 it has been able to carry out investigations overseas if necessary. It liaises with foreign national police services and maintains an active role in counter-narcotics and illegal immigration work.[94]

Other intelligence-gathering organisations

- The Political Work Department Liaison Bureau – part of the Central Military Commission – makes use of cover organisations to facilitate access to, and influence over, prominent figures overseas, with a particular focus on defence policy-makers.[95] It conducts operations at home and overseas, using officers posted under various covers in China and in embassies and consulates.[96]
- The United Front Work Department, one of the most important departments of the CCP, is tasked with building and maintaining support for the Party, both at home and overseas, and is therefore concerned with domestic influence and control, and influence and interference activities directed at the Chinese diaspora, from managing relations with prominent Chinese individuals and groups to co-ordinating support for Chinese positions or targeting dissident groups abroad.[97]
- The Ministry of Foreign Affairs, the official diplomatic service, has access to important stakeholders within foreign governments ***.[98] The International Liaison Department is responsible for cultivating relations with foreign political parties. Its overt functions include liaison with these parties and with pro-China friendship associations and 'peace movements' overseas. ***[99]

A broad remit

67. Like all intelligence services, the ChIS seek to obtain classified information regarding, for example, foreign powers' military operations, defence industries, national security decision-makers and government organisations.[100] However, the ChIS are also known to have a considerable appetite for collecting unclassified information. In 2008, MI5 had explained to the Committee:

[94] Written evidence – HMG, 18 April 2019.
[95] Written evidence – HMG, 31 May 2019.
[96] Written evidence – HMG, 18 April 2019.
[97] Written evidence – HMG, 31 May 2019; Charles Parton, 'China–UK Relations: Where to Draw the Border Between Influence and Interference', Royal United Services Institute (RUSI), 20 February 2019.
[98] Written evidence – HMG, 31 May 2019.
[99] Written evidence – HMG, 31 May 2019.
[100] Written evidence – HMG, *** April 2019.

What the Chinese do is a bit like … bees going out from the hive; they just go out and they collect little bits of pollen from all over the place and they bring it back to their hive and they turn it into honey.

**** What they have is a pretty indiscriminate system of masses of students, officials, businessmen, et cetera, *** all of whom bring back little bits, which actually is jolly difficult – it's the grains of sand problem.*

***[101]

During this Inquiry, MI5 noted that the ChIS threat had moved on from that analogy: Chinese intelligence officers directly target sensitive information and deploy more sophisticated tradecraft alongside developing those networks that collect lower-level information.

68. Nevertheless, a vast swathe of information collected by the ChIS would be considered to be 'open source': something they are able to do by virtue of the resources at their disposal – SIS explained that the ChIS are able to act in an opportunistic manner and gather everything they can without having to prioritise.[102] Most Western intelligence services – usually due to resource constraints – focus primarily on the collection of classified information and much of the information collected by the ChIS would be considered anodyne or innocuous by Western standards. ChIS activities also therefore take them beyond what would be considered the remit of most Western intelligence services (for example, some of the efforts by the United Front Work Department to influence politicians and public perceptions of China could be regarded as traditional diplomacy). The broad remit means that the ChIS engage in activities ***, such as seemingly innocuous relationships with academics, think tanks or those in industry. For example, a US citizen with an affiliation to a Washington DC think tank was approached by the ChIS, who deemed his regular access to contacts in the US think-tank community to be valuable, as he would be able to report – based solely on unclassified information – on US–China relations.[103]

69. The sheer size of the ChIS also means that ChIS officers are able to try multiple routes to acquire all, or part of, the information they seek. For example, trying small- and medium-sized enterprises rather than just primary contractors, or using third-party countries. DI told the Committee:

***[104]

In more ways than one, the broad remit of the ChIS poses a significant challenge to Western attempts to counter their activity.

[101] Oral evidence – MI5, *** January 2008.
[102] Oral evidence – SIS, *** October 2020.
[103] US–China Economic and Security Review Commission, '2016 Annual Report to Congress', November 2016.
[104] Oral evidence – DI, *** December 2020.

'Whole-of-state' approach

70. To compound the problem, there is not just the ChIS to consider. The UK Intelligence Community assess that: "*The Chinese government is agnostic about the means employed to achieve its objectives. It is willing to pull on whichever lever is most likely to succeed, often employing multiple levers at the same time*."[105] In practice, this means that Chinese state-owned and non-state-owned companies, as well as academic and cultural establishments and ordinary Chinese citizens, are liable to be (willingly or unwillingly) co-opted into espionage and interference operations overseas. SIS told the Committee:

> *when you look at the kind of threat surface, it is very big and the people gathering information will not always be intelligence services. So every state institution in China is ultimately subsumed to the Chinese Communist Party and the state and their military interests. So a university, with no formal link to the intelligence services, could be being used to gather information on technologies which China deems critical to its future place in the world. So it is a very, very big subject.*[106]

71. This 'whole-of-state' approach will clearly be more difficult to detect ***. Nevertheless, the sharpest, or most challenging, elements of China's acquisition programme will always be placed in the hands of the ChIS.[107] SIS warned that China has "*a whole service effort geared to Chinese strategic advantage and will seek to penetrate and potentially disrupt ... the UK to secure that advantage over time*".[108] This is the area that poses the greatest acquisition threat to the UK, whether via cyber intrusion, covert agents, penetration of HMG or collection of defence technology.

F. China almost certainly maintains the largest state intelligence apparatus in the world. The nature and scale of the Chinese Intelligence Services are – like many aspects of China's government – hard to grasp for the outsider, due to the size of the bureaucracy, the blurring of lines of accountability between party and state officials, a partially decentralised system, and a lack of verifiable information.

G. The Chinese Intelligence Services target the UK and its overseas interests prolifically and aggressively. While they seek to obtain classified information, they are willing to utilise intelligence officers and agents to collect open source information indiscriminately – given the vast resources at their disposal. In more ways than one, the broad remit of the Chinese Intelligence Services poses a significant challenge to Western attempts to counter their activity.

H. To compound the problem, it is not just the Chinese Intelligence Services: the Chinese Communist Party co-opts every state institution, company and citizen. This 'whole-of-state' approach means China can aggressively target the UK, yet the scale of the activity makes it more difficult to detect *.**

[105] Written evidence – HMG, 18 April 2019.
[106] Oral evidence – SIS, *** July 2019.
[107] Written evidence – HMG, 18 April 2019.
[108] Oral evidence – SIS, *** July 2019.

ESPIONAGE

Gathering human intelligence

72. The Ministry of State Security (MSS) *** lead on China's human intelligence (HUMINT) collection through both covert and overt operations, run both overseas and in China. Intelligence officers (predominantly based in China) send individuals overseas as business executives, academics, students etc., who seek to establish themselves in positions of value, embed themselves in local society and qualify for host nationality status.[109] Intelligence is then fed back to a controlling officer based in China via visits, social media or other electronic communications.

73. Commentators have noted the ChIS's sophisticated use of open source information to compile and catalogue lists of individuals and organisations that may be useful to China's aims, and how the ChIS embed themselves in positions to be able to direct information and knowledge back to China. The MSS also uses commercial, diplomatic and journalistic cover to access persons of interest and influence and conduct operations. They focus on gathering valuable open source information and cultivating contacts in government, business and local Chinese communities. These 'cultivees' are not necessarily agents (***) and, given that MSS officers are working under cover, they often are not aware they are talking to the MSS. MI5 explained:

> *what the Chinese will do is sift what they can from many, many, many sources, many people, and to do that you don't really need for this British person or academic to kind of radically alter their view of the whole universe, you just need them to, sort of, give you some articles or some insights or a certain amount of influence that is useful to you, and the British person who is doing this in some cases may even remain genuinely unwitting as to what they have done, or more often, I suppose, they probably half know that they haven't done something wholly noble, but they never have to quite confront the fact that they are in some sense betraying the advantage of their nation.*[110]

***.[111]

Targeting of diplomats and officials abroad

74. The ChIS routinely target foreign diplomats and embassy officials in China and its near abroad, and there has been greater scrutiny of HMG staff in China *** in recent years ***. China has been developing increasingly pervasive coverage, and technical and legal powers, and it has almost certainly been using these and other espionage levers ***. Although until recently the ChIS did not routinely engage in harassment, there has been increasing harassment of Foreign, Commonwealth and Development Office (FCDO) staff based in and travelling to China ***.[112] Recent examples of ChIS action *** include entering their accommodation, close surveillance and IT incidents ***.[113] It is possible that this increase

[109] Written evidence – HMG, 18 April 2019.
[110] Oral evidence – MI5, *** October 2020.
[111] Written evidence – HMG, 18 April 2019.
[112] Written evidence – HMG, 18 April 2019.
[113] Written evidence – HMG, 18 April 2019.

in aggressive action is in response to actions taken by the UK, which China perceives to be aggressive: Royal Navy activity in the South China Sea *** and statements made by UK officials that challenge Chinese 'core interests'.[114]

Case study: Targeting of British Embassy staff

***

***

***

*** Due to limited extra-territorial provisions in the Official Secrets Act 1989, which extend only to UK nationals overseas, the UK Intelligence Community were unable to pursue a prosecution.[115]

Using social media

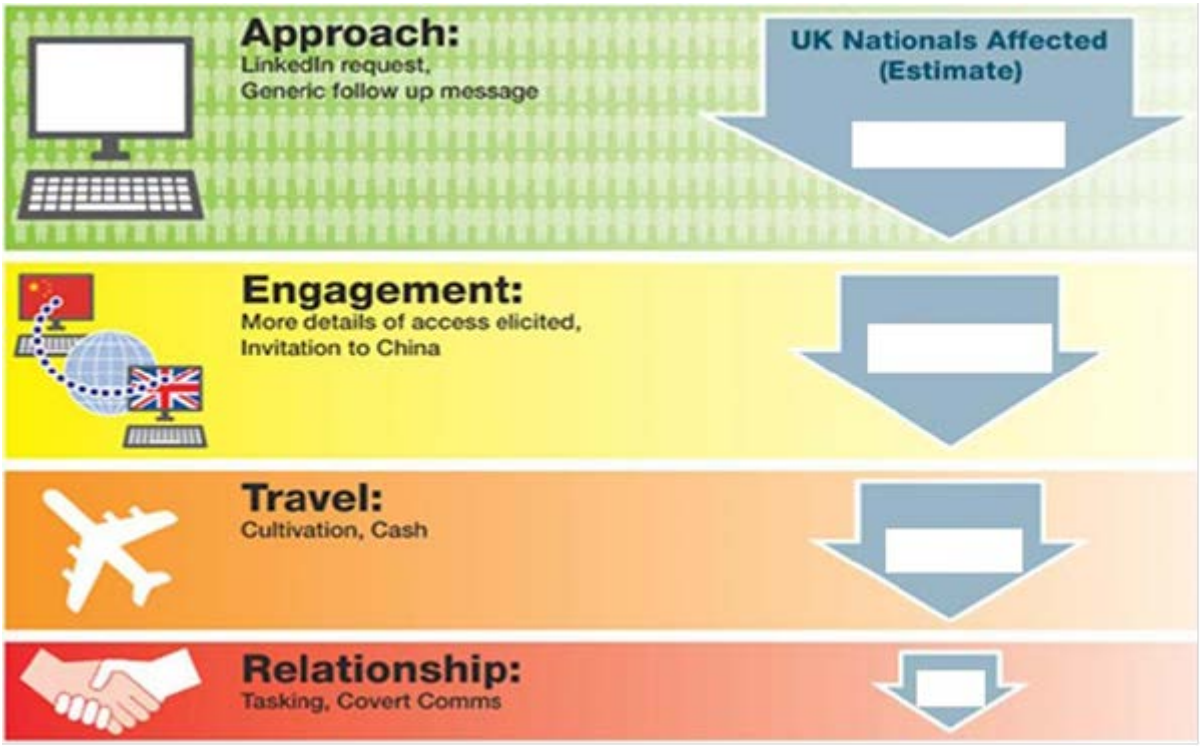
75. Social media is increasingly used to identify human targets overseas and to make initial introductions.[116] Bulk online methodology – using multiple fake profiles on social media – can be used to identify thousands of potential targets, including HMG officials, with all-expenses-paid invitations to China following.[117] Foreign business consultants based in China are increasingly used to help Chinese state targeting by advertising on Western websites for 'consultants' or 'associates' to provide assessments on various issues: good connections to Western governments are often a prerequisite.[118]

76. Academics are often initially approached through invitations to a conference in China, during which the academic would "*have a slightly strange encounter over coffee with someone who is not quite as presented*".[119] We questioned whether the methodology always focused on trips to China and were told that:

> *** *once they get you back to China, if you have shown vulnerability to them, they will absolutely do all the usual gamut of blackmail, honey-trapping, where they try and catch you in a sexually compromising position. They will do all of that.*[120]

77. The following graphic *** is useful in showing a potential pathway through which online cultivation may take place, and where the approaches have led to further cultivation.

[114] Written evidence – HMG, 18 April 2019.
[115] Written evidence – HMG, 18 April 2019.
[116] We note the Centre for the Protection of National Infrastructure's public Think Before You Link campaign. ('Think Before You Link (TBYL)', www.cpni.gov.uk/security-campaigns/think-you-link-tbyl-0, 30 September 2021.)
[117] Written evidence – HMG, 18 April 2019.
[118] Written evidence – HMG, 18 April 2019.
[119] Oral evidence – MI5, *** July 2019.
[120] Oral evidence – SIS, *** October 2020.



Bearing in mind that this would be just one department out of many, and just using one platform, it can be seen that China's use of social media to target individuals is prolific – and it is also global.

78. In December 2017, the German internal intelligence service (BfV) publicly accused the ChIS of using fake LinkedIn profiles to target German citizens – including politicians.[121] The following is a recent case of a retired CIA officer who was convicted of spying for China, having been recruited via LinkedIn.

Case study: Former CIA officer convicted of spying for China

Kevin Mallory, a former CIA and Defense Intelligence Agency officer, was found guilty of conspiracy to transmit national defence information to an agent of the Chinese Intelligence Services (ChIS) in May 2019. In February 2017, whilst heavily in debt, Mallory had responded to a LinkedIn message from a man purporting to be a researcher from a Chinese think tank, the Shanghai Academy of Social Sciences. The discussion resulted in Kevin Mallory taking two trips to China, in March and April 2017.

Following his return from China in April 2017, Mallory was subject to a Customs and Border Patrol (CBP) check. During the check, a CBP officer found that Mallory, despite declaring that he was not carrying over $10,000, had $16,500 in US dollars with him. He was allowed to amend his customs declaration.

In May 2017, Mallory submitted to a voluntary interview with the Federal Bureau of Investigation (FBI). During that interview, he stated that he had been contacted by an

[121] 'German spy agency warns of Chinese LinkedIn espionage', BBC News, 10 December 2017.

individual via social media whom he believed to be a Chinese recruiter. He now believed the individuals whom he had met in China to be from the ChIS.

According to Mallory, he had been tasked by the ChIS with producing two open source research papers on US policy matters. He had been paid $25,000 for the work and he expected to be paid a similar amount for work during a forthcoming trip to China in June 2017. He had also been encouraged to seek employment with the US Government. He had been given a covert communication device by the ChIS and was trained in how to use it. He agreed to supply the device to the FBI for investigation.

When demonstrating how the device worked, Mallory showed the FBI interviewers messages that had been sent whilst in 'secure message' mode. Mallory was surprised, as he had understood that all of the secure messages were automatically deleted by the device. Upon further technical examination of the device, the FBI recovered further messages in which Mallory made reference to deleting top security classification markers on documents that he was sending on the device. The FBI established that four documents had been sent on the device, including one classified as TOP SECRET and two classified as SECRET.

Kevin Mallory was sentenced to 20 years in prison, followed by 5 years of supervised release.

79. ***[122]

Seeding operations

80. *** the widespread targeting of foreign students in China. ***[123]

Case studies: British students targeted by ChIS officers

***

In ***, MI5 became aware of a British student in China *** who had been cultivated by ChIS officers. As the relationship progressed, the student introduced the officers to a friend ***[124]

81. *** an attempt by the ChIS to seed someone into one of the UK Agencies as a recruit. ***[125]

Cyber operations

82. China has a large and highly effective cyber espionage capability, consisting of official elements of both the MSS and the People's Liberation Army (PLA) and a range of non-official

[122] Written evidence – MI5, 24 September 2020.
[123] Written evidence – HMG, 18 April 2019.
[124] Written evidence – MI5, 12 June 2019.
[125] Written evidence – MI5, January 2021.

actors, including so-called 'patriotic hackers' (to whom the state turns a blind eye) and cyber criminals. GCHQ assesses that China focuses its UK cyber activity on *** rather than ***.[126]

83. Chinese cyber operations have achieved considerable success in penetrating foreign government and private sector IT systems. They also support HUMINT targeting efforts, providing useful insights into vulnerabilities or potential motivations. Defending against them requires ***: GCHQ told us that it assesses that there are between *** and *** active Chinese cyber groups ***. Its effort is focused ***.[127] GCHQ told the Committee that: ***[128]

84. Increasingly, sophisticated cyber operations have become a prominent feature of China's approach,[129] and the UK Government assesses that ChIS cyber and signals intelligence (SIGINT) actors ***.[130] GCHQ judges that, while campaigns around cyber security (for instance, not clicking links or downloading attachments) have been successful in increasing user awareness, the substantial rise in home working means that there are now more opportunities to get into an organisation as people use different technologies to connect remotely to a network.[131]

85. China's cyber expertise allows it to target a diverse range of organisations and datasets – and increasingly unusual ones. In 2015, the hacking of the US Federal Government's Office of Personnel Management (OPM) was attributed to a Chinese state-sponsored hacker group. The OPM held the data on background checks run by the US government on their employees, and the hackers obtained the personal details of around four million current and former federal employees.[132] Such a dataset could be used to help the ChIS identify potential HUMINT targets within the US Federal Government. China's acquisition of large amounts of data to enable it to identify, and track, targets is covered in more detail in the Case Study on Industry and Technology.

86. A more recent example of this expertise is the hacking of Equifax, an international credit reference agency, which took place in 2017. In February 2020, the FBI filed an indictment alleging that a branch of the PLA was responsible for the theft of a huge quantity of data, including the names and dates of birth of 145 million Americans and at least 13 million UK citizens (amongst other nationalities). Of those UK citizens, 841,000 had additional information, such as driving licence details and phone numbers, stolen, and 14,961 UK citizens also had passwords, usernames or partial credit card records stolen. There has been no evidence of criminal use of the data – instead, the information could be used to identify people working in sensitive research fields, politics or intelligence. There are also concerns that, depending on the level of information stolen, it could be used as a basis for blackmail.[133]

[126] Oral evidence – GCHQ, *** December 2020.
[127] Oral evidence – GCHQ, *** October 2020.
[128] Oral evidence – GCHQ, *** October 2020.
[129] Written evidence – HMG, 14 September 2020.
[130] Written evidence – ***, 24 September 2020.
[131] Oral evidence – GCHQ, *** December 2020.
[132] 'Millions of US government workers hit by data breach', BBC News, 5 June 2015.
[133] 'Chinese army's elite hackers steal Equifax data on 13m Britons', *Sunday Times*, 16 February 2020.

87. The UK Intelligence Community judge that their understanding of Chinese Computer Network Exploitation capability – for instance "*how they use that to hack, to hack and leak, to manipulate, to manage their campaigns*" – had *** since the National Cyber Security Centre (NCSC) was set up in 2016.[134] Western governments have, on the whole, been reticent about publicly attributing cyber attacks to China. However, in December 2018, the UK and US governments publicly attributed a series of major cyber attacks to the MSS,[135] ***[136]

88. We question whether it is yet having a 'deterrent effect'. On 19 July 2021, the FCDO issued a press release that attributed another cyber attack to Chinese state-backed actors. The statement read:

> *The UK is joining likeminded partners to confirm that Chinese state-backed actors were responsible for gaining access to computer networks around the world via Microsoft Exchange servers. The Foreign Secretary condemned China, commenting: "The cyber attack on Microsoft Exchange Server by Chinese state-backed groups was a reckless but familiar pattern of behaviour. The Chinese Government must end this systematic cyber sabotage and can expect to be held account if it does not."*[137]

89. We asked GCHQ whether it viewed China's offensive cyber capabilities as a similarly significant threat and were told that China has offensive cyber capabilities ***.[138]

90. The ChIS also have the capability to deploy what are known as close-proximity technical operations ***. This is offensive technical activity that requires physical access or proximity to a target, whether to gain access to premises (e.g. alarm defeats) or to acquire intelligence (e.g. eavesdropping, physical surveillance, cable-tapping or digital forensics). ***[139] ***[140]

I. In terms of espionage, China's human intelligence collection is prolific, using a vast network of individuals embedded in local society to access individuals of interest – often identified through social media. It is also clear from the evidence we have seen that China routinely targets current and former UK civil servants *. While there is good awareness of the danger posed, it is vital that vigilance is maintained.**

J. In relation to the cyber approach, whilst understanding has clearly improved in recent years, China has a highly capable cyber – and increasingly sophisticated cyber-espionage – operation: however, this is an area where the 'known unknowns' are concerning. Work on continuing coverage of its general capabilities must be maintained alongside further work on Chinese offensive cyber and close-proximity technical operations.

---

[134] Oral evidence – HMG, *** October 2020.
[135] 'UK and allies reveal global scale of Chinese cyber campaign', www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign, 20 December 2018.
[136] Written evidence – HMG, 18 April 2019.
[137] 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', FCDO press release, 19 July 2021.
[138] Oral evidence – GCHQ, *** December 2020.
[139] Written evidence – HMG, 18 April 2019.
[140] Oral evidence – MI5, *** October 2020.

INTERFERENCE

91. It appears that since 2018, under President Xi Jinping, China's appetite to expand and entrench its global influence has grown.[141] Seeking to exert influence is a legitimate goal: however, China's activity does not stop there, as it increasingly seeks to interfere.

92. HMG told us that China likely dedicates substantial resource to its interference operations, with *** its most important targets. Nevertheless, this does not mean that the UK is immune from targeting by Chinese political interference operations, since China seeks to gain wider legitimacy by influencing UK opinion.[142]

What constitutes interference?

The boundary between influence and interference is hard to define, but can be broadly articulated as the difference between those diplomatic and soft power activities that are generally considered 'legitimate', and those that are considered 'illegitimate' (although of course legitimacy is subjective and some countries – not least China itself – are likely to set a lower threshold for which activities they consider to be interference in their affairs).[143] The former Australian Prime Minister Malcolm Turnbull has described interference as "*foreign influence activities that are in any way covert, coercive, or corrupt*".[144]

There does not appear to have been a consistent definition within the UK Government of what constitutes interference until 2019, when the National Security Council was due to approve the following definition of 'foreign interference' (albeit it does not appear to have been discussed):

> *Foreign interference involves deceptive, coercive, corruptive or threatening actions on behalf of, in collaboration with, or directed by a foreign principal. Interference activity can be overt and/or covert. Interference is a spectrum of activity that is unfavourable to UK national security and/or economic wellbeing; detrimental to or undermines political or democratic processes at the local or national level; undermines academic thought and freedom of expression; or undermines UK sovereignty.*[145]

In May 2021, the consultation on Legislation to Counter State Threats (Hostile State Activity) gave the following definition:

> *a wide range of activity through which states seek to further their aims by use of covert means or by obfuscation of intent and originator, including disinformation,*

[141] ***

[142] Written evidence – HMG, 31 May 2019.

[143] Charles Parton, 'China–UK Relations: Where to Draw the Border Between Influence and Interference', Royal United Services Institute (RUSI), 20 February 2019.

[144] Charles Parton, 'China–UK Relations: Where to Draw the Border Between Influence and Interference', Royal United Services Institute (RUSI), 20 February 2019.

[145] Written evidence – JSTAT, 31 May 2019.

> *bribery and coercion. This also includes attempts to interfere in our democracy or Government policy making, including through interference in national, regional or local elections and referenda, as well as attempts to undermine academic freedoms. A number of states conduct persistent activity which attempts to distort UK and international information environments through the use of information operations which often play on existing divisions.*[146]

93. China's interference activities are – as with all its activity – primarily driven by the CCP's twin imperatives of: "[ensuring] *regime stability by defending against threats at home and overseas*"; and "[promoting] *its political and economic interests overseas in order to bolster its rise as a global power*".[147] HMG assesses that "*China has increasingly deployed aggressive propaganda and disinformation techniques to shape the information landscape and propagate narratives which promote the CCP's approach whilst denigrating the West*."[148] However, the two are very much linked – unlike in the case of Russia. Charles Parton has previously explained that "*unlike Moscow, Beijing's interference is not aimed at subverting the West, but represents a rigorous, ruthless advancement of China's interests and values at the expense of those of the West*".[149]

94. While the Chinese clearly do interfere overseas when it serves their perceived national interest, they nevertheless strongly resist accusations of interference – in part because they do not wish foreign powers to interfere in China's own affairs. Again, Charles Parton said, "*their whole narrative is that they don't interfere in other countries, so you should not interfere in the way they run their Confucian society*".[150] This stems from the deeply held fear that civil society organisations and global movements (in particular, those supposedly 'created' or 'supported' by Western democracies) calling for democratic accountability in China would challenge the legitimacy of CCP rule. Professor Steve Tsang noted that "*the Chinese saw from the 1990s onwards that colour revolutions ultimately would have China as the final ultimate goal, and they don't want that to happen ever*".[151]

95. China can be seen seeking to interfere with UK politicians, senior officials and military personnel, and they can be increasingly seen to interfere in the media, in Academia (covered in detail in the Case Study on Academia) and in relation to the Chinese diaspora.

Government

96. The JIC Chair told us, "[the Chinese government] *will certainly be seeking contact and to sustain relationships with elites …* [and] *decision-makers in different walks of life*".[152] Political decision-makers will therefore, inevitably, be targets of activity by the Chinese state – probably by the United Front Work Department (UFWD).

---

[146] 'Consultation document: legislation to counter state threats (accessible version)', GOV.UK, updated 22 November 2021.
[147] Written evidence – JSTAT, 31 May 2019.
[148] Written evidence – HMG, 14 September 2020.
[149] Charles Parton, 'China–UK Relations: Where to Draw the Border Between Influence and Interference', Royal United Services Institute (RUSI), 20 February 2019.
[150] Oral evidence – Charles Parton (RUSI), 9 May 2019.
[151] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[152] Oral evidence – JIO, *** July 2019.

97. It appears that China has a high level of intent to interfere with the UK Government, targeting officials and bodies at a range of levels to influence UK political thinking and decision-making relevant to China ***. Examples of such actions include:

- UK-based individuals associated with the UFWD and other CCP-linked groups have encouraged individuals, including those with Chinese heritage, whom they judge to have views that align with those of the CCP, to pursue political office.
- UFWD-linked individuals received funds from overseas sources for onward donation to political parties, prospective Parliamentary candidates (PPCs) ***.
- There have been attempts at a more generic political influence over a broader range of members of relevant legislatures (MRLs) who the UFWD perceive to be sympathetic to the Chinese world view and CCP priorities.
- In ***, MI5 investigations of the activities of several Chinese intelligence officers working *** in the UK, identified one of the intelligence officers gaining access to at least one UK Parliamentarian ***.
- ***[153]

98. Targets are not necessarily limited to serving politicians either. They can include former political figures, if they are sufficiently high profile. For example, it is possible that David Cameron's role as Vice President of a £1bn China–UK investment fund (itself an initiative of Lord Chadlington), and Sir Danny Alexander's February 2016 appointment as Vice President of the Asian Infrastructure Investment Bank (AIIB), were in some part engineered by the Chinese state to lend credibility to Chinese investment, as well as to the broader China brand ***.[154]

99. Security briefings are provided to politicians, including those who are targeted, and MI5 is able to take action where an attempt at interference is made:

In one case ***[155]

GCHQ observed that China frequently targeted Parliamentarians in their cyber operations ***.[156]

100. The UK does not appear to have suffered from some of the more egregious examples of Chinese political interference publicly disclosed in, for example, Australia and New Zealand.[157] We note, for example, the public case of an Australian investigation into Chinese government interference within the office of an Australian Parliamentarian. In October 2020, MI5 told the Committee:

[153] Written evidence – MI5, 16 November 2020.
[154] Written evidence – ***, 31 May 2019.
[155] Written evidence – MI5, 16 November 2020.
[156] Oral evidence – GCHQ, *** October 2020.
[157] We also note that MI5 issued an Interference Alert for Christine Lee in January 2022 (after the Committee had completed taking evidence for this Inquiry).

> **** because we are in close partnership with our Five Eyes counterparts, we can draw ... learning *** and be alive to the possible vectors of influence that might be brought to bear within our own system.*[158]

However, it appears that there are numerous instances of activity at the lower end of the influence/interference spectrum, and establishing whether approaches were legitimate lobbying on behalf of the Chinese embassy or whether there is the potential for an approach to develop into something inappropriate is not necessarily straightforward. By way of example, we were told that there had been cases of China offering to supply research staff to MPs.

101. Political interference has also been seen to include a degree of coercion. For example, in 2014 the Chinese state made it clear that it would refuse Members of the Foreign Affairs Committee entry to Hong Kong because it considered the Committee's Inquiry into Hong Kong to be an unacceptable interference in its affairs. The visit was cancelled, and the incident sparked a (somewhat muted) diplomatic protest from the UK Government.[159] In March 2021, the Chinese state sanctioned five MPs and two Members of the House of Lords in response to their work publicising the human rights abuses of the Uighur population in Xinjiang. It appears that the Chinese approach to countering the *** (***[160]).

102. However, distinguishing overt lobbying from covert or malign activity, and identifying relationships between UK-based actors and CCP-associated agencies or officials upstream ***[161]

Senior officials

103. There have been a number of high-profile examples of former UK officials being recruited by Chinese companies. The case that received the most scrutiny is that of John Suffolk, formerly the Government Chief Information Officer (2006–2011) and later, at the time of writing, Huawei's Global Head of Cyber Security.

104. In January 2011, as the then Government Chief Information Officer, Mr Suffolk travelled to China with GCHQ and BT to brief Huawei on serious security issues that GCHQ had discovered with Huawei's equipment.[162] Mr Suffolk's participation in the visit demonstrates the importance of his role in managing the risk associated with Huawei. Just one month later, Mr Suffolk applied for permission to join Huawei as their first Global Head of Cyber Security.[163] (It is unclear whether Mr Suffolk had been offered the role prior to the January 2011 trip, and if so, whether the Government knew about it.)

[158] Oral evidence – MI5, *** October 2020.
[159] House of Commons Foreign Affairs Committee, 'The UK's relations with Hong Kong: 30 years after the Joint Declaration', 3 March 2015.
[160] Written evidence – ***, 31 May 2019.
[161] Written evidence – MI5, 24 September 2020.
[162] *Foreign involvement in the Critical National Infrastructure*, Cm 8629, 6 June 2013.
[163] 'Following approval from the UK Government John Suffolk to join Huawei as their Global Head of Cyber Security reporting to the Group CEO', johnsuffolk.typepad.com, 29 July 2011.

105. In July 2011, the (then) Prime Minister, David Cameron, approved the appointment, on the advice of the Advisory Committee on Business Appointments (ACOBA).[164] However, media reporting at the time suggested that the intelligence Agencies had concerns about the appointment, and that Mr Suffolk was interviewed by the Cabinet Office to discuss these concerns.[165] Indeed, the conditions imposed on his appointment included a requirement for him to "*seek advice from the appropriate security authorities ... about any risks to the confidentiality of communications resulting from his new appointment which might be of concern to those authorities*".[166]

106. During this Inquiry our predecessor Committee specifically asked the Cabinet Office to provide any assessment or information they hold on whether the Chinese government or ChIS specifically targeted Mr Suffolk for recruitment to Huawei. Our request was refused, on the grounds that "*we do not comment on individuals*": the response is telling, given that it is not employed as routinely as it might suggest.[167]

107. Other examples include Sir Andrew Cahn, a former senior civil servant and head of UK Trade and Investment (2006–2011), who in March 2015 was appointed as a Non-Executive Director of Huawei's UK subsidiary, having been Chairman of the Huawei UK Advisory Board from 2011 to 2014. At the same time, Lord Browne of Madingley, former Chief Executive Officer of BP and Lead Non-Executive Director at the Cabinet Office (2010–2015), was appointed as an independent Non-Executive Chairman of Huawei UK.[168]

108. In October 2020, we asked the Acting National Security Adviser whether the ACOBA rules were fit for purpose, given what appeared to be a revolving door between the Government and Huawei, with officials involved in awarding the company contracts being apparently 'rewarded' with jobs. He told us that, across Government, the challenge presented by China meant that structures and processes were being kept under review and that included the ACOBA guidelines. However, he noted that those subject to the guidelines were "*often working with companies that we have welcomed to this country and whose investment we have welcomed and that are acting entirely legally here*".[169]

Military

109. In 2019, HMG noted that China was almost certainly seeking to court retired "*elites*". It would appear that the (state-run) China Association for International Friendly Contact (CAIFC) is one mechanism by which pro-China narratives might be being encouraged amongst this demographic, including amongst former senior military personnel. ***.[170]

---

[164] 'Following approval from the UK Government John Suffolk to join Huawei as their Global Head of Cyber Security reporting to the Group CEO', johnsuffolk.typepad.com, 29 July 2011.
[165] 'Government's former IT boss in MI6 grilling after taking job with Chinese mobile giant', *Daily Mail*, 7 August 2011; 'Former UK.gov CIO takes top security job at Huawei', *The Register*, 1 August 2011.
[166] ACOBA, 'Thirteenth Annual Report 2011–2012', December 2012.
[167] Written evidence – HMG, 31 January 2020.
[168] Lord Browne resigned as Chairman in July 2019, in advance of the announcement of HMG's Huawei decision.
[169] Oral evidence – NSS, *** October 2020.
[170] Written evidence – HMG, 31 May 2019.

110. The Sanya Initiative provided a key opportunity to do so. It was a military-to-military discussion forum organised by the CAIFC, often cited as a front organisation for the Political Work Department Liaison Bureau, an intelligence and political interference bureau of the Central Military Commission. Meetings took place between the US and China from 2008 to 2010, and between the UK and China from 2011 to 2013.[171] ***.

111. The Sanya Initiative would appear to have been an influence operation run by the ChIS, focused on targeting and co-opting senior officials and military personnel to support Chinese aims ***. *** they serve as an example of China's willingness to blend overt and covert activity in an attempt to influence and interfere.[172]

112. There are also concerns that China is recruiting former UK military personnel. The motivation appears to be to gain operational advantage (as opposed to employing them for the explicit purpose of interference). However, the possibility remains that former UK Armed Forces personnel could be utilised as part of a wider interference operation. We questioned DI about this threat, and the Chief of Defence Intelligence (CDI) told us:

> *I am very concerned in the defence space about particularly former military personnel being employed by China. So there's been an active campaign by the Chinese to recruit pilots*[173] ***[174]

113. Former UK military personnel are attractive to the Chinese as a way to improve their understanding of how Western planes and pilots operate. We were told that, although China had made advanced technological equipment available to their military, the lack of Chinese experience in the field (i.e. engaged in operations) meant that they did not have the experience of using it:

> *because they haven't been in combat,* [that] *means that they haven't learnt many of the lessons that the West has learnt and other nations over recent military operations. So therefore they're trying to not only short-circuit their R&D* [research and development] *through stealing secrets, but they're also trying to short-circuit their … operational development by attracting Western personnel.*[175]

When we questioned what could be done, we were told:

> *we're looking at options that we have* ***[176]

Interference in elections

114. In recent years, there has been significant coverage of state actors attempting to interfere in Western democratic elections. In the previous Committee's *Russia* Report, it was noted that the UK is "*clearly a target for Russian disinformation campaigns and*

[171] Open source reporting indicates that the US–China meetings have resumed in recent years.
[172] Written evidence – HMG, 21 January 2020; 12 February 2020.
[173] We note that the UK issued an intelligence alert to warn UK Armed Forces pilots against working for the Chinese military, in October 2022 (after evidence-taking had concluded for this Inquiry).
[174] Oral evidence – DI, *** December 2020.
[175] Oral evidence – DI, *** December 2020.
[176] Oral evidence – DI, *** December 2020.

political influence operations".[177] On 16 July 2020, the Foreign Secretary announced that HMG was "*almost certain that Russian actors sought to interfere in the 2019 general election through the online amplification of illicitly acquired and leaked Government documents*".[178]

115. The reputational risks of interfering in the democratic processes of others are significant. The UK Intelligence Community believe that these risks ***.[179] ***.[180] *** there is precedent for China seeking to influence democratic processes overseas[181] and ***.[182] Work to map foreign interference from Russia and China is ***.[183]

Media

116. Chinese interference in UK media has many facets – from the use of the UK media for the publication of Chinese content, to the expansion in the number of Chinese media outlets and journalists in the UK. (The use of journalist cover by ChIS officers for espionage operations is dealt with later in this Report.)

117. The Chinese government looks to use the UK's own media to its advantage. *The Telegraph* was reportedly paid £750,000 p.a. to carry the *China Daily* newspaper supplement (effectively a CCP mouthpiece), and it has been noted that since 2016 *The Telegraph* has carried twice the number of signed articles by the Chinese ambassador to the UK than the *Daily Mail*, *The Guardian* and the *Financial Times* put together.[184] In April 2020, content from the *China Daily* disappeared from *The Telegraph* website: when *Buzzfeed* and *The Guardian* asked *The Telegraph* to comment on its removal, *The Telegraph* refused to do so.[185] When we asked the JIC Chair whether he was concerned that the *China Daily* supplement was widely available in the UK, he told us that he was not convinced that it posed a significant threat:

> *The Chinese state, and individuals within it, are under quite a lot of pressure to show that they are doing things to advance the historical inevitability of the rise of China, and it is important that they can do things and report them, and they will report them as a great success. They will say that* Daily Telegraph *readers, a newspaper which is read by influential people in the United Kingdom, is now getting Chinese input. We might see it as being rather different but I am sure that is how they will be reporting it to Beijing and Beijing may well consider it money well spent.*[186]

---

[177] *Russia*, HC 632, 21 July 2020.
[178] HC Deb, 16 July 2020, HCWS384.
[179] Written evidence – JSTAT, 31 May 2019.
[180] Written evidence – JIO, 21 March 2021.
[181] We note, for instance, the allegations of Chinese interference in US and Canadian elections. ('Directors Remarks to Business Leaders in London', www.fbi.gov, 6 July 2022; 'Trudeau accuses China of 'aggressive' election interference', BBC News, 8 November 2022.)
[182] Written evidence – HMG, 21 January 2020.
[183] Written evidence – HMG, 21 January 2020.
[184] Charles Parton, 'China–UK Relations: Where to Draw the Border Between Influence and Interference', Royal United Services Institute (RUSI), 20 February 2019.
[185] 'A British Newspaper has given Chinese coronavirus propaganda a direct line to the UK', *Buzzfeed*, 1 April 2020; '*Daily Telegraph* stops publishing section paid for by China', *The Guardian*, 14 April 2020.
[186] Oral evidence – JIO, *** October 2020.

118. As well as seeking to influence the narrative through UK media outlets, China has also been seeking to expand its own media presence in the UK – another lever that can be used to promote values and standards at odds with those upheld by the UK. For example, China Global Television Network (CGTN), which was previously available in the UK on Sky and Freesat, created a new European headquarters in London in 2019.[187] However, in 2021, CGTN had its licence to broadcast in the UK suspended as the result of an Ofcom inquiry into its ownership, after it was found to have its editorial content directed by the CCP (a breach of Ofcom rules, which state that bodies wholly or mainly of a political nature, or those who are controlled by such bodies, are prohibited from holding a broadcasting licence).[188]

119. Ofcom has also upheld complaints against CGTN on the broadcasting of forced confessions by Chinese detainees and political prisoners, and in relation to the impartiality of its reporting on Hong Kong.[189] However, CGTN can still broadcast its UK content via its website, a YouTube Channel and internet TV platforms, such as Apple TV, Roku and Amazon Fire TV (which do not require a broadcast licence). CGTN is also seeking a broadcast licence in France where politically controlled broadcasters are permitted, and this would allow them to broadcast in the UK (under a convention to which the UK is a signatory, French TV channels can be broadcast in the UK with any content complaints going to the French regulator rather than Ofcom).[190]

120. ***.[191] ***.[192]

121. Chinese journalists operating in the UK have notably displayed behaviours not typically acceptable in the UK media. For example, in September 2018, a CGTN journalist was arrested at the Conservative Party conference after slapping a delegate in the course of an argument about Hong Kong (the journalist had disrupted an event being run by the UK-based NGO Hong Kong Watch and shouted, "*You guys are trying to separate China*").[193] In a public statement following the arrest (released on the Chinese embassy's website), the television station said, "*any attempt or action to divide China is futile and against the trend of history*", and "*we urge the UK side to take concrete steps to protect our journalist's legitimate rights and avoid such absurd incidents from happening again*".[194] The Chinese embassy also raised the matter with the FCDO at a working level, and again later when the case came to court; the FCDO firmly refuted any suggestion that it could influence the investigation.[195] The journalist was later convicted of assault.[196]

122. The case fits a pattern of the Chinese government robustly supporting Chinese nationals who 'stand up' for the perceived Chinese national interest, even when they break the law or

[187] Written evidence – JSTAT, 31 May 2019.
[188] 'Ofcom revokes CGTN's licence to broadcast in the UK', Ofcom press notice, 4 February 2021.
[189] *Broadcast and On Demand Bulletin*, Issues 403 (26 May 2020) and 406 (6 July 2020).
[190] 'War of the airwaves', *Index on Censorship*, Vol. 50, Issue 1, April 2021.
[191] ***
[192] Oral evidence – *** October 2020.
[193] 'Chinese TV journalist guilty of slapping Tory delegate', *The Guardian*, 29 November 2019.
[194] 'Chinese reporter who allegedly slapped Tory conference delegate released by police', *The Guardian*, 2 October 2018.
[195] Written evidence – HMG, 31 January 2020.
[196] 'Chinese TV journalist guilty of slapping Tory delegate', *The Guardian*, 29 November 2019.

risk damaging bilateral relations in the process. Chinese intelligence officers have been known to use journalistic cover[197] ***.

123. Finally, in terms of the media, the Chinese authorities have demonstrated a willingness to put pressure on British journalists who are perceived to be acting against China's core interests. For example, in 2018, Victor Mallet, the Asia Editor of the *Financial Times*, was denied a visa to remain in Hong Kong after meeting with a pro-Hong Kong independence figure.[198]

The Chinese diaspora in the UK

124. The Chinese authorities take a strong interest in the political views and activities of the Chinese diaspora overseas. According to Professor Steve Tsang, the CCP uses its influence to make "*Chinese communities feel that, if they don't support the Chinese government, they are being unpatriotic. The* [Chinese Communist] *Party is making the people of Chinese ethnicity great*".[199] The UK has a relatively small ethnic Chinese population. According to 2011 census data, the ethnic Chinese population was approximately 430,000 – about 0.7% of the total UK population. (By contrast, in 2016 Australia had an ethnic Chinese population of approximately 1.3m, equating to 5.6% of its 23.4m total population.)

125. Notwithstanding the size of the Chinese population, the JIC Chair told us: "*China will be seeking in some cases no doubt to coerce* [the Chinese diaspora in the UK], *but certainly to encourage* [it] *to follow a line which is consistent with China's interests*."[200] Family ties are often used as leverage in this context. With specific reference to academics, but in a broadly applicable observation, Charles Parton told the Committee: "[The CCP] *can put real pressure on people who still have strong ties* [to China] *because they have relatives* [there]*, or may even return*."[201]

Case study: Interference against the Chinese diaspora

It appears that, in 2019, a Chinese national studying for a PhD in a European country was coerced into travelling to a third country, where she was met by individuals who attempted to dissuade her from further engaging in activism activities.[202]

***[203]

126. Nevertheless, at the time of taking evidence, China's influence over its diaspora had not translated directly into any serious influence on electoral politics in the UK.[204] Charles Parton told the Committee that in his view the UK is less susceptible to widespread CCP

[197] 'UK expelled Chinese journalists "working as spies"', BBC News, 5 January 2021.
[198] Written evidence – JSTAT, 31 May 2019.
[199] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[200] Oral evidence – JIO, *** July 2019.
[201] Oral evidence – Charles Parton (RUSI), 9 May 2019.
[202] '"Damned if you do, damned if you don't?" I won't', Angela Gui, published on Medium, 13 February 2019.
[203] Written evidence – HMG, 31 May 2019.
[204] We note that MI5 issued an Interference Alert for Christine Lee in January 2022 (after the Committee had completed taking evidence for this Inquiry).

interference in elections than Australia or New Zealand because the ethnic Chinese population, particularly from the People's Republic of China (as opposed to Taiwan or Hong Kong), is relatively small.[205]

127. There is, however, a harder edge to China's interest in its citizens overseas. The UK's tradition of political tolerance has meant that many foreign dissidents have made their homes here over the years and this has often prompted the hostile interest of foreign intelligence services. This is particularly true also in the case of China, given its focus on muting criticism of the CCP and dissuading challenge to China's territorial claims.

128. The Chinese Ministry of Public Security (MPS) plays a key role in pursuing what China calls 'economic fugitives' (who are in fact more likely to be high-profile opposition figures) across the world, including in the UK. This global campaign to track down and repatriate individuals accused of corruption is known as Operation FOXHUNT. China is known to have repatriated Chinese nationals allegedly involved in corruption from the UK and conducted coerced repatriations of economic fugitives from the UK and kidnapping of dual nationals overseas. [206] ***.[207]

129. The MPS and other official bodies involved in FOXHUNT will typically 'persuade' the fugitive to return either by telephone calls or by visiting their place of residence abroad. The MPS also indirectly coerces fugitives by applying pressure on friends and family in China, for instance by suspending people from their jobs, withholding pension payments, physical threats and imprisonment, and by coercing them into visiting the fugitive abroad. ***.[208]

130. The Home Office has been seeking to understand and respond to the threat posed by FOXHUNT. During our Russia Inquiry, we were assured that all figures at risk – Russian or otherwise – received protection according to the level of risk, which is police-led. We investigated the provisions in place to respond to such action from the ChIS as part of this Inquiry. ***. In evidence to the Committee, MI5 noted that ***.[209]

131. When we asked why ***, we were told that: ***[210]

132. ***[211]

K. In terms of interference, China oversteps the boundary and crosses the line from exerting influence – a legitimate course of action – into interference, in the pursuit of its interests and values at the expense of those of the UK.

[205] Oral evidence – Charles Parton (RUSI), 9 May 2019.
[206] Written evidence – JIO, 17 November 2016; 30 November 2016.
[207] Written evidence – HMG, 18 April 2019.
[208] Written evidence – HMG, 18 April 2019.
[209] Oral evidence – HMG, *** July 2019.
[210] Oral evidence – HMG, *** July 2019.
[211] Written evidence – MI5, 24 September 2020.

L. Decision-makers – from serving politicians to former political figures, senior government officials and the military – are, inevitably, key targets. China employs a range of tactics, including seeking to recruit them into lucrative roles in Chinese companies – to the extent that we questioned whether there was a revolving door between the Government and certain Chinese companies, with those involved in awarding contracts being 'rewarded' with jobs.

M. The Cabinet Office must update the Advisory Committee on Business Appointments guidelines in relation to intelligence and security matters, including with particular reference to China, and ensure that their implementation is strictly enforced.

HOW IS THE UK RESPONDING?

There is no unified voice within Government about what our China strategy is … not only do you need a strategy but you actually need people to know what the strategy is and to follow it, and you need the Chinese to know what your strategy is – and none of that applies.

– Charles Parton, Royal United Services Institute

HMG'S BALANCING ACT

133. As the world's second largest economy (and one of the fastest growing), with a military increasing in size and capability, significant levels of diplomatic engagement and a large digital sector which acts as a force multiplier, China has a significant impact on global affairs. The Government's policy on, and strategy towards, China must take this into account when considering how to tackle the threats China poses to the UK.

Conflicting priorities

134. At the outset of this Inquiry in 2019, HMG emphasised that, while it recognised that China poses a security threat, it also viewed it as an economic opportunity:

> *China is the world's second largest economy and the UK's fifth largest trading partner.* [The] *growing number of Chinese students and tourists bring significant prosperity benefits to the UK, and our trade* [with] *China is an important source of investment for the UK.*[212]

135. In 2018, Chinese Foreign Direct Investment into the UK (investment which reflects a lasting interest and control by China in an enterprise resident in the UK) was £4.2bn, the highest in Europe.[213] At the time of taking evidence, Department for Business, Energy and Industrial Strategy (BEIS)[214] joint initiatives with China in the Industry and Energy sectors included the following:

- In December 2017, BEIS signed the UK–China Joint Strategy for Science, Technology and Innovation Co-operation, which resulted in a programme to develop technology to tackle global challenges resulting from climate change, population growth and environmental pollution.
- In June 2019, BEIS signed the UK–China Clean Energy Partnership, which allowed collaboration on transitioning to greener sources of energy.
- In March 2020, BEIS supported the sale of British Steel to a Chinese firm, Jingye Group.

136. The Department for Education (DfE) has similarly been keen to see UK universities benefit financially by attracting students from China: in the academic year 2018/19, more than 120,000 Chinese students were enrolled at UK universities, just under a quarter of the total 485,000 non-UK students. DfE has previously stated that it wants to increase the number of non-UK students studying in the UK to 600,000 by 2030.[215]

---

[212] Written evidence – HMG, 18 April 2019.
[213] 'Chinese FDI in Europe: 2018 trends and impact of new screening policies', Mercator Institute for China Studies, 6 March 2019.
[214] In February 2023, HMG announced the restructuring of several government departments, including BEIS (which no longer exists). The previous work of BEIS is now being carried out by the Department for Energy Security and Net Zero; the Department for Science, Innovation and Technology; and the Department for Business and Trade.
[215] 'Third of non-EU university students come from China', *The Guardian*, 16 January 2020.

137. HMG has, previously, chosen to portray this security/economy tension positively – as a 'balanced approach' – saying:

> *Government policy towards China is forward-leaning and robust, clear-eyed on the risks while engaging on areas where there are clear benefits to the UK.*[216]

A joined-up approach

138. However, the External Expert witnesses who gave evidence to this Committee in 2019 felt very strongly that HMG did not have any strategy on China, let alone an effective one, and that it was singularly failing to deploy a 'whole-of-government' approach when countering the threat from China – a damning appraisal indeed.

139. Raffaello Pantucci, of the Royal United Services Institute (RUSI), told the Committee:

> *I think the problem is that every department has seemingly a different* [China] *strategy … we do not have a China strategy and at the moment what has been allowed to happen is that each department had frankly been plugging along with their own iteration of a China strategy, meaning you don't have a coherent response. We have got essentially a situation where the centre has not made it clear what the China strategy is, articulated it in a clear and coherent fashion, and then everyone will flow from that. We have lots of institutions that are, frankly, doing their own thing.*[217]

When we put this to the Senior Responsible Owner (SRO) of HMG's China policy in July 2019, he admitted that the 'China Framework' (the strategy on China) was a relatively new development and "*a work in progress*".[218]

140. Until the publication of the Integrated Review in March 2021, HMG's overarching approach towards China had not officially changed since the China Framework was formally agreed by the National Security Council (NSC) in November 2018 – despite the fact that the landscape around the UK's China policy had changed significantly since then. In October 2020, the Acting National Security Adviser – who had taken over as SRO of HMG's China policy – told us that the Government's approach to China had been discussed over the course of NSC meetings in October 2019 and June 2020 and would be updated by way of the Integrated Review.[219]

141. Prior to its publication, the Committee was told that the Integrated Review would also address HMG's overall approach to economic security: whilst it was recognised that China's economic growth and influence cannot be ignored, nevertheless we were assured that there was an understanding in the Government of the need to "*robustly protect our domestic economic security … This includes a focus on increasing national economic resilience and*

[216] Written evidence – HMG, 18 April 2019.
[217] Oral evidence – Raffaello Pantucci (RUSI), 16 May 2019.
[218] Oral evidence – HMG, *** July 2019.
[219] Oral evidence – HMG, *** October 2020. *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy* (the 'Integrated Review') was published on 16 March 2021 and sets out the Government's vision of the UK's role in the world. It contains a number of actions which the Government commits to taking in support of that view. A refresh of the initial Integrated Review was later published on 13 March 2023 (after evidence-taking for this Inquiry had concluded).

reducing dependencies."[220] This would appear to indicate something of a departure from its previous approach – although HMG downplayed the shift, describing it as "*a pivot to greater resilience*", rather than there being a sense of an explicit shift away from China.[221]

142. The Integrated Review was published in March 2021. It is notable that, while the Review described Russia as an "*acute and direct threat*", it labelled China a "*systemic competitor*" and the "*biggest state-based threat to the UK's economic security*" – suggesting that Russia was still considered to pose the greater national security threat to the UK. Yet this contradicts the very clear impression given to this Committee that China is the main state security threat to British interests.[222]

143. It is at least clear that, following the global pandemic in 2020, and China's response to it, the security concerns previously raised by the UK Intelligence Community are now at the forefront of Ministers' minds – a change acknowledged in December 2020 by the Deputy National Security Adviser (DNSA) and Director General MI5. The Director General noted that, whilst it had been the case in the past that "*the national security community within Government and the prosperity community weren't really talking to each other*", he now considered that the need to "*integrate our understanding across both these domains to make the best possible choices*" was a well-established fact.[223] The DNSA told us:

> *in the past we have perhaps not had as rigorous a process at identifying across the board what needs to be protected, based on our sovereign interest. We've had a very sophisticated process in some areas – so, for example, Critical National Infrastructure, which includes Energy and so on. We've been weaker in other areas, for example, emerging technology, potentially strategic suppliers and interdependences and data and telecoms infrastructure particularly.*[224]

The DNSA cited forthcoming legislation and policy frameworks as a sign that "*we are beginning to establish some rigour in the system*" – better late than never, perhaps.[225]

144. However, there is still a question as to whether the planning that has finally now begun is too short term: when asked in July 2019 what was the greatest threat posed by China, Director GCHQ told us that his "*strategic concern*" was that:

> *we are not thinking long-term enough about the threat that China poses, given its aspirations are out to 2049, 2039, 2025, depending on which of their documents you read and of course all of those are way beyond traditional government planning cycles.*[226]

145. In July 2019, the previous DNSA had voiced similar concerns, noting that "*we tend to put a very short time horizon on things*" and that what the NSC needed to start doing was "*being a little bit more Chinese … taking a long term view about where do we need to be on*

[220] Written evidence – HMG, 14 September 2020.
[221] Written evidence – HMG, 14 September 2020.
[222] ***
[223] Oral evidence – HMG, *** December 2020.
[224] Oral evidence – HMG, *** December 2020.
[225] Oral evidence – HMG, *** December 2020.
[226] Oral evidence – GCHQ, *** July 2019.

some of these big critical issues, particularly around science and technology and emerging technology, looking much further out and then build back from that, so, okay, what do you need to do in [a] *Spending Review for a one year or three year period, rather than just sort of lurching from a one year to a one year to a one year*". The DNSA noted that HMG had started to consider options and was trying to understand how to bring an effort together, across departments, and decide who should be in charge of it. When we asked how that work would be taken forward, she told us that HMG was "*making sure that we bring all the right people around the table, whether it's the scientific community that support all of our departments to the policy people who support all departments. So we're having a cross-government discussion around all that*". Nevertheless, it was clear that in her words: "*We've got a lot more to do*".[227]

N. China is an economic power, and this cannot be ignored in formulating the UK's policy towards China. Balancing the tension between security and prosperity requires dexterity, and we understand that there are a number of difficult trade-offs involved.

O. The length of this Inquiry has allowed us to see the development of the China policy within Government and we are reassured that, belatedly, the security aspects are now being given prominence – notably more so after the pandemic.

P. It is nevertheless concerning that the security community, and the Government in general, were aware of many of these issues several years ago and yet we are only now beginning to see the introduction of measures taken to protect UK sovereign interests. The lack of action to protect our assets from a known threat was a serious failure, and one from which the UK may feel the consequences for years to come.

Q. Even now, HMG is focusing on short-term or acute threats, and failing to think long term – unlike China – and China has historically been able to take advantage of this. The Government must adopt a longer-term planning cycle in regard to the future security of the UK if it is to face Chinese ambitions, which are not reset every political cycle. This will mean adopting policies that may well take years to stand up and require multi-year spending commitments – something that may well require Opposition support – but the danger posed by doing too little, too late, in this area is too significant to fall prey to party politics.

R. Tackling the threats posed by China requires the UK to have a clear strategy on China, which is forward thinking, joined up and utilises a 'whole-of-government' approach. Work to develop such a strategy may now be in train, but there is still a long way to go.

[227] Oral evidence – HMG, *** July 2019.

THE 'STRATEGY': FRAMEWORKS, PLANS AND PILLARS

146. In 2019, the Committee was told that there were various documents addressing the Government's strategy on China:

- the China Framework;
- the Intelligence Outcomes Prioritisation (IOP) China Plan (previously known as the Intelligence Coverage and Effects Plan); and
- ***.[228]

There was also an HMG Hostile State Activity (HSA) Strategy which is actor-agnostic but apparently informed by discussions on the China Framework and the IOP Plan.

147. As ever with government strategy, it was not clear exactly how these various marginally different documents fit together, but the diagram overleaf was the best representation we were able to establish at the time of taking evidence, after lengthy discussions with those in NSS leading on the strategy.[229]

[228] *** (MI5 is a 'self-tasking' Agency – i.e. it cannot be directed to investigate or not to investigate an area ***.)
[229] ***


The Hostile State Activity Strategy
National Security Council
The National Security Council (NSC) owns and creates HMG policy on China, which is then set out in the China Framework, which is discussed (or aspects related to it) periodically at NSC meetings.
The China Framework
Six pillars
Senior Responsible Owner (SRO): ***
China National Strategy Implementation Group
The National Strategy Implementation Group (NSIG) – chaired by the SRO – implements the China Framework, co-ordinating policy decisions across Whitehall to avoid a binary prosperity vs security approach. Departmental representatives report back on NSIG discussions to Ministers and provide advice.
China NSIG members are: ***
China Intelligence Outcomes Prioritisation Plan
The Intelligence Outcomes Prioritisation (IOP) Plan is proposed by the NSIG on China. (The Joint Prioritisation Committee considers bids from every NSIG to balance them against the total operational effort available, and then recommends them to the NSC for approval.) The IOP Plan gives SIS and GCHQ HMG's requirements on China and allocates resources for them accordingly. It is agreed for a year, ***.[230]

230 ***

The China Senior Responsible Owner and National Strategy Implementation Group

148. The NSC approved the China Framework in November 2018. It is intended to cover “*the depth and breadth of UK–China engagement and the implications of China’s growing geopolitical and global role*”.[231]

149. The China SRO is responsible for developing the strategic framework (making sure it covers economic, security and influence interests) and getting it agreed by the NSC; for overseeing implementation of the strategic framework; and for co-ordinating issues relating to China across the Government. In 2019, the SRO explained the role:

> *I don’t see it as my role as SRO to be responsible for every single decision across government on China, that would be too big a task and would avoid the ownership that we need across the whole system, but it acts as a brokering mechanism so that, if there is a specific point on which a department are disagreeing, the NSIG which I chair can act as the triage and be clear how we want to resolve those differences and make sure clear advice is being given through Ministers, to Ministers, either through a ‘write-round’ or ultimately through a ministerial discussion at the NSC.*[232]

150. In 2019, the Committee was told that the cross-government National Strategy Implementation Group (NSIG) was responsible for developing and implementing policy in order to deliver the China Framework. The NSIG was an attempt to improve cross-government co-ordination without centralising the response. It meets monthly and is attended by: ***.[233] ***. The SRO explained:

> *what we are really trying to do is not have a process which has Ministers agreeing a set of priorities and the system not following up, which was very much our feeling of what had been happening in the past, but to have a clear set of objectives, indicators which then the system is being driven to follow through.*[234]

The China Framework

151. The 2018 China Framework consists of six ‘pillars’:

(i) ‘Trading Safely’;

(ii) ***;

(iii) ‘Countering Security Threats’;

(iv) ***;

(v) ‘Digital and Technology’; and

(vi) ***.

---

[231] Written evidence – Cabinet Office, 12 June 2019.

[232] Written evidence – HMG, 3 July 2019.

[233] ***

[234] Written evidence – HMG, 3 July 2019.

152. Each of the six pillars then has its own SRO, and these 'pillar SROs' each have their own developed objectives and key outcomes for each pillar.[235] The pillars feed into the IOP process (discussed later in this chapter). The China SRO explained the flexibility that this system offers:

> *So in the IOP process that is under way at the moment *** so we are confident that resource is applied in the right areas given the strategic direction set ***.*[236]

153. We were told that national security runs throughout the China Framework, but there are clearly three pillars which are more relevant – 'Trading Safely', 'Countering Security Threats', and 'Digital and Technology'. We have not therefore included a detailed analysis of the other, less relevant, pillars.

'Trading Safely'

154. In line with the aims of the Integrated Review, the objective of pillar 1 is to maximise the economic benefits of interacting with China while balancing this with the protection of national security and long-term prosperity. We were told that HMG's priority was to have:

> *a more comprehensive approach to our economic security in relation to China, ***. This includes a focus on increasing national economic resilience and reducing dependencies.*[237]

The six strands under 'Trading Safely' include, but are not limited to, themes such as investment, protection of Intellectual Property, trade, and research and development collaboration.

***

155. In September 2020, we were provided with a list of actions planned under this pillar, including the introduction of the (then) National Security and Investment (NSI) Bill and, in order to improve security, additional measures under the Enterprise Act to allow HMG to intervene if a business involved in the response to the pandemic is the target of a takeover, and to lower the scrutiny threshold for mergers in three sectors (artificial intelligence, cryptographic authentication technology and advanced materials).

156. The Committee was also told in 2020 that an economic security framework was being developed, which would allow Ministers to intervene in key areas of the economy on national security grounds under "*a clear framework, which can be communicated to business, potential investors and international stakeholders*".[238] At the beginning of this Inquiry, we were told that a new Economic Threats Unit was to be set up to identify, understand and act in cases of concern, replacing the Investment Security Group in the Cabinet Office. In addition to this, a wider set of current tools was being reviewed, including

[235] Written evidence – HMG, 14 September 2020.
[236] Oral evidence – HMG, *** October 2020.
[237] Written evidence – HMG, 14 September 2020.
[238] Written evidence – HMG, 14 September 2020.

"*the export control regime where specific consideration to new definitions of dual-use and emerging technology require consideration*" and "*an uplift to the investment screening capability to better monitor and scrutinise transactions, including those from China*".[239]

157. Upon publication of the NSI Bill in November 2020, it was apparent that the Economic Threats Unit in the Cabinet Office was instead to be a new Investment Security Unit (ISU) in the (then) Department for Business, Energy and Industrial Strategy (BEIS). However, there has been no indication that the ISU will carry out the proposed role to look "*upstream and understand the aggressive intent behind some of the investment in the UK and therefore pre-empt it*".[240]

158. During the passage of the NSI Bill, we sought assurances about the oversight of the ISU. We were informed that, despite the Unit relying on classified information, oversight would be undertaken by the BEIS Select Committee. However, such oversight can only be undertaken by the ISC – as the only Committee of Parliament with regular access to classified information, and to which the UK Intelligence Community have a statutory duty to provide information.[241] We discuss this further in our Case Study on Industry and Technology.

159. Project DEFEND was established as a result of difficulties experienced during the initial response to the pandemic. It focused on identifying vulnerabilities in the UK global supply chain and assessing threats to the supply of critical goods into the UK, "*to better safeguard critical supply chains. This includes diversification, greater HMG oversight of the procurement process and improved contingency planning*."[242] In October 2020, the Deputy National Security Adviser (DNSA) explained:

> *Covid has very sharply brought into relief the need to look at ... CNI* [Critical National Infrastructure] *... the supply chain, emerging technologies, critical suppliers to government, across the range and make some judgements about what we are, what we need to have sovereign, what we are prepared to work with trusted partners on and what we are prepared to leave to the global market ... the Department for International Trade is leading a very large project called Project DEFEND that very specifically looks to interrogate the security of our supply chains across the board* ***.[243]

160. While economic security is now more of a focus at policy level, it is important that the shift in focus to securing the UK's economic resilience is mirrored at an operational level ***.[244] One example of this is the investigation of the implications of a Chinese aerospace company's (***) move to purchase a UK Low Earth Orbit satellite company, OneWeb. This is explored further in our Case Study on Industry and Technology.

[239] Written evidence – HMG, 14 September 2020.
[240] Oral evidence – HMG, *** October 2020.
[241] Since evidence-taking for this Inquiry concluded, the ISU has been transferred back to the Cabinet Office, following the restructure of several government departments (including BEIS) announced in February 2023.
[242] Written evidence – HMG, 14 September 2020.
[243] Oral evidence – NSS, *** October 2020.
[244] ***

S. The Intelligence Community will play a key role in the work of the new Investment Security Unit (ISU): the classified and other technical advice that the Intelligence Community provide should shape the decisions made by the ISU as it seeks to balance the need for national security against economic priorities. It is essential that there is effective scrutiny and oversight of the ISU – and that can be undertaken only by this Committee.

'Countering Security Threats'

161. The objective of pillar 3 is to counter threats from China and to counter global threats by working with China. Work undertaken under this pillar is intended to protect the UK from a broad spectrum of threats ***.[245]

> The four strands under 'Countering Security Threats' include, but are not limited to, work on counter-influence, counter-espionage, serious organised crime ***
>
> ***

162. In terms of Academia, HMG (***) has been working with Universities UK to develop guidelines on countering foreign interference, and we were told that this included helping universities to diversify their international student recruitment. In relation to Industry, the National Cyber Security Centre and the Centre for the Protection of National Infrastructure were working on security advice concerning the threat to UK research and innovation;[246] and more broadly the HMG Defending Democracy programme was undertaking work to better understand the threat to Parliament, local government and the media. (The Committee was provided with a wider list of planned activities relating to this pillar in September 2020.)[247]

163. At the time of taking evidence, the Home Office was also working on a Counter-Hostile State Activity Bill – subsequently the Counter-State Threats Bill – to include reform of the Official Secrets Act and the creation of a Foreign Agent Registration Scheme alongside other new offences and civil measures provisions. This is covered later in the chapter on Legislation.[248]

[245] Written evidence – HMG, 14 September 2020.
[246] Known as 'Trusted Research', this was also published in autumn 2020 (Written evidence – HMG, 14 September 2020).
[247] Written evidence – HMG, 14 September 2020.
[248] Written evidence – HMG, 14 September 2020. On 11 May 2022 – after this Report was completed, but prior to publication – the National Security Bill was introduced in Parliament. The Committee was briefed on the Bill too late for it to be considered in this Report; however, we note that – disappointingly – the Bill as introduced does not include reform of the Official Secrets Act 1989 or introduce a Foreign Agent Registration Scheme (although the latter was later proposed via a Government amendment at Committee stage of the Bill).

Change in approach: Interference

At the beginning of this Inquiry, work to counter Chinese interference appeared very much to be a work in progress ***. The Senior Responsible Owner (SRO) for China told the Committee that this work was "***".[249] The SRO told us that it had been considered by the National Strategy Implementation Group (NSIG) ***:

> *** *it is certainly one of the top priorities where I think we have got to* *** *gain the understanding and then the response that we need.* ***[250]

In early 2020, HMG told the Committee that, since ***, the China NSIG has subsequently discussed Chinese interference ***, and later that year, work being done on Chinese interference in the UK was noted in evidence to the Committee.[251]

It is clear that Chinese interference has become a higher priority than it was when we began this Inquiry. Evidence that we have seen has noted that the Government is increasing its efforts to combat Chinese information operations particularly through:

- the cross-Whitehall counter-disinformation unit working to create a comprehensive picture of the extent, scope and potential impact of disinformation; and
- ***.[252]

We examine the effectiveness of the response to Chinese interference in the chapter on Defending the UK.

T. We commend the action now being taken by the Government to counter interference by China – it is encouraging that the Government has finally woken up to the grave threat this poses to our national security.

U. However, it is worrying that 'policy ownership' of this national security activity, rather than being gripped at the centre by the Cabinet Office, has instead been devolved across the Government – in many instances to departments with no security remit or expertise. We have not been kept informed of these developments and, despite numerous requests, are not permitted to scrutinise this activity.

V. Effective Parliamentary oversight is not some kind of 'optional extra' – it is a vital safeguard in any functioning Parliamentary democracy, and the ISC is the only body that can do that. Moving responsibility for security matters to bodies not named in the ISC's Memorandum of Understanding is not consistent with Parliament's intent in the Justice and Security Act 2013: the Government should not be giving departments a licence to operate in the name of national security and hiding it from view.

[249] Oral evidence – HMG, *** July 2019.
[250] Oral evidence – HMG, *** July 2019.
[251] Written evidence – HMG, 31 January 2020.
[252] Written evidence – HMG, 14 September 2020.

'Digital and Technology'

164. The objectives of pillar 5 are to: protect UK innovation and security; shape the norms and standards of emerging technology in line with UK values; embed human rights and the rule of law; and manage risk ***.[253]

> The seven strands under 'Digital and Technology' include, but are not limited to, themes such as: increasing supply chain resilience; maintaining influence over global technology standards; and promoting the UK's vision and norms ***.
>
> ***

165. In September 2020, we were provided with a list of actions planned under this pillar, including the (then) Telecommunications (Security) Bill, which set out guidelines for Telecommunications Network Operators, new powers for HMG in relation to high-risk vendors, and wider HMG work with international partners to diversify the telecommunications supply chain.

166. Other actions included: establishment of an Emerging Tech Board to identify nationally important technologies and assess opportunities and risks relating to them; the National Data Strategy, intended to ensure that data use is effective, efficient, ethical and secure; the establishment of a Digital Standards team ***; examination of rules around UK public sector procurement to see if companies potentially damaging to UK national security *** can be excluded from tendering for contracts; and raising awareness of relevant risks with British companies that wish to collaborate with Chinese digital and technology companies.[254]

W. The Telecommunications (Security) Act 2021 does not contain provision for effective oversight of the new measures being implemented. The Act provides that notification of a company or person being a 'high-risk vendor' of telecommunications equipment, and specification of the limits placed on the use of this equipment, be laid before Parliament unless provision of this information is deemed to be contrary to national security. In such circumstances it is logical – and in keeping with Parliament's intent in establishing the ISC – that this information should instead be provided to the ISC. This would ensure that Parliament could be duly notified without this information being made public and thereby endangering national security. However, this proposed amendment was rejected wholesale by the Government. This was particularly inappropriate – and, indeed, ironic – as it was the ISC that had originally raised concerns about the adoption of Huawei in the UK telecommunications network. It was our initiative that prompted the Government to introduce this legislation.[255]

[253] Written evidence – HMG, 14 September 2020.
[254] Written evidence – HMG, 14 September 2020.
[255] *Foreign involvement in the Critical National Infrastructure*, Cm 8629, 6 June 2013.

The Intelligence Outcomes Prioritisation process

167. As set out above, the Committee was told in 2019 that the China Framework lays out the NSC's policy goals, and the China NSIG is responsible for delivering those goals. The contribution of the Intelligence Community is then set out through the IOP process.

Intelligence Coverage and Effects

Until 2019, the tasking of SIS and GCHQ was carried out under an annual process called *Intelligence Coverage* (i.e. getting information) *and Effects* (i.e. doing something which has a real-world impact), known as ICE. Under ICE, NSS was responsible for ascertaining the priorities of the National Security Council (NSC) via a series of country and thematic strategies which were approved by the NSC throughout the year. SIS and GCHQ then responded to these strategies with an 'offer' of the intelligence coverage and effects they believed they could provide in relation to them. NSS then converted this 'offer' into the ICE Plan, resolving any resource or priority conflicts which might arise. This process gave SIS and GCHQ responsibility for allocating their operational effort to find the information which the policy-maker needed or realise an outcome which a policy-maker had requested (usually as part of an overarching strategy).

In March 2020, the process of tasking SIS and GCHQ changed from ICE to the Intelligence Outcomes Prioritisation process.

168. Under the IOP process, each NSIG[256] sets the intelligence requirements it needs in order to deliver its policy outcomes, and prioritises them in an IOP Plan.

169. Each IOP Plan is then sent by its NSIG to the Joint Prioritisation Committee (JPC) for discussion. The JPC is chaired by the DNSA and the Joint Intelligence Committee (JIC) Chair and the Foreign Commonwealth and Development Office's (FCDO's) Director General Consular and Security[257].[258] The JIO assists by examining the policy outcomes within each IOP Plan and assessing what level of understanding can be provided by different sources (including secret, open, diplomatic, academic and business sources). This helps to establish where secret intelligence is vital and where it could possibly be replaced by open source work.

170. Having reviewed the IOP Plans for the different NSIGs and taken into account ministerial priorities and the potential impact of changes in allocation, the JPC then recommends to the NSC the appropriate balance of Agency effort for the forthcoming year for each IOP.[259] The DNSA told us:

[256] There is not a set number of NSIGs – they are created and disbanded according to NSC priorities. In March 2020, we were told that there were 17 NSIGs, including one on China. ***

[257] This role has since been renamed Director General Defence and Intelligence.

[258] When required, the Agency heads, CDI, and personnel from the Ministry of Defence (MoD) and the Home Office can attend the JPC.

[259] If an SRO realises that they suddenly need additional effort midway through the year, they can bid for it as a reprioritisation. If the SRO thinks that this reprioritisation will be a long-term requirement then it will have to be considered as part of the annual round.

> *the prioritisation process that we have just gone through with the PM *** gives a really clear steer ***. So that gives the Agencies licence to operate on *** subjects with some discretion as to where you apply the resources.*[260]

171. We were provided with the agreed policy outcomes for 2020 – including in relation to the 'Trading Safely', 'Countering Security Threats' and 'Digital and Technology' pillars – against which SIS and GCHQ must deliver intelligence ***. ***

X. In December 2020, we asked how the policy outcomes against which SIS and GCHQ must deliver intelligence were being prioritised. We presume, for instance, that "*" is not considered to be of the same importance as "***"; however, we have not been provided with any information. Without any indication of prioritisation, it is difficult to judge the effectiveness of Agency efforts and it is therefore disappointing – and rather telling – that NSS has failed to provide such critical information in response to this major Inquiry.**

The tri-Agency approach

172. As set out in 2019, the Agencies take a tri-Agency approach ***. This is to ensure that – despite SIS and GCHQ having their priorities set by Ministers and MI5 being self-tasking – the Agencies can align at an operational level in terms of their contributions to the China Framework.[261]

173. ***

174. ***[262]

175. The current tri-Agency approach *** had been agreed in June 2018. Not long afterwards the NSC produced the China Framework ***. In April 2019, the Agencies said they were in the process of reviewing their approach in order to align with the new China Framework. However, in October 2020, with no further update, we questioned what was happening and Director General MI5 told us:

> *there is a logic I think to the next iteration* [of our approach] *... waiting until the Integrated Review and the Intelligence and Outcomes Prioritisation process have had their say, and then we respond to that, rather than sort of UKIC settling on something inside its own brain in advance of the top-level steer.*[263]

While we recognise that argument, we were surprised not to have been made aware of an updated approach whilst conducting our Inquiry – despite the Integrated Review having been published in March 2021, and the IOP Plan ***. (We were subsequently updated on the agreed revised approach in November 2021 – after we had concluded our oral evidence sessions and therefore too late for us to question the Agencies on it in order to reflect it in this Report.) It is simply not efficient to have these levels of planning so unsynchronised.

---

[260] Oral evidence – *** December 2020.
[261] Written evidence – HMG, 18 April 2019.
[262] Written evidence – HMG, 18 April 2019.
[263] Oral evidence – MI5, *** October 2020.

176. We also note that, as at 2019, DI is not included within the agreed tri-Agency approach ***. We were told that this is because DI was also not involved in the ICE process (the previous iteration of IOP) – its tasking/prioritisation is set by the Chief of Defence Staff.[264] When we asked what impact that had on joint working, MI5 told the previous Committee that the tri-Agency approach could, in time, include DI as the Agencies and DI are now engaging much more ***.[265]

Y. We were told in 2019 that the Agencies take a tri-Agency approach, but this does not cover DI. In October 2020 – over 15 months later – we asked if there had yet been any movement towards formally adding DI to the prioritisation process. The Acting National Security Adviser told us: "*DI are fully part of the IOP process … they are one of our main repositories of expertise on China.*" Director GCHQ noted that DI is a part of the National Cyber Force, and "*when you get into the effects world … they are completely there in every aspect*".[266] If DI is supposedly now fully integrated with the Intelligence Outcomes Prioritisation process, we expect the next iteration of the tri-Agency approach – when it is finally updated – to include DI.

HMG Hostile State Activity Strategy

177. In addition to the numerous levels of HMG's strategy on China, China also features in HMG's cross-cutting work on the threat posed by hostile activity carried out by states (as opposed to, for instance, terrorist organisations or serious organised crime groups).

178. The Government developed a Hostile State Activity (HSA) Strategy in 2017, defining HSA as "*overt or covert action orchestrated by foreign governments that undermines or threatens the UK's national security, the integrity of its democracy, its public safety, reputation or economic prosperity, short of armed conflict*".[267]

Hostile State Activity

This Report uses the term 'Hostile State Activity', which was used by HMG and the Intelligence Community throughout their evidence provided for this Inquiry.

'Hostile State Activity' was used to describe the full range of threats posed by hostile state actors. The UK Intelligence Community's work on Hostile State Activity was explained as comprising counter-espionage and counter-intelligence activity:

- Counter-espionage is the investigation of individuals (agents) who are suspected of passing sensitive information to foreign intelligence services.
- Counter-intelligence means investigating the activities of the officers and agents of overseas intelligence services and disrupting them when necessary.

[264] Oral evidence – DI, *** December 2018.
[265] Oral evidence – MI5, *** July 2019.
[266] Oral evidence – GCHQ, *** October 2020.
[267] Written evidence – HMG, 21 August 2019.

Since the Committee completed its evidence-taking, HMG has updated its terminology, and now refers to 'State Threats' instead of 'Hostile State Activity'. There appeared to be a number of reasons for this change: the Home Office explained that it was not felt to sufficiently reflect the complexity of the UK–China bilateral relationship and there were concerns over how the term could be received within East Asian-heritage communities in the UK. However, NSS subsequently explained that China was not the driving factor, and that the terminology had been changed because the term could be too easily misinterpreted as referring to a hostile state, rather than hostile activity as was originally intended.

179. Part of the Strategy focuses specifically on China, saying that: ***. Nevertheless, it adds that: ***.[268] HMG's aims in relation to HSA *** are set out as being to: ***

180. ***. The Committee was told in 2020 that a number of pieces of work have been carried out under the Strategy since it was introduced, including:

- *Establishing the Joint State Threats Assessment Team (JSTAT);*
- *** *publicly attributing cyber incidents alongside a range of allies and partners;*
- *Agreeing and initiating the Defending Democracy programme;*
- *Pursuing a comprehensive response to the threat of state-based disinformation, ***;*
- ***; *and*
- *Working with international ***.*[269]

181. While the Strategy is currently being refreshed, HMG has not – as at December 2021 – provided a date for when it expects it to be ready, despite the fact that the current refresh started before August 2019.[270] As with the emerging technology policy area, it is concerning that decisions on such an important policy area are not being made with any urgency.

182. HMG argues that there is a lot of work going on in the China portfolio. In October 2020, the Acting NSA told us that there was an "*enormous amount of work underway at the moment*" including:

> *** *lots of direct support to universities at the moment in that sector, for example, and lots of very demanding case work … it will be one of the major themes of the Integrated Review. We are creating new legislative powers through the Bills that I mentioned, we are trying to develop new capabilities across government, whether it is in investment screening, whether it is around education, whether it is around interference or disinformation, it is all a work in progress, given the evolution of the scale of the challenge that I mentioned earlier.*[271]

[268] Written evidence – HMG, 21 August 2019.
[269] Written evidence – HMG, 18 November 2020.
[270] Written evidence – HMG, 21 August 2019.
[271] Oral evidence – NSS, *** October 2020.

183. That is both welcome and absolutely necessary. The question is how effective that work will be. A number of new initiatives are cross-government and there is the potential for there to be significant change in the approach towards national security systems and processes. It is also worth noting that everything may change following the Integrated Review, which said:

> *The National Security Adviser will therefore review national security systems and processes to ensure that Integrated Review objectives and priority actions, as well as future policy decisions, are implemented swiftly and effectively, and to establish systems that better support the NSC.*[272]

Only time will tell whether the Government will be able to tackle the "*systemic challenge*"[273] of China but we have concerns that, at present, it is still doing so at far too slow a pace.

Z. As at 2021, the Government had a plethora of plans that laid out its China policies. The interaction between these documents has required a great deal of unpicking, and we have been surprised at the fact that changes in one document do not always lead to consequent changes in others. The slow speed at which strategies, and policies, are developed and implemented also leaves a lot to be desired – at the time of writing we await to see what impact the National Security Adviser's review of processes will have on the China policy area, but we would certainly hope it will become more coherent.

[272] *Global Britain in a competitive age – The Integrated Review of Security, Defence, Development and Foreign Policy*, HMG, March 2021.
[273] *Global Britain in a competitive age – The Integrated Review of Security, Defence, Development and Foreign Policy*, HMG, March 2021.

HMG RESOURCING

184. From the evidence provided by HMG to this Inquiry, there appears to have been an increase in the Government's focus on China since 2020, reflecting both the threat posed and the priorities of the Government. We would have expected to see a concurrent increase of resourcing dedicated to the China mission and therefore questioned each organisation on the resources it has been allocating to work on China,[274] and whether that has changed.

SIS

185. After 1997, SIS effort[275] on China reduced, but since 2004/05 it has been seeking to rebuild resources:[276]

- The percentage of operational effort dedicated to China has *** over the past 20 years, ranging between ***% (1999) and ***% (2003).
- For 2018/19 the figure stood at ***% (for comparative purposes, the figure for Russia was ***%).
- This equated to a financial spend of £*** (out of £***).[277]
- In 2020, the figure increased to ***%, and a financial spend of £*** (out of £***).[278]
- In terms of staff dedicated to China, figures[279] show *** from *** full-time equivalent (FTE) (2005/06) to *** FTE for 2019/20.[280]
- Of these, ***.[281]

[274] Each organisation records its resourcing and allocation of operational effort differently. Figures provided below relate to percentages of operational effort, financial spend and FTE staff numbers.
[275] ***
[276] Oral evidence – SIS, *** January 2008.
[277] Written evidence – SIS, 28 February 2020.
[278] Written evidence – SIS, 18 November 2020.
[279] Figures have only been provided from 2005 onwards.
[280] Written evidence – SIS, 18 November 2020.
[281] These figures include permanent staff and loans/contingent workers. SIS noted in its written evidence of 13 June 2019 that these numbers do not take into account the additional functions that support the China mission, such as *** and wider corporate services etc.

GCHQ

186. GCHQ statistics show a similar picture:

- Between 2000 and 2019, the number of GCHQ and National Cyber Security Centre (NCSC) staff working on China increased from *** FTE to *** FTE.
- In 2020, this increased to *** FTE.[282]
- The percentage of operational effort dedicated to China has increased from ***% in 2000 to ***% in 2019.[283]
- Operational effort on China rose to ***% in 2020.[284]
- ***.[285]

MI5

187. MI5 statistics provide an overall picture of work on Hostile State Activity (HSA), of which China is only one strand:

- For the financial year 2019/20, HSA[286] was allocated a total spend of £*** (International Counter-Terrorism and Northern Ireland-related terrorism received £*** and £*** respectively).
- Of that £***, work on China received £***.
- This was an increase of £*** from the previous year (but it nevertheless only represents a return to the levels of ***).[287]
- The proportion of mission effort on China is around ***%. This roughly equates to *** people.[288]

JIO

188. JIO similarly has found it difficult to disaggregate exactly:

- In March 2021, the JIO China Team[289] contained *** FTE staff with *** due to be advertised (an increase from *** FTE pre-2017 and *** FTE in early 2019). In addition, there *** dedicated to China open source work.[290]

---

[282] Oral evidence – GCHQ, *** October 2020.
[283] ***
[284] Oral evidence – GCHQ, *** October 2020.
[285] Written evidence – GCHQ, 4 March 2020. On *** December 2020, NCSC further explained that as well as those engaged in threat-focused work (i.e. an analysis and investigative point of view ***), there were also people who supported that analytical effort, and those whose work is threat-agnostic *** (although this work is informed by knowledge of the threat posed by China – amongst others).
[286] ***. These three operational themes are: International Counter-Terrorism (ICT), Northern Ireland-related terrorism (NIRT), and Hostile State Activity (HSA).
[287] Written evidence – MI5, 9 October 2020. MI5 told us that its "*operational model dynamically draws on a range of resources within MI5 and beyond*" ***. (Written evidence – MI5, 12 June 2019.)
[288] Director General MI5 explained: ***. (Oral evidence – MI5, *** October 2020.)
[289] JIO has noted that China assessments are produced by several different teams ***.
[290] However, the team also receives support from other teams working on HSA, economic assessments ***.

- The allocation of effort[291] has increased *** over the past two decades from ***% in 1999 to ***% in 2019 and then ***% in 2020.[292]
- Towards the end of 2020, the JIC Chair told us: "*** *In terms of my time, I would say that I probably spend about ***% of my time on China, something of that sort.*"[293]

Other organisations

189. DI statistics for 2020 show that:

- *** analysts spent 50% or more of their time on China (a decrease from *** last year) and *** analysts spent less than 50% of their time on China (an increase from *** last year).
- ***
- DI spends £*** on China-related activity.[294] Alongside broader politico-military analysis, this includes:
  - *** partnership programme with the defence industry in order to ensure that insights *** are then shared in an appropriate manner with the defence industry to advise them about how they can protect themselves;
  - ***; and
  - ***.[295]

190. DI has previously told the Committee that it does not hold comprehensive records relating to allocations of effort on China for past years.[296] We found that difficult to understand. DI explained that "*allocation of effort is challenging* [for it] *to calculate given the range of intelligence capabilities and specialisms within DI, many of which cover multiple geographic areas*". Notwithstanding that, we are surprised that information on allocation of effort on an area as supposedly significant as China is not readily to hand so that it can be kept under constant review.

191. Homeland Security Group[297] statistics for 2020 show that:

- Approximately *** staff[298] worked on China ***.[299]

[291] ***

[292] Written evidence – JIO, 8 March 2021.

[293] Oral evidence – JIO, *** October 2020.

[294] Written evidence – DI, 13 June 2019, 4 September 2020.

[295] Oral evidence – DI, *** December 2020.

[296] Written evidence – DI, 13 June 2019.

[297] From 1 April 2021, the Home Office moved to a new structure and the work of the Office for Security and Counter Terrorism (OSCT) is now carried out by Homeland Security Group. Therefore, OSCT is now referred to as Homeland Security Group.

[298] Senior staff have not been counted in this number, although a portion of their work will involve China-related issues. Homeland Security Group also notes that its contribution to the Home Office's China effort is wider than stated above "*as there are a number of areas (such as Border Security, HSA strategy and Counter-HSA legislation) where policy work is thematically rather than geographically focused*". ***. (Written evidence – OSCT, 28 February 2020.)

[299] Written evidence – OSCT, 28 February 2020.

- This is a decrease from 2019, when *** FTE staff worked on China. In 2019, the Committee was told that *** due to be recruited, which would raise the number of dedicated staff to *** FTE.[300] Then in 2020, we were informed that the figure "*will rise to *** FTE ****".[301] At the time of taking evidence, we had yet to receive confirmation that this uplift had taken place.

192. NSS has *** staff[302] working on China with an administrative spend of £*** per annum. This includes a secretariat for the China National Security Council (NSC) strategy and National Strategy Implementation Group (NSIG), co-ordination of cross-cutting policy in support of that strategy, and provision of advice to the Prime Minister.

Potential for increase in resourcing

193. When we took evidence in autumn 2019, the Intelligence Community told us that any increase in resources on China would have to be viewed as necessary by the NSC (and the Treasury) and it may be that the threat posed by Russia, Iran or counter-terrorism could be considered as more in need of increased resourcing. In the past, such balancing of priorities has seen resources being diverted away from China onto acute counter-terrorism priorities. As Director General MI5 explained to the Committee:

> *** *there are some difficult choices when the CT* [counter-terrorism] *thing has not reduced in its scale and its sharpness … we need to figure out how much of these kinds of capabilities feels enough or proportionate against this threat.*[303]

194. MI5 told the Committee that there were things that the Government could invest in that would improve overall defences (against HSA). But, if the NSC decided that a new area was of great ***.[304] GCHQ told the Committee that it was investing in training people to work on China *** but that, in terms of analytical effort, difficult decisions would have to be made in order to balance it alongside work on other areas ***.[305]

195. In 2019, the SRO for China was clear that there was "*a big set of questions for a Spending Review*" where the China effort was concerned.[306] The Agencies explained that they had submitted ambitious bids to the 2020 Spending Review but that there would be difficult decisions. According to MI5 ***[307] SIS echoed this, and also noted that despite increased focus on China ***.[308]

196. We were concerned in particular at the *** in Homeland Security Group working on China, but welcomed the expected increase in resourcing across the Intelligence Community. We expected to see resourcing of the upward trajectory maintained in the Spending Review,

[300] Written evidence – OSCT, 14 June 2019.
[301] Written evidence – OSCT, 28 February 2020.
[302] The Cabinet Office notes that its China team draws on China expertise from across Whitehall and that the majority of HMG work on China is done in other government departments. (Written evidence – HMG, 18 November 2020.)
[303] Oral evidence – MI5, *** July 2019.
[304] Oral evidence – MI5, *** July 2019.
[305] Oral evidence – GCHQ, *** July 2019.
[306] Oral evidence – *** July 2019.
[307] Oral evidence – MI5, *** October 2020.
[308] Oral evidence – SIS, *** October 2020.

given that China is now recognised as an enduring national security challenge. In 2021, we were told that a one-year annual uplift had been granted to the Agencies' China mission ***[309]

197. The Agencies also advised the Committee that this increased funding would be allocated to promoting resilience, specifically to:

> *support modest investment in MI5's efforts to raise awareness and provide advice to government and Industry on China-related threats, and the delivery of a more finely tuned response to the economic threat posed by China to the UK's Critical National Infrastructure and Science, Technology and Critical Knowledge sectors, and enabling us to better detect threats of hostile investment through data analysis.*[310]

198. However, the Agencies were clear that this additional funding was only a stop-gap: "*Whilst these investments allow us to grow and maintain critical mission capabilities, further growth in SR21* [Spending Review 2021] *is required to enable us to respond to the sheer scale of the China threat*."[311] Director GCHQ reinforced this message, telling the Committee: "*Russia has given us some really crappy weather but China is giving us the climate. We really have to think strategically and long term* [about China]."[312]

199. The National Cyber Force (NCF) – a partnership between GCHQ and the Ministry of Defence, including elements from SIS and the Defence Science and Technology Laboratory – was also announced as part of the Spending Review. The Intelligence Community told us that the NCF is expected to improve and increase the UK's cyber capability and "*enhance the UK's position and reputation as a top-tier cyber power*".[313] NCF priorities are derived from NSC priorities and are set through a forum chaired by the Deputy National Security Adviser, separate from the IOP process described (although we were told that IOP Plans do inform and are reflected in NCF priorities).[314] We have been told that, since the NCF started operating, it had been able to expose and counter false narratives ***. Countering interference was cited as another area *** for the NCF ***.[315]

200. In addition to the uplift under the Spending Review, MI5 has been able to increase the number of people working on the China threat area (from September 2020 to March 2022), doubling the overall effort on ***.[316] ***. [317] The Intelligence Community noted:

---

[309] Written evidence – HMG, 21 May 2021.
[310] Written evidence – HMG, 21 May 2021.
[311] Written evidence – HMG, 21 May 2021.
[312] Oral evidence – GCHQ, *** July 2019.
[313] Written evidence – HMG, 21 May 2021.
[314] A 'Whitehall Customer Group', chaired by the Deputy National Security Adviser, with the Foreign, Commonwealth and Development Office (FCDO), MoD and Home Office representation, will meet annually to establish a single national statement of prioritised outcomes to be supported by offensive cyber. This process will be informed by customer requirements articulated through the IOP process and by COBR, Armed Forces operational requirements, MoD contingency plans and law enforcement demands, amongst others. These engagements aim to provide assurance to departments that their requirements have been considered and prioritised appropriately.
[315] Written evidence – HMG, 21 May 2021.
[316] Written evidence – HMG, 21 May 2021.
[317] Written evidence – HMG, 21 May 2021.

Whilst these investments allow us to grow and maintain critical mission capabilities, further growth in SR21 is required to enable us to respond to the sheer scale of the China threat.[318]

AA. The level of resource dedicated to tackling the threat posed by China's 'whole-of-state' approach has been completely inadequate. While a shortage of resources had been identified as early as 2012, effort was diverted onto the acute counter-terrorism threat arising from Syria. The increase in funding on the China mission in 2020 was therefore both necessary and welcome. But it was only for one year. HMG cannot think or plan strategically with such short-term planning.

BB. HMG must explore the possibility of a multi-year Spending Review for the Agencies, in order to allow them to develop long-term, strategic programmes on China and respond to the enduring threat. The UK is severely handicapped by the short-termist approach currently being taken.

[318] Written evidence – HMG, 21 May 2021.

DEFENDING THE UK

Responsibility

201. Under the Security Services Act 1989, MI5 is responsible for countering Hostile State Activity (HSA), i.e. "*protection against threats from espionage, terrorism and sabotage* [and] *from the activities of agents of foreign powers*". In May 2019, MI5 had around *** full-time equivalent (FTE) staff working on State Threats – predominantly on counter-intelligence and counter-espionage but also on counter-proliferation and state-sponsored terrorism work. The HSA team primarily focuses on Russia, China and Iran but they also have a 'Rest of the World' remit.[319]

202. MI5 also has responsibility for the Joint State Threats Assessment Team (JSTAT). JSTAT provides assessments and a holistic view on the national security threat posed by:

- espionage;
- assassination;
- interference in our democracy and society;
- threats to the UK's economic security; and
- threats to the UK's people and assets overseas.[320]

It therefore looks in depth at the threats from *** activity, as well as niche and emerging threats, and provides assessment for a wide range of government departments.[321]

203. JSTAT works under MI5's legal authorisations. It is governed by a Board ***, and draws its staff from across government, including policy departments, MI5, DI, SIS and GCHQ. In 2019, the Committee was told that JSTAT had around *** analysts, *** of whom were working on China in February 2020 (the previous Committee was told that the intention was to increase that *** by the end of the financial year 2019/20).[322] By late 2020, the number had risen *** and the intention was for a further increase *** in 2021, subject to the outcome of the Spending Review.[323] MI5 explained that JSTAT was vital to countering the threat from China:

> *So we have already clocked that we need to bolster how we are bringing together a fragmentary complex intelligence picture, mixing that with what is in the public domain, because, as I have said, a lot of the China intent is very public, and then using that to inform the security aspect of the judgement that then is part of informing Ministers and the Departments about the overall balance.*[324]

[319] Written evidence – MI5, May 2019.
[320] Written evidence – MI5, May 2019.
[321] Written evidence – MI5, March 2020.
[322] Oral evidence – HMG, *** July 2019.
[323] Oral evidence – HMG, *** October 2020.
[324] Oral evidence – MI5, *** October 2020.

Focus and coverage

204. MI5's objectives in relation to HSA are to "*seek those trying to pass sensitive UK information and equipment to other countries and ensure they don't succeed*" (counter-espionage) and to "*disrupt the actions of foreign intelligence officers where these are damaging to our country's interests*" (counter-intelligence).[325] MI5 told us that its role is spread across a range of areas, including investigating activity against UK interests both within the UK and abroad (as well as remotely online) ***. MI5 also has responsibility for detecting (and countering) "*penetration of government, or the Agencies themselves for that matter*" ***.[326] MI5 told the Committee that:

> *the MI5 role is clearly central on the counter-intelligence element* ***[327]

205. In 2020, *** of MI5's operational effort was focused on China.[328] *** in order to counter the breadth of the China threat, MI5 has prioritised[329] its efforts "***".[330] MI5 told us that it was working on a number of areas relating ***, including:

- HMG – attempts to penetrate the UK Intelligence Community and wider HMG ***;
- ***;
- Science and Technology – attempts to obtain sensitive UK defence technology ***;
- ***;
- ***;
- ***;[331] and
- Cyber – developing HMG's understanding ***.[332]

206. ***[333]

207. Although MI5 argued that the measures it was taking were proving to be effective, it also accepted that ***. Director General MI5 told us:

> *We've built up quite an experience base now ***. So I don't think we are likely to be ***. Clearly that's in some ways not that different to the version I face of that around counter-terrorism, for example. ***.*[334]

[325] MI5 website.
[326] Oral evidence – MI5, *** July 2019.
[327] Oral evidence – MI5, *** July 2019.
[328] Compared with ***% for Russia. ***% of MI5's effort is focused on counter-terrorism work. (Oral evidence – MI5, *** October 2020.)
[329] MI5 prioritises its work using the *** model. This model (***) aims to "*drive operational outcomes* ***". It is used to prioritise *** to ensure MI5 delivers long-term *** against its core intelligence requirements. (Written evidence – HMG, 18 April 2019.)
[330] Written evidence – HMG, 18 April 2019.
[331] Written evidence – MI5, 11 June 2019.
[332] Written evidence – HMG, 18 April 2019.
[333] Oral evidence – MI5, *** December 2020.
[334] Oral evidence – MI5, *** December 2020.

Tools

HMG uses a variety of tools to disrupt Hostile State Activity (HSA):

- **Interviews:** *** there may be a discussion arranged with that individual ***.
- **Vetting action:** Removing the security clearance of British nationals with access to sensitive information who pose a national security risk, including those who may have been in contact with foreign intelligence services ***
- **Expulsion of intelligence officers:** Removal of intelligence officers operating in the UK under diplomatic cover (under the terms of the Vienna Convention). ***
- **Capacity-building with allies and partners:** This may involve *** training, support or skill development ***. ***. This is covered further in the chapter on Working with Allies.
- **Visa action:** As is standard, the Home Office can consider revoking a visa on the grounds that someone's presence in the UK is 'not conducive to the public good' ***[335] ***[336]
- **Legislative measures:** There are a number of different pieces of legislation available for the Agencies to use such as the Official Secrets Act, the Computer Misuse Act and civil law remedies such as patent or copyright infringement. However, according to the Agencies, they are of limited use in countering HSA (legislation is considered in more detail later in the Report).
- **Démarches:** This might include, amongst other things, requesting the removal of named intelligence officers from their positions ***.
- **Briefings to Industry:** These are used where intelligence indicates there is intent to target certain companies or Industry sectors ***. This work is led by the Centre for the Protection of National Infrastructure and the National Cyber Security Centre, but – given the wide range of individuals, assets and organisations – disrupting every incident cannot be guaranteed.
- **Countering cyber threats:** This includes exposing and disrupting the activities of state-sponsored hackers ***.[337]

Protective role: CPNI and NCSC

208. The Centre for the Protection of National Infrastructure (CPNI – accountable to MI5) and the National Cyber Security Centre (NCSC – part of GCHQ) play a key role in engaging with those both within and outside Government to protect national security:

- CPNI has a preventative and advisory role, dealing with the non-cyber threat to Industry. It follows a "*threat-focused and intelligence-led*" approach to engagement,

[335] Written evidence – GCHQ, 31 January 2020.
[336] Written evidence – MI5, 16 November 2020.
[337] Written evidence – HMG, 18 April 2019.

allocating resources to sectors, industries and businesses where there is evidence of Chinese desire to gain knowledge, technology, expertise and Intellectual Property (IP). CPNI works with cross-government partners "*to raise awareness of the threat, identify vulnerabilities, and to provide holistic advice and mitigations*".[338]

- NCSC was set up to be the single authority on UK cyber security. It works closely with government departments to help them own and manage the risks in their sectors of Critical National Infrastructure, including setting policy and direction for protecting the sector, ensuring legislation is fit for purpose, and understanding how the operators are responsible for the security and resilience of their own systems and assets.[339] It works jointly with CPNI in a number of areas, including recently producing guidance for Industry and Academia on engaging with foreign entities. This guidance (Trusted Research) provides advice to senior leaders and individuals about how to protect research, IP and products.[340]

209. MI5 told us that CPNI and NCSC carry out regular protective defensive briefings.[341] These can either be regularly scheduled briefings to a particular sector or they can be specific briefings in response to intelligence received suggesting that a company is being targeted. ***.[342] Although this work is actor-agnostic, China is acknowledged to be the greatest threat.[343] Director General MI5 noted:

> *when we are talking about the protection of Intellectual Property, economic security, those kinds of themes, mostly in that space we are talking about the threat of China. Russia does also spy against particular sectors, you know, most famously Energy, but for the most part the chunk of CPNI that is addressing espionage and the theft of information and those kinds of influence risks is mostly there to tackle* ***.[344]

210. Director GCHQ told us that NCSC "*seeks to investigate Chinese cyber intrusions and defend against them, including advising our Critical National Infrastructure, our military and defence colleagues on how best to defend*".[345] NCSC carries out its defensive role by:

- providing bespoke advice and guidance;
- working with providers of Critical National Infrastructure on bespoke projects to enhance standards;
- responding to incidents; and
- engaging in proactive research and design in order to help the sector think about its vulnerabilities end-to-end. This might include:
  - identifying the networks and information systems that are critical;
  - carrying out risk reviews;

[338] Written evidence – HMG, 18 April 2019.
[339] Oral evidence – NCSC, *** October 2020.
[340] CPNI.gov.uk/trusted-research
[341] Oral evidence – MI5, *** October 2020.
[342] Written evidence – HMG, 18 April 2019.
[343] Oral evidence – MI5, *** October 2020.
[344] Oral evidence – MI5, *** December 2020.
[345] Oral evidence – GCHQ, *** July 2019.

- producing guidance to help in sector-specific technologies; and
- working with key vendors to better secure their supply chains.[346]

A new approach

211. In June 2019, MI5 told the Committee that, instead of relying on uncovering HSA through investigations, in future it will place greater emphasis on making sure that the UK is a difficult operating environment for hostile state actors. ***.[347]

212. MI5 updated the Committee on this work in late 2020, saying that it believed its record over the past year was "***", in that it had ***.[348] The Director General told the Committee:

> *There is some good work happening, which is informing a range of policy action, and one recent example would be ***. That work has in part been stimulated by some very good analysis and assessment work which has brought together that picture.*[349]

213. However, the fact remains that there have been no prosecutions and only one arrest of a ***. This is partly down to the difficulty in prosecuting espionage offences (discussed further in the chapter on Legislation) as Director General MI5 explained:

> *** *more often it is information that confers a UK advantage but isn't necessarily a … state official secret, which is one of the reasons why the proposed new legislation is something that we see advantage in.*[350]

CC. MI5 is responsible for countering Hostile State Activity, and the Centre for the Protection of National Infrastructure and the National Cyber Security Centre play a key role in engaging with those within and outside government to protect national security. There is a wide array of defensive tools, which are being used to good effect, but the Government has come late to the party and has a lot of catching up to do. Our closest allies identified the need to use such tools against China long ago and we must learn from their experience and knowledge.

DD. It is also clear that this defensive effort requires a cross-government approach. However, this transfer of responsibility will need to be a well-thought-out, gradual process with adequate support provided to the departments and some degree of control retained at the centre. HMG needs to ensure that those departments not traditionally associated with security are properly resourced with security expertise, properly supported and properly scrutinised.

Challenges in tackling Chinese spying

Lack of Chinese Intelligence Services action in the UK

214. ***

[346] Oral evidence – NCSC, *** October 2020.
[347] Written evidence – MI5, 12 June 2019.
[348] Oral evidence – MI5, *** October 2020.
[349] Oral evidence – MI5, *** October 2020.
[350] Oral evidence – MI5, *** December 2020.

Global threat

215. The UK's significant economic, political, military and commercial co-operation with China provides the Chinese government with numerous opportunities to spy on the UK globally, including through the many British individuals based abroad ***. The work undertaken by the UK Agencies is therefore international and cross-Agency. MI5 noted that *** and told us that:

> ***[351]

An obligation on Chinese nationals

216. China has passed a number of pieces of security legislation in recent years.[352] These require Chinese citizens to provide assistance to the Chinese Intelligence Services (ChIS) and to protect state secrets – this includes Chinese locally engaged staff in embassies (and could also potentially be applied to foreign companies and even foreign nationals based in China). This would appear to be a clear avenue through which the Chinese staff of UK companies might be compelled to co-operate with China ***.[353]

217. In November 2021, China's Personal Information Protection Law (PIPL) – a Chinese version of the General Data Protection Regulation (GDPR) – came into effect. This asserts state power over data belonging to both Chinese and foreign companies. According to legal experts, "*the PIPL exerts certain exterritorial jurisdiction over data processing activities that happen outside China if the purpose is to provide products or services to individuals located in China, or to analyse or assess the behaviours of individuals located in China.*"[354] The Chinese government can therefore force Chinese and other companies to turn over their data as soon as it involves any Chinese citizens. However, in reality, it is not possible to compartmentalise Chinese citizens' data – meaning that China gets access to all data. A particular concern is China's use of this legislation to hoover up data from applications such as those used to book taxis and mini cabs – which can track a traveller's movements, capture photographs and link passengers to other users. We discuss China's collection of data in detail in our Case Study on Industry and Technology.

Use of journalist cover

218. We questioned whether the UK's freedom of speech might also be exploited for the benefit of intelligence operations by China, including through the use of ***.[355] ***[356] However, it must be noted that ***.

---

[351] Oral evidence – MI5, *** December 2020.
[352] Including the Counter-espionage Law (2014), the National Security Law (2015), the National Cybersecurity Law (2016), the National Intelligence Law (2017) and Personal Information Protection Law (2021).
[353] Written evidence – HMG, 18 April 2019.
[354] Elisabeth Braw with Franco Palazzolo, 'Emerging Insights: How Ride-Hailing Businesses Collect and Manage Data: A National Security Risk?', Royal United Services Institute (RUSI), 4 October 2021.
[355] China's use of Academia to influence free speech and obtain information beneficial to its objectives is covered in our Case Study on Academia.
[356] Written evidence – MI5, 31 July 2020.

Targeting of unclassified material

219. As has been mentioned previously, the ChIS also target unclassified UK material – an act which (in many circumstances) would not be an offence in UK law. This activity may be more difficult to detect and counter, although the Committee notes that this was an area being looked at by the (then) Department for Business, Energy and Industrial Strategy, and the Home Office, including through possible legislation.

EE. Chinese law now requires its citizens to provide assistance to the Chinese Intelligence Services (ChIS) and to protect state secrets. It is highly likely that the ChIS will use such legislation to compel the Chinese staff of UK companies to co-operate with them. It is also likely that China's Personal Information Protection Law will lead to the Chinese government forcing Chinese and other companies to turn over their data held on Chinese citizens. As compartmentalisation of Chinese citizens' data will be difficult, this is likely to mean that, in practice, China will obtain access to data held on non-Chinese citizens as well.

Challenges in countering Chinese interference operations

220. Much of the impact that China has on national security is overt – through its economic might, its takeovers and mergers, its interaction with Academia and Industry – as opposed to covert activity carried out by its intelligence officers ***. This means that 'interference' operations can be less easy to point to than traditional 'spying' operations ***.

221. The UK Intelligence Community have been open with the Committee about the challenges of detecting Chinese interference operations:

> *China's blended approach – its intertwining of overt and covert activity – poses significant challenges. ***. Unpicking this is difficult.*[357]

222. The JIC Chair acknowledged that "*** *some of it is legitimate activity, some of it …* [is not] *legitimate but not necessarily illegal*".[358] MI5 clarified the role that the UK Intelligence Community plays in identifying Chinese interference operations:

> *** *A lot of that will be visible, open, what I think diplomacy is about, that fostering of understanding, but we worry about where it is more covert or more nefarious.*[359]

Understanding the threat

223. ***

- ***
- ***
- ***

[357] Written evidence – HMG, 18 April 2019.
[358] Oral evidence – JIO, *** July 2019.
[359] Oral evidence – MI5, *** December 2020.

- ***[360]

224. ***

***

***[361]

225. The JIO, working with NSS and JSTAT, told this Inquiry that they were working to 'map' foreign interference ***.[362]

FF. The UK Intelligence Community have been open with the Committee about the challenges of detecting Chinese interference operations. ***

Taking responsibility

226. One of the factors in the lack of understanding is that, until recently, the Agencies did not recognise that they had any responsibility for countering Chinese interference activity in the UK, since they considered that the policy community had mandated them to focus on other threats. In 2019, they told the Committee that ***:

> *Responsibility for mitigating the more overt aspects of the* [Chinese] *threat to the UK ... rests with government policy departments* ***.[363]

227. Historically, this resulted in an intelligence gap as it meant that not only were the Agencies not taking responsibility for tackling it, they were not even proactively seeking to identify it. Instead, it 'fell through the cracks' as the Government was relying on government departments to identify and then tackle the threat posed by China on their policy areas. (This was not unusual – we reported a similar historic problem in our *Russia* Report.) Yet the whole-of-state approach used by China meant that various UK government departments were trying to tackle different versions of the same problem – that of Chinese nationals, whether employed by the Chinese Communist Party or private individuals, actively working for China's benefit. For example, at the time of taking evidence, the Department for Education (alongside the (then) Department for Business, Energy and Industrial Strategy) was responsible for identifying and tackling Chinese interference in UK Academia.[364]

228. However, there is no evidence that Whitehall policy departments have the necessary resources, expertise or knowledge of the threat to investigate and counter the Chinese whole-of-state approach. The nature of China's engagement, influence and interference activity in the UK is difficult to detect, but even more concerning is the fact that the Government may not previously have been looking for it. ***.

[360] Written evidence – JSTAT, 31 May 2019.
[361] Oral evidence – JIO, *** October 2020.
[362] Written evidence – HMG, 21 January 2020.
[363] Written evidence – HMG, *** April 2019; the Agencies focus their efforts on ***.
[364] Oral evidence – HMG, *** July 2019.

229. Since the Committee began taking evidence and questioning the Agencies on their lack of involvement in tackling overt aspects of the Chinese threat, there appears to have been a change in approach. ***[365], ***.[366]

230. MI5 told us that this decision was part of a "*gradual widening of our aperture*" to look beyond the traditional focus ***.[367] This allowed it to increase its work on influence alongside espionage. MI5 says that it is exploring ***.[368]

231. In October 2020, the Acting National Security Adviser (NSA) told the Committee that there was now "*an enormous amount of work underway, and of course it is not perfect at the moment, but it shows, I think, that we are joining up more effectively across government and between the covert side and the overt side, to get our arms around the scale of the threat*".[369] Director GCHQ also told us that the situation was improving. However, the Director also noted that there was a tension between centralising the response and empowering the lead government department to address the issue (which had, in the past, resulted in a lack of co-ordination).[370]

232. In December 2020, the DNSA acknowledged that neither the (then) Department for Business, Energy and Industrial Strategy (BEIS) nor the (then) Department for Digital, Culture, Media and Sport (DCMS) was yet able to engage fully in national security decision-making structures:

> *The one area probably of vulnerability at the moment, both for BEIS and for DCMS in handling some of their cases is their security expertise, their capabilities, their infrastructure … one of the reasons we have incubated the Economic Threats Unit/ Investment Security Unit in the Cabinet Office is because we have that very rich relationship and can do that kind of intelligence component. So the reason we haven't sort of chucked it straight over the fence is that we are trying to give BEIS some time to build that capability. They have just appointed a new security Director and that work is ongoing and we will support them with that. But I think it's important that we support and enable them rather than continue to hold everything at the centre, in the same way as the Department of Transport would run aviation security and have that connectivity into* [MI5]. *Similarly with BEIS on investment security, we have to help them to be able to run this themselves.*[371]

233. This is clearly a time of significant change within the national security structures across the Government. Whilst we are supportive of the notion of making every part of the

[365] The United Front Work Department (UFWD) is an arm of the CCP, which has a remit to engage in operational activity within China and overseas with the purpose of ensuring that potential critics and threats to the CCP are influenced, co-opted or coerced into silence. UFWD's remit includes engaging in political influence and interference operations overseas, to ensure that politicians and high-profile figures in foreign states are supportive of the CCP, or at the very least do not criticise China or counter its narrative.
[366] Written evidence – MI5, 24 September 2020.
[367] Oral evidence – MI5, *** October 2020.
[368] Written evidence – MI5, 24 September 2020.
[369] Oral evidence – *** October 2020.
[370] Oral evidence – GCHQ, *** October 2020.
[371] Oral evidence – *** December 2020.

Government responsible for national security, equally that must not result in no part of the Government being responsible for national security policy.

GG. It is incumbent on the Government to report on how national security decision-making powers are being dispersed across the Government. It should annually update this Committee on the number of personnel cleared to see Top Secret material in each of the departments with new national security decision-making powers, together with the facilities provided to them (secure IT terminals and telephones etc.).

HH. Failure to get this transition right from the outset could lead to decisions that fail to withstand external challenge. Furthermore, as there is an adjustment in national security responsibility, so too must there be an adjustment to ensure there is effective Parliamentary oversight of all aspects.

ON THE 'OFFENSIVE'

234. SIS and GCHQ's intelligence work encompasses both 'coverage' and 'effects'. 'Coverage' is the collection of information (or acquisition of information from allied intelligence services) by the Agencies, whereas 'effects' describes the Agencies' engagement in activities which have real-life outcomes. ***

The roles of SIS and GCHQ

SIS is the UK's foreign human intelligence (HUMINT) agency. Areas of work that SIS undertakes include:

- cultivating and maintaining agents who are in a position to pass on secret information; and
- obtaining and sharing information which our allies have gathered on China.

GCHQ is the UK's signals intelligence (SIGINT) agency. Areas of work that GCHQ undertakes include:

- applying selectors to emails obtained by bulk interception;
- intercepting material transmitted over military communications systems;
- covertly accessing computer systems in order to obtain the information they contain; and
- sharing information with our allies' intelligence agencies.

Allocation of effort

235. Operational effort within SIS and GCHQ is broken down into different 'missions' (as explained in the chapter on HMG Resourcing). As at 2020, SIS allocated ***% of its overall operational effort to China and GCHQ allocated ***% of its operational effort to China.[372] The China mission is then further broken down into the different 'requirements' on China which the Government has set for SIS and GCHQ.

236. In evidence in 2020, SIS broke down its operational effort in relation to China as ***

- ***
- ***
- ***[373]

This split has been broadly static since 2019.

[372] Written evidence – SIS, 18 November 2020; Oral evidence – GCHQ, *** October 2020.
[373] Oral evidence – SIS, *** July 2019; Oral evidence – SIS, *** October 2020.

237. In 2019, GCHQ noted that its operational effort was similarly divided but with an additional focus on ***.[374] A year later, Director GCHQ told us that there were between *** and *** active Chinese cyber groups, and that GCHQ was able to cover ***.[375]

Requirements

238. The outcomes – what the Government wants to achieve – in relation to China are set though the Intelligence Outcomes Prioritisation (IOP) process[376] (discussed in the earlier chapter on The Strategy). HMG says that the IOP process is designed to ensure that SIS and GCHQ's work accords with the priorities set by the National Security Council (NSC), so that the information and outcomes they provide will best serve the wide range of demands from their 'customer' departments in the Government. The IOP Plan is meant to set out the Government's priorities for SIS and GCHQ, to be delivered through 'coverage' and 'effects'.

239. In October 2020, the Committee was provided with the China Policy Outcomes, set within the China IOP process. As opposed to the tasking document previously produced, we were informed that instead these outcomes "*guide the setting of SIS & GCHQ contributions but are not themselves requirements for Agency coverage or effects*" and that the policy outcomes "*are not delivered by secret intelligence and effects alone*".[377] However, this change in emphasis (reflective of the Fusion Doctrine) means that it is now not possible to establish to what extent SIS and GCHQ are individually responsible for any progress made against these outcomes – and therefore how their effectiveness or performance can be meaningfully assessed. We question the logic behind this.

240. Nevertheless, we can examine the responsibilities of SIS and GCHQ by comparing the 2019 and 2018 Intelligence Coverage and Effects (ICE) Plans, which were tasking documents:

- ***[378]
- ***

When (in 2019) we asked about the 2018 ICE Plan, SIS told us that:

> ***[379]

241. Given that the ICE Plans were drawn up in consultation with SIS and GCHQ, it would suggest that the Cabinet Office and those Agencies felt that they were in a position to effect more real-world outcomes in 2019 than they were in 2018. This is reassuring, if that trajectory continues. Nevertheless, without knowing the current requirements set for both Agencies, we cannot judge what their current division of work is between finding out information and stopping the Chinese from doing things that hurt UK interests.

---

[374] Oral evidence – GCHQ, *** July 2019.
[375] Oral evidence – GCHQ, *** October 2020.
[376] The IOP process was established in March 2020, although as previously noted it may be reviewed following the Integrated Review.
[377] Written evidence – HMG, 14 October 2020.
[378] Written evidence – HMG, 30 August 2019.
[379] Oral evidence – SIS, *** July 2019.

Coverage

242. Examples of GCHQ and SIS China 'coverage' work provided in 2018 include:

- ***[380]
- ***[381]
- ***[382]

243. Although not part of the IOP Plan, DI also works to a number of intelligence collection goals. There is a particular focus on ***.[383]

Effects

244. Intelligence 'effects', also referred to as covert action, are SIS and GCHQ activities which have real-life outcomes. Effects work against hostile states was explored during the Russia Inquiry, when Committee Members were told that HMG does not deploy effects with the goal of effecting organisational collapse, in the way that they might be deployed against international terrorist groups, for example. As a result, the Agencies' effects work *** can involve capability-building (the sharing of knowledge and capabilities with partners), and counter-intelligence work to disrupt intelligence operations ***.[384] More broadly, HMG can employ intelligence diplomacy (the use of intelligence information and relationships to influence international action), which can range from using intelligence partnerships to build alliances or encourage action on a particular issue, to the maintenance of alternative diplomatic channels with governments or non-state actors with which it is considered impolitic to have overt diplomatic relations.

According to the evidence provided to the Committee in this Inquiry, the same principles broadly apply to SIS and GCHQ's work on China ***. When we questioned GCHQ in 2019, we were told that:

> ***[385]

245. As noted previously, the 2018 China ICE Plan ***.[386] This was being delivered through a counter-cyber programme known as Operation WINDERMERE.[387]

---

[380] Written evidence – GCHQ, 31 October 2018.
[381] Written evidence – SIS, 30 April 2019.
[382] Written evidence – GCHQ, 31 October 2018.
[383] Oral evidence – DI, *** December 2020.
[384] *Russia*, HC 632, 21 July 2020.
[385] Oral evidence – GCHQ, *** July 2019.
[386] Written evidence – HMG, 18 April 2019.
[387] In some instances in this Report, we have substituted an ISC-specific code word where it has been necessary to refer to the name of an operation or project, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to real operation names. The ISC code words have no operational significance.

Case study: Operation WINDERMERE (counter-cyber)

The UK Intelligence Community told the Committee in 2019 that the UK is leading internationally on countering the cyber threat from China. (Given that there has been a lot of public reporting regarding the UK's limited focus on China by comparison with its Five Eyes partners, it is interesting that the UK Intelligence Community consider that they are leading internationally on responding to the Chinese cyber threat.)

Operation WINDERMERE is a cross-UK Intelligence Community strategy to address Chinese cyber activity, led by GCHQ ***. It aims to "*reduce the impact of the Chinese State's cyber programme on UK* ***."[388]

The strategy focuses on taking intelligence *** and using it for defence means (in order to make UK cyber space a hard operating environment) ***.[389] The approach combines a mixture of diplomacy, law enforcement action and PROTECT[390] work. ***.

The UK Intelligence Community say that they are working to identify and build knowledge of the Chinese cyber actors assessed to pose the highest threat to UK national security ***.[391]

*** As such, encouraging other countries to demonstrate unity on the attribution of such behaviour (***) is key.[392]

246. The 2019 ICE Plan, by comparison ***. These included:

- Against the 'Trading Safely' pillar ***.
  - ***.[393]
- ***.
  - ***.
- Against the 'Countering Security Threats' pillar ***.
  - ***[394] ***.[395]
  - In late 2020, GCHQ told us that:

[388] Written evidence – GCHQ, 18 June 2019.
[389] Written evidence – HMG, 18 April 2019.
[390] PROTECT work focuses on protective security.
[391] Written evidence – GCHQ, 20 June 2019.
[392] Oral evidence – HMG, *** December 2020.
[393] Written evidence – GCHQ, 31 January 2020.
[394] The National Cyber Force (NCF) was launched in April 2020. The NCF is a distinct operational entity, a partnership between GCHQ and the Ministry of Defence, also incorporating elements from SIS and the Defence Science and Technology Laboratory. The NCF is intended to deliver an increase in the UK's cyber capability and carry out its programme of offensive cyber.
[395] Written evidence – HMG, 14 September 2020.

> *** [these] *include attribution – public attribution – they include working with other nations to call out Chinese malign activity in cyber space, they include technical advisories,* [and] *they include advice to companies to close off their capabilities.* [396]

- ***.
  - ***[397] ***. [398]
- Against the 'Digital and Technology' pillar ***.
  - ***.

247. Following the Spending Review, we were told that, since the National Cyber Force (NCF) had started operating, it had been able to expose and counter false narratives ***. Countering interference was cited as another area *** for the NCF ***.[399]

Are SIS and GCHQ 'achieving'?

248. Although SIS and GCHQ were judged by the Cabinet Office to be meeting or exceeding most of their ICE targets on China in 2018, this seems largely due to expectation management, as most targets were set to 'some' or 'limited' contribution – so, although they met their targets, the targets themselves were set rather low.[400]

249. When the Committee asked Director GCHQ in 2019 if he felt "*that in the circumstances* [GCHQ was] *not doing too badly*", the Director agreed with that assessment − but also said that it was still very much at the starting point.[401] ***.[402]

250. SIS noted that the 'coverage' targets in the 2018 ICE Plan had enabled it to start work, jointly with GCHQ and MI5, on *** – this, rather worryingly, implies that little had actually been achieved at that point.[403] When, in 2019, we pressed on why there appeared to be so little work ***, GCHQ told us that:

> *coverage leads directly to intelligence reporting, which can have an impact and does have an impact and affects the way we position the UK's policy, it affects the way we are conducting our international relations and it affects the way we are laying down our capability investments in the future. So *** then I think that is probably a more precise way of thinking about that. The answer to … why so much* [is directed] *at *** at the moment is because ***.*
>
> ***[404]

[396] Oral evidence – GCHQ, *** October 2020.
[397] Oral evidence – HMG, *** October 2020.
[398] Oral evidence – HMG, *** October 2020.
[399] Written evidence – GCHQ, 21 May 2021.
[400] Written evidence – GCHQ, 12 June 2019.
[401] Oral evidence – GCHQ, *** July 2019.
[402] Written evidence – GCHQ, 12 June 2019.
[403] Oral evidence – SIS, *** July 2019.
[404] Oral evidence – GCHQ, *** July 2019.

251. When we asked again, in late 2020, what had now been achieved, GCHQ said that the increase in effort could be seen in all areas of activity, including the collection of intelligence, effects work ***, and in the defensive aspects of the cyber effort. The progress *** meant that:

> *we have made massive headway, such that the issue is starting to be how do we deal with the scale of the information at our disposal? How do we get into and focus the effort on the things that we most care about* ***.[405]

252. In terms of other work *** brief reference has been made to work carried out in relation to health (and specifically Covid-19). In 2020, the Deputy National Security Adviser (DNSA) said "*... over the last ten months or so of Covid we have certainly seen on the health side some advantage* ***".[406] However, no further detail has been supplied.

253. In October 2020, the Acting NSA told us that a new group, which sits below the China NSIG, had been created to look at *** work, ensuring that it is joined up. One of the reasons why this group had been created was because the Government expected this work "*to grow in future*".[407]

254. However, when we asked, again, in 2020, how SIS and GCHQ had performed against the requirements set by the Cabinet Office, we were told that the pandemic meant that there had not been a Cabinet Office review of whether either Agency had met its targets.[408]

II. It is clear that there has been progress in terms of 'offensive' work since we started our Inquiry – for instance, an increase in 'effects' work. However, given what appears to be the extremely low starting point, this is not cause for celebration *. Both SIS and GCHQ say that working on China "*is a slow burn, slow-return effort*"[409] ***.**

JJ. GCHQ and SIS tasking is set by the Government and, rightly, they cannot work outside the Government's priorities. Nevertheless, the fact that China was such a relatively low priority in 2018 – the same year in which China approved the removal of term limits on the Presidency, allowing President Xi Jinping to remain in office as long as he wished – is concerning. Work must continue to be prioritised now to make up for this slow start and there must be clear measurement and evaluation of effort.

SIS and GCHQ challenges in operating against China

Political and economic considerations

255. Prior to the pandemic, the UK's relationship with China was based on an approach that sought to balance prosperity with national security issues – unlike Russia, which is seen unambiguously as a threat. Although that balance appears to have shifted since, with the

[405] Oral evidence – GCHQ, *** October 2020.
[406] Oral evidence – *** October 2020; Oral evidence – *** December 2020.
[407] Oral evidence – *** October 2020.
[408] Oral evidence – HMG, *** October 2020.
[409] Written evidence – GCHQ, 12 June 2019.

push to protect the UK's domestic economic security, HMG acknowledges that China's economic might cannot be ignored.[410]

256. This has an impact when planning action. For example, exposure of intelligence work may damage bilateral relations to the extent that UK trade and investment interests are affected.[411] Similarly, when HMS Albion performed a Freedom of Navigation Operation in the South China Sea in 2018, China appeared to reduce economic engagement with the UK. In 2019, the Senior Responsible Owner told us that HMG *** had discussed how to re-engage the Chinese:

> [it] *was re-established after *** diplomacy and engagement, there were some decisions that the Treasury had to take about how they were approaching that dialogue, ***. Because of the cross-cutting nature of that, that wasn't a decision that the Treasury could just take alone. So we worked through the coordinating process to get a clear set of choices and decisions* ***.[412]

Surveillance

257. China is often referred to as a surveillance state, using a range of methods from state-of-the-art technology to neighbourhood watch schemes to monitor its citizens and residents. There is near-comprehensive CCTV coverage in Beijing as well as in most other major cities.

258. The rapid pace of technological development is only increasing this challenge. China is in the process of integrating its world-leading technologies, such as face recognition and artificial intelligence (AI), in order to allow state authorities to track and follow all residents around its cities. Further development and integration of AI would allow monitoring and automated flagging of unusual behaviour or activities.[413]

259. When, in July 2019, we asked the Intelligence Community about this, China was described as a "*totally sensored environment ... sensors everywhere and computers making sense of those feeds for individuals to spot* [an] *anomaly*" ***. It was expected that such an environment would "*increasingly become the norm *** because this technology is cheap and will be exported*". [414] ***.[415]

260. ***. Surveillance of Chinese citizens with access to secret information is particularly acute: individuals working on sensitive areas are subject to travel bans and cannot leave the country without express permission. The Chinese intelligence system is both hugely capable and uncompromising: those convicted of espionage can face the death penalty.[416] ***.

261. Surveillance in China has also extended to the virtual world. China's well-established domestic technology sector poses a significant challenge in terms of SIGINT collection. The

[410] Written evidence – HMG, 14 September 2020.
[411] Written evidence – HMG, 18 April 2019.
[412] Oral evidence – *** July 2019.
[413] Written evidence – HMG, 18 April 2019.
[414] Oral evidence – SIS, *** July 2019.
[415] Oral evidence – SIS, *** July 2019.
[416] Written evidence – HMG, 18 April 2019.

blocking of Western web services and applications, and the dominance of Chinese apps ***[417]

Equipment Interference

Equipment Interference (EI) describes a range of techniques that may be used lawfully to obtain communications, equipment data or other information from equipment. In plain English, most people would call this 'hacking'; however, the Intelligence Community avoid this term because it lacks a formal legal definition and is widely used to imply illegal activity. EI is the official term used for such activity within the Investigatory Powers Act 2016 and associated Codes of Practice. This replaces the previous term 'Computer Network Exploitation'.

EI can be carried out remotely or by physically interacting with the equipment, and may include interference with computers, servers, routers, laptops, mobile phones and other devices, as well as cables, wires and storage devices.

EI can vary in complexity. Examples of EI might include:

- covertly downloading data from a subject mobile device when it is left unattended;
- using login credentials to gain access to data held on a computer;
- exploiting existing vulnerabilities in software to gain control of devices or networks; or
- remotely extracting material and monitoring the user of the device.

Size

262. Even without the challenges of Chinese surveillance, the sheer size of the Chinese state presents a significant challenge when it comes to gaining coverage. It can be extremely difficult to keep track of the vast host of Chinese ministries and party organs, the status of which within the Chinese Communist Party and government is constantly evolving. ***. [418]

KK. It is clear that both GCHQ and SIS face a formidable challenge in relation to China. What we were unable to assess – without the specific requirements set for the Agencies or any idea of the prioritisation of the 'outcomes' within the Intelligence Outcomes Prioritisation Plan – is how effective either Agency is at tackling that challenge. As a result of pressures placed on civil servants during the Covid-19 pandemic – including fewer people in offices with access to the necessary IT systems – the Cabinet Office has not measured the Agencies' success against its requirements, and so neither the Government nor Parliament has any assurance about their effectiveness.

[417] Written evidence – HMG, 18 April 2019.
[418] Written evidence – HMG, 18 April 2019.

LL. We have seen efforts grow over the duration of this Inquiry. We expect to see those efforts continue to increase as coverage leads to an increased programme of 'effects'. However, given the importance of the work, it is vital that the Cabinet Office carries out an evaluation on whether SIS and GCHQ are meeting their targets in relation to China. That evaluation must be shared with this Committee.

MM. *. Increased surveillance, both in the physical and virtual world, poses significant challenges to long-term intelligence-generating capabilities ***. This problem is only going to get more difficult. SIS and GCHQ should prioritise work on this ***[419] ***.**

[419] ***

WORKING WITH OUR ALLIES

263. Given the difficulty of obtaining intelligence on China and countering its activity, intelligence-sharing relationships with other countries are vital: one of the Government's key messages in the Integrated Review was that the UK is stronger as part of an alliance, and we have sought to establish whether that is being put into practice and where the challenges lie.

Five Eyes

264. The Five Eyes intelligence-sharing network is vital to UK efforts in countering the challenges posed by China. SIS told the Committee that, within the Five Eyes community, there is very strong, increasing co-operation on China.[420] Director GCHQ told the Committee: "*When the UK, with its allies, focuses on the targets it most cares about, it can have real ... impactful effect, and I have absolutely no doubt about that.*"[421] Of great importance is the burden-sharing arrangement between the partners ***. From the evidence presented below, it can be seen that the UK benefits significantly from the Five Eyes partnership in the case of China.

265. SIS told the Committee that, in 2020, ***% of UK coverage of China came from ***.[422] Without that *** assistance, tackling the threat would be much more difficult. This is also clear in relation to *** – in 2020, ***% of coverage was derived from *** collection.[423]

266. For GCHQ, it was a similar picture in terms of the "*collaborative … analytical sharing* ***", with ***; and ***.[424]

267. One of the ways in which GCHQ works with Five Eyes allies is on countering malign Chinese cyber activities[425] ***. GCHQ told us:

> *Predominantly, the key allies we have been working with are Five Eyes allies and we have had considerable success ***. So a really joined up effort ... and I see this continuing to expand into the foreseeable future ... we are calling out malign activity, we are trying to impose a cost on those actors *** for acting in that way. ***.*[426]

268. The Committee was told that China was the single biggest issue at the ***. ***.[427] The Joint Intelligence Committee (JIC) Chair told us that DI had been the primary organisation

[420] Oral evidence – SIS, *** July 2019.
[421] Oral evidence – GCHQ, *** July 2019.
[422] Oral evidence – SIS, *** July 2019.
[423] Oral evidence – SIS, *** July 2019.
[424] Oral evidence – GCHQ, *** July 2019.
[425] In July 2022, the Director of the Federal Bureau of Investigation (FBI) gave a joint address to industry with Director General MI5, in which he referred to work with the UK on the Chinese cyber threat and said that "*together* [with MI5] *we can also run joint, sequenced operations that disrupt Chinese government cyber attacks*".
[426] Oral evidence – GCHQ, *** October 2020.
[427] Written evidence – HMG, 9 August 2019.

involved in the mapping activity, and that it had "*produced some really good material in which they have gone round the globe drawing on that to assess activity*".[428]

269. We asked for sight of the product of this mapping activity ***. We were disappointed that it appears not to have fulfilled the agreed brief *** it is concerning that in this instance the Intelligence Community appear to have failed to provide their partners with the required assistance.

Other partners

270. China is a broad threat with significant geographic reach, therefore the Agencies work with overseas partners beyond the Five Eyes to tackle the China threat:

- In July 2019, the Deputy National Security Adviser (DNSA) told the Committee that some of his most important conversations on China had been with *** around ***.[429]
- GCHQ told us ***.[430] ***.[431] GCHQ also cited the importance of ***, noting, "*we will go where the capability is and where the accesses are – they have brilliant accesses* ***".[432]
- MI5 cited ***[433] as allowing MI5 to discuss both its operational and protective security role with ***.[434]
- SIS told us in 2019 that it was starting to do some capability-building work ***.[435] SIS told us ***:

> ***. *So most of these countries are very aware of the threat, and are very keen to talk ... about how we can work together. So that is quite a promising seam of activity* ***.[436]

271. The Agencies are working closely with overseas partners to tackle the China threat: they recognise that the UK can tackle the problem only by working with their international counterparts ***. We have also covered the Agencies' work with foreign services in our Inquiry on International Partnerships.

[428] Oral evidence – JIO, *** October 2020.
[429] Oral evidence – NSS, *** July 2019.
[430] Oral evidence – GCHQ, *** July 2019. ***.
[431] Oral evidence – GCHQ, *** October 2020.
[432] Oral evidence – GCHQ, *** July 2019.
[433] ***
[434] Oral evidence – MI5, *** July 2019.
[435] Oral evidence – SIS, *** July 2019.
[436] Oral evidence – SIS, *** October 2020.

272. It is clear from our Inquiry that China presents a rather different challenge for the Government, one that it is still struggling to get to grips with and which it may not yet have the right tools to tackle. One of the tools that can be developed and used quickly is legislation. We have already covered the National Security and Investment (NSI) Act 2021 and the Telecommunications (Security) Act 2021 in this Report, and we will need to see what difference both pieces of legislation make; however, at the time of writing we had yet to see legislation introduced specifically to tackle Hostile State Activity (HSA).[437]

The need for new legislation on Hostile State Activity

273. The Official Secrets Acts[438] are the only pieces of UK legislation that specifically address HSA.[439] However, the Agencies have previously explained that the Acts are inadequate in countering HSA, since it is not an offence to be a covert agent of a foreign power. The previous Committee concluded in its *Russia* Report:

> *it is very clear that the Official Secrets Act regime is not fit for purpose … It is essential that there is a clear commitment to bring forward new legislation to replace it … that can be used by MI5 to defend the UK against agents of a foreign power*.[440]

274. In evidence to this Inquiry, the Intelligence Community told the Committee that legislative change is even more necessary in relation to China. MI5 told us that "*a Foreign Agent Registration* [Act]-*type power, which the Australians and Americans enjoy …* [would] *have proportionately more effect against … Chinese activity*".[441] A key issue of concern is the theft of non-classified information, which can be difficult to grip because a significant amount of the activity does not currently constitute a serious criminal offence in the UK.

275. One example of such a case is from ***, when a suspect was arrested for ***. The material ***. Given the difficulties of prosecuting espionage activities under current legislation ***.[442]

276. In the December 2019 Queen's Speech, the Government confirmed plans to introduce a new Espionage Act to provide a legislative framework to deal with HSA.[443] Consideration

[437] The National Security Bill was introduced in Parliament on 11 May 2022, after the Committee had finished taking evidence for this Inquiry. However, we note that the Bill, as introduced, does not include reform of the Official Secrets Act 1989 or introduce a Foreign Agent Registration Scheme (although the latter was later proposed via a government amendment at Committee stage of the Bill).
[438] 1911, 1920 and 1939.
[439] Other than the 'ports stop' power introduced in the Counter-Terrorism and Border Security Act 2019. 'Queen's Speech December 2019: background briefing notes' (HMG, December 2019) states that the Counter-Terrorism and Border Security Act 2019, which received Royal Assent in February 2019, confers the power to stop, question, search or detain any person entering the UK (it is not necessary for there to be a suspicion of engagement in hostile activity in order to do so). These provisions were closely modelled on the 'Schedule 7 port stop' power provided for in the Terrorism Act 2000.
[440] *Russia*, HC 632, 21 July 2020.
[441] Oral evidence – MI5, *** July 2019.
[442] Oral evidence – MI5, *** December 2020.
[443] 'Queen's Speech December 2019: background briefing notes', HMG, December 2019.

is also apparently being given to updating treason laws.[444] In September 2020, HMG confirmed that the Home Office was working on a Counter-Hostile State Activity Bill, to create a Foreign Agents Registration Scheme and reform the Official Secrets Act,[445] in line with recent recommendations by the Law Commission (which found that the espionage offences in the Official Secrets Acts 1911–1939 were "*very wide but rarely prosecuted*", as a result of dated and obscure drafting and complex supporting case law).[446]

277. October 2020, the Acting National Security Adviser told us that this Bill would also address issues around foreign interference – with the inclusion of "*a package of measures around education, partly support to universities, partly acquiring new tools in which to address that kind of interference*".[447] In late 2020, MI5 told the Committee how it had been contributing to the development of the proposed legislation:

> *So there is a series of different choices and how far you do or don't go around any reform of the Official Secrets Act, there is a series of choices that are not yet landed or settled, but what MI5 is doing clearly is feeding in our perspective on the things that would make a difference and, from where I am sitting, the biggest gap at the moment is around interference. There are still plenty of gaps around espionage, but we do at least have some relevant powers there; whereas the act of being an agent of a foreign power engaged in things against the interests of the UK is one where we think there is a real gap and so I am very pleased that government has the intention to legislate.*[448]

278. The Integrated Review, published in March 2021, included a further commitment to introduce Counter-State Threats legislation – "*when Parliamentary time allows*".[449] A consultation on legislation was announced in May 2021 and concluded in July 2021.

279. At the time of taking evidence, one of the Committee's key concerns was that any such legislation must introduce an effective "*economic espionage*" offence – something that the UK Intelligence Community suggested could be an important tool in the battle against China. At present, there are no criminal offences covering economic espionage that are not specifically linked to classified research or technology. A new offence might cover companies, research collaborations, joint ventures, seed funding, venture capital and access to academics and students covertly to obtain Information Data and Intellectual Property to secure commercial advantage against the UK.[450]

[444] 'Queen's Speech December 2019: background briefing notes', HMG, December 2019.
[445] Written evidence – HMG, 14 September 2020.
[446] Law Commission Report, *Protection of Official Data*, September 2020.
[447] Oral evidence – NSS, *** October 2020.
[448] Oral evidence – MI5, *** October 2020.
[449] *Global Britain in a competitive age – The Integrated Review of Security, Defence, Development and Foreign Policy,* HMG, March 2021.
[450] Written evidence – HMG, 18 April 2019.

NN. Although we have stated this earlier in this Report, it bears repeating specifically in relation to legislation: the length of time it has taken to reform the Official Secrets Acts is unconscionable. Our predecessors were told that the Acts required updating as a matter of urgency in January 2019. Over three years later, we have yet to see the introduction of a Bill. National security legislation ought to be a priority for any UK Government – it is certainly not a matter to be kicked into the long grass by successive Governments.

OO. We recommend that HMG ensure that a Counter-State Threats Bill is enacted as a matter of urgency.

PART TWO:
CASE STUDIES

CASE STUDY: ACADEMIA

CHINESE INTERFERENCE IN UK ACADEMIA

As we have noted in Part One, the UK is a target for China in its efforts to build global support for its core interests, to mute international criticism and to gain economically. To achieve these aims, China seeks 'political influence' in the UK and 'economic advantage' over the UK. During this Inquiry, we have examined the influence and advantage China seeks through three areas: Academia, Industry and Technology, and Civil Nuclear energy. We explore the threat and response to these three key areas in the subsequent Case Studies, starting with Chinese interference in UK Academia.

280. The UK's academic institutions provide a rich feeding ground for China to achieve both political influence and economic advantage by both:

- controlling the narrative of debate about China within UK universities by exerting influence over institutions, individual UK academics and Chinese students; and
- obtaining Intellectual Property (IP) by directing or stealing UK academic research in order to build, or short-cut to, Chinese expertise.

281. These strands can often overlap, and the UK Intelligence Community assess that it is not always clear which is the driver: "*it is difficult to know if interference is the priority or whether it is a by-product of trying to acquire sensitive material and expertise*".[451]

282. What is clear from our Inquiry is that the academic sector has not received sufficient advice on, or protection from, either.

Influence and interference

283. The External Expert witnesses who gave evidence to the Committee were very clear that Chinese attempts to interfere and stifle debate amongst the academic community in the UK are a significant problem, and they provided us with numerous examples.

284. By contrast, historically, the Intelligence Community considered that, while China had "***" to interfere in UK Academia, there was not a broad evidence base for this[452] – although it is not clear whether this was because the evidence was not there or the Intelligence Community were not looking for it. In June 2019, we were told by the Deputy National Security Adviser (DNSA) that examining the threat from interference to Academia was a "*work in progress*" and that there was not a "*comprehensive understanding of the picture*".[453] However, towards the latter stages of our Inquiry it was recognised that evidence of malign Chinese interference in UK Academia appeared to be growing.

285. Pressure is primarily exerted on institutions, academics and students to prevent engagement with topics that harm the positive narrative presented by the Chinese Communist Party (CCP). This is particularly acute when it involves the so-called 'Five Poisons'

[451] Written evidence – NSS, 31 January 2020.
[452] Written evidence – HMG, 31 May 2019.
[453] Oral evidence – NSS, *** July 2019.

(Taiwanese independence, Tibetan independence, Xinjiang separatists, the Chinese democracy movement and the Falun Gong).

(i) Institutions: Fees and funding

> ***UK universities: Funding from overseas student fees***
>
> UK universities are reliant on income from students in order to operate. A decade ago, university funding comprised 72% public funding, with student fees providing 23%, but this has since been reversed, with student fees now making up 73% of funding.[454] (There are other sources of income available to UK universities – such as residences, catering, investments and endowments – but fees are the most significant revenue stream.[455]) In recent years, the number of 'home' students (who have their fees capped) has remained static whilst the number of overseas students has increased. Figures from February 2021 show that, in 2018/19, international (non-European Union) students accounted for 14% of UK university students, and their fees accounted for 14.4% of the total income of all UK universities.[456]

286. The fees paid by international students account for a large – and increasing – share of university income. The profit universities are able to make from teaching international students helps to fund loss-making activities, such as research.[457] Chinese students make up the largest overseas contingent of students in UK universities. Although estimates vary, it is believed that, in 2019, there were more than 120,000 Chinese students in the UK – more than in the rest of Europe combined. China sends five times as many students to the UK as any other country does. To put it in perspective, reporting in 2020 showed that there were only 27,000 students from India, the next largest source of international students in the UK.[458]

287. In financial terms, it was estimated that, in 2017/18, Chinese students were responsible for generating almost £600m,[459] which makes up a very significant proportion of universities' income. HMG evidence provided in September 2020 noted that the Department for Education (DfE) was working on "*geographically diversifying*" the recruitment of foreign students[460] – presumably to counteract the current over-reliance on income from Chinese students.

288. While the numbers are clearly significant, the question is whether, and if so how, China is actively using this 'buying power' as leverage. An article in *The Times* in 2019 reported that the intelligence Agencies were "*concerned that a reliance on Chinese money and students, particularly postgraduates paying up to £50,000 a year in fees, makes some universities particularly vulnerable* [to influence and interference by the Chinese government]".[461] During this Inquiry, we were told that "*China likely seeks to exert influence*

[454] 'Higher Education funding in England', House of Commons Library, 19 November 2021.
[455] 'Coronavirus: Financial impact on higher education', House of Commons Library, 8 February 2021.
[456] 'Coronavirus: Financial impact on higher education', House of Commons Library, 8 February 2021.
[457] 'Coronavirus: Financial impact on higher education', House of Commons Library, 8 February 2021.
[458] 'Number of international students at UK universities jumps', *Financial Times*, 16 January 2020.
[459] Written evidence – ***, February 2019.
[460] Written evidence – HMG, 14 September 2020.
[461] 'Security Services fear the march on universities of Beijing's spies', *The Times*, 27 October 2019.

over UK universities by threatening to withdraw scholarships or funding for Chinese nationals in the UK"[462] ***.[463]

289. Indeed, in some cases, China does not even have to issue a threat. Professor Steve Tsang (Director of the China Institute at the School of Oriental and African Studies (SOAS)) – who is known for being willing to challenge the CCP's narrative – told the Committee that institutions were actively avoiding taking action themselves for fear of upsetting the Chinese: he had been asked by *** the University of Nottingham not to accept any media requests during the visit of President Xi Jinping to the UK in 2015, for fear of causing offence to the Chinese.[464]

290. In terms of exerting control and influence, China does not just rely on the leverage that its student fees buy it; it also provides direct investment to academic institutions so that it can guarantee input into academic programmes, direct research (discussed later in this Case Study) and ensure that UK students are taught an interpretation of China that reflects the CCP's interests. The latter is primarily conducted through the Confucius Institutes in the UK.

291. There are 29 Confucius Institutes in the UK, with more than 160,000 registered students (not all of whom will be Chinese). They carry out entirely legitimate activities, such as fostering cultural ties and providing language teaching. However, they have also been accused of stifling academic debate about sensitive issues, such as Tibet. Confucius Institutes are run, and part-funded, by the Hanban, an educational organisation that is ultimately controlled by the CCP's Central Propaganda Department – an association that means that comparisons with the British Council or the Institut Français are misleading at best. The Hanban's charter stipulates that Confucius Institutes must obey Chinese law.

292. Confucius Institutes often occupy premises on university campuses free of charge, and some also provide funding to the university with which they are associated, meaning that the line between the institutions can become blurred. For example, it has previously been reported that the Nottingham University School of Contemporary Chinese Studies received money from the university's Confucius Institute to fund core academic activities – thereby giving it influence over who came to speak at the university on Chinese issues.

293. The Intelligence Community assess that Confucius Institutes are utilised by the Chinese government in order to dissuade universities from engaging in debates that the CCP considers to be unsuitable topics. The Joint Intelligence Committee (JIC) Chair told us in October 2020 that the operations of Confucius Institutes were primarily concerning for their role in intimidation:

> *The Confucius Institutes, I would say, are more of an instrument for pursuing that and at one level, if one takes it as a purely cultural issue, one could equate it with the British Council, but of course nothing in China is that simple and they are undoubtedly following a government line.*[465]

[462] Written evidence – ***, *** May 2019.
[463] Written evidence – ***, *** May 2019.
[464] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[465] Oral evidence – JIO, *** October 2020.

(ii) Academics: Threats and inducements

294. China not only seeks influence at an institutional level but will also target individual academics who focus on China, seeking to ensure that they act in the CCP's best interests either through professional inducements or, if that doesn't work, by intimidation.

295. China appears prepared to use levers, such as research funding and travel opportunities, to cultivate relationships with academics, and to encourage them to change their research direction or course content in line with CCP objectives. We heard from the External Experts that this can be very direct – Professor Steve Tsang told us that, within six months of him taking up a new appointment at SOAS, a political counsellor from the Chinese embassy approached him, offering him anything he wanted in an attempt to curry favour: "*It is as blatant as that*."[466]

296. If positive incentives do not work, the Chinese government is willing to apply pressure in other ways. The JIC Chair told us that they were aware of:

> *examples of intimidation, in different ways, sometimes with the Vice Chancellor getting a phone call, sometimes at student body level, to try to discourage universities from allowing speakers on issues like Tibet or Xinjiang.*[467]

Lord Patten told the Foreign Affairs Committee that, when, in the early days of his tenure as Chancellor of the University of Oxford, the Dalai Lama was invited to speak by the university's Buddhist Society, "*within 48 hours I had the then-Chinese ambassador on the phone saying, 'This is a disgraceful insult to the People's Republic of China', and so on*".[468] He refused to intervene. On a different occasion, the Vice Chancellor of the University of Oxford was asked by the Chinese embassy to prevent Lord Patten from visiting Hong Kong; she also refused.[469]

297. Chinese visas are also used as leverage. Professor Tsang stated: "*Research for academics entering China is weaponised. You say something that they don't like, they deny you a visa*."[470] As visas are essential to the academic research of many UK-based China scholars, this makes them a powerful lever that can be used to deter criticism of the CCP and its policies. In October 2020, the Chief of SIS told the Committee:

> *If you are an academic and you are specialising in China, and your entire academic life is focused on China, the threat of not allowing you to travel to the country of your academic* [focus] *is a very powerful threat.*[471]

---

[466] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[467] Oral evidence – JIO, *** October 2020.
[468] 'Security Services fear the march on universities of Beijing's spies', *The Times*, 27 October 2019.
[469] Charles Parton, 'China–UK Relations: Where to Draw the Border Between Influence and Interference', Royal United Services Institute (RUSI), 20 February 2019.
[470] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019. Professor Tsang has himself been denied a visa by China in the past.
[471] Oral evidence – SIS, *** October 2020.

(iii) Students: Monitoring and controlling

298. China also seeks to monitor and control Chinese students' behaviour – primarily via the network of Chinese Students and Scholars Associations (CSSAs). There are reportedly more than 90 CSSAs in the UK, all based at universities, and they are actively supported – and at least partly financed – by the Chinese embassy.[472] The CSSAs ostensibly exist to look after the interests of Chinese students in the UK, organising cultural activities for Chinese and non-Chinese students, and providing practical advice to Chinese students on living and studying in the host country. However, CSSAs are – along with Confucius Institutes – assessed to be used by the Chinese state to monitor Chinese students overseas and to exert influence over their behaviour.[473] Professor Steve Tsang told the Committee:

> *The student bodies are infiltrated ... We know that ... there are meetings that happen through the middle of the night and the following morning some Chinese students can get rung up by somebody at the cultural or education section of the embassy to ask them: why did you say that? Why did you do that?*[474]

299. This would appear to be resulting in a culture of fear and suspicion among Chinese students in the UK. According to Professor Tsang, "*we are seeing that ... in the class where there is only one Chinese student, that Chinese student usually engages in discussions and debates much more openly than in a class that has quite a few Chinese,* [where] *they don't know who* [if anyone] *is going to report on them*".[475] The protests in Hong Kong, and subsequent demonstrations in support of the protesters by some ethnic Chinese students in the UK, have brought to the fore the pressure exerted on Chinese students in the UK by the Chinese embassy and CSSAs.

300. Examples of such behaviour have been reported throughout the Western world over the past decade, but awareness of the issue has increased in recent years. The perception that the Chinese government is interfering with academic freedom across the world – including through surveillance of its own students overseas via Confucius Institutes, CSSAs and other means – is such that, in 2019, the non-governmental organisation (NGO) Human Rights Watch issued a Code of Conduct to help universities protect themselves against Chinese academic interference; the Code called for the rejection of Confucius Institutes and restrictions on CSSAs.[476]

---

[472] 'Authoritarian Advance: Responding to China's Growing Political Influence in Europe', Benner et al, Global Public Policy Institute, February 2018.
[473] Written evidence – ***, *** May 2019.
[474] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[475] Oral evidence – Professor Steve Tsang (SOAS), 9 May 2019.
[476] 'China: Government Threats to Academic Freedom Abroad', Human Rights Watch, 21 March 2019.

Pressures on Chinese students in the UK

- In November 2019, a Chinese student was photographed in Edinburgh with a sign supporting Hong Kong citizens' demands for free elections. The following day, he was secretly photographed at Edinburgh Airport while escorting his mother to her flight. Both pictures were circulated on Weibo, the Chinese social media site, by someone who believed he was returning to Chengdu, his hometown. The post – entitled 'Brothers from Chengdu, beat him to death' – contained the flight number and a call for him to be arrested by police or assaulted by citizens. It was shared 10,000 times.[477]
- In November 2019, it was reported that the Glasgow CSSA – which acknowledges that "*the Chinese embassy is one of the sponsors of our events*" – had promoted 'flash mobs' to confront Hong Kong demonstrations. One Hong Kong student who had attended protests in Edinburgh said that "*there is Chinese embassy involvement in these demonstrations … They surrounded us in a circle, waving Chinese flags, singing the national anthem and being threatening and hostile*." A spokesman for the Chinese consulate in Edinburgh told *The Times*: "*It is totally justifiable and understandable for Chinese students to express their indignation and opposition to words and actions that attempt to split the nation and smear China's image*."[478]
- A Hong Kong student at the University of Sheffield reported that he and his friends were surrounded by mainland Chinese students when they were handing out pro-democracy leaflets: "*A glass was thrown at one of my friends and one of our flags was broken … We were terrified. In Sheffield there are nearly 4,000 Chinese students and only a few hundred Hong Kong students … It's the fear of what they might do that scares us. We are sure we will be on watch lists when we go home*."[479] On another occasion, a film screening by Hong Kong students at Aston University, in Birmingham, was interrupted by mainland Chinese students who attempted to video those attending.[480]

(iv) Think tanks: Intimidation and coercion

301. In addition to mainstream Academia, China will also seek to influence think tanks and NGOs in the UK – again with the aim of influencing research agendas, making policy recommendations and influencing the narrative on China.[481] MI5 observed that:

> *think tanks that people are inserting themselves into, or think tanks which are essentially just ***, that is a methodology that we've seen since time immemorial and we certainly see it nowadays, and ***. So there are bits of the think tank activity that go on that we*

[477] 'Hong Kong crisis: Beat Edinburgh University student to death, Chinese students told', *The Times*, 26 November 2019.
[478] 'Beijing is backing attacks against us, say Hong Kong students in Scotland', *The Times*, 28 November 2019.
[479] 'Security Services fear the march on universities of Beijing's spies', *The Times*, 27 October 2019.
[480] 'Security Services fear the march on universities of Beijing's spies', *The Times*, 27 October 2019.
[481] We note that MI5 issued an espionage alert on an individual working in think tanks and Academia who was in regular contact with Chinese intelligence officers. ('Joint Address by MI5 and FBI Heads', www.mi5.gov.uk/news/speech-by-mi5-and-fbi, 6 July 2022.)

don't judge are causing deep damage … there are other cases where we think there is more concerning activity taking place ***.[482]

302. Engagement with think tanks in order to promote a particular view of the world is not unusual behaviour and would not generally reach the threshold for 'interference'. However, Chinese tactics extend to intimidation and coercion. For example, we were told that staff from at least one European think tank focusing on China are frequently followed by Chinese officials, and others have experienced difficulties obtaining Chinese visas.[483] Charles Parton, Senior Associate Fellow at the Royal United Services Institute (RUSI) told the Committee about one employee who "*knows if she wishes to return to China, temporarily or when she retires, she cannot say things that go against the Party, and she has told me, 'I have to clear things with my protector back in Beijing' … that is the way the Party forces* [ethnic Chinese academics] *to act*".[484]

PP. The UK's academic institutions provide a rich feeding ground for China to achieve political influence in the UK and economic advantage over the UK. China exerts influence over institutions, individual UK academics and Chinese students in order to control the narrative of debate about China – including through the use of Confucius Institutes in the UK – and it directs or steals UK academic research to obtain Intellectual Property in order to build, or short-cut to, Chinese expertise. However, the academic sector has not received sufficient advice on, or protection from, either.

QQ. In seeking political influence, there are obvious and repeated examples of Chinese attempts to interfere and stifle debate amongst the academic community in the UK. Universities are reliant on student fees, and the vast number of Chinese students in the UK – it is striking that there are more than five times the number than for any other country – provides China with significant leverage, which it is not afraid to exert. Yet the Government had shown very little interest in warnings from Academia: at the time of drafting, there was no point of contact in the Government for those in the sector to seek advice on these issues.

Economic advantage

303. In addition to influence and interference, Academia also provides China with a means of securing economic advantage over the UK. This can be overt – directing academic research for its own ends domestically, whether in an economic sense or militarily. It can also be covert – using collaborative projects to steal information and IP. In both respects, Academia is an 'easy option' since the information may be less protected than it might be in the private sector or in the Ministry of Defence, for example. Academic institutions often conduct research on behalf of UK Industry, and we were told that they can be more vulnerable than their Industry counterparts due to a combination of greater need for funding ***.[485]

[482] Oral evidence – MI5, *** December 2019.
[483] Written evidence – ***, *** May 2019.
[484] Oral evidence – Charles Parton (RUSI), 9 May 2019.
[485] Written evidence ***, February 2019.

(i) Using academia to steal Intellectual Property

304. China's theft of IP has often been cited as one of the reasons for its significant growth in technological expertise and market share. In July 2019, the Chief Executive Officer of the National Cyber Security Centre (NCSC) told us:

> *In our role trying to defend the UK from cyber-attacks, China's ambitions to steal IP is one of the principal things that we worry about. When we analyse how that whole attack ecosystem works … it's about China … using whatever means they can to attack a range of western organisations for their valuable Intellectual Property and then find use* [of that IP] *to China.*[486]

305. As such, it is clear that China's pursuit of key emerging technologies poses an increasing threat to UK Itellectual Property, including via UK universities and research institutions. The vast number of Chinese students – particularly post-graduates – in academic institutions in the UK that are involved in cutting-edge research must therefore raise concerns in this respect given the access and opportunities it affords them.

306. The United States (US) has already recognised this threat and has very publicly taken action to counter it. In 2020, then-President Trump issued a Presidential Proclamation[487] imposing additional entry requirements on post-graduate Chinese students with a demonstrable link to the CCP for study in the US. The Presidential Proclamation notes:

> *The PRC* [People's Republic of China] *authorities use some Chinese students, mostly post-graduate students and post-doctorate researchers, to operate as non-traditional collectors of intellectual property. Thus, students or researchers from the PRC studying or researching beyond the undergraduate level who are or have been associated with the PLA* [People's Liberation Army] *are at high risk of being exploited or co-opted by the PRC authorities and provide particular cause for concern.*[488]

The Presidential Proclamation led to the US Department of State revoking many existing visas for Chinese students and denying other visas to prospective Chinese students. At the time of writing, the Proclamation remains in force under the Biden Administration – meaning the new Administration also recognises the enduring threat posed by Chinese students.

307. With US Academia becoming an increasingly hard target for Chinese students, it is likely that more Chinese students will seek to study at UK academic institutions – meaning that UK IP and information is increasingly vulnerable. This concern is supported by public research. According to the Australian Strategic Policy Institute, the People's Liberation Army has sent approximately 500 military scientists to UK academic institutions in the period 2007–2017.[489] The author of the document suggested that the UK is a primary destination for Chinese military scientists studying abroad.[490] In some cases, these students

[486] Oral evidence – NCSC, *** July 2019.
[487] US Presidential Proclamation 10043 of May 29, 2020.
[488] 'Suspension of Entry as Non-immigrants of Certain Students and Researchers From the People's Republic of China', Federal Register, 4 June 2020.
[489] 'Picking flowers, making honey – The Chinese military's collaboration with foreign universities', Australian Strategic Policy Institute, 26 October 2018.
[490] 'China: A New World Order – Episode 3: IP Theft', BBC, 12 September 2019.

obscure their military affiliations, including through the use of misleading historical names for their institutions or even the use of non-existent institutions.[491] A document published by the leading Chinese defence university, the National University of Defence Technology, advises students that military and political courses can be excluded from their academic records when applying to foreign institutions.[492] Once established in academic institutions, these students are in a position to identify and exfiltrate valuable Information Data and IP back to China.

308. In addition to using students to steal information and IP, China also utilises so-called 'Talent Programmes'. Originally, these programmes were established to attract Chinese research scientists back to China; however, they now recruit Western scientists as well. For instance, the 'Thousand Talents' Programme is made up of a number of schemes that are aimed both at Chinese scientists working abroad, and at foreign scientists, offering very significant remuneration and research budgets to work and/or teach in China.

309. These programmes are established by the Chinese state and aim to transfer Information Data and IP from the participants to Chinese research entities or government agencies. This is not necessarily illegal and is done overtly – however, it is noteworthy that, in the US, researchers are obliged to disclose funding from foreign governments when applying for government grants. In 2018, Texas Tech University warned its staff that recipients of 'Thousand Talents' grants could, in future, be barred from working on research funded by the US Department of Defense or by federal research grants. The US Congress was told by the Federal Bureau of Investigation (FBI) in December 2018 that such programmes "*encourage theft of intellectual property from US institutions*".[493] No such action appears to have been taken in the UK to prevent IP and information being transferred out of the UK, either through 'Talent Programmes' or more generally.

Case study: Chinese Talent Programmes

China operates a number of Party- and state-sponsored Talent Programmes to recruit researchers (both Chinese and non-Chinese nationals), who are then incentivised to steal foreign technologies needed to advance China's national, military and economic goals.[494] Participants in Chinese Talent Programmes have been known to go on to register patents in China on behalf of the Chinese government[495] – yet these have been based on research funded by foreign governments. China benefits from this Intellectual Property and associated royalties, at the cost of others.

In one specific case ***.[496]

[491] 'Picking flowers, making honey – The Chinese military's collaboration with foreign universities', Australian Strategic Policy Institute, 26 October 2018.
[492] 'Picking flowers, making honey – The Chinese military's collaboration with foreign universities', Australian Strategic Policy Institute, 26 October 2018.
[493] 'China hushes up scheme to recruit overseas scientists', *Financial Times*, 10 January 2019.
[494] 'The China Threat: Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage', FBI website, accessed 26 April 2023.
[495] 'Threats to the US Research Enterprise: China's Talent Recruitment Plans', US Senate Permanent Subcommittee on Investigations, 18 November 2019.
[496] Written evidence – HMG, 18 April 2019.

Chinese Talent Programme participants have pleaded guilty or have been convicted of offences, including economic espionage and theft of trade secrets, export-control law violations, and grant and tax fraud.

(ii) Using UK research to support Chinese interests

310. While the potential theft of IP may have received the most headlines, China's overt use of UK Academia provides it with just as much of an opportunity to gain an economic advantage over the UK. China directs, funds and collaborates on research – in particular that which might benefit the Chinese military.

311. The risks of this can most clearly be seen in respect of dual-use technologies – defined as "*goods, software, technology, documents and diagrams which can be used for both civil and military applications*".[497] One of the problems with this is that the potential military use of dual-use technologies is not always apparent at the beginning of the research project and therefore the initial research is often unclassified. In this way, research on technological innovations – which might later be seen to have a clear military use, and perhaps offer a decisive military advantage – can be readily available via academic engagement.[498]

312. On the issue of diversion of UK–China joint research for military use, we were told that basic research is often open to collaboration, and individual academics and research groups ***. Universities themselves may intend to commercialise IP, but increasingly need Chinese financial support. Moreover, transfer of tangible or intangible goods to China only requires an export licence if they are in the Control List, or where there are specific concerns about military or Weapons of Mass Destruction end use. Emerging technologies without established military use are often not covered. ***.[499]

313. It appears highly likely therefore that collaboration on joint UK–China research projects is being exploited for military use ***. HMG noted that research related to engineering or physical sciences was most likely to have a defence use (and therefore was at greatest risk). ***.[500]

Case study: University of Manchester's National Graphene Institute

Shortly after President Xi Jinping visited the University of Manchester in 2015, the university's National Graphene Institute was involved in a five-year collaborative research project with the Aero Engine Corporation of China's Beijing Institute of Aeronautical Materials (BIAM). In a press release, the university stated that this partnership would "*accelerate the application of graphene in the aviation industry and other sectors*".[501]

[497] www.gov.uk/guidance/controls-on-dual-use-goods
[498] Written evidence – HMG, 18 April 2019.
[499] Written evidence – HMG, 10 December 2019.
[500] Written evidence – HMG, 10 December 2019.
[501] 'Graphene partnership could deliver next generation of aircraft', press release by the University of Manchester, 7 December 2015.

However, concerns have been raised that this collaboration could be used to develop China's military capabilities. A 2021 Civitas report into Chinese military exploitation of scientific research at UK universities highlighted this collaboration between BIAM and the University of Manchester. The report noted that BIAM was working in parallel to develop graphene for a range of uses, and that Chinese reports suggested that China's Z-10 attack helicopter had been equipped with graphene armour that may have been developed at BIAM.[502]

The University of Manchester has also acknowledged the potential dual-use of research jointly with other Chinese universities – for instance, collaboration between researchers at the University of Manchester and at Central South University China led to the creation of a new kind of ceramic coating that could "*revolutionise hypersonic travel for air, space and defence purposes*".[503]

***.[504]

It appears that any collaboration between a UK research institution and a Chinese institution will very probably be used to benefit China's military. By way of example, the case of Huang Xianjun was publicised by the Australian Strategic Policy Institute.[505] After completing his PhD at the University of Manchester, working with the discoverers of graphene, Huang is now a researcher at China's National University of Defence Technology, working on key defence projects for the People's Liberation Army. ***.[506]

314. There is a question as to whether academic institutions are sufficiently alive to this threat – particularly given that academic institutions will often accept the transfer of Information Data and IP as a condition of funding.[507] The JIC Chair told the Committee in October 2020 that the Intelligence Community have significant concerns about research partnerships where universities may "*unwisely not recognise who they are actually dealing with and the sensitivity of information which may be being transferred as a result*".[508]

315. Some universities clearly are aware of the threat posed by collaboration: the University of Cambridge has expressed concern that its science and technology research projects are being exposed to espionage via the university's collaborative projects with, and investment from, Huawei.[509] They are particularly concerned about exposing 'high-risk' projects that require additional layers of vetting – for example, research collaboration with Rolls-Royce on aerospace technology.

[502] 'Inadvertently arming China? The Chinese military complex and its potential exploitation of scientific research at UK universities', Civitas, February 2021.
[503] 'Chances of hypersonic travel heat up with new materials discovery', press release by the University of Manchester, 6 July 2017.
[504] Written evidence – HMG, 18 April 2019.
[505] 'How the West's research aids China's military', Australian Strategic Policy Institute, 30 October 2018.
[506] Written evidence – GCHQ, 31 July 2019.
[507] Written evidence – HMG, 18 April 2019.
[508] Oral evidence – JIO, *** October 2020.
[509] Written evidence – HMG, 18 April 2019.

316. However, other universities seem to be turning a blind eye to the risk: for example, the University of Surrey received a £7.5m 'donation' to its 5G/6G Innovation Centre from Huawei – which it described as a 'key partner' that the university would continue to do research with "*unless there were clear and compelling reasons not to do so*".[510]

RR. In its quest for economic advantage, China often acts in plain sight – directing, funding and collaborating on academic research for its own ends. In particular, it seeks to benefit the Chinese military through research on dual-use technologies, which is often unclassified in its early stages. There is a question as to whether academic institutions are alive to the threat posed by such collaboration, particularly given that they often accept transfer of Information Data and Intellectual Property as a condition of funding. While some have expressed concern, others seem to be turning a blind eye, happy simply to take the money.

SS. The UK Government must ensure that transparency around the source of foreign donations to Higher Education institutions is improved: a public register of donations must be created by the Department for Education and monitored by the State Threats Unit in the Home Office.

TT. Academia is also an 'easy option' when it comes to the theft of Intellectual Property, by taking advantage of collaborative projects to steal information which is less protected than it might be in the private sector or the Ministry of Defence, for example. The vast number of Chinese students – particularly post-graduates – in academic institutions in the UK that are involved in cutting-edge research must therefore raise concerns, given the access and opportunities they are afforded.

[510] 'UK Universities to stick with Huawei despite Oxford University's decision to suspend funding', CityAM.com, 18 January 2019.

Who: Taking responsibility for tackling influence and interference

317. In 2019, the External Expert witnesses we spoke to told the Committee that the Government had shown very little interest in their warnings that China was actively attempting to influence and utilise Academia in the UK for its own purposes: Lord Patten noted that there was not even a point of contact in the Government for advice on these issues.

318. HMG appears now to recognise that Chinese engagement with the UK's academic sector – while yielding many benefits – is not without risk. The Foreign, Commonwealth and Development Office noted in 2020:

> *in the UK we are aware of cases such as autocratic state actors putting pressure on universities and academics to avoid certain topics or self-censor their research or course content. There are also reports of pressure or influence exerted on overseas students. We are also aware of autocratic state actors targeting research collaboration.*[511]

However, as in so many areas, the devolution of responsibility for security to policy departments means that the security aspects are being lost. In July 2019, the DNSA and Senior Responsible Owner for China told us that "*the Department for Education and BEIS* [the Department for Business, Energy and Industrial Strategy] *are the ones who we have tasked to be the lead government departments to understand the threat from influence and interference in the academic sector*".[512] However, in December 2020, 18 months later, the DNSA told the Committee:

> *we need DfE* [the Department for Education] *to be able to understand that agenda, to have a high level of awareness of the risks of the potential of intelligence and a covert capability to support them in that.*[513]

319. It appears therefore that the policy departments still do not have the understanding needed. This problem can be seen by the lack of engagement we have received during this Inquiry from DfE and the (then) Department for Business, Energy and Industrial Strategy (BEIS). In April 2021, we contacted both departments to request information on issues on which they are the 'lead' departments. At the time of writing, we were still waiting to receive a response from DfE – despite having chased this request with the Secretary of State's office. No explanation has been provided for the department's failure to engage with this Inquiry. This is particularly concerning when DfE is supposed to play a pivotal role in countering nefarious Chinese activity in academic institutions.

320. BEIS did respond to our requests – only to refuse them outright. The department refused to provide any information to the Committee, citing commercial sensitivities and

[511] 'A cautious embrace: defending democracy in an age of autocracies: Government Response to the Committee's Second Report of Session 2019, First Special Report of Session 2019–21', House of Commons Foreign Affairs Committee, 17 February 2020.
[512] Oral evidence – NSS, *** July 2019.
[513] Oral evidence – NSS, *** December 2020.

the fact that it provides its information to the BEIS Select Committee[514] and to the Science and Technology Committee. We also note that its response was provided on an email system accredited only to 'Official-Sensitive', yet it referenced information in our more highly classified communication. We are worried that a department charged with security matters would make such a basic error. The BEIS Select Committee may wish to assure itself as to the security processes in place with the department to avoid such errors.

321. We have previously addressed the lack of oversight resulting from the Fusion Doctrine.[515] The responses from DfE and BEIS in relation to our Inquiry into China – one of the key national security threats facing the UK – are clear examples of the unacceptable nature of the current system, both in terms of the failure of policy departments to be alert to security matters and to take responsibility for tackling them, and the lack of effective oversight if this Committee is not formally given a remit in this area.

How: Taking action on influence and interference

322. In terms of tackling Chinese influence over, and interference in, many of our academic institutions, while the dawning recognition that there is a problem is welcome, the Committee has still not seen any detail as to what action is planned to tackle it – which reinforces our concern that policy departments are not taking it sufficiently seriously.[516]

323. In the evidence received, the only step that was pointed to was the championing of the importance of freedom of speech and academic freedom in our academic institutions, which, as the (then) Universities Minister noted, "*are a huge part of what makes our higher education system so well-respected around the world*".[517] The UK Government says that, in order to protect free speech, it has worked with Universities UK on guidelines that provided advice on a wide range of national security issues, including the protection of values (this guidance is discussed further below). In addition, the Higher Education (Freedom of Speech) Bill was introduced in the House of Commons in May 2021 and is making progress. At the time of writing, it was still at Report stage in the House of Commons.

324. Nevertheless, the scant response from the Government demonstrates there is still a long way to go before we can stem the tide of Chinese political influence in UK academic institutions bought by Chinese money – money that China uses to control and validate its own political narrative and to shut down criticism. The introduction of the Government's Higher Education (Freedom of Speech) Bill is not – in and of itself – going to solve this systemic problem.

What: Understanding the threat from theft and subversion

325. As at 2021, HMG still seemed to be at the stage of trying to understand the threat from Chinese students stealing IP from UK Academia, or the Chinese subverting UK research to

[514] Now the Business and Trade Committee, as of 26 April 2023.
[515] The Government's Fusion Doctrine aims "*to deploy security, economic and influence capabilities to protect, promote and project our national security, economic and influence goals*". (HMG, National Security Capability Review, March 2018.)
[516] Written evidence – HMG, 14 September 2020.
[517] 'Universities to comply with free speech duties or face sanction', Department for Education, Office for Students, 12 May 2021.

its own ends, at the most basic level – i.e. what it is they are trying to steal. There was still no comprehensive list of the areas of UK research that need protecting from China.

326. The broad areas would appear to be self-evident – those which the Chinese have themselves identified – as the NCSC told the Committee in 2019:

> *if you look at 'Made in China 2025', there are a set of technologies in there that the Chinese wish to dominate where currently the vast majority of academic research is in the UK.*[518]

Yet, in October 2020, the Acting National Security Adviser (NSA) and GCHQ suggested that work was still being done by the Government to identify these areas of sensitivity – or at least to agree a comprehensive list amongst departments. The Acting NSA told the Committee: "*We are looking at what more we can do ***, so that we can be clear about where we think the areas of greatest sensitivity are for research.*" [519]

327. Director GCHQ clearly recognised this lack of clarity and the need for action:

> *we don't have a joined-up view on the things that we most need to protect ***. So, you know, a particular area of technology that the UK might find or think is very important, linking that to where we are academically the most strong, linking that to how we encourage inward investment, including in research, and then linking that back to our knowledge and understanding of ***, it has to be a whole of system approach and I can see some real positive developments in that, but we are coming from a situation where Chinese involvement at student level and investment level has been welcomed for a number of years ***.*[520]

UU. At present, HMG still seems to be trying to understand the threat from Chinese students stealing Intellectual Property from UK Academia, or the Chinese subverting UK research to its own ends, at the most basic level – i.e. what it is they are trying to steal. There is still no comprehensive list of the areas of sensitive UK research that need protecting from China. Identifying these key areas of research must be a priority, and they must be communicated to Academia as a matter of urgency so that protective action can be taken. Unless and until this is done, then the UK is handing China a clear economic advantage over the UK, and indeed the rest of the world.

How: Taking action on economic advantage

328. In terms of tackling the manipulation of Academia for economic advantage, we were told that the Government was now talking to Academia about the threat. Director GCHQ noted in July 2019 that part of the reason for its new Manchester office "*is because of the preponderance of big academic institutions that need to get closer proximity to some of our advice*".[521] NCSC later noted that it was now "*talking to those universities to say, as a priority, to make sure that they understand what the risks are*".[522] In May 2021, a new

[518] Oral evidence – NCSC, *** July 2019.
[519] Oral evidence – HMG, *** October 2020.
[520] Oral evidence – GCHQ, *** October 2020.
[521] Oral evidence – GCHQ, *** July 2019.
[522] Oral evidence – NCSC, *** July 2019.

Research Collaboration Advice Team was established within the (then) Department for Business, Energy and Industrial Strategy to "*promote government advice on security-related topics, such as export controls, cyber security, and protection of intellectual property*".[523]

329. In December 2020, the DNSA noted the close relationship between the Government and Universities UK in the dissemination of advice to the sector.[524] Universities UK published its guide 'Managing Risks in Internationalisation: Security Related Issues' in October 2020, which drew heavily on resources from the Centre for the Protection of National Infrastructure and NCSC. The guide was designed to be used in conjunction with Project DERWENT[525] – which aims to deliver greater awareness and protective security advice around the threat from Hostile State Activity to UK research and innovation – and provides advice on the protection of reputation and values, people, campuses and partnerships.[526]

Project DERWENT/Trusted Research

Project DERWENT aims to deliver greater awareness and protective security advice around the threat from Hostile State Activity (HSA) to UK research and innovation, particularly presented by joint research ventures and academic collaboration. The work aligns with the Cabinet Office-led 'Trading Safely' pillar.

Objectives

- To increase understanding and awareness of the threat from HSA to research and innovation posed by academic collaboration and joint research ventures.
- To jointly (between the Centre for the Protection of National Infrastructure and the National Cyber Security Centre) develop a package of proportionate protective security measures to make the UK's cutting-edge research and innovation a harder target for HSA.
- To identify and deploy levers which encourage good security behaviour within the sector.
- To enable government departments and other organisations to disseminate advice and guidance products to the sector.

The Government's approach will focus on the departments and private sector organisations that fund and set the strategic direction for research and innovation, in order to influence

[523] 'Dedicated government team to protect researchers' work from hostile activity', GOV.UK, 25 May 2021, www.gov.uk/government/news/dedicated-government-team-to-protect-researchers-work-from-hostile-activity
[524] Oral evidence, NSS – *** December 2020.
[525] In some instances in this Report, we have substituted an ISC-specific code word where it has been necessary to refer to the name of an operation or project, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to real operation names. The ISC code words have no operational significance.
[526] 'Managing Risks in Internationalisation: Security Related Issues', Universities UK, 15 October 2020, www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing-risks-in-internationalisation.pdf

and inform the sector. This approach is also driven by an understanding that the threat message is likely to be better received by those involved with research and innovation if it is delivered through a variety of routes, including those responsible for sponsorship, funding and strategic direction.

Project DERWENT also aims to engage directly with Academia to develop protective security guidance and threat briefings, which are tailored for the sector. Given the broad range of academic relationships, the project aims to deliver a core script, in order to ensure a consistent message from those who engage with organisations involved in research and innovation.[527]

330. While Project DERWENT certainly has worthy aims, we nevertheless must come back to the fact that, from the evidence given to this Inquiry, HMG is still not clear which areas of research and collaboration it is trying to protect from China. That, surely, must be the first step, to communicate to academic institutions a comprehensive list of the areas of greatest research sensitivity. Unless, and until, this is done, then China is able to direct and collaborate on – unfettered – research that provides it with an economic advantage.

331. Furthermore, it is clear that, even if the areas could be agreed upon, the Intelligence Community acknowledge that the Government has little leverage in this area to prevent Chinese research or collaboration. In July 2019, NCSC told the Committee:

> *at the moment Government has no way of stopping a university collaborating with a Chinese Professor or a Chinese company.*[528]

This was echoed in December 2020 by the DNSA, who noted that engagement with Academia could be challenging, given that it "*highly prizes its independence*".[529]

332. Perhaps the only area that is ahead of this rather bleak picture is those academic posts ***. These posts are subject to more stringent vetting controls than other posts.[530] In 2019, DI told the Committee that it was undertaking a programme of work to *** university degree courses that could potentially be utilised for Weapons of Mass Destruction programmes.[531] The Academic Technology Approval Scheme, which students had to apply to in advance of starting such courses, has now been expanded to cover courses which could potentially be utilised for developing Advanced Conventional Military Technology.[532]

[527] Written evidence – ***, CPNI and NCSC.
[528] Oral evidence – NCSC, *** July 2019.
[529] Oral evidence – NSS, *** December 2020.
[530] Written evidence – HMG, 18 April 2019.
[531] Written evidence – DI, 31 July 2019.
[532] Oral evidence – DI, *** October 2020; GOV.UK guidance on the Academic Technology Approval Scheme (accessed 20 October 2020).

The Academic Technology Approval Scheme

The UK has not explicitly banned any Chinese students or researchers from applying to its academic or research institutions. However, since 2007, the UK has operated the Academic Technology Approval Scheme (ATAS) to "*address transfers of sensitive knowledge through postgraduate study*".[533] ATAS certificates may be issued to prospective post-graduate students and researchers after an assessment of their previous publications and studies, previous employment, arrangements for funding, declarations by referees and vetting of their personal details.[534]

The scheme was originally designed to protect the transfer of knowledge that could be used to construct or deploy Weapons of Mass Destruction. The scheme was broadened to include Advanced Conventional Military Technology in September 2020, and to "*cover researchers with access to proliferation sensitive information in universities and research institutes*" in May 2021.

While we were informed that the latter change was "*not a China specific measure and relates solely to research*",[535] the initial change was widely reported to be in response to concerns over Chinese nationals.[536] Indeed, the Chief of Defence Intelligence (CDI) told the Committee in December 2020 that the September 2020 change had been informed by the results of a June 2019 pilot, which demonstrated the disproportionate scale of the threat posed by Chinese students. Of the students examined under the pilot, *** of those refused had been Chinese (the other *** were from "*the rest of the world*", so a wide geographical spread). CDI explained that the pilot had refused *** out of the *** Chinese students who had been looked at, meaning that ***% of those Chinese students who had had their activity examined had been refused.

He told the Committee:

> *that pilot showed the scale of the problem and therefore the* [changes] *that have been brought in since October now give us the opportunity to be more rigorous in our approach around ATAS, both in terms of its scope so it's more than just Weapons of Mass Destruction and associated technology, it now includes advanced conventional weapons ...* ***.[537]

[533] 'Student Vetting: The UK's Academic Technology Approval Scheme', Foreign, Commonwealth and Development Office, February 2015.
[534] 'Guidance on how to apply for an ATAS certificate', Foreign, Commonwealth and Development Office, 14 May 2021.
[535] Written evidence – HMG, 2 February 2021.
[536] 'Chinese students face ban amid security fears', *The Times*, 1 October 2020.
[537] Oral evidence – DI, *** December 2020.

VV. Unlike other countries, such as the United States (US), the UK has taken no preventative action. This is particularly concerning, as US restrictions on Chinese students will make UK institutions more attractive to those seeking to gain Intellectual Property and expertise. The Research Collaboration Advice Team should submit a quarterly report on the progress and outcomes of its work to the State Threats Unit in the Home Office to ensure there is cross-government awareness of the scale of the issue.

WW. It is clear that the Academic Technology Approval Scheme (ATAS) is an effective tool. Once the Government has identified the sensitive areas of research that need protecting from China, consideration should be given to ensuring that ATAS certificates are required for foreign nationals undertaking post-graduate study in UK institutions in those areas. Furthermore, we recommend that ATAS be expanded to cover post-graduate doctoral study.

XX. Tackling the threat in relation to Academia could have been an example of the Fusion Doctrine working seamlessly – with each policy department clearly contributing to an overall goal. But, as in so many areas, the devolution of responsibility for security to policy departments means that the ball is being dropped on security. Policy departments still do not have the understanding needed and have no plan to tackle it.

YY. This must change: there must be an effective cross-government approach to Academia, with clear responsibility and accountability for countering this multi-faceted threat. In the meantime, China is on hand to collect – and exploit – all that the UK's best and brightest achieve as the UK knowingly lets it fall between the cracks.

CASE STUDY: INDUSTRY AND TECHNOLOGY

CHINA'S APPROACH TO TECHNOLOGY

333. As made clear in Part One of our Report, China's national imperative is the continuing dominance and governance of the Chinese Communist Party (CCP). However, it is its ambition at a global level – to become a technological and economic superpower, on which other countries are reliant – that represents the greatest risk to the UK.

334. Today, China has advanced research, development and manufacturing capabilities across a broad range of high-tech sectors, from nuclear energy to telecommunications. But, in order to understand China's approach to technology today, you have to look to the past: China's ambition to be a global technological and economic superpower is rooted in its history. China's perception that the Chinese nation – one of the world's great civilisations – was humiliated repeatedly by more technologically advanced Western nations prior to the CCP takeover in 1949 is key to understanding why economic and technological development is central to China's ambitions today. The Intelligence Community, in evidence to the Committee, were unambiguous about the importance China places on this:

> *The Communist Party of China (CCP) deems both economic well-being and technological advancement as essential to its national security and maintaining power, and to mitigate perceived threats from the West … China's overall aims are to gain technological parity with the West, and eventually to surpass them, in a process it identifies as 'national rejuvenation'.*[538]

335. China is seeking technological dominance over the West, particularly in emerging technologies, such as artificial intelligence (AI), 5G telecommunications, supercomputing and quantum computing. An assessment by the National Cyber Security Centre (NCSC) summarised the thinking as:

> *Modern great-power dominance has been based on the mastery of key technologies. China is investing huge sums in a series of 'Manhattan Projects',*[539] *intended to make it a leader in advanced technologies, which it almost certainly intends to export worldwide.*
>
> *Success will enable China to project its economic, military and political power globally, as steam and computing did for Britain and the US* [United States] *respectively in the 19th and 20th centuries.*[540]

[538] Written evidence – HMG, 18 April 2019. JIO subsequently advised that 'national rejuvenation' is in fact a set of broad strategic goals which go wider than technological advantage.
[539] The Manhattan Project was the name for the pioneering US project to develop – with support from the UK and Canada – the first nuclear weapon. It began during the Second World War and continued until 1947.
[540] Written evidence – NCSC, provided 27 October 2020.

336. China has underpinned its economic and technological aspirations with a number of strategic documents, including the 'Made in China 2025' strategy. This strategy lists the ten key industrial sectors in which the CCP intends China to become a world leader – many of which are fields in which the UK has particular expertise:

- electric cars and other new energy vehicles;
- next-generation Information Technology (IT) and telecommunications;
- advanced robotics and AI;
- agricultural technology;
- aerospace engineering;
- new synthetic materials;
- advanced electrical equipment;
- emerging biomedicine;
- high-end rail infrastructure; and
- high-tech maritime engineering.[541]

337. China is willing to employ a 'whole-of-state' approach, using all levers of Chinese state power to support its technological goals. This includes legitimate routes – using influence via investment, directing the huge resources of the Chinese state into vast research and development programmes, and investing in high-tech overseas companies with a view to transferring legally the technology to China and undercutting Western competitors. It also includes espionage on an industrial scale – stealing the fruits of Western research and development efforts and high-value Intellectual Property (IP) so that it can develop and manufacture technologies faster and cheaper than the rest of the world. As the NCSC explained, China can "*shortcut* [its] *need to do research and development by targeting Intellectual Property*".[542] MI5 was equally clear, telling the Committee that China is using "*intelligence collection … to support* [its] *commercial mercantile ambition*".[543]

338. In 2019, when the Intelligence and Security Committee of Parliament issued a statement on the inclusion of Huawei in the UK's 5G network, we warned that the problem was far bigger than that single issue: the West is over-reliant on Chinese technology and must act now to tackle China's technological dominance.[544] The same month that our statement was released, the Intelligence Community accepted that China's rising technological dominance posed a genuine threat to the West, with SIS telling the Committee that "*the biggest risk from China is that the alliance of state control and 21st century technology will allow China to dominate technologies that shape our world*".[545] This is a long-term issue, and one on which we are already lagging well behind. As MI5 told us:

[541] 'Is "Made in China 2025" a threat to Global Trade?', Council on Foreign Relations, 13 May 2019.
[542] Oral evidence – NCSC, *** October 2020.
[543] Oral evidence – MI5, *** October 2020.
[544] 'ISC statement on 5G suppliers', Intelligence and Security Committee of Parliament, 19 July 2019.
[545] Oral evidence – SIS, *** July 2019.

> *the challenge of the rise of China absolutely raises huge questions for the future of the western alliance … At the moment, it is still the case that, broadly speaking, the Chinese are seeking to use espionage and influence to steal advantage that the West itself still holds, and then clearly the balance of that will tilt across the next few years and China will become – has already, in effect, become – the world's leader in many areas of manufacturing, and may become the world's leader in almost all the world's areas of manufacturing.*[546]

339. We asked the NCSC about the threats to the UK from China and were told that 'Made in China 2025' is a "*classic Chinese long-term programme with the most profound implications for us and our allies*".[547] If China achieves technological dominance, it will make it harder for the UK to protect its information and retain defence, economic and intelligence advantages. A 2018 Joint Intelligence Committee (JIC) Assessment noted that China is the main hostile state threat to UK prosperity.[548] The actions of China against UK Industry therefore pose both a threat to national security and a threat to our economic well-being.

National security concerns over Chinese dominance in technology

Artificial intelligence: HMG cites artificial intelligence (AI) as an area where increasing Chinese dominance is causing concern since, if China becomes the market leader, Western countries might have to accept the rules and regulations that China attaches to the technology and Chinese standards on AI applications. This might then allow the Chinese state to access data collected and processed by Chinese AI, or to accept the global use of AI in citizen monitoring and control. Furthermore, there are significant intelligence and military uses of AI, such as obtaining and analysing data and evaluating numerous scenarios ('war-gaming') at a faster rate than humanly possible. AI surveillance systems could obtain and analyse data on ***.

Quantum computing: As with AI, key concerns in relation to quantum computing centre round the susceptibility of data to state acquisition and exploitation, and the compulsion to accept Chinese norms and standards even if they do not comply with the UK's own. ***.[549]

Why the UK?

340. As an advanced and open economy, the UK is a clear target for China. The UK has a reputation for being open to foreign investment, and China invests in the UK more than in any other European state. Foreign Direct Investment into the UK from China between 2000 and 2017 was approximately £37bn (with the next largest recipient of Chinese investment being Germany, at £18bn).[550]

[546] Oral evidence – MI5, *** December 2020.
[547] Oral evidence – NCSC, *** July 2019.
[548] Written evidence – JIO, *** June 2018.
[549] Written evidence – HMG, 30 August 2019.
[550] 'Chinese FDI in Europe in 2017', Mercator Institute for China Studies, April 2017.

341. Since 2017, the majority of Chinese investment in the UK appears to have been strategically driven, with clear links between areas of investment and Chinese state objectives. When we questioned the Intelligence Community on this, the JIC Chair emphasised the importance that China places on the UK as a centre of scientific and technological excellence, noting that the UK has world-class research and development (and, in some cases, industrial activity) in many of the technologies mentioned in the 'Made in China 2025' strategy.[551] Chinese science and technology requirements therefore correspond closely to UK strengths in military capabilities, and industrial and emerging technology.

342. The UK sectors of particular interest to the Chinese include defence, telecommunications, new or emerging digital technologies and other strategic industries not necessarily part of the UK's Critical National Infrastructure (CNI), but which are nevertheless considered sensitive (for example ***).[552] Director General MI5 told us:

> ***[553]

What does China target in the UK?

343. When targeting UK Industry, China has two key priorities: the acquisition of IP and technology; and the acquisition of data.

Acquisition of Intellectual Property and technology

344. Intellectual Property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs and symbols, and names and images used in commerce. IP rights give the creator an exclusive right over the use of his/her creation for a certain period of time and enable him/her to earn recognition or financial benefit from what they invent or create. IP is protected in law in various ways.[554]

345. China's apparent unwillingness to recognise (or enforce) IP rights has been an issue since the country 'opened' to the world in the 1970s. Originally, this was centred on copyright and trademark infringement – with pirate DVDs, CDs and counterfeit goods being readily produced by Chinese companies. Today, it is focused on much higher value goods, in particular cutting-edge technology. However, the same principle applies – by stealing IP, the Chinese save money on research and development, thereby lowering the overall 'to-market' cost so that they can undercut the original product and dominate the market.

---

[551] Oral evidence – JIO, *** July 2019.
[552] Written evidence – JIO, 10 August 2020.
[553] Oral evidence – MI5, *** October 2020.
[554] Copyright covers artistic content, which includes novels, plays, poems, films, music, drawings, paintings, photographs, sculptures, maps, technical drawings and architectural design. Copyright allows creators to retain control over the use of their material, authorising or prohibiting its performance, display or reproduction. Patents are exclusive rights to an invention (defined as a product or process which provides a new way of doing something or a new technical solution to a problem). Patents provide protection against an inventor's creation being made, used, distributed or sold without the inventor's consent. Trademark protection allows the owner of a trademark to use it exclusively to identify goods or services they (or someone they have licensed to use their trademark) produce or provide. Industrial Design protection is used to protect aesthetic, rather than technical, inventions (i.e. the way a product looks, not the way it works, which would be covered by a patent).

Data

346. The Chinese also target data. The UK Government has said that it considers data and "*its associated infrastructure*" to be a "*strategic national asset*",[555] as the NCSC explained:

> *data has both economic and intelligence value. It can be used to train artificial intelligence systems and identify individual targets of interest for future exploitation. It also has applications in research and development and commercial decision-making.*[556]

347. Much of China's data acquisition is conducted with a view to maintaining the stability of the Communist regime. GCHQ told us that China's overarching aim is to identify and monitor the threat posed by its population.[557] The Intelligence Community explained:

> *the Chinese state views surveillance and big data analytics as essential tools to maintain Chinese social and economic stability and national security. It collects data from a wide range of sources, such as China's public surveillance apparatus, privately and commercially available, and open source information. The collection and aggregation of personally identifiable information and bulk datasets enables the ChIS* [Chinese Intelligence Services] *to identify and track targets of interest, and will aid technology development, such as the training of AI systems. China is investing heavily in AI through academia, the purchasing of AI technology companies, and through indigenous development.*[558]

348. However, the Chinese are also assessed to target data for intelligence purposes. The Intelligence Community cited the hacking in 2015 of the United States (US) Office of Personnel Management – with the loss of personal information of more than 20m US government officials – as evidence of this. MI5 explained that even apparently innocuous personal information can be useful when combined with other sources of data:

> *in isolation most of these data sets don't enable you to do much at all, but when you build a layered mosaic* [of data sets] *it does then enable *** it enables them potentially to talent spot people that they might be able to make a recruitment approach to ...*[559]

The Chinese Intelligence Services (ChIS) may use bulk data to provide additional intelligence to support their targeting efforts against UK politicians.[560] We were told that using data in this way could "*identify background details on the* [potential] *target, including finances, personal weaknesses and the circles of the people they are close to*".[561]

349. Data comes in many forms, and data-collection platforms all have potential intelligence value. China's Personal Information Protection Law (PIPL), billed as a Chinese version of the General Data Protection Regulation (GDPR), came into effect in November 2021. This law asserts state power over data belonging to both Chinese and foreign companies.

---

[555] Written evidence – HMG, 14 September 2020.
[556] Written evidence – NCSC, provided 27 October 2020.
[557] Oral evidence – GCHQ, *** December 2020.
[558] Written evidence – HMG, 3 December 2020.
[559] Oral evidence – MI5, *** December 2020.
[560] ***
[561] Written evidence – MI5, 16 November 2020.

According to legal experts, "*the PIPL exerts certain exterritorial jurisdiction over data processing activities that happen outside China if the purpose is to provide products or services to individuals located in China, or to analyse or assess the behaviours of individuals located in China*". This means that, on the basis of the PIPL, the Chinese government can force Chinese and other companies to turn over their data as soon as it involves any Chinese citizens. However, as in practice it is not possible to compartmentalise Chinese citizens' data, the Chinese government is likely to get access to whole datasets, including information pertaining to non-Chinese nationals. It has been suggested that the data collected by ride-hailing applications may be of interest to authoritarian regimes such as China due to the potential for it allow the gathering of data on individuals of intelligence interest.[562] When combined with the Chinese government's sweeping powers to force companies operating in China to co-operate, this means that data acquired legitimately by such companies may find its way into the hands of the Chinese state, for further exploitation and analysis.

350. GCHQ observed that China's advanced AI and machine learning industry means that it can process large amounts of raw data, which it can then attempt to leverage in order to meet strategic aims:

> *increasingly* [the Chinese] *are just looking to collect very large quantities of personal information and personal data … with not a huge amount of focus.*
>
> **** with those data sets … it increasingly allows them to control their own … state* [and also to attempt to influence the] *large anti-Chinese community outside China.*[563]

ZZ. China is seeking technological dominance over the West and is targeting the acquisition of Intellectual Property and data in ten key industrial sectors in which the Chinese Communist Party intends China to become a world leader – many of which are fields where the UK has particular expertise.

AAA. As this Committee has previously warned, the West is over-reliant on Chinese technology. As the role of technology in everyday life increases exponentially, so therefore the UK will be at an increasing disadvantage compared to China – with all the attendant risks for our security and our prosperity. British technology and innovation is therefore critical and must be robustly protected.

[562] 'How Ride-Hailing Businesses Collect and Manage Data: A National Security Risk?', Royal United Services Institute (RUSI), 1 December 2021.
[563] Oral evidence – GCHQ, *** December 2020.

METHODOLOGY: OVERT

351. Many of the methods used by China to acquire UK technology, IP and data are entirely legal under UK law. Indeed, in October 2020, the Acting NSA made it clear that "*there is much licit Chinese activity in this country that we welcome and that we want to continue … there is no way that we can cut ourselves off from China*".[564]

352. We have already considered China's overt use of Academia to acquire information at the 'front end' – i.e. at the research or development stage. Once technology has been developed, and is in use by a company, China exploits all possible avenues to acquire it by legitimate means – whether that be through licensing agreements, buying the company, obligations placed on foreign companies investing in China, opportunities offered by trade shows, or influencing standards-setting bodies to favour Chinese products. The DNSA told us in December 2020 that "[China] *understand*[s] *the interdependencies between all of those things. So it's a very sophisticated joined-up programme of work that seeks to exploit whatever is the most expeditious route to the Intellectual Property that they're targeting*."[565]

Licensing agreements

353. In the past, China has made use of legitimate licensing agreements, entered into in good faith by UK companies, to advance its technological capabilities. Through such agreements, China pays for the technology and the skills, equipment and expertise it requires to produce the technology, without taking ownership of the IP itself.

354. For example, in the 1970s, China entered into an agreement with Rolls-Royce to manufacture, under licence, the Rolls-Royce Spey Mk 202 jet engine. This gave China access to advanced technology that it could not, at that time, produce itself. In time, the Chinese produced their own variant of the Mk 202 engine, which was subsequently used in the JH-7 fighter-bomber aircraft used by the People's Liberation Army (PLA) (and produced for export, with the potential to undercut UK and other Western defence exports).[566] Thus, British technology is used today by the Chinese armed forces to advance the CCP's ambitions.

Foreign Direct Investment

355. Notwithstanding a notable, more recent, hardening of the Government's rhetoric and action towards China,[567] it is likely that the UK Government – as well as the Devolved Administrations and local government – will continue to court investment from China to a greater or lesser degree. The (then) Prime Minister said in October 2021: "*I am no Sinophobe – very far from it. I'm not going to tell you that the UK Government is going to pitchfork away every overture from China*."[568] Indeed, it was reported in February 2022 that the (then) Prime Minister had asked the (then) Department for International Trade to set up a meeting

[564] Oral evidence – NSS, *** October 2020.
[565] Oral evidence – NSS, *** December 2020.
[566] Written evidence – HMG, 18 April 2019.
[567] In September 2020, we were told that the Government was "*building a more comprehensive approach to our economic security in relation to China*". (Written evidence – HMG, 14 September 2020.)
[568] 'Boris Johnson Says U.K. Doesn't Want to Turn Away Chinese Investment', *Bloomberg*, 18 October 2021.

of the ministerial-level UK–China Joint Economic and Trade Commission, which had not met since 2018.[569]

356. While foreign investment is often positive, it also provides a legitimate route through which the CCP can acquire technology to which it may not otherwise have had ready access, and which it can transfer to China and use in ways which may be against the interests of the UK and its allies. When proposed investments are in high-tech industries with potential 'dual-use' (i.e. civilian and military) applications, this is of particular concern from a national security perspective.

357. In 2020, the JIC assessed that the main potential threats from foreign investment were that: our adversaries' defence and intelligence capabilities are thereby developed; CNI and related supply chains are interrupted; and ***. Investment can also enable espionage and be used to gain influence, credibility and leverage over the UK.[570]

358. All of these considerations are relevant to Chinese investment in the UK. The assessment acknowledged that the majority of Chinese investment in the UK is almost certainly in non-sensitive sectors,[571] but noted significant investments in sensitive sectors including ***. Furthermore, investments in areas not traditionally considered sensitive can also have national security implications.[572]

359. The CCP views investment in UK companies as a legitimate means to access and transfer "*strategically important knowledge*" to China.[573] This information is not restricted to the design of the technology in question, but often includes the knowledge needed to manufacture the product, including "*physical skills (e.g. machine use), labour organisation, factory and machine design and construction, research skills and quality assurance procedures*".[574] As a consequence, "*acquisitions by Chinese companies of UK defence and aerospace companies often include a plan to improve the production capability of the Chinese company and the construction of a new factory in China*".[575]

360. This is the 'added value' that China obtains from its legitimate investments. A 2019 Intelligence Community assessment paper noted:

> *Foreign Direct Investment allows Chinese entities to master the complex interconnected systems involved in manufacturing a product from concept to production. There is a remote chance individual human experts or data acquisition alone could provide this level of insight in most cases*.[576]

361. While Chinese acquisitions in a broad range of sectors could be of potential national security concern, the risk is most acute in the defence sector. The Intelligence Community told the Committee that acquisitions of UK defence companies by Chinese companies

[569] 'Met runners and riders – China trade talks – P.P.S. It's over', *Politico London Playbook*, 11 February 2022.
[570] Written evidence – JIO, August 2020.
[571] Written evidence – JIO, August 2020.
[572] Written evidence – JIO, August 2020.
[573] Written evidence – HMG, 18 April 2019.
[574] Written evidence – HMG, 18 April 2019.
[575] Written evidence – HMG, 18 April 2019.
[576] Written evidence – JIO, June 2019.

present a threat to UK national security ***.[577] Due to China's legal requirement for co-operation by its companies and citizens, and its Civil–Military Integration doctrine, it is highly likely that defence-relevant technologies in China will be incorporated into its military supply chain, which is dominated by state-owned enterprises.[578]

362. Civil–Military Integration is a key driver of Chinese military modernisation as it exploits civilian technology for military applications with no acquisition cost to the state. The Intelligence Community told the Committee that as China advances economically this will almost inevitably lead to Chinese military advancement, since commercial power in the technology field provides "*extensive opportunities to support military technological advancement and expansion*".[579] Commenting on the highly integrated nature of the Chinese state, MI5 told the Committee:

> *China … is absolutely determined to accelerate as rapidly as it can its rise to global pre-eminence across a range of economic and technological fronts, and I don't think within their system that a distinction is drawn between national security or economic prosperity. I think they absolutely see these two things as intertwined and … within their own doctrine of Civil–Military Integration, they are very explicit about that and they are also very explicit about expecting both state-owned enterprises and private sector companies, as so far as that means anything in a communist state, to contribute to the whole-state strategic goals. So we …* [have] *a China that integrates its own efforts in a very strong and effective way.*[580]

363. The threat is exacerbated by the fact that the provenance of an investor is not always readily apparent. While in most cases Chinese investment in a foreign company is overt, it is highly likely that the Chinese state, and some Chinese companies, would attempt to obfuscate Chinese ownership in order to avoid scrutiny when purchasing or investing in UK companies.

364. Despite increased scrutiny, Chinese investment remains a significant concern. In September 2020, *** assessed that there was a risk that China would seek to buy companies in financial difficulties (particularly due to Covid-19) at cheap prices in order to acquire valuable IP in areas including emerging technology, advanced manufacturing and military development.[581]

Inward investment into China

365. In addition to China's own foreign investment plans, inward investment into China has offered opportunities for technology acquisition. A foreign company investing in certain industries in China was, until 2019,[582] required by law to enter into a joint venture with a Chinese company. In such joint ventures, the foreign company could not hold the controlling interest and may have been subject to requirements under which they had, in effect, to

[577] Written evidence – HMG, 18 April 2019.
[578] Written evidence – HMG, 18 April 2019.
[579] Written evidence – HMG, 18 April 2019.
[580] Oral evidence – MI5, *** December 2020.
[581] Written evidence – ***, 24 September 2020. The Committee has subsequently been advised that ***.
[582] Until the passage of the 2019 Foreign Investment Law, which abolished the Joint Venture Regulations.

transfer their technology to the Chinese partner.[583] A decision to invest in the lucrative (and expanding) Chinese market is, therefore, often a trade-off between short- to medium-term gain and the likely loss of control of proprietary information.

366. The Intelligence Community previously reported examples of China targeting UK Industry (***) to obtain intelligence, broader information and skills through such joint ventures:

> ***[584]

367. Such actions may have been entirely legitimate commercial engagements under Chinese law, with UK companies being aware of the risks they were subjecting themselves to. However, it is also possible that joint ventures could be used to steal technology and data. MI5 told the Committee that China could:

> *spot something it likes, to get quite close to that,* [and] *to get to the point where you are looking at a joint venture, you host a visit, you get lots of the* [employees of the] *Chinese company that you are going to do the joint venture with coming round, they look at how you are set up, they look at your factory, they spend lots of time and then – at the last minute – the joint venture collapses and a few months later you see* [your own technology] *produced by China cheaper.*[585]

Standards-setting bodies

368. The critical and far-reaching importance of technical standards set by international bodies was raised by Director GCHQ in evidence to the Committee in October 2020, when he noted that the Chinese strategy to increase its presence at standards-setting bodies meant that it had now begun to dominate them. He cited the International Telecommunication Union and 3rd Generation Partnership Project – influential telecommunications technical standards-setting bodies – as organisations in which China has acquired disproportionate influence, including numerous leadership positions.[586] The Intelligence Community judge that:

> *China is using international forums to shape emerging international standards on key emerging technologies. Defining international standards will enable China to shape technology to suit its own values and priorities, which may differ substantially and be at odds with those of the West. There are significant concerns over the susceptibility of data to state acquisition and exploitation, and the compulsion to accept Chinese norms and standards even if they do not comply with our own. An example of this would be concerns over a free and open internet, compared to China's commitment to central state control over information flow.*[587]

369. Influence over international standards-setting fora is extremely valuable from a commercial perspective. If companies from a given country – in this case, China – own the

[583] Written evidence – HMG, 18 April 2019.
[584] Written evidence – HMG, 1 May 2019.
[585] Oral evidence – MI5, *** October 2020.
[586] Oral evidence – GCHQ, *** October, 2020.
[587] Written evidence – HMG, 30 August 2019.

'standard essential patents' necessary to implement the technical standards in question, all other companies will have to license the patent.[588] As well as an immediate commercial gain, such influence can also have long-term, strategic consequences, as future technology development may rely on the same or similar patented technology, thereby helping to embed a commercial and strategic advantage. In other words, if China has influence over the technical standards, it can influence the long-term direction of travel for technology development – with all the economic and national security implications that this would have for the UK and its allies.

370. One example of this is the use of Chinese technology in so-called 'smart cities' (or, as the NCSC has referred to them, 'connected places') which rely on Information and Communication Technology and the Internet of Things devices to collect and analyse data to improve municipal services.[589] The online forum 'Just Security' has reported that smart cities are an integral part of what it describes as China's "*AI-driven domestic repression, with highly escalated surveillance capacities*" and that China is shaping the international debate around normalising the use of such technology "*by flooding the zone of multi-lateral tech-related diplomacy*". It cites China's "*ability to exert influence at tech-standard setting bodies, like the International Telecommunications Industry (ITU) where interoperability standards for the future are set* [and where China's] *aim has been to push China's preferred protocols as the global default for Internet of Things and other emerging technologies*".[590]

371. MI5 told the Committee that Chinese dominance of technical standards would *** create opportunities for China to influence the future of the internet:

> *if China, say, were to be in a position to substantially influence or even control the future generations of technical standards, with large parts of the globe then essentially following a Chinese technological agenda … that would inevitably … ***, because at the moment the global standards essentially were set in the US in the 70s around the internet protocols and so forth.*
>
> *… If gradually over the next few decades you were to shift to a model where states control the internet, that has huge obligations for freedom of speech and very long-term national security implications in that sense, because … China could be in a position to persuade a lot of other states to side with it around having a more kind of authoritarian view, not just on the standards of how the internet runs technically, but what control states are able to have over content within their own borders.*[591]

BBB. China's joined-up approach can be clearly seen from its use of all possible legitimate routes to acquire UK technology, Intellectual Property and data – from buy-in at the 'front end' via Academia, to actual buying-in through licensing agreements and Foreign Direct Investment, to the exertion of control over inward investments and standards-setting bodies. Each represents an individual threat, but it is the cumulative threat that can now be clearly seen.

---

[588] Oral evidence – NCSC, *** October 2020.
[589] Written evidence – NCSC, May 2021.
[590] 'System Rivalry: How Democracies must compete with digital authoritarianism', JustSecurity.org, 27 September 2021.
[591] Oral evidence – MI5, *** December 2020.

CCC. Overt acquisition routes have been welcomed by HMG for economic reasons, regardless of risks to national security. The threat to future prosperity and independence was discounted in favour of current investment. This was short-sighted, and allowed China to develop significant stakes in various UK industries and Critical National Infrastructure.

DDD. Without swift and decisive action, we are on a trajectory for the nightmare scenario where China steals blueprints, sets standards and builds products, exerting political and economic influence at every step. Such prevalence in every part of the supply chain will mean that, in the export of its goods or services, China will have a pliable vehicle through which it can also export its values. This presents a serious commercial challenge, but also has the potential to pose an existential threat to liberal democratic systems.

METHODOLOGY: COVERT

372. While China is adept at exploiting legitimate routes to advance technologically, it also utilises the full range of its espionage capabilities. The NCSC told the Committee:

> *to fulfil any national strategic outcome …* [the Chinese Communist Party] *will use the* [intelligence] *capabilities they've got – be it cyber espionage* [or] *human espionage – and they really don't seek a distinction … of using those capabilities for purely national security reasons. They see the whole spectrum of strategic national outcomes as being fair game for those capabilities.*[592]

373. China uses its covert capabilities to target other countries' technology, IP and data in order to – as previously noted – "*bypass costly and time-consuming research, development and training*".[593] This gives it a significant commercial advantage and, over time, strategic advantage.

374. This looks set to continue – and to increase: ***.[594] ***. [595]

Human intelligence

375. The ChIS have *** human intelligence (HUMINT) capabilities. They seek to identify individuals who have access to sensitive information which is of particular value to them – "*** *providing easier access to otherwise restricted UK military or commercially sensitive information*".[596] For example, China uses opportunities provided by ***, or by social media to recruit individuals. MI5 told us that:

> *the use of LinkedIn, the social/professional networking site, for example, is very widespread... well over *** UK-based individuals* [have been] *the subject of a very light initial approach ***, where someone is presenting* [themselves] *as maybe a consultant who is interested in an article this person may have written or wishes to invite them to a conference and … seeing whether they can suck this person into some … form of communication away from the LinkedIn site, perhaps email – and then maybe, if this develops, there is an invitation to a conference or a seminar, or somebody gets paid a small sum for writing an article...*[597]

376. ***.[598] ***. [599]

[592] Oral evidence – NCSC, *** December 2020.
[593] Written evidence – HMG, 18 April 2019.
[594] Written evidence – ***, March 2020.
[595] Written evidence – ***, June 2019.
[596] Written evidence – ***, June 2019.
[597] Oral evidence – MI5, *** October 2020.
[598] Oral evidence – MI5, *** October 2020.
[599] Oral evidence – MI5, *** October 2020.

Chinese targeting of UK Industry

A UK-based *** expert was recruited by the ChIS when working at ***. They tasked him to exploit his role at a UK organisation to provide Intellectual Property, written reports, *** and referrals for other experts to travel to China. He also introduced UK experts with access to Chinese intelligence officers. ***.[600]

Another case involved ***[601] ***[602]

Visits and trade shows

377. ***.[603] According to the Ministry of Defence (MoD), Chinese delegates make more requests to visit defence industry and defence sites than any other nationality and are by far the most numerous nationality to visit sites controlled by the MoD's International Visits Control Office (IVCO), showing particular interest in sites connected to the aerospace sector.[604]

378. The Committee was told that, whilst attending visits, Chinese delegates have ***, been extremely forward in their questioning, ignored instructions not to photograph items of interest, and may in some cases have smuggled cameras and recording equipment onto visit sites.[605] The Committee is concerned that such events may have been used to collect industrial information (potentially including IP) as well as personal information on individuals of interest working within the defence sector. ***[606]

379. When we asked about the scale of the problem, MI5 told us:

> *we do from time to time hear reports from *** of visits of whatever sort where Chinese individuals have sort of taken photographs when they've been told not to, that sort of thing … as a general rule, people in particularly advanced technology sectors, when they are receiving Chinese delegations, would be wise to be alert to the possibility that their visitors will be seeking to acquire more in depth insight or information than their host intends, so it pays to manage those kinds of visits carefully.*[607]

However, MI5 noted that to a certain extent some such activity might be expected from any foreign delegation, and emphasised the need to keep such incidents in proportion: "***".[608]

380. When we asked the Chief of Defence Intelligence (CDI) what more could be done to prevent the exploitation of trade shows, he acknowledged that there were significant difficulties in doing so, but suggested that instead the focus should be on ensuring that both

[600] Written evidence – JSTAT, August 2019.
[601] ***
[602] Written evidence – MI5, 31 July 2018; Written evidence – HMG, 18 April 2019.
[603] Written evidence – HMG, 18 April 2019.
[604] Written evidence – HMG, 18 April 2019.
[605] Written evidence – HMG, 18 April 2019.
[606] Written evidence – HMG, 18 April 2019.
[607] Oral evidence – MI5, *** December 2020.
[608] Oral evidence – MI5, *** December 2020.

the authorities and industry representatives were aware of the threat in order to limit any potential damage:

> *It's difficult, I think, in that circumstance to prevent people from coming often to those defence exhibitions which are not MOD controlled;* [they] *are often commercial activities. *** China is an exporter of weapons, sells about 5% of the world's exports currently …*
>
> **** banning those Chinese companies who of course have a commercial right to be able to sell their goods would be a difficult thing to achieve.*[609]

Cyber

381. Equipment Interference (EI) (described in Part One of the Report) refers to techniques used to obtain communications, equipment data or other information from a range of types of equipment. It is, relatively speaking, a low-cost means of acquiring IP and data – it can be conducted remotely, deniably and at-scale, and as such is a technique highly valued by China.[610]

382. In 2015, the UK and China signed an agreement that prohibited cyber-enabled theft for commercial (rather than strategic) advantage. China subsequently made similar bilateral declarations with the United States, G20, Australia and Germany.[611] ***.[612]

383. We were told that there was frequent Chinese cyber targeting of UK companies and academic organisations, much of which ***. Chinese cyber victims include those with legitimate relationships with Chinese partners on science and technology ***.[613] ***.[614] ***.[615]

384. As well as conducting EI against UK-based organisations, the Committee was told that attacks have included targeting Academia, as well as supply chains and third-party service providers (including Managed Service Providers – for instance, companies which provide outsourced IT functions).[616] EI can be used to obtain technical information or to harvest Bulk Personal Datasets ***.[617] ***.[618]

---

[609] Oral evidence – DI, *** December 2020.
[610] Written evidence – HMG, 18 April 2019.
[611] 'Agreements on commercial cyber espionage: an emerging norm?', Lawfare, 4 December 2015; 'Hacking for Ca$h', Australian Strategic Policy Institute, 25 September 2018.
[612] Written evidence – HMG, 14 September 2020.
[613] Written evidence – JSTAT, June 2019.
[614] Written evidence – HMG, 30 August 2019.
[615] Written evidence – HMG, 30 August 2019; Written evidence – JSTAT, August 2019.
[616] Written evidence – HMG, 18 April 2019.
[617] Oral evidence – HMG, *** October 2020. Bulk Personal Datasets would be, for instance, medical records, travel records or the HR data held on file by an institution or a company. An extreme example of such exfiltration is the 2014 hack of the US Office of Personnel Management which held all of the information supplied by government employees and contractors in order to undergo security vetting. This meant that the exfiltration (believed to have been perpetrated by the Chinese state) allowed access to extremely personal information (including drug use, debt levels and sexuality) about individuals who had access to classified material, potentially making them vulnerable to blackmail.
[618] Written evidence – HMG, 18 April 2019.

385. The cyber threat from China emanates principally from the Ministry of State Security and the PLA. These organisations are almost certainly responsible for ***, and their cyber activity is closely correlated with the Chinese government's economic and military development goals.[619]

APT10

APT10[620] is one of the best-known Chinese hacking groups, and has carried out numerous malicious cyber campaigns on behalf of the Chinese Ministry of State Security (MSS). *** it has targeted government, defence, mining, information technology, *** with victims identified worldwide, including in Europe, Asia, and the United States ***. ***.[621]

In 2016, *** it was detected that there had been a large-scale compromise of a number of Managed Service Providers (MSPs) (companies which provide IT and network support, including hosting emails). The attack, widely known as 'Cloud Hopper', facilitated economic and strategic espionage.

The UK Government publicly attributed the Cloud Hopper MSP campaign to APT10 in December 2018, linking the group explicitly to the MSS. This was the first time that HMG had publicly named elements of the Chinese government as being responsible for a cyber campaign.[622]

386. China's sophisticated cyber capabilities could, in theory, be employed to conduct a cyber attack against UK infrastructure. ***. In the words of NCSC:

> *on cyber attacks that* [the Chinese] *undertake, ****.
>
> *** *they use their intelligence capabilities very much for ****. *They do have offensive cyber capabilities. *** exercising those cyber capabilities *** … around the blurring of some of their capabilities … I think absolutely we're alive to them using cyber as a means to enable HUMINT and the other way round and so work very closely together to sort of make sure that ****.[623]

EEE. We welcome the Government's attribution of attacks to the Chinese hacking group APT10. Public condemnation of such groups explicitly linked to the Chinese government is an essential tool in tackling the increasing cyber threat from China. The Government should continue to work with allies to highlight and condemn hostile Chinese government activity.

[619] Written evidence – NCSC, October 2021.
[620] APT10 stands for 'Advanced Persistent Threat 10'.
[621] Written evidence – NCSC, August 2018.
[622] 'UK and Allies reveal global scale of Chinese cyber campaign', HMG press release, 20 December 2018.
[623] Oral evidence – NCSC, *** December 2020.

THE UK GOVERNMENT RESPONSE

Understanding the task

387. As noted previously, the CCP is clear – including through its 'Made in China 2025' strategy – about its ambition to become the world leader in advanced technologies such as AI and new synthetic materials. UK scientists and academics are at the cutting edge of the development of many of these technologies; however, despite this, successive UK Governments have been criticised for failing to act to protect UK science and technology against Chinese economic influence and espionage. This is a point which the Government has acknowledged. In December 2020, the Committee was told by the Deputy National Security Adviser (DNSA):

> *in the past we have perhaps not had as rigorous a process at identifying, across the board, what needs to be protected based on our sovereign interest. We've had a very sophisticated process in some areas, so for example Critical National Infrastructure, which includes energy and so on. We've been weaker* [historically] *in other areas, for example emerging technology, potentially strategic suppliers and interdependences and data and telecoms infrastructure particularly.* [624]

However, the DNSA emphasised that there was now increasing recognition of the problem, and that matters were beginning to improve:

> *I think we have, over the past couple of years, been very conscious that we needed to both fix the system and get after some of those very specific threats in a more cohesive way across the whole of Government, and with a structured policy framework and new infrastructure …*[625]

388. In August 2020, the Government had, through its Emerging Technology Board, identified a number of critical and emerging technologies:

- Artificial Intelligence and Machine Learning;
- Robotics and Autonomous Systems;
- Quantum Technologies;
- Engineering / Synthetic Biology;
- Mobile or Consumer Telecommunications;
- Advanced Materials;
- Novel Connectivity;
- Digital Finances;
- Imaging, Sensors and Photonics;
- Space-related Technologies;

[624] Oral evidence – *** December 2020.
[625] Oral evidence – *** December 2020.

- Smart Cities;
- Fuels from Alternative Sources;
- Energy Storage;
- Privacy Enhancing Technologies;
- Human Augmentation; and
- Nanotechnology.

We were told that the next step was for a cross-HMG agreement as to "*the technologies the UK wants to Own, Collaborate and Access*". As part of this effort, the Cabinet Secretary commissioned a review to:

> *look at the wider issues for delivering strategic advantage through S&T* [science and technology] *alongside making 'clear, proactive and strategic policy choices on the science and technologies that will matter most'*.[626]

389. In June 2021, the Government announced the establishment of a new Cabinet Committee, the National Science and Technology Council, to "*provide strategic direction on the use of science and technology*".[627] The Council is supported by a new Office for Science and Technology Strategy, based in the Cabinet Office, which is intended to "*strengthen the Government's insight into cutting-edge research and technologies*" and "*identify what is needed to secure and protect the capability in science and technology required in the UK to deliver the Government's ambitions*".[628] The Government's Chief Scientific Adviser was additionally appointed as the National Technology Adviser.

390. In terms of the Intelligence Community's contribution, SIS and GCHQ have also been tasked to collect strategic intelligence ***. In 2019, SIS and GCHQ were tasked to:

- ***
- ***
- ***.[629]

391. We were subsequently advised that this tasking would be replaced with the following policy outcomes to which their intelligence is expected to contribute:

- ***
- ***
- ***.[630]

[626] Written evidence – HMG, 12 February 2021.
[627] 'Prime Minister sets out plans to realise and maximise the opportunities of scientific and technological breakthroughs', HMG press release, 21 June 2021.
[628] 'Prime Minister sets out plans to realise and maximise the opportunities of scientific and technological breakthroughs', HMG press release, 21 June 2021.
[629] Written evidence – HMG, 21 January 2020.
[630] Written evidence – Cabinet Office, 14 October 2020.

392. Director General MI5 told the Committee that he had seen an improvement in joined-up thinking on these issues:

> *I think I would be more concerned if we remained in a position we probably arguably were in five or ten years ago, where the national security community within Government and the prosperity community weren't really talking to each other – because I think that to do this well we really do need to integrate our understanding across both these domains to make the best possible choices.*[631]

Foreign investment and national security

393. As noted in the main body of the Report, the Government has previously failed to take national security into account when considering foreign investment. Two developments in recent years have improved the situation: the introduction of new legislation to strengthen the Government's powers to intervene in potential investments on national security grounds; and the introduction of new processes for the Intelligence Community routinely to provide input to central Government on the security implications of potential investments.

Legislation

394. Prior to 2022, the power for Government to intervene in mergers and acquisitions was drawn from the Enterprise Act 2002. It set a very high bar for government intervention: the Intelligence Community were clear that, under the Enterprise Act, "*levers for HMG intervention in Foreign Direct Investment cases* [were] *limited*".[632] Ultimately, it proved to be an ineffective mechanism from a national security perspective: in October 2020 the DNSA told the Committee that the Act had "*only been used six times between 2004 and 2009 and then six times since 2017, so it is not a thing we can very readily bring to bear in some of these cases* [of national security concern]".[633] Four further interventions were made in 2021. Of these 16 interventions, none had resulted in a deal being blocked.

395. The Government sought to remedy this situation through the National Security and Investment (NSI) Act 2021. The NSI Act, which entered into force in January 2022, designated the Secretary of State for Business, Energy and Industrial Strategy (BEIS) as the single decision-maker in cases of acquisitions (of companies, assets and IP) which may have an adverse impact upon UK national security.[634] The Secretary of State was to be supported by a newly created Investment Security Unit (ISU) sitting in the (then) Department for Business, Energy and Industrial Strategy.

396. The ability of a Secretary of State now to intervene in mergers and acquisitions was described to the Committee as a "*big upgrade*" in the Government's "*investment screening capabilities and powers*".[635] Interventions may be made in any acquisition that grants control of a company, regardless of company size or sector, as long as there is a sufficient connection to the UK. The NSI regime also utilises a combination of comprehensive market monitoring

[631] Oral evidence – MI5, *** December 2020.
[632] Written evidence – HMG, 18 April 2019.
[633] Oral evidence – NSS, *** October 2020.
[634] Academia and academic collaborations are also now subject to a scheme of voluntary referral, and individual collaborations or the transfer of assets could be subject to call-in powers.
[635] Oral evidence – HMG, *** October 2020.

and notification by industry (both voluntary and mandatory, dependent on the threshold), although interventions are not strictly contingent on notification. In 2018, the Government anticipated that there would be 200 notifications from industry each year, of which around half would raise a national security concern. However, by September 2020, HMG was estimating that there would be between 1,000 and 1,800 notifications per year from industry – although they still considered that fewer than 100 would be called in for review under the legislation.[636] The remainder are subject to a national security assessment. If the Government decides national security is at risk, it could impose remedies where necessary and proportionate.

397. NCSC explained that Huawei's 2012 purchase – from the East of England Development Agency, then a UK Government non-departmental public body – of the Centre for Integrated Photonics (CIP), is the sort of case in which the Government should intervene:

> *one of the things is we have allowed foreign investment to take early-stage technology out of the UK. ... Huawei bought* [CIP] *for 70 million quid [British pounds] because it was going under. That's how they got a head start on 100GB optics. That's not something we should allow to happen. There was no law in place … that would allow us to stop that.*[637]

Intelligence Community input to the investment security regime

398. As noted above, under the NSI Act, a team called the ISU was established in BEIS to co-ordinate advice and expertise from across Government on the risks from potential foreign investments. It took an 'actor-agnostic' approach to investment scrutiny, considering each case on its merits rather than solely through the prism of country of origin. The ISU replaced the Investment Security Group (ISG), which had been established in May 2017 as part of the Cabinet Office and which had been performing a similar function. During the passage of the NSI Act, Parliament was told that the ISU "*will work closely with the security agencies and other departments with real sector expertise*".[638]

399. The Intelligence Community's input into the ISU is now channelled through ***, a joint team from the Centre for the Protection of National Infrastructure (CPNI – accountable to MI5) and NCSC (part of GCHQ). Established in July 2020, it is designed to "*bring coordination to the identification and mitigation of the national security risks posed by a sub-set of foreign investment transactions*".[639] These new arrangements enhance the Intelligence Community's ability to draw on secret intelligence to inform the work of the ISU and ministers' decisions.

400. As of September 2021 (when the NSI regime had not entered fully into force), the joint team was providing support to the ISU on *** investment cases.[640] Between July and September 2021, the joint team received *** 'triage' requests from the ISU, a quarter of which related to proposed investments or acquisitions from China (not all triage requests will result in ongoing support from the joint team).[641] Following the NSI Act entering into

[636] NSI Impact Assessment, 9 November 2020.
[637] Oral evidence – NCSC, *** October 2020.
[638] HC Deb, 17 November 2020, col. 277–8.
[639] Written evidence – MI5, 3 February 2021.
[640] Written evidence – MI5, 31 January 2022.
[641] Written evidence – MI5, 31 January 2022.

force in January 2022, the joint team has sight of all notifications under the new Act, and provides advice ***.

401. ***[642]

402. The Joint State Threats Assessment Team (JSTAT), NCSC and DI also provide *** reports to inform the work of the ISU.[643] In addition, the National Security Strategic Investment Fund (NSSIF) – a collaboration between the UK Government and the British Business Bank – provides ad hoc advice to policy-makers in respect of investment security matters.[644]

403. MoD also provides subject matter expertise and advice to help inform investment scrutiny processes and export licensing decisions (the latter being a separate issue from foreign investments, but nevertheless highly relevant to the protection of the UK's IP. A new Defence Investment Security Team was established in 2017 to co-ordinate this work within the Department and link into wider cross-Government investment security processes. CDI told the Committee:

> *we provide advice both through* [the cross-Government investment security process] *and directly to the Department of International Trade on end user*[s] *of high-tech goods and looking at export licence applications. So in 2017 there were *** export licence applications for China looking at the security goods;* [in] *2019, there were ***, so they are expanding; we've received over *** this year so far. That proportion is probably about ***% of the export licences that we review using the intelligence available to us and so far this year we've recommended a refusal of *** of those applications, because we believe they've met the threshold where those technologies should not be transferred out to China. Then, of those, over *** have been refused by DIT, *** are still being considered and *** were overturned.*[645]

OneWeb

In July 2020, the UK Government announced that it was investing $500m in order to acquire the satellite technology company OneWeb, as part of a consortium with Indian telecommunications conglomerate Bharti Global. OneWeb, which had filed for bankruptcy in March 2020, is constructing a global satellite constellation to provide "*enhanced broadband and other services to countries around the world*".[646]

[642] Written evidence – HMG, 18 April 2019.
[643] Written evidence – MI5, 31 January 2022.
[644] Written evidence – ***, 25 May 2021. Established as part of the 2017 Budget, the NSSIF aims "*to accelerate the adoption of HMG's future national security and defence capabilities and the development of the UK's dual-use technology ecosystem*". (British Business Bank website, www.british-business-bank.co.uk/national-security-strategic-investment-fund)

In a November 2021 speech, the Chief of SIS acknowledged: "*We cannot match the scale and resources of the global tech industry, so we shouldn't try.*" Instead, through the NSSIF, SIS and the broader Intelligence Community are "*opening up our mission problems to those with talent in organisations that wouldn't normally work with national security*". (Chief of SIS's speech to the International Institute for Strategic Studies', GOV.UK, 30 November 2021.)
[645] Oral evidence – DI, *** December 2020.
[646] 'UK government to acquire cutting-edge satellite network', HMG press release, 3 July 2020.

While some, including the Chair of the (then) Business, Energy and Industrial Strategy (BEIS) Select Committee, questioned the rationale for the Government's investment, and there was criticism in some quarters after officials sought (and received) a formal ministerial direction to proceed with the investment due to the risk of public money being lost, the Government described the investment as signalling its "*ambition for the UK to be a pioneer in the research, development, manufacturing, and exploitation of a fleet of Low Earth Orbit* [LEO] *satellites*".[647]

***

The Cabinet Office-led Investment Security Group – since superseded by the Investment Security Unit – opened a case on OneWeb once it became aware of the company's financial difficulties. OneWeb's decision to file for bankruptcy in March 2020 ***.[648]

***.

***.[649] ***.[650]

*** [651] ***.[652] ***.[653]

***.[654]

***.[655]

At the time of taking evidence, we requested further written evidence on the OneWeb deal from BEIS, but this was refused on the grounds that "*Information relating to OneWeb has already been provided to the BEIS Select Committee and to the Science and Technology Committee, both of which have oversight of BEIS' work*".[656]

However, the BEIS Select Committee and the Science and Technology Committee have not been in a position to adequately scrutinise the Government's investment in OneWeb ***.[657] The Government has therefore avoided scrutiny on this use of public money.

404. Overall, the challenge of disrupting malign Chinese investments is a significant one. As MI5 told us:

[647] 'UK government to acquire cutting-edge satellite network', HMG press release, 3 July 2020.
[648] Written evidence – ***, 25 May 2021.
[649] Written evidence – MI5, 7 September 2020.
[650] Written evidence – MI5, 25 May 2021.
[651] Written evidence – GCHQ, 25 May 2021.
[652] Written evidence – SIS, 25 May 2021.
[653] Written evidence – GCHQ, 25 May 2021.
[654] Written evidence – MI5/GCHQ, 23 June 2020.
[655] Written evidence – MI5, 7 September 2020.
[656] Written evidence – BEIS, 17 May 2021.
[657] Although this is a good example of *** investment security cases, it is also not a typical case at all. ***, we cannot say for sure which factors were considered as BEIS has refused to engage with us on this matter.

as we get into places where Chinese investments in our economy are as much of a threat as Intellectual Property stolen across a cyber domain or by a spy, that is a deeper and broader issue ***

… a lot of the damage, some of it is not deeply clandestine, some of it is sort of hiding in plain sight – but trying to form wise judgements across the whole of Government and beyond, into Academia and elsewhere, is a genuinely difficult challenge and that is where I think we will face, over the next few years, some really interesting things about how do we build that teamwork to meet a whole-of-state Chinese approach with, as it were, a whole-of-nation, UK approach.

The answers are not always straightforward, but it is the changing nature of it – well beyond, as it were, the intelligence domain – that is the trickiest part.[658, 659]

Advice to Industry

405. As noted in the main body of the Report, MI5, CPNI, and GCHQ (through the NCSC), provide vital advice on protective security and cyber security to Industry, with a view to increasing the UK's resilience to threats (including from China). MI5 highlighted the importance of this engagement:

We need to have a resilient, well-protected, well-educated industrial base that protects itself in its dealings with China, and we obviously do, I think, a good and professional job in using the finite operational capacity that we have *** *the worst and most damaging parts of what's going on…*[660]

The National Cyber Security Centre

406. In July 2019, the Chief Executive Officer of the NCSC told the Committee: "*In our role trying to defend the UK from cyber-attacks, China's ambitions to steal IP is one of the principal things that we worry about*."[661] One of NCSC's key tasks is therefore to engage with Industry in order better to understand the vulnerabilities in their systems and to share information about threats they may face. While much of the information they provide is 'actor-agnostic', it is highly applicable to the cyber threat from China.

407. Examples of NCSC's recent work with Industry include collaborating with small Voice over Internet Protocols providers to improve their protection against cyber attacks;

[658] Oral evidence – MI5, *** October 2020.

[659] As noted at the start of this Report, HMG announced a restructure of several government departments on 7 February 2023. As a result of this restructure, the Investment Security Unit has moved to the Cabinet Office, and other responsibilities which previously fell to BEIS now sit within several new departments: the Department for Energy Security and Net Zero; the Department for Science, Innovation and Technology; and the Department for Business and Trade.

The Committee has not been in a position to scrutinise the impact and effectiveness of this change during this Inquiry. As noted previously, the Government has assigned Parliamentary scrutiny of the ISU – now that it has returned to the Cabinet Office – to the BEIS Select Committee. However, we urge the Government to reconsider and confirm the ISC's responsibility for oversight of the ISU, as the only Parliamentary body able to perform effective oversight of investment security decisions taken on the basis of classified intelligence.

[660] Oral evidence – MI5, *** December 2020.

[661] Oral evidence – NCSC, *** July 2019.

working with the Prudential Regulation Authority to issue guidance on Cloud-based security to companies in the finance sector; and partnering with MoD to deliver workshops on secure IT networks to companies in the defence sector.[662]

The Centre for the Protection of National Infrastructure

408. CPNI – accountable to MI5 – has a preventative and advisory role, providing protective security advice to Industry and the Government. It follows a "*threat-focused and intelligence-led*" approach to engagement, allocating resources to sectors, industries and businesses where there is evidence of Chinese desire to gain technology, IP and Information Data.[663] Around ***% of CPNI's work is directed towards countering Hostile State Activity (HSA), and it works with cross-government partners "*to raise awareness of the threat, identify vulnerabilities, and to provide advice and mitigations*".[664]

409. *** CPNI says that it has been able to feed in information to MI5 that has been reported to it by Industry, resulting in leads and investigations being opened, the development of existing investigations, or the successful conclusion of an investigation.[665]

410. Action is being taken to provide advice on the risks presented by certain types of engagement or approaches from Chinese actors. One such initiative – Project CONISTON[666] – was an awareness-raising campaign run by CPNI that highlighted the use of social media by hostile actors to target and recruit UK nationals working in HMG and Industry. During the campaign, CPNI released information about an investigation to allow Industry partners to assess their level of exposure and set up groups (***) to allow Industry partners to share the results of their internal investigations.

411. There is some indication that the message is getting out to the right places. MI5 told us that:

> *awareness is growing, but it's not yet as fully embedded in the sort of UK bloodstream as it will need to be in the years to come. So we do these days receive more proactive tip-offs from people who have realised that they have received some kind of approach, whereas ten years ago more often we were noticing first and then alerting the individual or company involved.*
>
> *...* [the] *balance is shifting through good work done in lots of places over the last decade or so, and I think the ... public discourse around things like Huawei and 5G, Hong Kong and so forth is ... raising wider awareness within the business community that they need to be quite thoughtful about the risks they may be exposed to; and then on particular things like the 'Think Before You Link' campaign that we've run, that has*

[662] Written evidence – GCHQ, 31 January 2022.
[663] Written evidence – HMG, 18 April 2019.
[664] Written evidence – HMG, 18 April 2019.
[665] Written evidence – HMG, 18 April 2019.
[666] In some instances in this Report, we have substituted an ISC-specific code word where it has been necessary to refer to the name of an operation or project, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to real operation names. The ISC code words have no operational significance.

successfully ... generated more awareness and more leads for us to pursue into possible intelligence activity.[667]

412. CPNI also briefs Industry where intelligence indicates there is specific Chinese intent to target certain companies or sectors. For example, NCSC worked with CPNI to assess security practices at a *** site. This involved a comprehensive review of site risks ***. As a result, additional measures were put in place at the site. However, given the wide range of individuals, assets and organisations, it is clearly difficult to detect and disrupt every incident.

DI

413. DI also provides briefings to industry and government partners where it has information and expertise to share. CDI told the Committee that DI provides focused intelligence briefings to elements of the defence industry in order to ensure that they understand the level of threat posed to them, and also to provide oversight and assurance "*to ensure that they're adopting the appropriate security protocols to protect themselves*".[668]

414. In addition, DI provides security advice to Defence Equipment & Support (DE&S), a part of MoD that provides security accreditation for defence contractors and controls access of foreign nationals to UK defence industry sites through the International Visits Control Office (IVCO).[669]

Disrupting activity

MI5

415. In September 2020, MI5 told the Committee that "*in line with HMG policy, we are now seeking to identify where MI5 can add further value to defend our economic resilience*".[670] Director General MI5 described this as "*widening the aperture*", a process he said was necessary given "*Chinese investments in our economy are as much of a threat as Intellectual Property stolen across a cyber domain or by a spy*".[671]

416. In addition to providing support to the Government's investment security processes through the aforementioned joint CPNI and NCSC team, and providing advice to Industry, MI5 also has a key role in disrupting the most acute economic espionage threats from China. In relation to IP and data theft, MI5 say it focuses on: ***.[672]

417. Under current UK law, it is not a criminal offence to be an agent of a foreign intelligence service, and, as such, prosecution of suspected Chinese spies committing economic espionage in the UK is rarely possible. While the Government has committed to bringing in new legislation to rectify this,[673] and MI5 has supported the introduction of a specific 'economic espionage offence', at present MI5 has to rely on a range of non-legislative tools

[667] Oral evidence – MI5, *** December 2020.
[668] Oral evidence – DI, *** December 2020.
[669] Written evidence – HMG, 18 April 2019.
[670] Written evidence – MI5, 24 September 2020.
[671] Oral evidence – MI5, *** October 2020.
[672] Written evidence – HMG, 18 April 2019.
[673] The National Security Bill was subsequently introduced to Parliament on 11 May 2022 (after the Committee had concluded taking evidence for this Inquiry).

to effect disruptions; in practice, many of these are the same as for other forms of espionage. These sit under a range of HMG tools, which are outlined earlier in this Report, and include:

- interviews: there may be a discussion arranged with an individual ***;
- the removal of security clearance from British nationals with access to sensitive information who pose a national security risk, including those who may have been in contact with foreign intelligence services (***);
- the lawful expulsion of intelligence officers should they be found to engage in activities contrary to the UK national interest;
- the issuing of MI5 'Espionage Alerts' to affected industries and foreign partners, to increase awareness of the activities of suspected intelligence officers[674]; and
- visa action: as is standard, the Home Office can consider revoking a visa on the grounds that someone's presence in the UK is 'not conducive to the public good' (***); and official reprimands, under which a warning is conveyed to foreign liaison officers regarding the activities of foreign intelligence services.

Interviews

A British national *** was determined to have been in contact with the Chinese Intelligence Services (ChIS) for a number of years. The individual had travelled to China frequently *** and had offered to talent-spot other experts on behalf of the ChIS. HMG carried out an interview with the individual at the end of 2018 ***.[675]

GCHQ

418. GCHQ engages in cyber operations that expose and disrupt the activities of Chinese state-sponsored hackers. This acts both as a 'tactical' tool, in that it counters individual groups, and 'strategic', in that it has the potential to undermine the credibility of such groups within China – with ramifications for China's credibility as a state actor ostensibly opposed to cyber operations. The Intelligence Community have noted that they have dedicated significant effort to identifying and building knowledge of the Chinese cyber actors ***. ***. The naming of APT10 in December 2018 is a key result of this Intelligence Community effort.

DI

419. In 2020, DI told the Committee that it provides Analysis & Assessment to MoD and HMG partners (such as CPNI, JSTAT and the ISG) and policy-makers on the threat to the UK defence industry from China. In one such example, DI provided assessment on a case that allowed the (then) Secretary of State for BEIS to intervene in the acquisition of a British company (***) by a Chinese-owned company (***). A public interest intervention notice was issued under the Enterprise Act 2002, meaning that the transaction was subject to a

[674] As was issued by MI5 in January 2022 in the case of Christine Lee.
[675] Written evidence – HMG, 18 April 2019.

report by the Competition and Markets Authority, and leading to the Chinese-owned company withdrawing from the purchase.[676]

420. CDI further explained the role that DI and its partners play in ensuring the physical security of both MoD and industry sites:

> *We'll also ***, often in conjunction with MI5 and other partners, to ensure that we test the security and efficacy of both our own facilities but also part of the commercial facilities as well ***.*[677]

421. DI also plays a role within the National Cyber Force (alongside wider MoD personnel, GCHQ and SIS). The Agencies told us that "*the National Cyber Force (NCF) … is expected to deliver a step change in the nation's cyber capability, and enhance the UK's position and reputation as a top-tier cyber power. The growth of the NCF will make increased* [offensive cyber] *capacity available*".[678] The Agencies noted that:

> *Since the NCF was stood up, on China specifically* ***[679]

FFF. The threat posed by Chinese targeting of experts in UK Industry is of concern. While the expulsion of intelligence officers and the disruption of Chinese efforts are to be commended, the lack of prosecutions is worrying. We note that the Government is intending to introduce new legislation that will make it easier to prosecute such behaviour. Convictions under such new legislation would act as a strong deterrent to those contemplating engaging in such relationships.

[676] Written evidence – DI, 31 July 2020.
[677] Oral evidence – DI, *** December 2020.
[678] Written evidence – GCHQ, SIS and MI5, 21 May 2020.
[679] Written evidence – GCHQ, SIS and MI5, 21 May 2020.

CASE STUDY: CIVIL NUCLEAR ENERGY

CHINESE INTEREST AND INVESTMENTS

422. In addition to the overarching threat to UK Industry from China's attempts to gain economically from the UK, and to ensure that the UK becomes increasingly reliant on China, as part of this Inquiry we also considered the specific case of the Civil Nuclear and Energy sectors in terms of the UK's Critical National Infrastructure (CNI).

Critical National Infrastructure

The Government defines Critical National Infrastructure (CNI) as:

> *Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*
>
> - *major detrimental impact on the availability, integrity or delivery, of essential services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic and social impacts; and/or*
> - *significant impact on national security, national defence, or the functioning of the state.*[680]
>
> There are 13 areas of CNI in the UK, including the separately designated 'Civil Nuclear' and 'Energy' sectors.[681]

423. The importance of these parts of the UK's CNI is clear: energy is essential – described by one witness as the "*über CNI*", on the basis that "*all other CNI requires an energy source*".[682]

424. In terms of energy sources, the Government announced in the 2021 Integrated Review that its "*aim is to become the world's leading centre for green technology, finance and wind energy*".[683] The Government has also set a target of 'net zero' for carbon emissions by 2050, and will scale up renewable energy while scaling down coal and gas power stations. Nevertheless, successive Governments have backed nuclear power as a long-term source of

[680] Centre for the Protection of National Infrastructure (CPNI) website.
[681] The remaining 11 sectors are: Chemicals, Defence, Emergency Services, Finance, Food, Government, Health, Space, Telecommunications, Transport and Water.
[682] Oral evidence – GCHQ, *** October 2020.
[683] *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy* (the 'Integrated Review') was published on 16 March 2021 and sets out the Government's vision of the UK's role in the world. It contains a number of actions which the Government commits to taking in support of that view. A refresh of the initial Integrated Review was later published on 13 March 2023 (after evidence-taking for this Inquiry had concluded).

electricity production:[684] it is set to continue to be "*a key part of the energy mix*", accounting for approximately 17% of the UK's energy supply.[685]

425. However, the UK's stock of 15 Civil Nuclear reactors is ageing, with 14 of them expected to be shut down by 2030. The Government therefore needs to replace reactors as they are decommissioned – and this is where Chinese investment is focused. That investment has come under increased scrutiny amid rising concern, given the clear security risks in this sector, which the National Security Secretariat (NSS) summarised as:

> [the] *unique hazards which the dispersal (either malevolent or accidental) of nuclear and radiological material present; the specific international obligations* [the Government has] *to protect nuclear material and uranium enrichment technology to reduce the risks of nuclear proliferation; and* [the fact that] *the Civil Nuclear sector includes a range of services beyond electricity generation – notably decommissioning, enrichment/fuel fabrication, and specialist rail/maritime transport, none of which have direct parallels in the Energy sector.*[686]

Given these factors, we focused our scrutiny on a case study of the Civil Nuclear sector.

China's interest in the UK Civil Nuclear sector

426. Foreign Direct Investment (FDI) in the UK's Civil Nuclear sector is not unusual: the UK's current 15 reactors were all acquired by French company EDF in 2009. However, China has shown a particular interest in five Civil Nuclear power sites, which are at various stages of development: Hinkley Point, Sizewell, Bradwell, Moorside and Wylfa. Chinese investment plans are spearheaded by the China General Nuclear Power Group (CGN), a major state-owned energy company. CGN is one of around 100 strategic state-owned enterprises managed by the State-Owned Assets Supervision and Administration Commission of the State Council (SASAC), and as such is closely and – unlike other Chinese-based companies such as Huawei, AliBaba or TenCent – explicitly linked to the Chinese state.[687]

427. China intends to source approximately 20% of its primary energy consumption from non-fossil fuels by 2030. While China's indigenous expertise is clearly growing, they still require foreign expertise to supplement innovation and translate technology into capability, and therefore use their investment in the Civil Nuclear sector both to gain Intellectual Property (IP) and improve their own nuclear capabilities ***.[688] ***.[689]

428. However, this accounts for only part of its interest in the UK Civil Nuclear sector. As we have explored in Part One of the Report, China is seeking economic advantage in its quest to become a global superpower. It appears that China regards Civil Nuclear power as

[684] 'Briefing Paper: New Nuclear Power', House of Commons Library, 29 July 2020.
[685] Department for Business, Energy and Industrial Strategy, *Digest of United Kingdom Energy Statistics 2020*, 30 July 2020. The UK's nuclear energy output was reduced in 2019 due to a series of prolonged outages at two nuclear plants (Dungeness B and Hunterston B). In 2018, nuclear power accounted for 20% of UK electricity supply.
[686] Written evidence – Cabinet Office, 3 September 2019.
[687] In 2016, the European Commission found that CGN could not be considered to be independent of SASAC. 'RPT-Chinese state-owned companies face greater scrutiny of EU deals after ruling', Reuters, 13 June 2016.
[688] Written evidence – ***, *** October 2020.
[689] Written evidence – ***, *** December 2018.

a key industry that will support economic growth. Its interest in the UK's new reactors is therefore underpinned by a strategic gambit, as the Joint Intelligence Committee (JIC) assessed ***:

> ***. *China also wants to become a global Civil Nuclear supplier.*
>
> *For China, the proposed investment in the UK nuclear industry is intended to provide expertise, experience and credibility to support the export of nuclear technology and services.*[690]

429. In its bid to become a global supplier, China is looking to capitalise on the UK's international leadership position: China sees UK regulatory approval as a valuable 'test bed' for proving Chinese technology for export to other Western markets. The Chief Operating Officer of China General Nuclear UK – the main Chinese investor in the Civil Nuclear sector – has said: "*For us, the UK is an important stepping stone into Europe. The* [UK's regulatory] *process is recognised in the nuclear world as having a lot of clout*." [691] Since this Inquiry concluded, the Office for Nuclear Regulation (ONR) has approved CGN's design for its Hualong One reactor[692] (although local permissions would still need to be sought before it could be built in the UK).

Chinese investments

Hinkley Point C (financing)

430. Two new reactors at Hinkley Point – the first to be constructed in the UK for over 20 years – are due to enter service in 2027 and will, together, produce 7% of the UK's total electricity. The site is being developed by EDF, the eventual operators; however, the Government announced in September 2015 that CGN would be investing in the project and providing construction engineers. This decision was reviewed in September 2016 and approved. As a result, CGN owns a 33.5% stake in the site.

Bradwell B (financing, building and operating)

431. Bradwell B in Essex would be the first nuclear reactor in the UK to employ Chinese nuclear technology. As noted previously, CGN has been explicit about its desire to use the UK as a springboard for exporting Chinese nuclear technology to other countries, with approval by the UK's robust nuclear regulatory regime seen as being key to this.[693] Under a deal agreed in October 2015, CGN will own a 66.5% share in the project to build the new reactors – with EDF owning the remainder.

432. While it is assumed that CGN will operate the Bradwell reactors once completed, it has been reported that CGN may be willing to consider "*not being the majority operator*", due to "*political and local sensitivities*".[694] In September 2020, the BBC reported Industry and Government sources saying that the CGN plan to build its own reactor at Bradwell

[690] Written evidence – JIO, 24 August 2016.
[691] 'China's long game to dominate nuclear power relies on the UK', *The Guardian*, 26 July 2018.
[692] Also known as the UK HPR1000.
[693] 'China's long game to dominate nuclear power relies on the UK', *The Guardian*, 26 July 2018.
[694] 'Chinese willing to hand over control of UK nuclear plant', *Financial Times*, 18 September 2018.

"*looks dead*", given revived security concerns and deteriorating diplomatic relations following the Government's decision to ban Huawei from the UK's mobile telecommunications networks.[695] The question of operation is considered in the next section, on linked investments.

Sizewell C (financing)

433. As part of the Bradwell agreement, CGN also agreed to provide 20% of the capital for EDF's planned reactor at Sizewell in Suffolk, which is intended to be a 'clone' of Hinkley Point C.[696] It was reported in the media in September 2020 that the Government is looking at options to replace CGN as an investor in Sizewell C. One of these options would involve the Government taking a stake in the plant itself, in an attempt to accelerate the approvals process for the plant.[697] The (then) Energy Minister, the Rt Hon. Kwasi Kwarteng MP, later confirmed that the Government is considering taking equity stakes in future nuclear plants, including Sizewell C.[698]

Possible investment at Moorside (unconfirmed)

434. Japanese company Toshiba had planned to build three reactors at the Moorside site near Sellafield in Cumbria through its NuGen subsidiary, but – due to its own concerns about the project's financial viability – began winding up its UK nuclear business in January 2019 after failing to find a buyer to take on the project.[699]

435. In 2017, CGN had attempted to buy NuGen and its Moorside project from Toshiba, but lost out to a South Korean energy firm (the South Korean deal subsequently fell through).[700] Following the November 2018 announcement that Toshiba was going to wind up NuGen, it was reported that CGN was still interested in the project, but that there were reservations within the Government about allowing CGN to gain a further foothold in the UK Civil Nuclear sector.[701] The potential CGN investment at Moorside was scrutinised by the Government in 2017 for national security risks.

436. In July 2020, it was announced that EDF is part of a 15 company-strong consortium which has entered a bid to build a nuclear reactor at Moorside "*similar to Hinkley Point C*". There has been no indication as to whether CGN will have any investment in this new reactor.[702]

Possible investment at Wylfa (unconfirmed)

437. It has been reported by the media that CGN is interested in buying the Horizon nuclear project at Wylfa on Anglesey. The project's owners, Hitachi, withdrew from the scheme in September 2020, having failed to reach agreement with the Government about funding

[695] 'UK government could take stake in Sizewell nuclear power station', BBC News, 16 September 2020.
[696] 'China's long game to dominate nuclear power relies on the UK', *The Guardian*, 26 July 2018.
[697] 'UK government could take stake in Sizewell nuclear power station', BBC News, 16 September 2020.
[698] 'Government considers taking equity stakes in nuclear plants', *The Times*, 6 October 2020.
[699] 'Toshiba's UK withdrawal puts Cumbria nuclear plant in doubt', BBC News, 8 November 2018.
[700] 'Korean energy firm rescues UK's Moorside nuclear power project', *The Guardian*, 6 December 2017.
[701] 'UK close to ditching plan for Cumbria nuclear plant', *Financial Times*, 9 November 2018.
[702] 'Clean energy hub proposes nuclear development for Moorside', *Nuclear Engineering International*, July 2020.

arrangements.[703] In June 2020, Hitachi said: "*We are not aware of any plans to sell the project to China*."[704]

Linked investments

438. The Government announced CGN's investment in Hinkley Point C in September 2015, although that decision was reviewed in September 2016. In January 2017, we were told by the Chief Executive Officer (CEO) of the National Cyber Security Centre (NCSC) that the 2016 review was not prompted by the Intelligence Community, although they did contribute to the review.[705]

439. As part of the 2016 review, NSS co-ordinated an assessment of the potential national security risks from Chinese investment in the UK's Civil Nuclear sector and identified espionage, leverage and disruption as the potential risks.[706] However, the Cabinet Office explained that in 're-approving' the deal in 2016 "*an important consideration was that China's involvement in* [Hinkley Point C] *consists of financial investment in the project only: the French company EDF will own the majority share and will have sole operational control of the site*".[707]

440. This point was reiterated by Director GCHQ in January 2017, when he told the Committee: "*ownership and sovereignty are much less of an issue than operational control ... in the modern world frankly ownership of companies is pretty fluid and pretty complex. Much more important to us is the hardware but also the operational control and the control of the information and that's where we are engaged*."[708] In December 2016, (then) Director General MI5 seemed similarly content with the approval, telling the Committee:

> *One of the really well-functioning bits of structure we have in Government these days is the fact that there is an NSC* [National Security Council] *that takes all of these big questions and the Agencies' Heads are there as well as the key Ministers, so questions like this get dealt with collectively ... We went through* [the risks of espionage, leverage and disruption] *as you would expect ... and an informed decision was made.*[709]

441. Nevertheless, Chinese entry into the UK Civil Nuclear sector appears to be being managed under a policy known as 'progressive entry', whereby CGN has to demonstrate it can be a trustworthy and regulation-compliant partner. The Chairman of the UK's Nuclear Industry Association was quoted in the *Financial Times*, explaining:

> *Progressive entry can be viewed as a sort of trade; if you do X we will give you Y ... CGN had to back Hinkley, which they have done, and put up some of the capital for the follow-up EDF plant at Sizewell, which they have indicated they are willing to do* [in

[703] 'Nuclear: Hitachi "withdraws" from £20bn Wylfa project', BBC News, 15 September 2020.
[704] 'Wylfa nuclear project: Donald Trump plea over site sale dismissed', BBC News, 28 June 2020.
[705] Oral evidence – GCHQ, *** January 2017.
[706] ***
[707] Written evidence – Cabinet Office, 31 October 2016.
[708] Oral evidence – GCHQ, *** January 2017.
[709] Oral evidence – MI5, *** December 2016.

> order to secure agreement for a Chinese reactor at Bradwell] ... *That's a pretty major commitment.*[710]

442. This notion of a link between the different investments is significant: Chinese investment in Hinkley Point would appear to be predicated on an understanding that they would subsequently receive permission to use their own technology at Bradwell – i.e. Bradwell is the key, and if Bradwell was not able to proceed for some reason then they may not be interested in Hinkley Point. ***.[711]

443. While the Intelligence Community's argument that ownership is not the primary concern may be persuasive with regard to the Hinkley Point C decision, it seriously undermines the case for allowing Chinese involvement in Bradwell B, where – as things stand – a Chinese company will exercise operational control over a Chinese-designed reactor. Using the fact that Hinkley Point C will be operated by a French company as a justification for allowing Chinese involvement was obfuscatory, as it is clear from the Government's own evidence that China considers the Hinkley Point C and Bradwell B investments to be directly linked. The Government was therefore entering into an agreement on Hinkley Point C in the clear knowledge that it was – diplomatically and politically – entering into an agreement on allowing the use of Chinese technology, and the exercise of Chinese operational control, at Bradwell B (subject to further regulatory requirements being met by the Chinese).

444. It has also been suggested that this apparent quid pro quo could bind the Government legally into approving CGN's plans for Bradwell B, due to the legal principle of 'legitimate expectation' – under which the investment of large sums on the basis of a Government understanding can be taken to be an enforceable contract.[712] We questioned the Deputy National Security Adviser (DNSA) on the extent to which these factors were considered by Government when approving Chinese investment in Hinkley Point C:

> *STEWART HOSIE: ... why was there no mention of Bradwell or the security risks involved in Chinese operation in the October 2016 Cabinet Office note on Hinkley Point, even though the Government consistently assessed at the time that China viewed its assessment in Hinkley as being linked to Bradwell?*
>
> *DEPUTY NATIONAL SECURITY ADVISER: So to be clear, there has been no investment security process in relation to Bradwell. The investment security process was purely related to the Hinkley C question. So we have not taken a judgement on that.*
>
> *STEWART HOSIE: I understand there has been no investigation potentially into Bradwell; the question was why was there no reference to Bradwell in the Hinkley C report, given that the Government assessed in the Chinese mind these two things were inexorably linked?*

[710] 'UK's reliance on China's nuclear tech poses test for policymakers', *Financial Times*, 14 February 2019.
[711] Written evidence – HMG, 24 August 2016.
[712] 'UK's reliance on China's nuclear tech poses test for policymakers', *Financial Times*, 14 February 2019.

> *DEPUTY NATIONAL SECURITY ADVISER: Because the process that we used through the Investment Security Group is intended on a case-by-case basis to look at individual Foreign Direct Investments into the UK. That is not to say that the broader questions were not discussed or were not part of the equation. As I say, I have not seen the minutes of the* [NSC] *discussion from that time but certainly the advice that we gave as intelligence professionals and security professionals was on the basis of the Hinkley project.*[713]

This is astonishing. If correct, then it raises very serious questions as to the basis on which the Government is allowing foreign companies into our CNI – and shows that lessons have not been learned.

445. Numerous sources indicate that China's investment in Bradwell B is contingent on its investment in Hinkley Point C. Furthermore, this assessment was available to Government in 2016 when investment in Hinkley Point C was being considered. We would have expected this information to have been a principal factor in the Government's decision-making process. However, the omission of any reference to it in the 2016 Cabinet Office note suggests otherwise.

446. We asked why the linked investment had not been highlighted to Ministers and were told that there had been no investment security process undertaken in relation to Bradwell B and that each case was looked at on its own merits.[714] We then requested sight of the NSC minutes on the Hinkley Point C decision to ascertain whether the linked investment in Bradwell was discussed. The (then) Prime Minister refused to provide these, on the grounds of Cabinet collective responsibility.[715]

447. Our concerns on this matter are grounded in experience: in 2013 this Committee held an Inquiry into the decision to allow BT to purchase Huawei telecommunications equipment. The Committee concluded:

> *The Committee's investigation into the handling of the BT/Huawei case highlights a number of weaknesses in the UK's approach to investment in the Critical National Infrastructure (CNI). The Government's duty to protect the safety and security of its citizens should not be compromised by fears of financial consequences, or lack of appropriate protocols. However, a lack of clarity around procedures, responsibility and powers means that national security issues risked, and continue to risk, being overlooked.*
>
> *The BT/Huawei relationship began nearly ten years ago; the process for considering national security issues at that time was insufficiently robust. The Committee was shocked that officials chose not to inform, let alone consult, Ministers on such an issue.*[716]

It appears that, by 2016, the Government had still failed to take action, and that security decisions were still being compromised in a way that leaves the UK at risk.

---

[713] Oral evidence – NSS, *** October 2020.
[714] Oral evidence – NSS, *** October 2020.
[715] Letter to the ISC Director from the Private Secretary to the Prime Minister, 30 April 2021.
[716] *Foreign involvement in the Critical National Infrastructure*, Cm 8629, 6 June 2013.

GGG. The scale of investments by the China General Nuclear Power Group in the UK Civil Nuclear sector – and its willingness to undergo expensive and lengthy regulatory approval processes – demonstrates China's determination to become a permanent and significant player in the UK Civil Nuclear sector, as a stepping stone in its bid to become a global supplier. Involvement will provide China with an opportunity to develop its expertise and gain both experience and credibility as a partner.

HHH. The question is to what extent the Government is prepared to let China invest in such a sensitive sector, for the sake of investment, and whether the security risks have been clearly communicated to Ministers – and understood. The Government would be naïve to assume that allowing Chinese companies to exert influence over the UK's Civil Nuclear and Energy sectors is not ceding control to the Chinese Communist Party.

III. Using the fact that Hinkley Point C will be operated by a French company as justification for allowing Chinese involvement was obfuscatory: the Government clearly knew that that decision would lead to it allowing the use of Chinese technology and Chinese operational control at Bradwell B. It is astonishing that the investment security process for Hinkley Point C did not therefore take Bradwell B into account. It is unacceptable for the Government still to be considering Chinese involvement in the UK's Critical National Infrastructure (CNI) at a granular level, taking each case individually and without regard for the wider security risk. It is imperative that linked investments are considered in the round and that Ministers are consulted on the cumulative security risk brought by linked Chinese investments. Effective Ministerial oversight in this area is still lacking, more than eight years on from the Committee's Report on the national security implications of foreign involvement in the UK's CNI.

ESPIONAGE AND INFLUENCE

Espionage: Incentive and opportunity

448. China is interested in the UK Civil Nuclear sector because it offers it the chance to develop its expertise, experience and credibility in the industry, both for domestic and international gain. As previously noted, it will use overt channels in service of these goals, such as exploitation of UK Academia, technology transfer (including via manufacturing license agreements with UK companies), joint ventures, and FDI (including purchasing specialist manufacturers). According to HMG assessment, methods such as these may also be "*providing China with *** access to manufacturing and tooling expertise and knowledge*".[717]

449. However, China's involvement also provides it with both incentive and opportunity for espionage. There have been public allegations of systemic espionage and theft of commercially valuable information from the UK and other countries,[718] and charges that this has enabled China to simply re-engineer technology developed by others. These are concerns that should be taken seriously ***. In terms of incentive, *** the JIC assessed:

> *The implementation of China's strategy of becoming a global Civil Nuclear supplier, including investment in the UK* ***.[719]

***[720] ***.[721]

450. In terms of opportunity, the UK Intelligence Community made clear that "*Chinese espionage does not depend on inward investment*". They noted that:

> *the access generated by or through China General Nuclear (CGN) personnel involved in Hinkley Point C (HPC) and Sizewell C (SZC) *** overt and espionage activities.*[722]

Nevertheless, China appears to be willing and able to conduct espionage through its investments in CNI, including in the Civil Nuclear sector – we note for instance the Federal Bureau of Investigation (FBI) indictment of CGN in 2016, addressed in the case study of Allen Ho later in this section ***.[723]

451. There is little doubt that the Chinese state is willing to use intelligence collection to give state-owned enterprises such as CGN a commercial edge, and it is unlikely that CGN is merely a beneficiary of such intelligence; it is believed that ***. Chinese businesses are required to maintain a symbiotic relationship with the Chinese state, as MI5 noted:

---

[717] Written evidence – HMG, October 2020.
[718] For example, 'Chinese Hinkley backer is accused of espionage', *The Times*, 11 August 2016; and 'Nuclear espionage charge for China firm with one-third stake in UK's Hinkley Point', *The Guardian*, 11 August 2016.
[719] Written evidence – JIO, 24 August 2016.
[720] Written evidence – JIO, 27 October 2017.
[721] Written evidence – HMG, 18 April 2019.
[722] Written evidence – JSTAT, October 2020.
[723] ***

> *There is no ability … to be a big enterprise in China without complete interdependency with the state, and you will have seen that a lot in the kind of conversation around Huawei.*
>
> *So in terms of state control, state influence, state ability to use any bit of industry, to deliver a wider state ambition, that is as true of Chinese* [General] *Nuclear as it is of any other large organisation in China.*[724]

452. While Chinese investment in Hinkley Point C might open the door for the UK to allow CGN to build and operate, Bradwell B would be opening a direct channel from the UK nuclear enterprise to the Chinese state. MI5 explained:

> *There is a Chinese state law around sharing data with the state, and that applies to all industries and all organisations. ***. There are expectations around sharing of expertise; so if you have got a particular individual in your industry who is developing a capability that the state is interested in, particularly for dual use, *** there would be an expectation of sharing.*[725]

JJJ. We have serious concerns about the incentive and opportunity for espionage that Chinese involvement in the UK's Civil Nuclear sector provides. Investment in Hinkley Point C opened the door, but for the UK to allow the China General Nuclear Power Group to build and operate Bradwell B would be opening a direct channel from the UK nuclear enterprise to the Chinese state.

Cover, contacts and access

453. China is unlikely to glean commercially valuable information directly from its investments, but Chinese involvement in the sector inevitably increases the risk of espionage by providing legitimate cover for Chinese nationals whose primary role may be to conduct espionage activity (either against the Civil Nuclear sector in particular, or UK targets more broadly)[726] and access to facilities and Intellectual Property (IP) that may not otherwise have been available.[727]

454. As noted above, CGN, as a state-owned enterprise, is ***.[728] ***.[729]

455. MI5 noted that there had been instances *** where employees in the Civil Nuclear sector had conducted espionage (the Allen Ho case study below is one such example), and we questioned witnesses as to whether such cases had been seen in the UK. They stated that ***.[730] MI5 explained that experts are cultivated in all fields:

> *That can start from university … how to look at the right university students and what subjects they are studying.*

[724] Oral evidence – MI5, *** October 2020.
[725] Oral evidence – MI5, *** October 2020.
[726] Written evidence – HMG, 18 April 2019.
[727] Written evidence – JIO, 27 October 2017.
[728] Written evidence – JSTAT and NCSC, 5 December 2018.
[729] Written evidence – JSTAT, October 2020.
[730] Oral evidence – MI5, *** October 2020.

It goes absolutely into deep expertise … [with] *active LinkedIn campaigns of reaching out to people* ***.

Then [there are] *** *industries of particular interest and concern.*

So it is the full range. ***. *The very focused stuff tends to be going after an individual with particular expertise that is then going to accelerate your build* ***.[731]

Case study: Allen Ho

In 2016, the Federal Bureau of Investigation indicted a naturalised United States (US) citizen, Allen Szuhsiung Ho, and the Chinese state-owned enterprise China General Nuclear (CGN), for conspiracy to engage in the production of special nuclear material in China without authorisation from the US Department of Energy. Ho is now serving a two-year sentence.

Ho, a former employee of US nuclear company Westinghouse, worked at CGN for over 20 years. By 2004 at the latest, he had moved into a role recruiting consultants with experience in the US nuclear industry for CGN ***.

Later, Ho assisted CGN with its Small Modular Reactor Program, in order to help them produce nuclear small module reactors ***. ***.

Throughout his time working for CGN ***. ***.[732]

456. In 2016, it was anticipated that, by 2020, there would be around 90 CGN personnel split between the Hinkley Point C and Bradwell B projects, with the number for Sizewell C to be determined.[733] While many (if not most) of these members of staff are not expected to be based on site, as we have previously outlined, there is always a degree of risk in granting Chinese nationals legitimate access to these sites. (While not all CGN staff will be Chinese nationals, it is likely that many will be.) The risk in the case of Hinkley Point and Sizewell was explained as arising because the presence of CGN in the sector facilitates access to UK nuclear experts and thereby increases opportunities for espionage.[734] The level of risk at Hinkley Point and Sizewell is therefore described as ***.[735] However, were CGN to construct Bradwell, the risks would presumably be more significant, due to the greater access this would provide into the UK's nuclear industry. ***

***[736]

457. Even though Chinese nationals are unlikely to be granted the level of security clearance necessary for unescorted access to sensitive parts of a nuclear power station, the very fact of

[731] Oral evidence – MI5, *** October 2020.
[732] Written evidence – HMG, 18 April 2019.
[733] Written evidence – CPNI, February 2016.
[734] ***
[735] Written evidence – HMG, 13 November 2020.
[736] Written evidence – HMG, 13 November 2020.

their presence and of their legitimate ***.[737] MI5 noted the Chinese state's ability to use its people, industries and companies to gather information, and said that:

> ***.[738]

458. It is also worth noting that the Civil Nuclear sector will be a user of the Government's Secret-level IT system (known as ROSA), which is explicitly designed to protect against hostile states.[739] Providing an agent of a foreign state with even irregular access to the system could undermine its viability as a tool of secure communications.

459. Nevertheless, witnesses were keen to emphasise that, while the question of physical access to sensitive sites by Chinese nationals is taken seriously, it is more of an issue that might "*provide good media headlines and be an alarming picture*" than is really the case in practice, since "*you really don't need to be present to get the scale of data and have the opportunity*".[740] In October 2020 the DNSA explained that:

> *there will be some forms of threat that physical access will offer greater opportunity for. That said, the nuclear sector is extremely highly regulated and inspected and, as part of the Energy Act, there are a whole set of provisions in there that mean that the site operators have security plans, that they are assured, and they will work with the CPNI* [Centre for the Protection of National Infrastructure] *on the particular kind of insider risks and the specific technical insider risks and get the best professional advice on staff access, everything from pass routines, and we do that for the Energy sector in the same way as we do for other sectors with CNI.*[741]

KKK. While we accept that the risk posed by physical access to Civil Nuclear sites is overshadowed by the vulnerabilities exposed by Chinese investment and operational control, it would be wrong to dismiss the former outright. The Government recognises the risk that a digital back door into the UK's Critical National Infrastructure might create, but the risk posed by the literal back door of human actors with access to sensitive sites should not be dismissed.

Cyber

460. Chinese cyber actors appear to have an interest in, and ability to target, a broad range of international companies and agencies in the Civil Nuclear sector. An assessment *** stated that, "*in the last twelve months* [the Chinese] *have compromised* ***".[742]

461. There also appears to be indications of Chinese cyber attacks targeting UK firms with links to the Civil Nuclear sector. For example, ***.[743] ***.[744]

---

[737] Written evidence – HMG ***, August 2016.
[738] Oral evidence – MI5, *** October 2020.
[739] Written evidence – HMG ***, August 2016.
[740] Oral evidence – HMG, *** October 2020.
[741] Oral evidence – NSS, *** October 2020.
[742] ***
[743] Written evidence – CPNI, 2014.
[744] Written evidence – CPNI, 2014.

462. Such attacks are designed to provide China with – primarily – IP, in order to give it a shortcut on research and development time and costs, thereby giving it an advantage over competitors.[745] It also allows China to identify technologies and IP that could be acquired through legitimate investment.

463. Of potentially greater concern than the power stations themselves are the supply chains. The supply chains for Hinkley Point C and Bradwell B will each involve large numbers of UK companies ***. We questioned witnesses who told us that *** in the supply chains in the Civil Nuclear sector ***. NCSC described ***.[746] The Joint State Threats Assessment Centre (JSTAT) and NCSC assess that ***.[747]

464. NCSC explained that, in conjunction with MI5 ***:

> *** *previously we looked very much at our National Infrastructure in counter-terrorism terms – things you can put bollards around – and that didn't help very well with the logical assets and digital infrastructure that webbed across our infrastructure – you know, how telco* [telecommunications] *is linked to Energy…*
>
> *** *allows us to understand how these things touch – and what that is bringing out, of course* ***

NCSC said that, as a result:

> *we have stood up new capability in this area, *** and will allow Government to target our resource in the areas that reach across sectors in a way that we have not been able to do before.*[748]

LLL. We are reassured that the Intelligence Community have recognised the * vulnerability that potentially lies in the supply chains: effort to protect against cyber attacks must include the supply chains.**

Influence: Leverage and disruption

465. China appears routinely to use its proposed foreign investments for political leverage ***. China's very significant investment in the UK's Civil Nuclear sector would therefore seem to provide it with very significant leverage. However, the Intelligence Community *** assess that China is unlikely explicitly to use those investments to exert leverage over the UK, as doing so may compromise China's wider economic and commercial objectives:[749] the DNSA confirmed that the Intelligence Community have ***.[750]

466. Nevertheless, they acknowledge that "[the application of leverage] *is still possible and over the lifetime of the projects Chinese tactics may change*".[751] We should not therefore be

[745] Oral evidence – NCSC, *** October 2020.
[746] Oral evidence – NCSC, *** October 2020.
[747] Written evidence – JSTAT and NCSC, *** December 2018.
[748] Oral evidence – NCSC, *** October 2020.
[749] Written evidence – JIO, 24 August 2016.
[750] Oral evidence – NSS, *** October 2020.
[751] Written evidence – JIO, 24 August 2016.

blind to the possibility that the Chinese investments in Hinkley Point, Bradwell and Sizewell could be used as political leverage over the UK Government, both on the narrow issue of the Civil Nuclear sector itself, and on broader Chinese issues: first, in the initial stages, as the threat of withholding or withdrawing funding could place the future of a project (and its intended outcome) in jeopardy; and second, once construction has finished and generation begins, by having control of the sites that generate a substantial proportion of the UK's electricity and therefore potentially holding it to ransom.

467. The potential for involvement in one industry to be used as leverage to gain a foothold in another industry can be clearly seen from the Chinese messaging in 2020, when the Chinese Ambassador to the UK told business leaders that a UK decision to ban Huawei could undermine plans for Chinese companies to build nuclear power plants and the HS2 high-speed rail network.[752]

468. There is also a geostrategic concern around the UK becoming reliant on China for the ongoing maintenance of Chinese-built nuclear reactors (particularly given the very long operating life of nuclear reactors). This reliance could give China another 'lever' to apply pressure if diplomatic relations decline in future.[753]

469. It could also be argued that the very fact that China will be able to exert some control over the UK's CNI will complicate the Government's calculations when trying to challenge Chinese behaviour in other areas – for example, in relation to human rights. In other words, it may not be possible to separate the Civil Nuclear sector from wider geopolitical and diplomatic considerations.

470. The Committee asked the Intelligence Community if there had been any indications that China would use its foothold in the Civil Nuclear sector to exert pressure in other areas. We were told that that was a question for the (then) Department for Business, Energy and Industrial Strategy (BEIS) to answer.[754] Unfortunately, the Government has refused to allow this Committee access to BEIS – this is yet another example of the failure of the Fusion Doctrine when it comes to oversight.

471. Part of the concern about the influence and control that Chinese investment in the UK Civil Nuclear sector might secure is around the threat of disruption. Disruption could mean temporarily shutting down a power network (at a localised or even national level) or causing irreparable damage to an energy-production facility, which could result in an energy shortage and/or a greater burden on alternative energy production. Depending on the means used to disrupt an energy-production facility, there could well be an impact on the local environment.

472. During the course of this Inquiry, we were concerned that increased physical access to nuclear power stations could aid the exercise of these capabilities, whether to disrupt energy supply or to cause physical or environmental damage. Physical access to nuclear sites would presumably mean that an individual with the right access might be able to shut the system down. While the degree of disruption would depend on the incident ***.[755] Furthermore, it

[752] 'China threatens to pull plug on new British nuclear plants', *The Times*, 7 June 2020.
[753] 'UK's reliance on China's nuclear tech poses test for policymakers', *Financial Times*, 14 February 2019.
[754] Oral evidence – HMG, *** October 2020.
[755] Written evidence – HMG ***, August 2016.

is recognised that physical access would help facilitate cyber attacks, which could cause disruption. In 2016, a review by a Government 'Red Team' – made up of representatives from *** – assessed that ***. The UK Intelligence Community told the Committee that ***.[756]

473. Witnesses emphasised that a cyber attack is not contingent on having direct access to infrastructure. NCSC noted that, in the cyber world, "*it is no longer something about physical presence, actually there are many different ways you can access this data*".[757] The point was reiterated by MI5, who noted that "*it is much, much, cheaper to sit outside* [it] *with a laptop than it is to buy a nuclear power station*".[758] ***.[759]

474. ***.[760] The long-term nature of Civil Nuclear CNI means that HMG must be alert to the potential for threats to emerge in future if circumstances change ***.[761] Such a threat therefore should not be discounted.

475. In November 2019, an article in *The Telegraph* alleged that there had been an attack against an unspecified UK nuclear facility.[762] We questioned the NCSC, who noted that there was not enough information in the original article to definitively link it to an incident they had dealt with, but stated that "*none* [of the cyber attacks against the UK Civil Nuclear sector] *were deemed to have triggered what the press reports described as a 'security crisis'*".[763]

MMM. While we recognise that the threat of disruption is less likely, the threat of leverage is very real: the fact that China will be able to exert some control over the UK's Critical National Infrastructure will complicate the Government's calculations in its broader approach to China. In other words, it may not be possible to separate the Civil Nuclear sector from wider geopolitical and diplomatic considerations.

The position of the United States

476. As with telecommunications (until the reversal of policy on Huawei), the UK Government appears to be out of step with the United States (US) with regard to the threat of Chinese espionage in relation to the Civil Nuclear sector. According to the *Sunday Times*, the Allen Ho case prompted "*a full-scale review by the US National Security Council, which led to new rules blocking CGN from acquiring American technology*", and the US added CGN to the Entity List[764] in August 2019, thereby barring US companies from selling

[756] Written evidence – HMG, August 2016.
[757] Oral evidence – NCSC, *** October 2020.
[758] Oral evidence – MI5, *** October 2020.
[759] Written evidence – JSTAT and NCSC, *** December 2018.
[760] Written evidence – JSTAT and NCSC, *** December 2018.
[761] Written evidence – JSTAT and NCSC, *** December 2018.
[762] 'Cyber-attack targets UK's nuclear industry', *The Telegraph*, 30 November 2019.
[763] Written evidence – NCSC, 3 December 2020.
[764] The US Entity List is a tool used by the Department of Commerce to restrict the export, re-export and in-country transfer of certain items, listed under the Export Administration Regulations, to entities (individuals, organisations or companies) that are potentially involved in activities that are contrary to the national security or foreign policy interests of the US.

products to them.[765] In August 2021, the Biden Administration restricted US citizens from investing in 59 "*Chinese companies that undermine the security or democratic values of the United States and our allies*", one of which was CGN.[766]

477. While CGN has not – at the time of writing – been the subject of a concerted US diplomatic offensive in quite the same way as Huawei, US officials have publicly warned the UK against dealing with CGN. For instance, *The Times* reported: "*Christopher Ashley Ford, US assistant secretary* [of State] *for international security and non-proliferation, said the UK had been given intelligence showing China General Nuclear transferred technologies from civilian enterprise for military uses*."[767] The *Financial Times* reported in August 2020 that, at a private meeting with MPs in July 2020, the (then) US Secretary of State, Mike Pompeo, raised the subject of CGN's activities in the UK.[768] CGN's interest in Hitachi's Wylfa project has led to objections from the US as well. The *Sunday Times* reported that "*officials from the US State Department ... have heaped pressure on*" the Japanese industrial giant not to sell the project to the Chinese.[769]

478. Somewhat surprisingly, witnesses told this Inquiry in October 2020 that they had not "*had a direct conversation with* [their] *counterpart in the US about CGN*".[770] They noted that their counterparts at the (then) Department for Business, Energy and Industrial Strategy (BEIS) might have engaged in such conversations with US interlocutors but did not appear to know. In October 2020, the DNSA simply said that she "*could well imagine it becoming more of a topic of conversation*".[771] This lack of knowledge, or even interest, is surprising given the JSTAT and NCSC assessment that "*it is likely that increased cooperation with* ***".[772]

479. Witnesses were keen to note that the current discussion on CGN should not be equated with the longstanding concerns over Huawei. ***:

> *it is that there are not the same *** equities in what the UK is doing in its Civil Nuclear, that there are in Huawei and telecoms, which ... is that sort of global web.* ***.[773]

480. The location of the sites in which the Chinese have invested has also proved contentious with the US. It has been reported that US officials have raised concerns with the UK Government about the prospect of CGN taking on the Moorside site, due to the site's proximity to BAE Systems' facility at Barrow-in-Furness (where the UK's nuclear

[765] 'US warning on Chinese nuke plans in Cumbria', *Sunday Times*, 16 December 2018; 'U.S. Blacklists China Nuclear Firms Accused of Aiding Military', Bloomberg, 15 August 2019.
[766] 'Fact Sheet: Executive Order addressing the threat from securities investments that finance certain companies of the People's Republic of China', White House, 3 June 2021.
[767] 'Spy warning on Chinese nuclear company', *The Times*, 25 October 2018.
[768] 'China tensions raise doubts over UK nuclear projects', *Financial Times,* 6 August 2020.
[769] 'Donald Trump warns Hitachi not to sell Anglesey nuclear site to China', *Sunday Times*, 28 June 2020.
[770] Oral evidence – NSS, *** October 2020.
[771] Oral evidence – NSS, *** October 2020.
[772] Written evidence – JSTAT and NCSC, 5 December 2018.
[773] ***

submarines are built; the two sites are 20 miles apart).[774] These are legitimate concerns ***. The JIC concluded that ***.[775]

481. However, even if the UK makes a decision in regards to Chinese investment in nuclear based on its own national security concerns, the Chinese will see it as stemming from US concerns and pressure. In 2020, the JIC assessed:

> *No matter how any* [hypothetical] *action* [opposing a Chinese role at Bradwell] *is presented to China* ***[776]

The non-nuclear Energy Sector

Public attention has focused primarily on the Civil Nuclear sector, as does this Case Study. However, during our inquiry we did consider whether there was a similar threat to UK's non-nuclear Energy sector. In simple terms, the 'Energy' Critical National Infrastructure (CNI) sector comprises all UK infrastructure associated with Energy which is not Civil Nuclear. There are three sub-sectors – electricity, gas and oil.[777]

China's interest in the non-nuclear Energy sector is primarily driven by its huge domestic demand for energy: China alone accounts for 25% of global daily energy consumption; its electricity requirements have quadrupled since 2000; it is the world's biggest consumer and producer of coal, which accounts for three-fifths of its energy use; and it is the world's largest oil importer.[778] However, with severe pollution and environmental damage posing a possible threat to popular support for the Chinese Communist Party (CCP), it has also invested heavily in renewables (with the result that it now has a quarter of the world's solar panels, and a third of the world's wind turbines).[779]

[774] 'US warning on Chinese nuke plans in Cumbria', *Sunday Times*, 16 December 2018.
[775] Written evidence – JIO, 27 October 2017.
[776] Written evidence – JIO, 13 November 2020.
[777] 'CNI Series: Energy (Strategic cyber threat assessment)', NCSC, 2017. The electricity network is made up of assets that generate, transmit and distribute electricity across the UK (for example generation stations, substations, cable tunnels, switching equipment and control rooms managing the network). National Grid, SSE and Scottish Power are responsible for electricity transmission. There are considerable interdependencies between the electricity sector and other critical assets across other CNI sectors (such as telecommunications, finance and transport), meaning that of the Energy sub-sectors, electricity is perhaps the most important. The gas sector comprises assets such as gas platforms, terminals, storage facilities, odourisation plants, pressure reduction and compressor stations, and control rooms managing the network. The downstream gas sector includes 250,000km of pipelines (known as the National Transmission System), and 21m consumers. National Grid is the sole owner and operator for gas transmission, but no longer deals with gas distribution, which is handled by four companies: Northern Gas Networks, SGN, Cadent Gas, and Wales and West Utilities. The oil sector is made up of assets such as oil platforms, terminals, refineries, storage facilities, pumping stations, control rooms managing the network, and transport to the forecourts and airports. Pipelines are also part of the sector; a small number of these are owned by the UK Government, with the rest being owned by oil companies.
[778] 'China's promised energy revolution', *Financial Times*, 20 November 2017.
[779] 'The world is investing less in clean energy', *The Economist*, 5 September 2019.

By contrast with the nuclear sector, there does not appear to be a threat from investment: the wider UK Energy sector is diverse and competitive, and therefore, while there is little information available on the scale of China's investments in the UK Energy sector, the size of the sector means that these will be proportionally less significant. Overall, there is no evidence that China's investments in UK Energy amount to a 'critical mass' of control over the sector that would cause concern.

The primary threat appears to be in relation to Intellectual Property (IP). The Chinese government has a strategic imperative to acquire technology that will enable it to improve and increase its domestic energy production. However, as it is likely that China will remain reliant on imports for much of its energy requirements in the medium term, it also needs to secure its energy supply overseas, including through the direct acquisition of energy assets (such as oil fields). The Deputy National Security Adviser noted that China's principal concern was to "[ensure] *it has got technology to sustain its own energy consumption*".[780]

As a result, the National Cyber Security Centre (NCSC) assesses that China presents a *** cyber espionage threat to the UK Energy sector.[781] *** The UK Intelligence Community assesses ***.[782] Chinese cyber actors have previously targeted the UK Energy sector; in ***, a FTSE 100 energy company, was compromised, with commercially sensitive information stolen.[783]

Despite this threat, in evidence, the NCSC was keen to emphasise the importance of investment to the sector:

> *Chinese interest is live and it is also really good investment. You know, utilities, and our network operators and oil and gas and electricity and smart meters are really good investments in terms of economic terms, and it fulfils the requirements as I said before that Chinese, in building their own energy knowledge, legitimately acquiring IP by buying companies and driving that commercial agenda that we have repeatedly referred to, so it meets the domestic and the economic criteria.*[784]

There have been suspected incidents of hostile reconnaissance by *** at Energy CNI sites ***: we were told ***.[785] ***

***.[786]

[780] Oral evidence – NSS, *** October 2020.
[781] Written evidence – NCSC, 2017.
[782] Written evidence – NCSC, 2017.
[783] Written evidence – GCHQ, 8 May and 26 September 2019.
[784] Oral evidence – NCSC, *** October 2020.
[785] Written evidence – HMG, 18 April 2019.
[786] Oral evidence – MI5, *** October 2020.

In terms of the threat to the Energy sector from disruption, the potential impact of offensive cyber operations can be seen from the 2016 and 2017 attacks on the Ukrainian energy grid, which caused the temporary loss of power to hundreds of thousands of people. Even relatively small-scale disruptions to electricity generation can have significant knock-on effects. For example, when just two British power generators went offline in August 2019 due to a lightning strike, over 1,000 train services were cancelled or delayed, and 1.1m people were left without power for up to 50 minutes.[787] ***.[788]

***.[789] ***.[790]

A lack of diversity in the infrastructure is also an issue. ***. ***.[791] ***.[792] ***.[793]

***.[794]

Chinese cyber actors have also conducted Computer Network Exploitation against UK and international companies *** within the Energy sector ***[795]

***.[796]

NNN. Unlike the Civil Nuclear sector, the Energy sector appears to provide China with less potential for leverage, as it does not have the same long-term reliance issues that we see in the Civil Nuclear sector. Nevertheless, there are concerns in relation to the threat to the Energy sector from economic espionage (particularly in the area of new 'green' energy) and disruption.

[787] 'National Grid blames lightning strike for blackout', *The Guardian*, 20 August 2019; 'National Grid blames lightning strike as it faces Ofgem power cut investigation', Sky News, 20 August 2019.
[788] Written evidence – Cabinet Office, 16 August 2019.
[789] Written evidence – UK Intelligence Community, October 2018.
[790] Written evidence – NCSC, 2017.
[791] Written evidence – NCSC, 2017.
[792] Written evidence – NCSC, 2017.
[793] Written evidence – NCSC, 2017.
[794] Written evidence – NCSC, 2017.
[795] Written evidence – NCSC, 2017.
[796] Written evidence – UK Intelligence Community, October 2018; NCSC, 2017.

482. As previously noted, boosting economic ties with China has been a clear priority for recent Governments, with the Coalition Government, Cameron Government and – to a lesser extent – the May Government all seeking Chinese investment in the UK. This desire is what has driven Government strategy in relation to the Civil Nuclear sector. In 2013 the National Security Council (NSC) decided that there was no bar to Chinese investment in the UK Civil Nuclear sector in principle (including, in time, majority ownership and the use of Chinese technology), provided all regulatory requirements were met.[797]

483. Chinese investments in the sector have been underpinned by several strategic dialogues and agreements. During President Xi Jinping's state visit in 2015, a 'Statement of Cooperation in the field of Civil Nuclear Energy' was signed by the UK and China. This statement confirmed that the UK and China "*welcome investment and participation in each other's nuclear new build programmes*". It specifically welcomed the Hinkley Point C, Sizewell C and Bradwell B proposals, and noted that the successful approval of a Chinese reactor design for use in the UK would "*mark the beginning of a genuine long-term strategic partnership*".[798]

484. The 2015 National Security Strategy stated the Government's wish to "[modernise] *the UK's Energy infrastructure, including by attracting inward investors, with appropriate assessment of any national security risks, and mitigation*" and adds that, "*this approach has resulted in the recent investment by China into the new Hinkley Point C power station, supporting our longer-term Energy security*".[799]

485. The annual UK–China Economic and Financial Dialogue includes specific discussions on energy co-operation: the policy outcomes statement issued following the 2019 dialogue noted that "*both sides attach importance to cooperation in the field of Civil Nuclear energy* ... [and] *recognise the potential for further mutual beneficial commercial partnerships* … [including in the] *nuclear energy supply chain*".[800]

486. However, while the Government has previously emphasised that the UK is open for investment, the high-profile 2020 review of the 2016 Hinkley Point C decision, followed by the decision to ban Huawei from the 5G telecommunications network, mean that national security considerations have risen up the agenda. There have been reports that the Government considers China's involvement in the UK Civil Nuclear sector (particularly in relation to Bradwell B) to be "*politically unpalatable*".[801] It is also noteworthy that no specific reference to Chinese investment in UK nuclear energy was made in the Integrated Review.

[797] 'National security assessment of scenarios of Chinese majority and minority ownership in Hinkley', Department for Energy and Climate Change, July 2015.
[798] 'Statement of Cooperation in the Field of Civil Nuclear Energy 2015', HMG, 21 October 2015.
[799] 'National Security Strategy and Strategic Defence and Security Review 2015', HMG, November 2015.
[800] 'Policy Outcomes of the 10th UK–China Economic and Financial Dialogue', HMG, 17 June 2019. At the time of writing, there was also a separate UK–China Energy Dialogue, co-chaired by the Secretary of State for BEIS along with their Chinese counterpart.
[801] 'UK looks to remove China's CGN from nuclear power project', *Financial Times*, 25 July 2021; 'China's nuclear power firm could be blocked from UK projects', *The Guardian*, 26 July 2021.

Cross-government scrutiny of foreign investment

487. Under the Enterprise Act 2002, the (then) Department for Business, Energy and Industry Strategy (BEIS) was responsible for intervening in mergers and takeovers on national security grounds. However, in 2013, this Committee found that there was a lack of effective scrutiny when Huawei's entry into the UK's telecommunications CNI was under consideration in the early 2000s, and we recommended that security concerns must be factored into any decision on foreign investment in the UK's CNI.[802]

488. In 2016, the Investment Security Group (ISG) was established in the Cabinet Office to formalise consideration of foreign investment in CNI. The DNSA told us that "*really, what that* [establishment of the ISG] *did was provide more resourcing*" and a request "*that BEIS review the legislative powers that underpin the work in this area which has of course since resulted in the National Security and Investment Bill*". In 2019, the process was once again reviewed – the DNSA told us in October 2020 that this was because the caseload was increasing. The result of the review was that:

> *the numbers of people across Whitehall ... doubled ... to deal with the case workload that we were looking at, focused very much on upskilling departments to understand their sectors and have better insights and a larger unit for processing the casework.*[803]

489. The ISG was tasked with assessing the national security implications of foreign investment, and ensuring that Ministers and officials were provided with timely, comprehensive and balanced advice when taking decisions on such investment. Chaired by the DNSA (Intelligence, Security and Resilience), and supported by the Cabinet Office, the ISG comprised Director General- and Director-level representatives from across Whitehall.

490. China represented the single largest country of origin for ISG investigations. However, it became apparent during this Inquiry that the ISG looked at cases individually, rather than examining linked investments and overall impact across the sector. When we questioned why, we were told that the overall security of the sector and China's involvement in it "*is very much a BEIS policy lead*" and that BEIS is accountable for it.[804] It therefore appears that, as a matter of policy, BEIS considered that foreign investment in the Civil Nuclear sector did not need to be looked at in the round, and the ISG simply followed that direction. This is clearly absurd: we question how any department can consider that a foreign country single-handedly running our nuclear power stations should not give pause for thought.

491. This concern was reinforced when, less than six weeks later, we were told that BEIS's lack of security expertise, capabilities and infrastructure was such that the Investment Security Unit (ISU) (the new unit set to take over the work of the ISG following the passage of the National Security Investment Act 2021) had to be "*incubated*" in the Cabinet Office because the Cabinet Office could "*do that kind of intelligence component*" – implying that BEIS couldn't.[805]

---

[802] *Foreign involvement in the Critical National Infrastructure*, Cm 8629.
[803] Oral evidence – NSS, *** October 2020.
[804] Oral evidence – NSS, *** October 2020.
[805] Oral evidence – NSS, *** October 2020.

492. In October 2020, the DNSA explained that "*the reason we haven't sort of chucked it straight over the fence is that we are trying to give BEIS some time to build that capability*".[806] The DNSA went on to say:

> *That doesn't mean it's easy to build that capability, but in key areas, and I think particularly DCMS* [the Department for Digital, Culture, Media and Sport] *and BEIS, we've really got to help them and support them develop the same level of maturity we see in other areas of government, particularly DfT* [the Department for Transport].[807]

In other words, BEIS is responsible for countering the threat emanating from China's involvement in the Energy sector, but, in October 2020, it was readily acknowledged by the DNSA – at the heart of the UK Intelligence Community – that BEIS did not and does not have the expertise, capabilities or infrastructure to do so.[808]

493. Returning to the issue of cumulative threat, in December 2020, we wrote to the BEIS Minister to ask whether the ISU would be able to consider the cumulative effect of investments and were assured that it would be able to do so.[809] We understand this to mean that a situation where there are concerns about linked investments would also be considered. If so, this is a positive change and an improvement on what appears to have happened in the case of Hinkley Point C/Bradwell B.

OOO. We reiterate that foreign investment cases cannot be looked at in isolation and on their own merits. It is absurd that the (then) Department for Business, Energy and Industrial Strategy (BEIS) considered that foreign investment in the Civil Nuclear sector did not need to be looked at in the round: we question how any department can consider that a foreign country single-handedly running our nuclear power stations shouldn't give pause for thought. This clearly demonstrates that BEIS does not have the expertise to be responsible for such sensitive security matters.[810]

PPP. Previous investments in the sector, or the potential for there to be 'legitimate expectation' that an investment in one area ought to facilitate a linked investment, must be taken into account. If the Investment Security Unit fails to do so, then it will be unable to counteract the 'whole-of-state' approach so effectively utilised by China (amongst others).

---

[806] Oral evidence – NSS, *** October 2020.
[807] Oral evidence – NSS, *** October 2020.
[808] We now understand that, as part of the restructure of several government departments in February 2023, the Investment Security Unit (ISU) has returned from BEIS to the Cabinet Office. The Committee has not been in a position during this Inquiry to scrutinise the effectiveness of this transfer, or the reasons behind it. Whilst, in principle, we would have welcomed the move to return the ISU to the Cabinet Office, where the relevant security expertise, capabilities and infrastructure are more likely to be in place, as we have previously noted, unfortunately, effective oversight has not been put in place.
[809] Letter from Minister for Business and Industry to the ISC Chairman, 7 December 2020. (This letter was placed in the Libraries of both Houses and is publicly available).
[810] As previously noted, as part of the restructure of several government departments in February 2023, the Investment Security Unit (ISU) has returned from BEIS to the Cabinet Office. The Committee has not been in a position during this Inquiry to scrutinise the effectiveness of this transfer, or the reasons behind it. In principle, we would have welcomed the move to return the ISU to the Cabinet Office, where the relevant security expertise, capabilities and infrastructure are more likely to be in place. However, as outlined earlier, unfortunately, effective oversight has not been put in place.

Regulation

494. The ONR is an independent regulator established under the Energy Act 2013. It regulates nuclear safety, nuclear security, conventional health and safety on nuclear sites, and the transport of radioactive materials. In addition, the ONR regulates the holders of sensitive nuclear information, which are normally corporate headquarters and supply chain organisations.[811]

495. The Nuclear Installations Act 1965 empowers the ONR to attach to each nuclear site such licence conditions as it considers necessary either in the interests of safety or with respect to the handling, treatment and disposal of nuclear matter. Licence conditions can include requirements for cyber security and resilience.

496. The ONR is responsible for inspections of nuclear sites and for enforcement of the laws and regulations concerning the Civil Nuclear sector, and has the power to prosecute for breaches of relevant legislation in England and Wales, and to recommend prosecution in Scotland. Witnesses noted that these responsibilities can be altered by the Secretary of State:

> *in the Civil Nuclear sector, the regulation covers two areas. That is unplanned radiological release and sensitive nuclear information, and the definition ... of that is anything interesting to an adversary. So that is extremely broad. Therefore it has to be narrowed down by the Secretary of State for BEIS. ... ONR ... have a letter from the Secretary of State for BEIS, who dictate the parameters of what they are to regulate for.*
>
> *So it is within Government's purview, the Secretary of State, to define how broad or how narrow that is. So we work with ONR and with BEIS to articulate the threat and how that is changing, and then they interpret that to regulate.*[812]

497. In the context of Chinese investment in the Civil Nuclear sector, the ONR is responsible for the approvals process for new reactor designs, and is therefore key to China's ambitions to showcase its Hualong One reactor technology at Bradwell. Although the design has been approved from a regulatory point of view, the ONR would also have to approve a nuclear site licence for the Bradwell project.

498. The ONR has a working relationship with the Centre for the Protection of National Infrastructure (CPNI), NCSC and Joint Terrorism Analysis Centre (JTAC) (and the ONR had staff embedded within JTAC until 2021). As the CEO of NCSC explained to us in January 2017:

> [There] *isn't any legislation specifically passed to enforce cybersecurity standards in any* [CNI] *sector ...* [but] *the Office of the Nuclear Regulator has the power to direct that certain standards in the engineering must be adhered to and the* [ONR] *consults us on what* [those standards] *should be in the age of cyber defence and that is, I think, a helpful process.*[813]

---

[811] The ONR does not regulate defence nuclear sites and activities.
[812] Oral evidence – HMG, *** October 2020.
[813] Oral evidence – GCHQ, *** January 2017; HMG answer to Parliamentary Written Question 20270, 17 December 2015.

499. While there is no doubt that the Civil Nuclear sector has a much more robust regulatory framework than other CNI sectors (notably telecommunications), the effectiveness of the ONR in countering threats from Hostile State Activity (HSA) (which might be considered to be part of its overall remit of ensuring safety standards are met) is unclear. For example, the ONR seeks to verify that electronic components used in key systems in nuclear power stations meet the necessary safety standards ***.[814] It appears that their powers are not designed to address espionage, sabotage or leverage by investors. In 2016 the Government Red Team noted that:

> ***.[815]

500. We questioned whether, should the decision be made to allow CGN to build and operate the proposed Hualong One Chinese-designed reactor, a 'cell' (similar to the Huawei Cyber Security Evaluation Centre (HCSEC)[816]) could be introduced to provide security evaluation from within CGN. We were told that such a decision would be taken by the ONR, in conjunction with the (then) Department for Business, Energy and Industrial Strategy (BEIS).[817]

QQQ. The regulation of the Civil Nuclear sector (through the Office of Nuclear Regulation (ONR)) is robust. However, we have not been able to evaluate the effectiveness of the ONR in countering Hostile State Activity – indeed, when we tried to ascertain whether the powers held by the ONR were sufficient to protect national security, witnesses from the Agencies and the Cabinet Office were unable to answer. Given the significant Chinese investment in this sector, we recommend that a review of the ONR's ability to counter Hostile State Activity is undertaken.

RRR. Should the Government allow China General Nuclear Power Group (CGN) to build and operate the proposed Hualong One reactor at Bradwell (or any other UK nuclear power station), we recommend that the Government set up a 'cell' – a 'nuclear' version of the Huawei Cyber Security Evaluation Centre – in order to monitor the technology and its operation and address any perceived risks arising from the involvement of CGN in the UK's Civil Nuclear sector.

Intervention: The 'special share'

501. Following the 2016 review of the Hinkley Point C decision, the Business Secretary announced an agreement in principle, confirmed by an exchange of letters, with EDF. This 'special share' means that the Government would have the legal right to be able to prevent

[814] Written evidence – HMG Red Team, August 2016.
[815] Written evidence – HMG Red Team, August 2016.
[816] The Huawei Cyber Security Evaluation Centre (HCSEC) (commonly referred to as the 'Cell') opened in November 2010 under a set of arrangements between Huawei and HMG to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's Critical National Infrastructure. HCSEC provides security evaluation for a range of products used in the UK telecommunications market. Through HCSEC, the Government is provided with insight into Huawei's UK strategies and product ranges. NCSC, as the national technical authority for information assurance and the lead government operational agency on cyber security, leads for the Government in dealing with HCSEC and with Huawei more generally on technical security matters. (Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2021.)
[817] Oral evidence – NCSC, *** October 2020.

the sale of EDF's controlling stake in Hinkley Point C before the completion of construction. It was further announced that the Government would take a 'special share' in all future nuclear new-build projects, giving the Government the ability to intervene in any proposed sale of more than 15% of shares in a project to another party on grounds of national security.

502. At the time of writing, the Government does not yet hold a special share in the Bradwell B or Sizewell C projects, on the basis that they are pending ONR approval, and so there has not been a formal stakeholder decision to proceed with the projects. NSS informed the Committee that it "*would not expect to seek or secure a special share in advance of ... those decisions*".[818]

503. While a special share may provide some greater powers for the Government, it would not apply retrospectively; in other words, if the sale of shares in a nuclear project from, say, a French company to a Chinese company was allowed by the Government in 2022 (following assessment that the transaction did not pose a national security threat), the 'special share' would not give the Government any means to intervene in 2032 if the assessment of the national security implications had changed by that point.[819]

504. It is of note that the Treasury, under the (then) Chancellor, George Osborne, twice rejected the need for the Government to take a special share in Hinkley Point C. In 2016, the Rt Hon. Sir Ed Davey MP (who, as Secretary of State for Energy and Climate Change, had granted original planning permission for Hinkley Point C in 2013, prior to Chinese involvement) suggested that Mr Osborne had vetoed the idea of a special share because he was "*so keen to send positive signals to the Chinese that he was prepared not to go the extra mile for national security*".[820]

505. For his part, Mr Osborne stated that he had been advised by security experts and civil servants that a special share "*would not add more protection*" because the nuclear industry was already so highly regulated.[821] This accords with advice in a paper circulated by the Department for Energy and Climate Change (the predecessor to BEIS) in 2015, which stated that "*a special share provides only limited protection in that it could only stop a proposed transfer of shares to an entity that was considered to be a security risk at the point of sale ...* [and] *the UK operational regulatory framework is set up to protect against dangerous operations*".[822]

506. In evidence to this Inquiry, the DNSA noted that:

> *there are limitations to special shares. I think it is fair to say that they provide limited assurance in particular circumstances. Regardless of how they are drafted, they are a kind of one-point-in-time instrument and do not reflect the evolving threat of the future.*

[818] Written evidence – Cabinet Office, 22 October 2019.
[819] 'National security assessment of scenarios of Chinese majority and minority ownership in Hinkley', Department for Energy and Climate Change, July 2015.
[820] 'Hinkley Point: George Osborne says new deal is unchanged', BBC News, 16 September 2016.
[821] 'Hinkley Point: George Osborne says new deal is unchanged', BBC News, 16 September 2016.
[822] 'National security assessment of scenarios of Chinese majority and minority ownership in Hinkley', Department for Energy and Climate Change, July 2015.

So I think what they can do is buy you a bit of assurance over a period of time, for example with Hinkley it could have been that ministers chose to take a special share to see them through the construction phase until the Enterprise Act could have been activated, if necessary, on national security grounds.

As it was, I think EDF offered a letter of assurance around ownership up until the point of construction, which meant Ministers were not minded to pursue the special share but could have done, but I think you are right to say they are limited in what they can find. [823]

Advice to Industry

507. Advice to support the protection of the UK's CNI falls to the NCSC, which provides advice and assessments on cyber security, and CPNI, which is the UK's national technical authority for personnel and physical security advice. Around a third of CPNI's work is directed towards countering HSA, with a focus on work which is sector-specific and actor-agnostic.[824]

508. HMG considers that it is impractical and disproportionate to try to detect and disrupt all HSA threats to the UK's CNI. There is therefore a focus on countering threats before they materialise through "*hardening*" HMG and UK Industry (i.e. making UK CNI a hard target) by providing thorough protective security advice for them to follow.[825] CPNI and NCSC expend considerable effort on a proactive approach to briefing and engagement with Industry, as described in the earlier Industry Case Study.

509. Representatives from the UK's Civil Nuclear and Energy sectors have access to dedicated CPNI and NCSC advisers who provide them with guidance and information on how to reduce the threat: CPNI have *** dedicated advisers for Civil Nuclear and Energy ***; NCSC have *** dedicated advisers for Civil Nuclear and *** for Energy.[826] CPNI and NCSC also host regular information exchanges, ***, at which industry representatives can receive HSA threat briefings and mitigation advice.[827]

510. We were told that this element of the UK Intelligence Community's advisory work was in support of BEIS, as the lead Government department – and therefore the key decision-maker – for policy on the Civil Nuclear and Energy sectors.

The Civil Nuclear sector

511. CPNI and NCSC have provided specific advice to the Civil Nuclear sector on insider threats – including the need for robust screening and vetting controls, promoting workforce security awareness and an effective security culture, and ensuring appropriate controls of access to sensitive assets. Given the long lifespan of nuclear reactors, NCSC is conscious that the range of threats may change during that time, and explained:

[823] Oral evidence – NSS, *** October 2020.
[824] Written evidence – HMG, 18 April 2019; no comparable figure was provided for NCSC.
[825] Written evidence – HMG, 18 April 2019.
[826] In its evidence, MI5 explained that CPNI increasingly *** with most of its advice and campaigns applicable to many different CNI sectors ***.
[827] Written evidence – HMG, 18 April 2019.

> *we take an actor agnostic approach to making sure that industry is capable of dealing with any of the threats that it could face in the next decades and thinks about how to build that in now, but also how to ensure resilience over time.*[828]

NCSC explained that its approach is as much about considering the future intentions and capabilities of states like China, as it is about understanding its current capabilities – particularly given that these have already "*changed very dramatically over time*".[829]

512. CPNI and NCSC contributed to an initiative *** intended to increase understanding of the risks posed *** in the nuclear industry and to identify ways to counter the threat. These include providing ongoing oversight and analysis *** in the sector, and supporting enhanced verification and oversight of companies in the nuclear supply chain.[830] We asked about this programme and were told that the focus was not so much about strengthening personnel security controls, but "*about giving us more opportunities to act *** if there is a breach of those processes*".[831]

513. While these 'upstream' efforts to limit the risks from Chinese investment are welcome, they are just the beginning of the process. The Intelligence Community told the Committee that ***.[832] We were told about the process for accreditation and formulation of reactor designs before the sites go live, and MI5 explained the UK Intelligence Community's role within this process:

> ***
>
> *The Office of Nuclear Regulation is* [an] *incredibly detailed and a powerful regulator, so we can define things* ***[833]

SSS. While it is understandable that * – given that Hinkley Point C is still under construction, and the remainder had not been approved at the time of writing – the finished projects must be subject to detailed (and continuing) scrutiny by the Centre for the Protection of National Infrastructure and the Intelligence Community. We expect to be kept informed of the advice provided by the Agencies and key decision timelines.**

Advice to the Energy Sector

The Intelligence Community say that "*the relationship between* CPNI [the Centre for the Protection of National Infrastructure] *and the Energy sector is already mature and the understanding of the overall level of threat is well developed*".[834] Examples of CPNI's work are as follows:

[828] Oral evidence – NCSC, *** October 2020.
[829] Oral evidence – NCSC, *** October 2020.
[830] Written evidence – HMG, 18 April 2019.
[831] Oral evidence – MI5, *** October 2020.
[832] Written evidence – Cabinet Office, 16 August 2019.
[833] ***
[834] Written evidence – HMG, 18 April 2019.

- It carries out a number of tailored briefings and engagements at Energy sector forums, which include a considerable focus on China and the wider HSA threat.[835]
- In response to suspected hostile reconnaissance by *** at Energy CNI sites ***.[836] (This is an example of non-China-specific work which will nonetheless help harden the UK's CNI ***.)

At the time of writing, the National Cyber Security Centre (NCSC) agreed an annual plan of work with the (then) Department for Business, Energy and Industrial Strategy (BEIS) for its support to the Energy sector. Examples of NCSC's work in this area include:

- the provision of technical support to a new Industrial Control System for Electricity Northwest, one of the UK's six electricity distribution companies, serving over 2.4m homes;
- a technical design review of Greenergy's implementation of Fuel-FACS, a piece of software that is used to automate fuel terminal operations (Greenergy supplies up to 35% of the UK's road fuel);
- a review of cyber security improvements at South Hook Liquefied Natural Gas Terminal, a facility that has the capability to supply up to 20% of the UK's gas; and
- a 'deep-dive' consulting exercise with National Grid over changes to the Balancing Mechanism, the system that ensures the UK's electricity supply meets demand.[837]

Non sector-specific initiatives

514. In addition to the specific advice offered to the Civil Nuclear or Energy sectors, there are a number of CPNI/NCSC initiatives that are not sector-specific – for example:

- 'Secure Business' risk management advice for UK companies doing business with hostile states – which is freely available on the CPNI and NCSC websites;
- Project CONISTON, which sought to communicate the Chinese insider threat across Government and Industry[838] (amongst the CONISTON work strands were a series of briefings advising Government departments and UK Industry representatives on how to detect malicious targeting of staff on their networks); and [839]

[835] Written evidence – HMG, 18 April 2019.
[836] Written evidence – HMG, 18 April 2019.
[837] Written evidence – HMG, 18 April 2019.
[838] Written evidence – HMG, 18 April 2019.
[839] Written evidence – HMG, 18 April 2019.

- Cyber Security Information Sharing Partnership, a joint industry and Government initiative set up to exchange cyber threat information in real time, in a secure and confidential manner.[840]

Wider UK Intelligence Community efforts

515. Investigating the broader Chinese threat to science and technology (of which Chinese targeting of the Civil Nuclear and Energy sectors would form a part) is a key priority for MI5 ***. ***.[841] When we asked whether other powers were required to respond to the threat posed, MI5 told us that the forthcoming Counter-State Threat Bill[842] would give it:

> *more teeth than we have at the moment to be able to go after individual recruitments in the same way that the FBI indictment … gives American colleagues. So I think there is a gap there and we are looking for that legislation to help us plug it and that will be very helpful. It will take us away from having to prove OSA* [Official Secrets Act] *links to an ancient piece of legislation.*[843]

516. The Counter-State Threat Bill was subject to a public consultation that closed on 22 July 2021. Our concerns about the slow progress being made on this legislation are set out in Part One of the Report.

***[844]

TTT. Although Chinese involvement in, and control over, UK nuclear power stations is deeply concerning, it offers only a small snapshot of the attempt to gain control over a range of sectors, and technologies, by an increasingly assertive China. The Government should commission an urgent review to examine and report on the extent to which Chinese involvement in the sector should be minimised, if not excluded.

[840] NCSC website.
[841] Written evidence – MI5, 23 October 2019.
[842] Now known as the National Security Bill, which was introduced in Parliament on 11 May 2022 (after evidence-taking had concluded for this Inquiry).
[843] Oral evidence – MI5, *** October 2020.
[844] Written evidence – HMG, 18 April 2019.

ANNEX A: COVID-19

517. On 12 January 2020, the World Health Organization (WHO) announced that a "*2019 novel coronavirus*" had been identified, originating in Wuhan, China, in late 2019. It noted that "*most cases* [of people contracting the virus at the time] *worked at or were handlers and frequent visitors to the Huanan Seafood Wholesale Market*" and that: "*The* [Chinese] *Government reports that there is no clear evidence that the virus passes easily from person to person*."[845]

518. The exact origin of Covid-19[846] remains unknown but heavily speculated upon. Some reports have suggested the virus may have been circulating globally in the latter quarter of 2019. In the absence of conclusive evidence, it is generally accepted that the first cases of the virus were detected in Wuhan, China, in December 2019. From there, it spread first through Asia – most notably Iran – before finding a centre in Europe, initially in Italy and Spain.

519. By the end of January 2020, the WHO had acknowledged significant evidence of human-to-human transmission outside of China and declared a "*Public Health Emergency of International Concern*". On 11 March 2020, the WHO declared Covid-19 a pandemic.[847]

520. The first death from Covid-19 in the UK was, at the time, believed to have been on 5 March 2020, although it is now generally accepted that several deaths in February and January 2020 are plausibly earlier instances. The Government moved the UK into 'lockdown': a period of restrictions from March 2020 which limited social and professional interactions in a bid to contain the virus. Concurrently, the Government heavily pushed for the development of a vaccine – for many, seen as the best way to combat the pandemic. At this point, the worldwide figures stood at 270,000 cases and 11,000 deaths. By 2 April 2020, there were 1m cases of Covid-19 worldwide and, within a fortnight, that figure had doubled.

521. On 8 December 2020, the UK became the first country in the world to begin the process of vaccinating its citizens with a fully clinically approved vaccine. Despite this, at the time of drafting, cases of coronavirus remained carefully monitored in the UK, and international travel remained restricted. At this time, over 6m[848] global deaths have been officially reported, although studies based on excess mortality indicate the true figure could be double that. As of 25 March 2022, 186,094 deaths had been recorded in the UK where Covid-19 was mentioned on the death certificate.[849]

522. The broader consequences of the pandemic – from home-working, to medical development, to international co-operation – have had an impact on the substance and methodology of the work of the UK Intelligence Community. Additionally, the pandemic has awoken in the popular consciousness the nature of the UK's relationship with China.

[845] 'Novel Coronavirus – China', World Health Organization, 12 January 2020.
[846] The virus is known as Severe Acute Respiratory Syndrome Coronavirus 2 or SARS-CoV-2.
[847] 'Timeline of WHO's response to COVID-19', World Health Organization, 29 June 2020.
[848] 'World Health Organization (Covid-19) Dashboard', World Health Organization, 25 March 2022.
[849] 'Coronavirus Dashboard', HMG, 25 March 2022.

523. China's behaviour since the start of the pandemic has also been under the microscope. Questions have been raised as to whether it may have accidentally or deliberately released the virus, and whether it may have exacerbated or exploited the situation for its own gain or to others' detriment.

Investigation of origin

524. Wet markets – where SARS-CoV-2 (the virus which causes Covid-19) is thought to have originated – are found across East Asia and often feature a trade in wild animals including birds, rabbits, bats and snakes, alongside the sale of raw meat. They have long been known as a potential source for the emergence of respiratory diseases.[850]

525. There has been significant scientific consensus that this was a natural outbreak. For example, a group of researchers from the UK, United States (US) and Australia, in a letter to *Nature Medicine* in March 2020, noted that "*our analyses clearly show that SARS-CoV-2 is not a laboratory construct or a purposefully manipulated virus*".[851] In February 2020, a group of public health scientists had written to the medical journal *The Lancet* to "*condemn conspiracy theories that COVID-19 does not have a natural origin*".[852] (Subsequent releases of emails – as a result of a freedom of information request in the US and subsequent Congressional scrutiny – between a number of scientists revealed that one of those who had signed the letter to *The Lancet* had put the chance of Covid-19 being a leak from a laboratory at "*70:30 or 60:40*" two weeks prior, a figure he downgraded to 50:50 several days after his initial judgement. However, when questioned as to why he had signed the letter to *The Lancet* – which took a different stance – he said his view had changed in line with the evidence).[853] In April 2020, US intelligence agencies released a public statement noting: "*The Intelligence Community also concurs with the wide scientific consensus that the COVID-19 virus was not manmade or genetically modified*."[854]

526. Despite this, there has been speculation about the origins of the virus – typically centring on the nearby laboratories in Wuhan that study bat coronaviruses (the Wuhan Institute of Virology, which is a level 4 biosecurity facility – the highest for biocontainment – and the level 2 Wuhan Centre for Disease Control). Senior US figures – including then-President Trump and former Secretary of State Mike Pompeo – have stated that there is "*enormous evidence*"[855] that the virus came from a lab, in direct contradiction of their own intelligence agencies. More broadly, some have suggested possible Chinese complicity or negligence in the origins of the virus (including a former Chief of SIS).[856]

---

[850] 'Wet markets – a continuing source of severe acute respiratory syndrome and influenza?', Webster, R. G., *The Lancet*, 2004;363(9404): 234–236.
[851] 'The proximal origin of SARS-CoV-2', *Nature Medicine*, 17 March 2020.
[852] 'Statement in support of the scientist, public health professionals, and medical professionals of China combatting COVID-19', *The Lancet*, 2020;395(10226): 42–43.
[853] 'Top SAGE adviser admitted lab leak theory was "most likely" origin of COVID in February 2020 but debate was shut down because it could "cause harm to China", bombshell emails reveal', *MailOnline*, 12 January 2022.
[854] 'Intelligence Community Statement on Origins of COVID-19', Office of the Director of National Intelligence, 30 April 2020.
[855] 'Pompeo Ties Coronavirus to China Lab Despite Spy Agencies' Uncertainty', *New York Times*, 7 May 2020.
[856] 'Coronavirus: Former MI6 boss says theory COVID-19 came from Wuhan lab must not be dismissed as conspiracy', Sky News, 6 July 2020.

527. The Committee questioned whether there is any intelligence or intelligence assessment on the origins of the outbreak. What the Intelligence Community told us appeared to be not too dissimilar to the assessment made by the US Intelligence Community in 2020: that it is highly likely that SARS-CoV2 (the virus which causes Covid-19) is naturally occurring – as opposed to a laboratory-acquired infection or one manufactured as an offensive or defensive weapon, and it is likely that the first human infection originated from a natural human–animal interaction unconnected to a laboratory. They also told us that it does not appear that the virus was manufactured or intentionally spread by China. Having been tasked to look for intelligence on the origins of the virus, GCHQ told us that ***.[857] The Intelligence Community said that:

> ***[858,859]

528. In response to global speculation – and perhaps in an effort to shape its global image – China has attempted to "*sow seeds of doubt about the origins of the virus, to try and get its audiences in its own terms to believe that China was not at fault*".[860] Chinese diplomats and officials have, alongside state media, repeatedly reiterated that the virus may have originated outside China, and have claimed that the US is a more likely source.[861] There are no credible sources that support this assertion, and the general consensus remains that the virus originated in Wuhan. We were told that, while it is difficult to determine the exact location of the first infection, it is unlikely that Covid-19 originated from a laboratory-acquired infection or accidental release from a laboratory. Even if it did, it is highly likely the original source was a natural pathogen. However, HMG noted that:

> ***[862] ***[863]

529. It may be that neither the UK Intelligence Community nor our Five Eyes partners will ever be able to confirm the origin of Covid-19. While this is both expected and understandable, there nonetheless remain significant benefits in attempting to determine the origin of Covid-19, principally to inform our responses to future pandemics and develop preventative measures.

530. China's deliberate obstruction of international efforts in this regard is inexcusable. In May 2020, it was reported that China would refuse access to investigators until the pandemic

[857] Oral evidence – GCHQ, *** October 2020.
[858] Written evidence – HMG, 18 November 2020.
[859] HMG subsequently advised the Committee that the evidence provided was inaccurate and that the penultimate sentence should read ***.
[860] Oral evidence – GCHQ, *** October 2020.
[861] '"American Coronavirus": China pushes propaganda casting doubt on virus origin', *The Guardian,* 13 March 2020.
[862] JIO assessments are measured on 'confidence' and 'probability'. The 'probability yardstick' states how likely something is: up to 5% (i.e. a 1 in 20 chance) is a 'remote' chance; 10–20% (between 1 in 10 and 1 in 20) is 'highly unlikely'; 25–35% (1 in 4 to 1 in 3) is 'unlikely'; 40–50% (2 in 5 to 1 in 2) is a 'realistic possibility'; 55–75% (5 in 9 to 3 in 4) is 'likely or probable'; 80–90% (4 in 5 or 9 in 10) is 'highly likely'; and 95–100% (19 in 20) is 'almost certain'. 'Low' confidence means that reports are based on fragmentary, ambiguous and/or contradictory source material; 'medium' or 'moderate' confidence reports will have elements of corroboration, based on quality material but have key gaps, concerns or weaknesses; and 'high' confidence means that reports are based on a range of good-quality sources, potentially with some corroboration.
[863] Written evidence – HMG, 7 June 2021.

had ended[864] and, in January 2021, a team of WHO investigators were refused entry to China.[865] Instances such as these are a stark reminder of China's preponderance to favour its narrow ideological objectives over international co-operation, the implications of which will be felt for years to come.

531. It may be the case that China has been obstructive because it has something it wishes to hide. However, ***.[866]

China's initial response

532. Accusations have also been levelled at China that its initial domestic response hindered later global containment efforts. However, there does not appear to be clear evidence that China deliberately released or allowed the release of the virus. What we have seen appears to echo reporting that suggested that, in the early days of the pandemic, the Chinese authorities appeared to emphasise information control at the expense of standard epidemic response measures. A reluctance to pass bad news up the chain hindered the response, as did widespread censorship of stories about the virus, and it appears that more decisive action only materialised when the issue reached higher levels of the Chinese government.[867] The JIC Chair ***

> ***
>
> *** [868]

The response was characterised in evidence to us as part 'to be expected', and part 'typical Chinese aversion to bad news':

> *I would characterise it in part as what would have been a challenge to any government dealing with a new virus, trying to work out what it was, trying to work out what measures should be taken and requiring a period of time as it flowed up through the system before it got to real decision-making level, but I would also say that they are handicapped by the Chinese system, because of a reluctance to share information, certainly a reluctance to allow information to become public and a reluctance to pass bad news up the chain.*[869]

533. China has faced considerable public scrutiny for its role in containing the pandemic, playing down the potential impacts of the disease – including, crucially, its potential for human-to-human transmission, about which they are alleged to have delayed releasing information to the public for up to six days in January 2020.[870] China's reporting of infections and deaths has also been widely criticised for introducing uncertainty into modelling by

[864] 'China refuses international probe on Covid-19 source until "final victory" over disease', France 24, 6 May 2020.
[865] 'Covid-19: WHO investigators are still blocked from entering China as two cities lock down', Owen Dyer, *British Medical Journal*, 8 January 2021.
[866] Oral evidence – GCHQ, *** October 2020.
[867] Written evidence – JIO, 22 May 2022.
[868] Oral evidence – JIO, *** October 2020.
[869] Oral evidence – JIO, *** October 2020.
[870] 'Taiwanese official reveals China suspected "human to human" transmission by January 13', *The Telegraph*, 6 May 2020.

others when trying to ascertain the future spread and danger of the virus, and for providing a basis on which to downplay China's role and responsibilities.[871]

534. In the early stages of the pandemic, open source reporting alleged that China closed internal flights in January 2020 while leaving international flights open until March 2020.[872] If true, this may indicate culpability for the global reach of the virus – whether through negligence, or a deliberate effort to spread the virus beyond China's borders. The Committee therefore questioned whether there was any intelligence on, or intelligence assessment of, the issue. The UK Intelligence Community told us their assessment is as follows:

> *At the end of January, China initiated the highest levels of public emergency in all provinces, restricting almost all forms of travel for ordinary citizens. Foreign consular services were required to arrange chartered flights to assist their citizens' return to home countries.*
>
> *During the strictest period of lockdown, approximately 23 January to mid-March, although China did not formally close its borders, the number of total domestic and international flights departing dropped from about 15,000 per day, to 1,800-2,000. Approximately 75% of these flights were domestic. In addition to the epicentre, in the most restricted cities (Beijing, Shanghai, Guangzhou), which account for the top three busiest airports for international and domestic travel, the number of weekly flights dropped to less than 100, and some weeks less than ten.*
>
> *On 28 March China banned foreign citizens entering China, and sought to dissuade Chinese citizens from returning. This marked a change in China epidemic control strategy. After it had officially declared the epidemic under control domestically, having brought the number of cases down to single digits, and declared most provinces virus free, it focused on preventing imported cases entering the country and causing a second wave. ***.*[873]

535. It is not clear from this reply what the proportions were of international and domestic flights which were stopped. ***.

536. Furthermore the JIO has since advised that, from updated open source data, this "*statistic* [of 75%] *is no longer the most accurate*" and that "*the flight numbers provided ought to be treated with caution given that in some cases flights included were subsequently found to have been cancelled or the layover in Wuhan aborted whilst others could have been empty return flights or chartered flights evacuating foreign nationals from Wuhan*".[874] There is therefore no evidence base on which to assess the validity of the allegations made in the open source reporting.

[871] 'C.I.A. Hunts for Authentic Virus Totals in China, Dismissing Government Tallies', *New York Times*, 2 April 2020.
[872] 'How China locked down internally for COVID-19, but pushed foreign travel', *Economic Times*, 30 April 2020.
[873] Written evidence – JIO, 18 November 2020.
[874] Written evidence – JIO, 24 February 2022.

Disinformation

537. Alongside the Covid-19 pandemic, various commentators have discussed the 'pandemic of disinformation',[875] or an 'infodemic'. The WHO characterises the latter term as an abundance of information, including false information, which causes confusion, undermines confidence in public health responses, and can intensify or lengthen outbreaks.[876] This presents clear challenges to governments as they attempt to develop and implement public health responses.

538. The origins of misinformation and disinformation are complicated and reflect the underlying purposes of their promulgators. Russian disinformation throughout the pandemic has been frequently alleged. When we speak of threats to the UK, we often talk of 'Russia and China' in the same breath. While each stands in opposition to Western liberal democratic values, the two present very different challenges and engage with the UK in very different ways. In our predecessor Committee's 2020 *Russia* Report, we discussed efforts to discredit and undermine the democratic process in the UK, including during the 2014 Scottish independence and 2016 EU membership referenda, through disinformation.[877]

539. With disinformation reported so readily in the media throughout the Covid-19 pandemic, we asked the JIC Chair for his assessment of comparisons which could be drawn between Russian and Chinese efforts. The JIC Chair noted that disinformation campaigns by Russia and China seek to fulfil their respective political objectives: while Russia seeks actively to undermine trust in Western democratic institutions and values, China remains focused on controlling the narrative around its position in the world and its domestic challenges.[878] As a result, we heard from Director General MI5 that the "*other audience that China is seeking to influence is its own diaspora communities*".[879] Although this is concerning, we were told that the scale of the effort expended by China in the UK media is not "*as vigorous*" as that from Russia, and that targeting of social media, while engaged in extensively by China, is predominantly in Chinese languages rather than English.[880]

540. As we noted when discussing the role of China in Academia, disinformation can be used as a means to shape the narrative on, or shut down discussion of, the domestic challenges that China considers as presenting the greatest risk to its international reputation or its internal suppression of dissent. Director General MI5 noted that:

> *if that is their objective in respect of the UK media over the last year, they probably regard themselves as not having done a brilliant job, because, if you look at the balance of stories appearing in the UK media over the last year, there has been a lot of discussion around things like Huawei, Hong Kong, Xinjiang … the tide of public opinion and the opinion polling shows … that the UK public are more conscious of China as presenting threats and challenges to the UK than was the case two or three, four years ago.*[881]

---

[875] *The* "*Pandemic*" *of Disinformation in COVID-19*, Fabio Tagliabue et al, 1 August 2020.
[876] 'Infodemic', World Health Organization, 11 June 2021.
[877] *Russia*, HC 632, 21 July 2020.
[878] Oral evidence – JIO, *** October 2020.
[879] Oral evidence – MI5, *** October 2020.
[880] Oral evidence – JIO, *** October 2020.
[881] Oral evidence – MI5, *** October 2020.

541. As well as using disinformation to limit damage to its own image, China is also accused of spreading disinformation and discord abroad in a bid to damage democracies by suggesting that autocracies have managed to contain the virus whereas democracies have failed to protect their populations.[882] GCHQ told us:

> *China has been very keen to promote its role in health diplomacy, to show where it is helping other nations, to amplify, over exaggerate in some ways its work to counter the virus and to develop vaccines, and so on, but it has equally, at the same time, been putting out disinformation to try and sow seeds of doubt about the origins of the virus, to try and get its audiences in its own terms to believe that China was not at fault with this and to promulgate fake news and conspiracy theories.*[883]

UUU. Now is not the time to try to reach conclusions about Chinese intent or actions over the origins and development of the pandemic – it is still too soon, as it is likely that more information will come to light about Covid-19 as investigations continue. Initial work * does appear to support public statements made by the World Health Organization and the Intelligence Community in the United States that the virus was not man-made and China did not deliberately let it spread – beyond cultural issues around failure.**

VVV. However, those cultural issues – a failure to share information due to a reluctance to pass bad news up the chain, and a tendency to censor press and social media reports considered to present a negative impression – were in themselves extremely damaging to efforts to contain and, later, counter the disease. Attempts by China to suggest that the pandemic originated elsewhere show an unwillingness to change its approach – a concern, given the possibility of future pandemics.

Vaccine development and medical espionage

542. The work which has led to the development of several effective Covid-19 vaccines built on the response to SARS (Severe Acute Respiratory Syndrome) in 2002 and MERS (Middle Eastern Respiratory Syndrome) in 2012. Chinese research was instrumental in sequencing the virus's full genome and sharing it globally on 11 January 2020. From that point, several teams around the world were able to work independently on potential vaccines, and several had received regulatory approval by early 2021. Further efforts to promote equitable distribution saw the establishment of Covid-19 Vaccines Global Access (or 'COVAX'), which laid the foundation for ongoing vaccine rollout in lower-income countries.

543. The development of an effective vaccine to combat Covid-19 was considered to be the most crucial aspect in managing the pandemic over the long term. There was a race to be the first to develop a vaccine and therefore work on a vaccine was judged to be highly likely to be targeted by hostile states. At the outset of the pandemic, MI5 judged that "*COVID-related intelligence would almost certainly be a high priority. We considered it almost certain they would target global healthcare organisations, especially those engaged in*

[882] 'How China Ramped Up Disinformation Efforts During the Pandemic', Council on Foreign Relations, 10 September 2020.
[883] Oral evidence – GCHQ, *** October 2020.

vaccine discovery and manufacture, and organisations involved in the vaccine supply chain."[884]

544. The National Cyber Security Centre (NCSC) has publicly identified Russian efforts to target UK vaccine work (and indeed Russian disinformation around the vaccine, with the aim of undermining public confidence in it, appeared to be the primary hostile state threat in this area[885] ***), but there have also been allegations in the press that China has used information supplied to the WHO in order to guide its targeting of companies and institutions working on coronavirus vaccines. The JIO told us ***.[886]

545. While China would seemingly gain no clear advantage in sabotaging efforts to create a vaccine – given the benefits it would likely reap – it is nevertheless very interested in the UK's vaccine development. MI5 told us that:

> ***[887]

546. Furthermore, China stands to gain clear benefits from medical espionage while there remain exploitable commercial opportunities in connection with the pandemic. Both Russia and China appear to have used 'medical diplomacy' in the context of Covid-19 to further their own positions: offers of personal protective equipment or medical support may appear to be generous on the surface, but may have conditions attached. CDI told us that the ***.[888]

547. The UK Intelligence Community should be commended for the proactive measures they have taken to defend the UK's medical infrastructure and capabilities from possible interference. NCSC increased its support to the UK Government Vaccine Taskforce, which makes decisions on research funding and purchase of vaccines, and to universities involved in the research and development of a vaccine.[889] The Centre for the Protection of National Infrastructure is helping to secure Covid-19 testing, treatment and vaccine research and development,[890] and ***.[891]

548. Indeed, the pandemic has raised an important issue: namely that sectors that are not traditionally considered 'critical' became hugely significant in co-ordinating and facilitating the UK's response. As a consequence, support was rapidly required from Government to counter the interest shown in them by – and threat from – a wide range of actors, including hostile states. GCHQ noted:

> *These are companies that are generally not classed as Critical National Infrastructure but became essential to the UK's response to the Covid-19 crisis including: supermarkets, haulage companies to ventilator manufacturers, healthcare suppliers and charities. No priority list of these existed, we had to work with a range of*

[884] Written evidence – MI5, 24 September 2020.
[885] 'Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, US Officials Say', *Wall Street Journal*, 7 March 2021.
[886] Written evidence – JIO, 18 November 2020.
[887] Oral evidence – MI5, *** October 2020.
[888] Oral evidence – DI, *** October 2020.
[889] Written evidence – GCHQ, 31 July 2020.
[890] Written evidence – MI5, 31 July 2020.
[891] ***

> *organisations – from central Government departments to trade associations – to ensure that our efforts were appropriately targeted. We produced 17 new pieces of guidance and a range of material to support the ESPs* [Essential Service Providers] *and advise on how to reduce their cyber risk.*[892]

549. NCSC noted that *** and that the pandemic also caused it to work much more closely with the UK's Health Critical National Infrastructure given the greater interest shown in it as a result of Covid-19. This has included working with the Department of Health and Social Care to tackle the range of cyber threats that have emerged, and NCSC notes that ***.[893]

WWW. During the pandemic, sectors not traditionally considered 'critical' – such as organisations working on a vaccine, supermarkets, logistics, haulage and medical equipment supply companies – became essential to the UK's response. The support of the Intelligence Community was key to protect the vaccine supply chain and to counter the interest shown in these 'critical' areas by hostile foreign actors.

Debt leverage

550. China is well documented as a generous lender to developing countries. While exact figures are difficult to obtain, it is thought that China lends extensively across Africa, South America, the Middle East, and South East Asia. As noted in the main body of this Report, China has taken advantage of developing countries, particularly during the Covid-19 pandemic, but this is not without its drawbacks. The JIC Chair noted that:

> *the debt issue is a problem for China. China has loaned a lot of relatively poor countries a lot of money to do infrastructure projects, and they have wanted it, on the whole. Now they are reaching the point where, partly because of Covid-19, they cannot actually meet their repayment obligations. So China is facing a reputational problem with those countries.*
>
> *If you looked in the* Financial Times*, earlier this week, you will have seen the Finance Minister of Ghana, a Commonwealth country, saying, yes, China is an important lender in Africa but it is problematic that they want to renegotiate bilaterally, rather than within a multilateral framework, because what that means is that Western countries are reluctant to do deals because they think that will just let the Chinese off the hook.*
>
> *So this is not all up-sides for China. There are real reputational problems. You will have seen some of the reputational hits that China took over the distribution of sub-quality protective equipment in the context of Covid-19. So it is, as I say, quite a complex picture.*[894]

[892] Written evidence – GCHQ, 31 July 2020.
[893] Oral evidence – NCSC, *** October 2020.
[894] Oral evidence – JIO, *** October 2020.

Capitalising on the pandemic

551. The Secretary General of NATO (the North Atlantic Treaty Organization), Jens Stoltenberg, and Sir John Sawers, former Chief of SIS, amongst others, have raised concerns about China buying strategic assets and critical infrastructure cheaply as a result of the crisis. MI5 told us that, at the time, it and the Joint State Threats Assessment Team (JSTAT) recognised this risk, and assessed that:

> ***[895]

552. The UK Intelligence Community judged that China had used the opportunities presented by Covid-19 in the commercial space and also to increase its influence in global organisations, such as the WHO.[896] We were warned *** that, overall, the threat from China had increased and that it was likely to emerge from the pandemic "*stronger and more aggressive than before*".[897]

XXX. The key issue for the future is the extent to which China will now capitalise on the pandemic as other countries suffer its effects and how the UK Intelligence Community and their allies will stop this growing threat.

Impact on the UK Intelligence Community

553. One of the broader consequences of the pandemic domestically was the large increase in the number of people in the UK who worked principally, or partly, from home. This included the staff of the Agencies. The (then) Deputy National Security Adviser told us that this had several implications for HMG's effort on China:

> *China is a cross-Government effort and any work on China needs to be done in a secure way. For these organisations, they are very used to communicating at very high levels of security.*
>
> *One thing Covid did show us earlier this year was that when much of the Civil Service went to working from home, most departments* ***.
>
> ***[898]

554. MI5 told us that the pandemic had caused it to rapidly alter its processes to equip staff for low-side working, and noted that this approach had seen productive outcomes:

> ***[899]

[895] Written evidence – MI5, 24 September 2020.
[896] Oral evidence – HMG, *** October 2020.
[897] Written evidence – MI5, 24 September 2020.
[898] Oral evidence – NSS, *** October 2020.
[899] Written evidence – MI5, 31 July 2021.

YYY. In terms of the work of the Intelligence Community generally, while it may have been reasonable for staff to work partially from home during the pandemic, it would obviously not be feasible for organisations that rely on secret material to carry out all their work over less secure systems. Yet even now, with the country having fully reopened, we continue to see the Intelligence Community working partially from home (some more than others). It appears that the response to our requests for information has slowed dramatically as a result: the 'new normal' for some organisations means deadlines have been missed or responses have been sanitised to enable them to be sent from home. This has had – and continues to have – an impact on the Committee's ability to scrutinise security and intelligence issues properly and in a timely fashion.

ZZZ. **The pandemic had a notable impact in terms of staff across the Intelligence Community working from home, without continual access to classified systems – other than for those working on the most critical priorities. In this respect we take the opportunity to pay tribute to the Committee's own staff, who have continued to work from the office full time (a rarity in the Civil Service) so as to ensure that the Committee was able to function efficiently and effectively.**

ANNEX B: FULL LIST OF CONCLUSIONS AND RECOMMENDATIONS

PART ONE: THREAT AND RESPONSE

A. China's national imperative is to ensure that the Chinese Communist Party remains in power. Everything else is subservient to that.

B. However, it is its ambition at a global level – to become a technological and economic superpower, on which other countries are reliant – that poses a national security threat to the UK.

C. China views the UK through the optic of the struggle between the United States and China. When combined with the UK's membership of significant international bodies, and the perception of the UK as an international opinion-former, these factors would appear to place the UK just below China's top priority targets.

D. China views the UK as being of use in its efforts to mute international criticism and to gain economically: this, in the short term at least, will temper China's targeting of the UK.

E. China is seeking both political influence and economic advantage in order to achieve its aims in relation to the UK. It seeks to acquire information and influence elites and decision-makers, and to acquire Intellectual Property using covert and overt methods to gain technological supremacy.

F. China almost certainly maintains the largest state intelligence apparatus in the world. The nature and scale of the Chinese Intelligence Services are – like many aspects of China's government – hard to grasp for the outsider, due to the size of the bureaucracy, the blurring of lines of accountability between party and state officials, a partially decentralised system, and a lack of verifiable information.

G. The Chinese Intelligence Services target the UK and its overseas interests prolifically and aggressively. While they seek to obtain classified information, they are willing to utilise intelligence officers and agents to collect open source information indiscriminately – given the vast resources at their disposal. In more ways than one, the broad remit of the Chinese Intelligence Services poses a significant challenge to Western attempts to counter their activity.

H. To compound the problem, it is not just the Chinese Intelligence Services: the Chinese Communist Party co-opts every state institution, company and citizen. This 'whole-of-state' approach means China can aggressively target the UK, yet the scale of the activity makes it more difficult to detect *.**

I. In terms of espionage, China's human intelligence collection is prolific, using a vast network of individuals embedded in local society to access individuals of interest – often identified through social media. It is also clear from the evidence we have seen that China routinely targets current and former UK civil servants *. While there is good awareness of the danger posed, it is vital that vigilance is maintained.**

J. In relation to the cyber approach, whilst understanding has clearly improved in recent years, China has a highly capable cyber – and increasingly sophisticated cyber-espionage – operation: however, this is an area where the 'known unknowns' are concerning. Work on continuing coverage of its general capabilities must be maintained alongside further work on Chinese offensive cyber and close-proximity technical operations.

K. In terms of interference, China oversteps the boundary and crosses the line from exerting influence – a legitimate course of action – into interference, in the pursuit of its interests and values at the expense of those of the UK.

L. Decision-makers – from serving politicians to former political figures, senior government officials and the military – are, inevitably, key targets. China employs a range of tactics, including seeking to recruit them into lucrative roles in Chinese companies – to the extent that we questioned whether there was a revolving door between the Government and certain Chinese companies, with those involved in awarding contracts being 'rewarded' with jobs.

M. The Cabinet Office must update the Advisory Committee on Business Appointments guidelines in relation to intelligence and security matters, including with particular reference to China, and ensure that their implementation is strictly enforced.

N. China is an economic power, and this cannot be ignored in formulating the UK's policy towards China. Balancing the tension between security and prosperity requires dexterity, and we understand that there are a number of difficult trade-offs involved.

O. The length of this Inquiry has allowed us to see the development of the China policy within Government and we are reassured that, belatedly, the security aspects are now being given prominence – notably more so after the pandemic.

P. It is nevertheless concerning that the security community, and the Government in general, were aware of many of these issues several years ago and yet we are only now beginning to see the introduction of measures taken to protect UK sovereign interests. The lack of action to protect our assets from a known threat was a serious failure, and one from which the UK may feel the consequences for years to come.

Q. Even now, HMG is focusing on short-term or acute threats, and failing to think long term – unlike China – and China has historically been able to take advantage of this. The Government must adopt a longer-term planning cycle in regard to the future security of the UK if it is to face Chinese ambitions, which are not reset every political cycle. This will mean adopting policies that may well take years to stand up and require multi-year spending commitments – something that may well require Opposition support – but the danger posed by doing too little, too late, in this area is too significant to fall prey to party politics.

R. Tackling the threats posed by China requires the UK to have a clear strategy on China, which is forward thinking, joined up and utilises a 'whole-of-government' approach. Work to develop such a strategy may now be in train, but there is still a long way to go.

S. The Intelligence Community will play a key role in the work of the new Investment Security Unit (ISU): the classified and other technical advice that the Intelligence Community provide should shape the decisions made by the ISU as it seeks to balance the need for national security against economic priorities. It is essential that there is effective scrutiny and oversight of the ISU – and that can be undertaken only by this Committee.

T. We commend the action now being taken by the Government to counter interference by China – it is encouraging that the Government has finally woken up to the grave threat this poses to our national security.

U. However, it is worrying that 'policy ownership' of this national security activity, rather than being gripped at the centre by the Cabinet Office, has instead been devolved across the Government – in many instances to departments with no security remit or expertise. We have not been kept informed of these developments and, despite numerous requests, are not permitted to scrutinise this activity.

V. Effective Parliamentary oversight is not some kind of 'optional extra' – it is a vital safeguard in any functioning Parliamentary democracy, and the ISC is the only body that can do that. Moving responsibility for security matters to bodies not named in the ISC's Memorandum of Understanding is not consistent with Parliament's intent in the Justice and Security Act 2013: the Government should not be giving departments a licence to operate in the name of national security and hiding it from view.

W. The Telecommunications (Security) Act 2021 does not contain provision for effective oversight of the new measures being implemented. The Act provides that notification of a company or person being a 'high-risk vendor' of telecommunications equipment, and specification of the limits placed on the use of this equipment, be laid before Parliament unless provision of this information is deemed to be contrary to national security. In such circumstances it is logical – and in keeping with Parliament's intent in establishing the ISC – that this information should instead be provided to the ISC. This would ensure that Parliament could be duly notified without this information being made public and thereby endangering national security. However, this proposed amendment was rejected wholesale by the Government. This was particularly inappropriate – and, indeed, ironic – as it was the ISC that had originally raised concerns about the adoption of Huawei in the UK telecommunications network. It was our initiative that prompted the Government to introduce this legislation.[900]

X. In December 2020, we asked how the policy outcomes against which SIS and GCHQ must deliver intelligence were being prioritised. We presume, for instance, that "*" is not considered to be of the same importance as "***"; however, we have not been provided with any information. Without any indication of prioritisation, it is difficult to judge the effectiveness of Agency efforts and it is therefore disappointing – and rather telling – that NSS has failed to provide such critical information in response to this major Inquiry.**

Y. We were told in 2019 that the Agencies take a tri-Agency approach, but this does not cover DI. In October 2020 – over 15 months later – we asked if there had yet been any movement towards formally adding DI to the prioritisation process. The Acting National Security Adviser told us: "*DI are fully part of the IOP process … they are one of our main repositories of expertise on China.*" Director GCHQ noted that DI is a part of the National Cyber Force, and "*when you get into the effects world … they are completely there in every aspect*".[901] If DI is supposedly now fully integrated with the Intelligence Outcomes Prioritisation process, we expect the next iteration of the tri-Agency approach – when it is finally updated – to include DI.

Z. As at 2021, the Government had a plethora of plans that laid out its China policies. The interaction between these documents has required a great deal of unpicking, and we have been surprised at the fact that changes in one document do not always lead to consequent changes in others. The slow speed at which strategies, and policies, are developed and implemented also leaves a lot to be desired – at the time of writing we await to see what impact the National Security Adviser's review of processes will have on the China policy area, but we would certainly hope it will become more coherent.

AA. The level of resource dedicated to tackling the threat posed by China's 'whole-of-state' approach has been completely inadequate. While a shortage of resources had been identified as early as 2012, effort was diverted onto the acute counter-terrorism threat arising from Syria. The increase in funding on the China mission in 2020 was therefore both necessary and welcome. But it was only for one year. HMG cannot think or plan strategically with such short-term planning.

---

[900] *Foreign involvement in the Critical National Infrastructure*, Cm 8629, 6 June 2013.
[901] Oral evidence – GCHQ, *** October 2020.

BB. HMG must explore the possibility of a multi-year Spending Review for the Agencies, in order to allow them to develop long-term, strategic programmes on China and respond to the enduring threat. The UK is severely handicapped by the short-termist approach currently being taken.

CC. MI5 is responsible for countering Hostile State Activity, and the Centre for the Protection of National Infrastructure and the National Cyber Security Centre play a key role in engaging with those within and outside the Government to protect national security. There is a wide array of defensive tools, which are being used to good effect, but the Government has come late to the party and has a lot of catching up to do. Our closest allies identified the need to use such tools against China long ago and we must learn from their experience and knowledge.

DD. It is also clear that this defensive effort requires a cross-government approach. However, this transfer of responsibility will need to be a well-thought-out, gradual process with adequate support provided to the departments and some degree of control retained at the centre. HMG needs to ensure that those departments not traditionally associated with security are properly resourced with security expertise, properly supported and properly scrutinised.

EE. Chinese law now requires its citizens to provide assistance to the Chinese Intelligence Services (ChIS) and to protect state secrets. It is highly likely that the ChIS will use such legislation to compel the Chinese staff of UK companies to co-operate with them. It is also likely that China's Personal Information Protection Law will lead to the Chinese government forcing Chinese and other companies to turn over their data held on Chinese citizens. As compartmentalisation of Chinese citizens' data will be difficult, this is likely to mean that, in practice, China will obtain access to data held on non-Chinese citizens as well.

FF. The UK Intelligence Community have been open with the Committee about the challenges of detecting Chinese interference operations. ***

GG. It is incumbent on the Government to report on how national security decision-making powers are being dispersed across the Government. It should annually update this Committee on the number of personnel cleared to see Top Secret material in each of the departments with new national security decision-making powers, together with the facilities provided to them (secure IT terminals and telephones etc.).

HH. Failure to get this transition right from the outset could lead to decisions that fail to withstand external challenge. Furthermore, as there is an adjustment in national security responsibility, so too must there be an adjustment to ensure there is effective Parliamentary oversight of all aspects.

II. It is clear that there has been progress in terms of 'offensive' work since we started our Inquiry – for instance, an increase in 'effects' work. However, given what appears to be the extremely low starting point, this is not cause for celebration *. Both SIS and GCHQ say that working on China "*is a slow burn, slow-return effort*"[902] ***.**

[902] Written evidence – GCHQ, 12 June 2019.

JJ. GCHQ and SIS tasking is set by the Government and, rightly, they cannot work outside the Government's priorities. Nevertheless, the fact that China was such a relatively low priority in 2018 – the same year in which China approved the removal of term limits on the Presidency, allowing President Xi Jinping to remain in office as long as he wished – is concerning. Work must continue to be prioritised now to make up for this slow start and there must be clear measurement and evaluation of effort.

KK. It is clear that both GCHQ and SIS face a formidable challenge in relation to China. What we were unable to assess – without the specific requirements set for the Agencies or any idea of the prioritisation of the 'outcomes' within the Intelligence Outcomes Prioritisation Plan – is how effective either Agency is at tackling that challenge. As a result of pressures placed on civil servants during the Covid-19 pandemic – including fewer people in offices with access to the necessary IT systems – the Cabinet Office has not measured the Agencies' success against its requirements, and so neither the Government nor Parliament has any assurance about their effectiveness.

LL. We have seen efforts grow over the duration of this Inquiry. We expect to see those efforts continue to increase as coverage leads to an increased programme of 'effects'. However, given the importance of the work, it is vital that the Cabinet Office carries out an evaluation on whether SIS and GCHQ are meeting their targets in relation to China. That evaluation must be shared with this Committee.

MM. *. Increased surveillance, both in the physical and virtual world, poses significant challenges to long-term intelligence-generating capabilities ***. This problem is only going to get more difficult. SIS and GCHQ should prioritise work on this ***[903] ***.**

NN. Although we have stated this earlier in this Report, it bears repeating specifically in relation to legislation: the length of time it has taken to reform the Official Secrets Acts is unconscionable. Our predecessors were told that the Acts required updating as a matter of urgency in January 2019. Over three years later, we have yet to see the introduction of a Bill. National security legislation ought to be a priority for any UK Government – it is certainly not a matter to be kicked into the long grass by successive Governments.

OO. We recommend that HMG ensure that a Counter-State Threats Bill is enacted as a matter of urgency.

903 ***

PART TWO: CASE STUDIES

PP. The UK's academic institutions provide a rich feeding ground for China to achieve political influence in the UK and economic advantage over the UK. China exerts influence over institutions, individual UK academics and Chinese students in order to control the narrative of debate about China – including through the use of Confucius Institutes in the UK – and it directs or steals UK academic research to obtain Intellectual Property in order to build, or short-cut to, Chinese expertise. However, the academic sector has not received sufficient advice on, or protection from, either.

QQ. In seeking political influence, there are obvious and repeated examples of Chinese attempts to interfere and stifle debate amongst the academic community in the UK. Universities are reliant on student fees, and the vast number of Chinese students in the UK – it is striking that there are more than five times the number than for any other country – provides China with significant leverage, which it is not afraid to exert. Yet the Government had shown very little interest in warnings from Academia: at the time of drafting, there was no point of contact in the Government for those in the sector to seek advice on these issues.

RR. In its quest for economic advantage, China often acts in plain sight – directing, funding and collaborating on academic research for its own ends. In particular, it seeks to benefit the Chinese military through research on dual-use technologies, which is often unclassified in its early stages. There is a question as to whether academic institutions are alive to the threat posed by such collaboration, particularly given that they often accept transfer of Information Data and Intellectual Property as a condition of funding. While some have expressed concern, others seem to be turning a blind eye, happy simply to take the money.

SS. The UK Government must ensure that transparency around the source of foreign donations to Higher Education institutions is improved: a public register of donations must be created by the Department for Education and monitored by the State Threats Unit in the Home Office.

TT. Academia is also an 'easy option' when it comes to the theft of Intellectual Property, by taking advantage of collaborative projects to steal information which is less protected than it might be in the private sector or the Ministry of Defence, for example. The vast number of Chinese students – particularly post-graduates – in academic institutions in the UK that are involved in cutting-edge research must therefore raise concerns, given the access and opportunities they are afforded.

UU. At present, HMG still seems to be trying to understand the threat from Chinese students stealing Intellectual Property from UK Academia, or the Chinese subverting UK research to its own ends, at the most basic level – i.e. what it is they are trying to steal. There is still no comprehensive list of the areas of sensitive UK research that need protecting from China. Identifying these key areas of research must be a priority, and they must be communicated to Academia as a matter of urgency so that protective action can be taken. Unless and until this is done, then the UK is handing China a clear economic advantage over the UK, and indeed the rest of the world.

VV. Unlike other countries, such as the United States (US), the UK has taken no preventative action. This is particularly concerning, as US restrictions on Chinese students will make UK institutions more attractive to those seeking to gain Intellectual Property and expertise. The Research Collaboration Advice Team should submit a quarterly report on the progress and outcomes of its work to the State Threats Unit in the Home Office to ensure there is cross-government awareness of the scale of the issue.

WW. It is clear that the Academic Technology Approval Scheme (ATAS) is an effective tool. Once the Government has identified the sensitive areas of research that need protecting from China, consideration should be given to ensuring that ATAS certificates are required for foreign nationals undertaking post-graduate study in UK institutions in those areas. Furthermore, we recommend that ATAS be expanded to cover post-graduate doctoral study.

XX. Tackling the threat in relation to Academia could have been an example of the Fusion Doctrine working seamlessly – with each policy department clearly contributing to an overall goal. But, as in so many areas, the devolution of responsibility for security to policy departments means that the ball is being dropped on security. Policy departments still do not have the understanding needed and have no plan to tackle it.

YY. This must change: there must be an effective cross-government approach to Academia, with clear responsibility and accountability for countering this multi-faceted threat. In the meantime, China is on hand to collect – and exploit – all that the UK's best and brightest achieve as the UK knowingly lets it fall between the cracks.

ZZ. China is seeking technological dominance over the West and is targeting the acquisition of Intellectual Property and data in ten key industrial sectors in which the Chinese Communist Party intends China to become a world leader – many of which are fields where the UK has particular expertise.

AAA. As this Committee has previously warned, the West is over-reliant on Chinese technology. As the role of technology in everyday life increases exponentially, so therefore the UK will be at an increasing disadvantage compared to China – with all the attendant risks for our security and our prosperity. British technology and innovation is therefore critical and must be robustly protected.

BBB. China's joined-up approach can be clearly seen from its use of all possible legitimate routes to acquire UK technology, Intellectual Property and data – from buy-in at the 'front end' via Academia, to actual buying-in through licensing agreements and Foreign Direct Investment, to the exertion of control over inward investments and standards-setting bodies. Each represents an individual threat, but it is the cumulative threat that can now be clearly seen.

CCC. Overt acquisition routes have been welcomed by HMG for economic reasons, regardless of risks to national security. The threat to future prosperity and independence was discounted in favour of current investment. This was short-sighted, and allowed China to develop significant stakes in various UK industries and Critical National Infrastructure.

DDD. Without swift and decisive action, we are on a trajectory for the nightmare scenario where China steals blueprints, sets standards and builds products, exerting political and economic influence at every step. Such prevalence in every part of the supply chain will mean that, in the export of its goods or services, China will have a pliable vehicle through which it can also export its values. This presents a serious commercial challenge, but also has the potential to pose an existential threat to liberal democratic systems.

EEE. We welcome the Government's attribution of attacks to the Chinese hacking group APT10. Public condemnation of such groups explicitly linked to the Chinese government is an essential tool in tackling the increasing cyber threat from China. The Government should continue to work with allies to highlight and condemn hostile Chinese government activity.

FFF. The threat posed by Chinese targeting of experts in UK Industry is of concern. While the expulsion of intelligence officers and the disruption of Chinese efforts are to be commended, the lack of prosecutions is worrying. We note that the Government is intending to introduce new legislation that will make it easier to prosecute such behaviour. Convictions under such new legislation would act as a strong deterrent to those contemplating engaging in such relationships.

GGG. The scale of investments by the China General Nuclear Power Group in the UK Civil Nuclear sector – and its willingness to undergo expensive and lengthy regulatory approval processes – demonstrates China's determination to become a permanent and significant player in the UK Civil Nuclear sector, as a stepping stone in its bid to become a global supplier. Involvement will provide China with an opportunity to develop its expertise and gain both experience and credibility as a partner.

HHH. The question is to what extent the Government is prepared to let China invest in such a sensitive sector, for the sake of investment, and whether the security risks have been clearly communicated to Ministers – and understood. The Government would be naïve to assume that allowing Chinese companies to exert influence over the UK's Civil Nuclear and Energy sectors is not ceding control to the Chinese Communist Party.

III. Using the fact that Hinkley Point C will be operated by a French company as justification for allowing Chinese involvement was obfuscatory: the Government clearly knew that that decision would lead to it allowing the use of Chinese technology and Chinese operational control at Bradwell B. It is astonishing that the investment security process for Hinkley Point C did not therefore take Bradwell B into account. It is unacceptable for the Government still to be considering Chinese involvement in the UK's Critical National Infrastructure (CNI) at a granular level, taking each case individually and without regard for the wider security risk. It is imperative that linked investments are considered in the round and that Ministers are consulted on the cumulative security risk brought by linked Chinese investments. Effective Ministerial oversight in this area is still lacking, more than eight years on from the Committee's Report on the national security implications of foreign involvement in the UK's CNI.

JJJ. We have serious concerns about the incentive and opportunity for espionage that Chinese involvement in the UK's Civil Nuclear sector provides. Investment in Hinkley Point C opened the door, but for the UK to allow the China General Nuclear Power Group to build and operate Bradwell B would be opening a direct channel from the UK nuclear enterprise to the Chinese state.

KKK. While we accept that the risk posed by physical access to Civil Nuclear sites is overshadowed by the vulnerabilities exposed by Chinese investment and operational control, it would be wrong to dismiss the former outright. The Government recognises the risk that a digital back door into the UK's Critical National Infrastructure might create, but the risk posed by the literal back door of human actors with access to sensitive sites should not be dismissed.

LLL. We are reassured that the Intelligence Community have recognised the * vulnerability that potentially lies in the supply chains: effort to protect against cyber attacks must include the supply chains.**

MMM. While we recognise that the threat of disruption is less likely, the threat of leverage is very real: the fact that China will be able to exert some control over the UK's Critical National Infrastructure will complicate the Government's calculations in its broader approach to China. In other words, it may not be possible to separate the Civil Nuclear sector from wider geopolitical and diplomatic considerations.

NNN. Unlike the Civil Nuclear sector, the Energy sector appears to provide China with less potential for leverage, as it does not have the same long-term reliance issues that we see in the Civil Nuclear sector. Nevertheless, there are concerns in relation to the threat to the Energy sector from economic espionage (particularly in the area of new 'green' energy) and disruption.

OOO. We reiterate that foreign investment cases cannot be looked at in isolation and on their own merits. It is absurd that the (then) Department for Business, Energy and Industrial Strategy (BEIS) considered that foreign investment in the Civil Nuclear sector did not need to be looked at in the round: we question how any department can consider that a foreign country single-handedly running our nuclear power stations shouldn't give pause for thought. This clearly demonstrates that BEIS does not have the expertise to be responsible for such sensitive security matters.[904]

PPP. Previous investments in the sector, or the potential for there to be 'legitimate expectation' that an investment in one area ought to facilitate a linked investment, must be taken into account. If the Investment Security Unit fails to do so, then it will be unable to counteract the 'whole-of-state' approach so effectively utilised by China (amongst others).

[904] As previously noted, as part of the restructure of several government departments in February 2023, the Investment Security Unit (ISU) has returned from BEIS to the Cabinet Office. The Committee has not been in a position during this Inquiry to scrutinise the effectiveness of this transfer, or the reasons behind it. In principle, we would have welcomed the move to return the ISU to the Cabinet Office, where the relevant security expertise, capabilities and infrastructure are more likely to be in place. However, as outlined earlier, unfortunately, effective oversight has not been put in place.

QQQ. The regulation of the Civil Nuclear sector (through the Office of Nuclear Regulation (ONR)) is robust. However, we have not been able to evaluate the effectiveness of the ONR in countering Hostile State Activity – indeed, when we tried to ascertain whether the powers held by the ONR were sufficient to protect national security, witnesses from the Agencies and the Cabinet Office were unable to answer. Given the significant Chinese investment in this sector, we recommend that a review of the ONR's ability to counter Hostile State Activity is undertaken.

RRR. Should the Government allow China General Nuclear Power Group (CGN) to build and operate the proposed Hualong One reactor at Bradwell (or any other UK nuclear power station), we recommend that the Government set up a 'cell' – a 'nuclear' version of the Huawei Cyber Security Evaluation Centre – in order to monitor the technology and its operation and address any perceived risks arising from the involvement of CGN in the UK's Civil Nuclear sector.

SSS. While it is understandable that * – given that Hinkley Point C is still under construction, and the remainder had not been approved at the time of writing – the finished projects must be subject to detailed (and continuing) scrutiny by the Centre for the Protection of National Infrastructure and the Intelligence Community. We expect to be kept informed of the advice provided by the Agencies and key decision timelines.**

TTT. Although Chinese involvement in, and control over, UK nuclear power stations is deeply concerning, it offers only a small snapshot of the attempt to gain control over a range of sectors, and technologies, by an increasingly assertive China. The Government should commission an urgent review to examine and report on the extent to which Chinese involvement in the sector should be minimised, if not excluded.

UUU. Now is not the time to try to reach conclusions about Chinese intent or actions over the origins and development of the pandemic – it is still too soon, as it is likely that more information will come to light about Covid-19 as investigations continue. Initial work * does appear to support public statements made by the World Health Organization and the Intelligence Community in the United States that the virus was not man-made and China did not deliberately let it spread – beyond cultural issues around failure.**

VVV. However, those cultural issues – a failure to share information due to a reluctance to pass bad news up the chain, and a tendency to censor press and social media reports considered to present a negative impression – were in themselves extremely damaging to efforts to contain and, later, counter the disease. Attempts by China to suggest that the pandemic originated elsewhere show an unwillingness to change its approach – a concern, given the possibility of future pandemics.

WWW. During the pandemic, sectors not traditionally considered 'critical' – such as organisations working on a vaccine, supermarkets, logistics, haulage and medical equipment supply companies – became essential to the UK's response. The support of the Intelligence Community was key to protect the vaccine supply chain and to counter the interest shown in these 'critical' areas by hostile foreign actors.

XXX. The key issue for the future is the extent to which China will now capitalise on the pandemic as other countries suffer its effects and how the UK Intelligence Community and their allies will stop this growing threat.

YYY. In terms of the work of the Intelligence Community generally, while it may have been reasonable for staff to work partially from home during the pandemic, it would obviously not be feasible for organisations that rely on secret material to carry out all their work over less secure systems. Yet even now, with the country having fully reopened, we continue to see the Intelligence Community working partially from home (some more than others). It appears that the response to our requests for information has slowed dramatically as a result: the 'new normal' for some organisations means deadlines have been missed or responses have been sanitised to enable them to be sent from home. This has had – and continues to have – an impact on the Committee's ability to scrutinise security and intelligence issues properly and in a timely fashion.

ZZZ. **The pandemic had a notable impact in terms of staff across the Intelligence Community working from home, without continual access to classified systems – other than for those working on the most critical priorities. In this respect we take the opportunity to pay tribute to the Committee's own staff, who have continued to work from the office full time (a rarity in the Civil Service) so as to ensure that the Committee was able to function efficiently and effectively.**

ANNEX C: CODE WORDS

In some instances in this Report we have substituted an ISC-specific code word where it has been necessary to refer to the name of an operation or project, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to real operation names. The ISC code words have no operational significance.

CONISTON .....***

DERWENT ……..***

WINDERMERE ……...***

ANNEX D: LIST OF WITNESSES

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Sir Jeremy Fleming KCMG CB – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir Richard Moore KCMG – Chief, SIS

Other officials

SECURITY SERVICE (MI5)

Mr Ken McCallum – Director General, MI5

Other officials

DEFENCE INTELLIGENCE

General Sir James Hockenhull KBE ADC Gen – Chief of Defence Intelligence (2018–2022)

Other officials

CABINET OFFICE

Sir Simon Gass KCMG CVO – Chair, Joint Intelligence Committee

David Quarrey CMG – Acting National Security Adviser (2020–2021)

Dr Christian Turner CMG – Deputy National Security Adviser (2017–2019)

Madeleine Alessandri CMG – Deputy National Security Adviser (2018–2020)

Beth Sizeland – Deputy National Security Adviser (2020–2021)

Other officials

External Expert witnesses

Mr John Gerson CMG – Visiting Professor (then Visiting Senior Fellow), King's College London Policy Institute

Mr Raffaello Pantucci – Senior Associate Fellow (then Director of International Security Studies), Royal United Services Institute (RUSI)

Mr Charles Parton OBE – Senior Associate Fellow, Royal United Services Institute (RUSI)

Rt Hon. Lord Patten of Barnes KG CH PC – Chancellor of the University of Oxford

Dr Tim Stevens – Reader in International Security (then Lecturer in Global Security), King's College London

Professor Steve Tsang – Director of the China Institute, School of Oriental and African Studies (SOAS), University of London

ISBN 978-1-5286-4302
E02938943