Government Response to the Intelligence and Security Committee of Parliament Report 'China'

Presented to Parliament
by the Prime Minister
by Command of His Majesty

September 2023

CP 929

Government Response to the Intelligence and Security Committee of Parliament Report 'China'

Presented to Parliament
by the Prime Minister
by Command of His Majesty

September 2023

CP 929

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at **publiccorrespondence@cabinetoffice.gov.uk.**

ISBN 978-1-5286-4437-2

E02979899 09/23

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

Contents

Foreword

HM Government is grateful to the Intelligence and Security Committee (ISC) for its report entitled *China*, published on 13th July 2023. The Prime Minister acknowledged and thanked the committee for its report in a written ministerial statement on the same day.

The committee's inquiry began in 2019 and it took the bulk of its evidence in 2020. The report reflects the detailed evidence that was provided to the committee up to and including the intelligence cut-off date of January 2022.

The government published the Integrated Review of Security, Defence, Development and Foreign Policy[1] in 2021, and its subsequent refresh[2] in 2023. These reviews strengthened the United Kingdom's position on China, recognising the epoch-defining and systemic challenge that the country represents, and set out a comprehensive approach to China through three integrated themes — Protect, Align and Engage. The government has taken a proactive approach and is already addressing a number of the issues the committee has raised. The government has been clear that when tensions arise between its objectives in relation to China, national security will always come first.

As an absolute priority, the government takes action to protect the United Kingdom from any state activity which seeks to damage and undermine our security, prosperity and values. State threats are increasing and diversifying so it is crucial that the United Kingdom's tools and legislation are able to mitigate and respond to threats regardless of origin.

This year, parliament passed the National Security Act, which overhauls legislation applicable to espionage, sabotage and persons acting for foreign powers against the safety and interest of the United Kingdom. It materially increases our ability to deter, detect and disrupt state threats, making the United Kingdom a harder target for those seeking to overtly or covertly interfere in its democracy and society. Together with the previously legislated National Security and Investment Act and the Telecommunications (Security) Act, it addresses many of the committee's concerns.

The government recognises that the report identified areas where we can do better, and has considered the committee's conclusions and recommendations in full with this in mind, to assess where further action should be taken. While the government has carefully considered every conclusion and recommendation made by the committee, given their interrelated and mutually-reinforcing nature, and to avoid

[1] https://www.gov.uk/government/collections/the-integrated-review-2021
[2] https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world

repetition, this response groups them thematically, making reference to some specific recommendations where appropriate.

The committee's recommendations and conclusions are in bold in text boxes below, followed immediately by the government's reply.

The Strategic Context

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 *.**

The government recognises the committee's concerns about the long-term strategic challenge posed by China under the Chinese authorities.

IR2021 established the United Kingdom's robust stance towards China. It highlighted China's increasing international assertiveness and identified China as the biggest state-based threat to the United Kingdom's economic security. It placed greater emphasis on defending the United Kingdom's interests and values, while preserving the potential for cooperation on shared interests.

IR2023 went further, responding to changes in the strategic environment, recognising China under the Chinese authorities as an epoch-defining and systemic challenge with implications for almost every area of government policy and the everyday lives of the British people. It also recognised China's size and significance on almost every global issue, and set out the United Kingdom's preference for better cooperation, understanding, predictability and stability with China,where this can be achieved without weakening or undermining our national security.

IR2023 noted that China has continued its rapid and opaque military modernisation, has used its economic power to coerce countries with which it disagrees, and has deployed cyber to exploit vulnerabilities and steal data. There has also been Chinese activity within the United Kingdom to undermine free speech and to engage in espionage and interference. MI5 Director General Ken McCallum addressed this directly in a July 2022 speech, saying "the most game-changing challenge we face comes from the Chinese Communist Party… the right model can't be to scale the agencies to somehow take on all of this activity… In our view the most crucial improvement is to make the UK a harder target."

Responding to this systemic challenge, the government committed to:

- greater national security protections to safeguard the United Kingdom's people, prosperity and security, including to communities now at home in Britain;

- deeper cooperation and closer alignment with allies and partners to call out and counter behaviours that undermine international law, violate human rights and seek to undermine the integrity of our democracy or coerce other sovereign nations; and

- engagement with China bilaterally and in international fora to preserve and strengthen open, constructive, predictable, and stable relations where it is in the national interest.

The conclusions of the Integrated Review Refresh have set the direction across government for a consistent, coherent and robust approach to China—rooted in the United Kingdom's national interests and aligned with allies.

The Cross-Government Approach

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.

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.

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.

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.

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.

The government recognises that the United Kingdom has both security and prosperity interests relating to China. A core part of the government's approach is to engage directly with China, bilaterally and multilaterally, to preserve and create open, constructive and stable relations that can support both security and prosperity. The government will also pursue a positive trade and investment relationship where this is in the United Kingdom's national interest and is safe and reciprocal.

At the same time, the government's approach to China (as set out in IR2023) confirms that where tensions arise between its objectives in relation to China, national security will always come first.

The government welcomes the committee's recognition that as far back as 2020, it was making progress in protecting the United Kingdom's economic security. This work has continued and the government has taken substantial action to build domestic resilience and to protect the economy, critical national infrastructure, supply

chains, and the United Kingdom's ability to generate strategic advantage through science and technology (S&T).

The government agrees that a more strategic approach was required, which resulted in the development and subsequent publication of IR2021, and subsequently IR2023. Both iterations of the Integrated Review make it clear that the United Kingdom's policy is anchored in its core national interests, as well as a higher interest in an open and stable international order, based on the UN Charter and international law. As noted in the foreword, the whole of government pursues this policy through the three interrelated lines of effort, entitled Protect, Align, and Engage.

IR2023 also outlined a new approach to countering state threats wherever they come from, organising activity into four lines of effort: protecting the United Kingdom's interests, values, assets, and allies and partners from the impact of this activity; engaging domestically and internationally to raise awareness of it and to deepen cooperation on countering it; building a deeper understanding of states' activity and how to respond effectively; and competing directly with these states by disrupting, degrading and deterring threats upstream in creative and assertive ways, when appropriate.

The National Security Council (NSC) remains responsible for ensuring coherence of national strategy and its effective delivery. To support the NSC in its functions, and aligned to the areas that the committee examined in its report, additional NSC sub-committees have been established including for overall economic security and for resilience against a range of threats and hazards, both chaired by the Deputy Prime Minister (DPM). Whilst neither of these are country-specific and are not targeted specifically at China, they bring coherence to these activities and directly address the committee's recommendations.

The Cabinet Office is responsible for coordinating cross-government strategy across a range of issues including China, with departments responsible for delivery of that strategy. This allows for a coherent view across the extent of China's activity, and allows the government to prioritise work, assess trade-offs, and mitigate risks, with delivery across all departments.

The Joint State Threats Assessment Team (JSTAT) continues to support this approach through the provision of cross-departmental assessment on state threats to the United Kingdom and its interests, ensuring that government activity is focused on the current threats.

The government does, however, recognise that further investment in capabilities will be needed to ensure the government is equipped with the tools, expertise and knowledge to respond to the systemic challenge that China poses to the United Kingdom's security, prosperity, and values. IR2023 took the first steps towards this,

doubling funding for a government-wide programme, including further investing in Mandarin language training and deepening diplomatic, and wider, expertise. We will continue building expertise across the system to better address the long-term challenge that China poses.

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.

Since evidence was taken for this Report, the government has introduced and passed the National Security Act 2023, which overhauls the United Kingdom's espionage laws and will provide law enforcement and intelligence agencies with new and updated tools to deter, detect and disrupt modern-day state threats. It will ensure that the United Kingdom remains a hard operating environment for malign activity from those states who seek to conduct espionage, foreign interference (including in the political system), sabotage, and acts that endanger life (such as assassination). For the first time, there is an offence of Foreign Interference, meaning it will now be illegal to engage in conduct that interferes with fundamental rights, such as voting and freedom of speech, that are essential to the United Kingdom's democracy. Other new offences include Supporting a Foreign Intelligence Service, Theft of Trade Secrets and Sabotage.

The Act introduces a new Foreign Influence Registration Scheme (FIRS), which will provide greater assurance around the activities of specific foreign powers or entities, and will promote greater transparency around political influence carried out on behalf of foreign powers. This means that the United Kingdom's democratic institutions are better protected from covert influence wherever it comes from and the government is better informed about the nature, scale, and extent of foreign influence in its political affairs. The scheme is split into two parts: firstly, the political tier of FIRS requires the registration of any political influence activity undertaken at the direction of a foreign power; secondly, the enhanced tier — designed to target those countries that pose a risk to the safety or interests of the United Kingdom — will require registration of arrangements that are entered into with a specified foreign power, part of a foreign power, or entity controlled by a foreign power where necessary to protect the safety or interests of the United Kingdom. Failure to register, or to comply with an information notice, when required to do so will be a criminal offence.

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.

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.

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.**

Tackling state threats to British interests requires a whole of government approach. A significant amount of resource is focused on these threats across a wide range of departments and their work is informed and supported by the security and intelligence agencies.

The government agrees with the committee that the United Kingdom should seek to learn from allies' experience and knowledge, and can assure the committee that relevant teams work in lockstep with allies.The 'Align' pillar of the cross-government China approach embeds a commitment to deepening cooperation with partners including learning from and sharing experience and knowledge from across the international community. This builds upon the United Kingdom's existing experience undertaking joint work with both Five Eyes and European partners.

The government has a programme of work in place to make the United Kingdom a hard operating environment for any hostile actor. The United Kingdom has a history of changing the structures of intelligence and security agencies in response to policy, technological and other developments. This includes launching the National Cyber Security Centre (NCSC) as part of GCHQ in 2016, and the National Protective Security Authority (NPSA) as part of MI5 in 2023.

The NCSC manages and responds to cyber incidents and provides advice to government, industry, and citizens on improving cyber resilience overall. The government recognises that the cyber threat from China-linked actors is widespread and prolific, with China's intelligence agencies having developed into sophisticated, highly capable cyber operators.

Two major strategies support the government's efforts to defend against the full range of cyber threats:

- The National Cyber Strategy is delivering a step-change in British cyber resilience, and sets out the government's ambitions to raise levels of resilience across all sectors by 2025. It is building a resilient and prosperous digital United Kingdom, better prepared for cyber threats, reducing cyber risks and ensuring citizens feel safe online and confident that their data is protected.
- The Government Cyber Security Strategy (GCSS) sets out the plan to maintain and develop the United Kingdom's cyber defences in government by improving cyber resilience across all government organisations.

The government welcomes the committee's acknowledgement of the array of defensive tools in place. The report references the Centre for the Protection of National Infrastructure (CPNI), which, as noted above, has since been strengthened and relaunched as the National Protective Security Authority (NPSA), with a broader remit for developing resilience through protective security.

In principle, the government is committed to multi-year spending settlements for GCHQ, MI5 and SIS (collectively, "the Agencies"), as well as wider cross-governmental national security priorities. Single year spending settlements create challenges given the medium- to long-term nature of much of national security expenditure.

In practice, spending reviews usually result in multi-year financial settlements. The 2021 Spending Review gave the Agencies certainty over the funding available to them over the next three years, and provided ring-fenced funding for specific programmes. The Agencies have set in motion long-term strategic programmes of work. China-related capabilities will continue to be a priority area of investment, and there are robust mechanisms to oversee and monitor spending, implementation and effectiveness. The government is planning for the long-term with a clear strategy,

which will necessarily take place over a number of spending periods and Parliaments.

Between spending periods, the Agencies deploy their investigative, analytical and operational resources flexibly across all areas of national security threat in response to demand. MI5 is operationally independent in prioritising threats to national security, but aligns with government priorities as set in the Integrated Review and by the NSC. Prioritisation of GCHQ and SIS overseas intelligence effort is agreed through the Intelligence Outcomes Prioritisation (IOP) process, overseen by the Cabinet Office and approved through the Joint Prioritisation Committee (JPC). The 2023 IOP process was designed to respond to IR2023, and confirmed the government's commitment to prioritising the long term national security interests referenced in the Refresh. The NSC, which signs off the final balance of intelligence effort, takes a long-term approach, particularly in light of the resources and time it takes for intelligence agencies to build the necessary capabilities to pursue new priorities. The process to prioritise intelligence collection is rigorously focussed on where effort can achieve impact on the highest priority policy objectives, and is completed with the involvement of all relevant agencies, and a wide range of government departments with national security interests.

Across the Agencies, effort and resource flex over time in response to demand. Given the acute terrorist threat arising from Syria, it was right at the time that the intelligence community surged resources to tackle the substantial terrorist threat to the United Kingdom. Resources are rebalanced on the basis of evidence and data. MI5 is now running seven times as many investigations into Chinese activity than in 2018, and plans to grow further.

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 movment 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". 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.

The Chief of Defence Intelligence (CDI), as the Functional Owner of Intelligence for Defence, represents Defence Intelligence at Joint Prioritisation Committee (JPC) meetings, and has taken significant steps to ensure that Defence's intelligence priorities align with those of the Agencies, and deliver against national security requirements.

Tasking authority over Defence Intelligence (DI) assessment and collection priorities and outputs remains within Defence under the direction of Chief Defence Staff (CDS), via the Defence Strategic Intelligence Prioritisation Process (DSIPP). DI works closely with SIS, GCHQ and MI5 to identify areas for collaboration, and to collectively understand and deliver against intelligence requirements.

DI is closely aligned with the Intelligence Outcomes Prioritisation (IOP) process, and contributes to it as an intelligence customer. These efforts enable DI to deliver comprehensive all source intelligence assessment to its customers in Defence and across government.

Addressing The Committee's Policy Recommendations

a. Interference and espionage

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.**

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.

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.

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

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.

The government agrees with the committee that some Chinese action crosses the line from influence into interference. As the committee has noted, action is being taken to address this.

In 2022, the government established the Defending Democracy Taskforce to coordinate work across government to protect the integrity of democracy in the United Kingdom. It works across government and with parliament, the intelligence community, the devolved administrations, local authorities and the private sector on the full range of threats facing democratic institutions. JSTAT assessment is further deepening the government's understanding of these threats — drawing on both British and international experience — to inform and shape the government's response

NPSA, previously CPNI, launched the "Think Before You Link" app in May 2022. It allows users of social media and professional networking sites such as LinkedIn and Facebook to better identify the hallmarks of fake profiles used by malicious actors, including those from the Chinese Intelligence Services. The app has been developed with behavioural scientists and includes features such as a profile reviewer, which will help individuals – including current and former civil servants – identify and report anything that they deem suspicious. In just over one year, there have been 25,000 app users who have generated a number of suspicious reports into social media accounts of concern. Plans are in place to further promote use of the app and its ability to raise awareness of the threat posed by malicious approaches by state actors with civil servants and others.

The government is taking decisive steps to stop active targeting and recruitment of British individuals with sensitive knowledge and experience, including serving and former military personnel. All serving and former personnel are already subject to the Official Secrets Act, and the use of confidentiality contracts and non-disclosure agreements is being reviewed across Defence.

The new espionage offences in the National Security Act will ensure that tactics, techniques and procedures are explicitly covered as protected information. Unauthorised sharing will be an offence. The Act creates new offences for Foreign Interference, Assisting a Foreign Intelligence Service, and Theft of Trade Secrets. This will create a harder operating environment for those acting on behalf of foreign powers against the safety or interests of the United Kingdom. It will also ensure that a greater range of sensitive information is protected and will deter those who seek to share the most sensitive information with malign actors.

The government recognises that Chinese recruitment schemes have tried to headhunt British and allied nationals in key positions and with sensitive knowledge

and experience, including from government, military, industry and wider society. As the committee notes, there is more work to be done.

The aim of the Business Appointment Rules is to avoid any reasonable concerns that:

- a civil servant might be influenced in carrying out his or her official duties by the hope or expectation of future employment with a particular firm or organisation, or in a specific sector; or
- on leaving the Civil Service, a former civil servant might improperly exploit privileged access to contacts in Government or sensitive information; or
- a particular firm or organisation might gain an improper advantage by employing someone who, in the course of their official duties, has had access to:
    - information relating to unannounced or proposed developments in Government policy, knowledge of which may affect the prospective employer or any competitors; or
    - commercially valuable or sensitive information about any competitors.

When making a decision, the Advisory Committee on Business Appointments (ACOBA) must strike a balance between concerns about the circumstances of an outside appointment (as set out in the Business Appointment Rules), and the right of individuals to earn a living after leaving the government, reflecting the legal position on restraints of trade. Depending on the nature of the proposed role, ACOBA can consider national security implications — informed where necessary by information from the relevant government departments. ACOBA rules apply to all civil servants who intend to take up an appointment or employment after leaving the Civil Service, and employees of the Intelligence Agencies are subject to further rules and processes.

The government has recently published[3] its response to reports from the Committee on Standards in Public Life (CSPL), the Public Administration and Constitutional Affairs Committee (PACAC), and the Boardman Review of Government Procurement in the COVID-19 pandemic. The response outlines proposals for a package of reform to the Business Appointment Rules, which focus on improved enforcement of the Rules via staff contracts and a ministerial deed. The government will consider the findings of the committee's report as part of this work, and consider strengthening the Business Appointment Rules in relation to intelligence and security matters as appropriate.

As the committee notes, China's human intelligence collection is prolific. The intelligence community is acutely aware and vigilant regarding China's targeting of current and former civil servants and a range of mitigations are in place in order to

[3] https://www.gov.uk/government/publications/strengthening-ethics-and-integrity-in-central-government

minimise the risk. A robust personnel vetting regime is in place to ensure the identification and management of risks arising from staff with access to sensitive government assets and intelligence. Those with security clearance are re-vetted throughout their careers. This re-vetting aims to ensure that those who may be susceptible to pressure or improper influence - or who may even actively seek to act on behalf of a foreign intelligence service - are identified.

Civil servants are educated on the risks posed by hostile intelligence services, so they can best protect themselves and identify suspicious behaviour. A strong security culture is ingrained across the civil service through regular training and awareness campaigns on good security practice. Safeguards are in place to ensure sensitive material is protected and only accessed by those who need to see it.

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.

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.

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

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.

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.**

The government shares the committee's concerns about the widespread and credible evidence demonstrating prolific, sustained and irresponsible cyber threat activity emanating from China. The Chinese Ministry of State Security (MSS) has emerged as a prolific and pervasive actor in cyberspace, undertaking a substantial global espionage campaign to meet political, socio-economic and strategic objectives. The People's Liberation Army (PLA) has consolidated its electronic warfare, cyber and space capabilities to enhance the military cyber power and information operations capabilities. China's rapidly advancing cyber, surveillance, data and analytical capabilities, and enormous intelligence and counter-intelligence resources represent a significant challenge. Global use of Chinese surveillance equipment and communications infrastructure likely supports Chinese cyber operations. There is particular concern that many groups responsible for malicious cyber activity appear to be linked to the Chinese state. The government continues to urge the MSS and PLA to end their inappropriate relationship with such groups and to hold them to account.

As noted in the committee's report, China has a large and highly effective cyber espionage capability and has had considerable success in penetrating foreign government and private sector IT systems. Such activity runs counter to the bilateral commitments China had made to the United Kingdom in 2015 and as a G20 member to not conduct or support cyber-enabled theft of intellectual property or trade secrets. It also runs counter to China's own Global Data Security Initiative announced in 2020, which specifically opposes using cyber capabilities to damage other countries' critical infrastructure or steal important data.

Strong defences and resilient systems remain the best ways to mitigate the risks and impact of malicious cyber activity, wherever it originates from. The government recognises the urgent need to defend against Chinese cyber operations and has invested significant resources into improving the United Kingdom's overall cyber security. The 2022 National Cyber Strategy sets out the government's ambition to raise levels of resilience across all sectors by 2025. It aims to build a resilient and prosperous digital United Kingdom that is better prepared for cyber threats, to reduce cyber risks and to ensure citizens feel safe online and confident that their data is protected. The *UK Government Resilience Framework*[4] was published in December 2022 and sets out the government's approach to strengthen systems and capabilities that support collective resilience.

The government has also taken action to harden its own defences. As set out above, in January 2022, the government launched the first Government Cyber Security Strategy (GCSS) to build and maintain its cyber defences; build greater cyber resilience across all government organisations; and work across government to 'defend as one'—exerting a defensive force greater than the sum of its parts.

[4] https://www.gov.uk/government/publications/the-uk-government-resilience-framework

Good progress has been made to deliver the central initiatives in the GCSS. In April 2023, the Cabinet Office launched GovAssure, a transformational cyber assurance regime for the whole of government. GovAssure will provide a clear and objective view of government cyber resilience and enable measurement of progress towards strategic targets. Design work has also started on the Government Cyber Coordination Centre (GCCC), which will be the central hub across government where responses to cyber security incidents, vulnerabilities and threats are coordinated and managed across government.

The United Kingdom continues to work with international partners to ensure the perpetrators of malicious cyber activity, including those in China, are held to account. The government frequently raises evidence of malicious cyber activity with relevant authorities. For example, it issued an advisory[5] jointly with Five Eyes partners in May 2023 that warned of China state-sponsored activity targeting CNI networks.

b. Academia

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.

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

[5] https://www.ncsc.gov.uk/news/ncsc-joins-partners-to-issue-warning-about-chinese-cyber-activity-targeting-cni

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.

The government welcomes international students to study in the United Kingdom, and encourages British institutions to partner and collaborate with international institutions. As set out in IR2023, the government will engage with the Chinese government and people, and cooperate on shared priorities, where it is consistent with the national interest. This includes shared objectives in the research and academia sectors, where these do not undermine national security or erode UK technological advantages. Such partnerships have many benefits - for example, a 2021/22 cohort of first year international students boosted the economy by £41.9bn.[6]

As with any actor, wherever the Chinese authorities' actions and stated intent threaten the United Kingdom's interests, action will be taken to protect those interests, including in academia. The government recognises the committee's

[6] https://www.hepi.ac.uk/2023/05/16/international-students-boost-uk-economy-by-41-9-billion/

concerns about interference in the higher education sector; the potential for stifling debate; the threat of intellectual property theft; and the risks of sensitive technology transfer. Government regularly assesses the threats facing academia, and takes a cross-government approach in response.

The government has made a great deal of progress in this area since 2020 when the committee took the bulk of its evidence on this issue. This includes legislative and non-legislative measures such as expansion of the Academic Technology Approval Scheme (ATAS) and the adoption of the National Security Act and Higher Education (Freedom of Speech) Act.

The National Security and Investment Act 2021 enables the government to scrutinise and intervene in acquisitions of control over entities and assets across the economy that may pose national security risks. Alongside this, the United Kingdom's export controls regime has been strengthened, including to add China as an embargoed destination subject to the 'military end-use' controls and by publishing specific guidance on Export Controls for the academic community.

The Higher Education (Freedom of Speech) Act 2023 includes a measure to require greater transparency in reporting sources of income by universities in England, supporting the Office for Students to understand the scale and impact of any overseas income on freedom of speech, and to monitor any trends and patterns of concern. The National Security Act 2023 also contains measures that can be used to disrupt state threat actors working in the research sector.

The government recognises the committee's recommendation that the sector would value additional government advice, support and a point of contact. The Research Collaboration Advice Team (RCAT), which has been operating since March 2022 as part of the Department for Science, Innovation and Technology (DSIT), fulfils this role. In 2020, Universities UK (UUK), with support from government, CPNI and NCSC published guidelines to help universities tackle security risks related to international collaboration. UUK continues to evaluate the effectiveness of, and to update, their guidelines.

The government acknowledges the committee's recommendation that RCAT should produce a quarterly report for the Home Office on its work, but considers that existing RCAT reporting structures are sufficient. There is cross-government oversight of the RCAT through its governance board, in addition to governance accountability within DSIT.

IR2023 committed to carry out a comprehensive review of security within higher education. This review will work cross-government to evaluate the measures currently in place and to identify what more the government could or should be doing. It will carefully consider the committee's recommendations and conclusions (it would

be inappropriate to comment on what changes might be required until the review is complete).

The complexity of research subjects combined with the pace of development is such that any single, definitive list of sensitive areas of research would not capture sufficient detail and would be quickly out of date. Existing guidance includes the National Security and Investment Act which sets out 17 sensitive areas of the economy (including Quantum, Artificial Intelligence and Synthetic Biology) that are subject to the Act; and the technology areas covered under the ATAS regime. RCAT helps institutions to understand what activity and collaborations are deemed higher risk.

NCSC and NPSA have been active in the sector: the “Trusted Research” campaign was launched by CPNI - NPSA’s predecessor organisation - and NCSC in September 2019.

From the outset of the campaign NPSA and NCSC have co-created solutions with the sector and supported self-regulation. This reflects the challenges of keeping a list current, given the speed of technological development, and that academics may be better placed to recognise the potential dual uses or misuse of the technologies that they are researching. Through guidance and engagement, NCSC and NPSA have sought to equip academics with the ability to recognise risks, and to make the right decisions.

Like any international body operating in the United Kingdom, Confucius Institutes need to operate transparently and within the law and should engage with full commitment to British values of openness and freedom of expression. The government recognises concerns about overseas interference in the higher education sector, including through Confucius Institutes, and keeps the risks under regular review. The government is taking action to remove any direct or indirect government funding from these institutions in the United Kingdom and currently judges that it would be disproportionate to ban them. This policy remains under active review, but wider measures, including those introduced through the National Security Act 2023 and Higher Education (Freedom of Speech) Act 2023, are expected to provide effective tools to prevent any malign behaviour within the higher education sector.

Recognising that most countries with an advanced R&D base face similar issues around research security and integrity, the United Kingdom is leading work within the G7 on this and is supporting capacity building in central and eastern Europe.

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.

The government recognises the committee's concerns about attempts to stifle debate on university campuses and is committed to ensuring freedom of speech and to tackle transnational repression wherever it originates.

Any attempt by any foreign power to intimidate, harass or harm individuals or communities in the United Kingdom—including in universities—will not be tolerated. As set out in the Security Minister's recent statement[7] on Overseas Police Service Stations, any allegations will be investigated in line with the law.

The Higher Education (Freedom of Speech) Act 2023 will ensure that universities in England have the tools they need to tackle interference in, and threats to, freedom of speech and academic freedom, wherever they originate. The Act addresses the committee's concerns about the transparency and influence of overseas money in English higher education, without reducing the ability of the United Kingdom's world class universities to engage internationally. New measures will help the regulator, the Office for Students (OfS), understand the scale and impact of overseas income on freedom of speech and academic freedom, and monitor any trends and patterns of concern.

The Act will also ensure that lawful freedom of speech is fully supported. It will require registered higher education providers in England to push back on threats to freedom of speech. If a provider engages in any activity with an international partner that limits lawful freedom of speech and academic freedom on campus, this is likely to be a breach of their duties.

In June 2023 the government announced the appointment of the first Director for Freedom of Speech and Academic Freedom at the OfS, Professor Arif Ahmed. This new role will champion freedom of speech and academic freedom on campuses and will have responsibility for investigating infringements of freedom of speech duties in higher education. There will be new sanctions and the possibility of individual redress under the complaints scheme. The Director will bring experience and knowledge

[7] https://questions-statements.parliament.uk/written-statements/detail/2023-06-06/hcws822

from the higher education sector to spearhead the implementation of the new duties in the Act. In particular, this role will be critical as OfS develops guidance for higher education providers, constituent colleges and students' unions to help them comply with their new duties, including highlighting best practice.

As the government's International Education Strategy sets out, the United Kingdom continues to welcome international students, including those from China. The government will ensure that recruitment is sustainable and that British universities are not reliant on one source of funding. This is a core focus of the work of Sir Steve Smith, the United Kingdom's International Education Champion.

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 postgraduate doctoral study.

The government is grateful to the committee for recognising the value of ATAS, the scheme designed to prevent the transfer of sensitive and/or dual-use knowledge to any military programmes of concern. In October 2020 the government expanded ATAS to cover a wider range of technologies—including advanced conventional military technology in addition to its initial weapons of mass destruction remit. In May 2021 the government decided to apply ATAS requirements to researchers in addition to post-graduates in these technologies, lowering the risk presented by academic knowledge transfer.

Academic subjects covered by ATAS are listed on GOV.UK so that prospective students and researchers can see whether or not their proposed work requires ATAS clearance. Universities also have a responsibility to categorise their courses and alert prospective students if ATAS clearance is required. The ATAS scheme will be considered as part of the review into security in higher education to ensure that it remains targeted and proportionate.

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 multifaceted 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.

As noted previously, the Cabinet Office is responsible for coordinating cross-government strategy across a range of issues including China, with departments responsible for delivery of that strategy.

As an example, "Trusted Research" has exemplified a whole of government approach with a joint campaign led by the Government's National Technical Authorities for physical, personnel and cyber security – NPSA and NCSC in strong partnership with DSIT (formerly BEIS), Department for Education and Cabinet Office. This has extended into a supportive and aligned response from the sector itself, in partnership with UUK, the Russell Group, the Royal Society, Royal Academy of Engineering and many institutions.

There remains more to do to support and to defend the higher education sector and, as already noted, the government committed to a comprehensive review of higher education through IR2023.

Whilst the government continues to work with British universities on threats facing the sector, it should be noted that British universities are independent. This is valued both by the government and the education sector. However, when collaborating with international partners, the government expects universities to carry out due diligence to ensure compliance with regulation and consideration of reputational, ethical and security risks. It is critical for institutions to own their own risks and make sensible and mature decisions about their own activities.

c. Economic security, CNI and the energy sector

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.

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.

As set out in IR2023, the United Kingdom should, and will, continue to engage constructively with China, including on the economic relationship and to shape a positive environment for British businesses in China, where it is consistent with the national interest. The government believes that a positive trade and investment relationship can benefit both the United Kingdom and China, and will work with industry to ensure that trade and investment are safe, reciprocal and mutually beneficial.

At the same time, the government will always put national security first. The government recognises the risks and the need to protect the economy, critical national infrastructure, supply chains and strategic capabilities. The government has therefore taken robust action to build national domestic resilience and to enhance the government's economic security levers to enable the United Kingdom to engage globally with confidence.

As described above, the National Security & Investment Act 2021 gives the government robust powers to block or impose remedies on acquisitions that pose a national security risk, whilst providing businesses and investors with the certainty and transparency they need to do business in the United Kingdom. Certain investments in 17 sensitive areas of the United Kingdom's economy (for example investment into critical infrastructure in the energy and civil nuclear sectors) must be notified to the government. The NSI Annual Report 2022-23 shows that in the 12-month reporting period, the government called in 65 acquisitions for further assessment and made

proportionate interventions through 15 final orders to block, unwind or impose conditions on acquisitions that represented a risk to the United Kingdom's national security. The report shows that in the same period, four transactions involving acquirers associated with China were blocked, and four were allowed to proceed subject to remedies to mitigate national security risks. Acquisitions involving acquirers associated with China accounted for the most call-ins and final orders, but also the most final notifications (clearances). This demonstrates that the government has taken an evidence and risk-based approach to decisions in recognition that, whilst China presents an epoch-defining challenge for the United Kingdom, a positive trading relationship benefits both the United Kingdom and China.

Across all sectors, the government is providing clarity to businesses on how to conduct their activities safely. The NPSA provides British businesses and other organisations with access to expert security advice to counter state threats, including to critical national infrastructure. In April 2022, NPSA (as CPNI) launched its supply chain campaign "Protected Procurement" alongside Department for Business and Trade (DBT) "Safeguarding Supply" campaign. These joint campaigns with DBT and the Chartered Institute of Procurement and Supply showcased best practice in joint development and delivery between NPSA, government, and industry. Since the launch the government has sought to embed the "Protected Procurement" principles within its procurement processes, including contributing to modular security schedules. The publication of the Overseas Business Risk Guidance helps British firms to negotiate issues they may encounter when operating overseas. The government is also establishing an Economic Security Private-Public Sector Forum, so that the United Kingdom's economic security policies can be better communicated, and the government can develop joint actions and strategies with businesses.

Action is also being taken to protect the United Kingdom's supply chains and promote resilience internationally. The government committed in IR2023 to publish a new strategy on semiconductors[8] (done in May 2023) and to refresh the critical minerals strategy[9] (done in March 2023). IR2023 reinforced the importance of strong and resilient supply chains to economic and national security. The government has also published, in conjunction with the NPSA and the Chartered Institute of Procurement and Supply, information that provides businesses with tools to understand their supply chains better and to manage risks and future shocks.[10] The government also committed to publish a new Supply Chains and Imports Strategy to support government and business action to strengthen resilience in critical sectors.

---

[8] https://www.gov.uk/government/publications/national-semiconductor-strategy/national-semiconductor-strategy

[9] https://www.gov.uk/government/publications/uk-critical-mineral-strategy

[10] https://www.npsa.gov.uk/supply-chain-resilience

The government is legislating to reform the way public authorities purchase goods, services and public works by simplifying and modernising procurement rules and procedures. The Procurement Bill will introduce new 'exclusion' and 'debarment' grounds enabling contracting authorities across the public sector to reject bids from any supplier that poses a threat to national security. Where there is a national security concern, the government investigates companies to decide whether the risk is intolerable and requires the use of powers.

The United Kingdom has been at the forefront of international activity to improve resilience. It has worked to secure commitments to joint action with the G7 and other partners, to challenge harmful practices which threaten economic security, such as economic coercion, and to strengthen economic resilience, reduce strategic dependencies and protect emerging technologies. Earlier this year, the United Kingdom and G7 partners launched the G7 Coordination Platform on economic coercion. This platform will provide a forum for identifying vulnerabilities and information sharing, as well as coordinating on rapid responses to economic coercion when it occurs. Through the Atlantic Declaration with the United States the government has agreed to closer cooperation on critical supply chains and national protective toolkits as part of a broader economic partnership covering technology, economic security and clean energy.

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.

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).

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.

The United Kingdom remains one of the most attractive global investment destinations and has one of the most reliable and safest energy systems in the world. All British energy projects are subject to robust,independent regulation which ensures that the United Kingdom's interests are protected.

The government continues to work with international partners, including through the G7 Clean Energy Economy Action Plan, to diversify clean energy supply chains in a way that ensures they are secure, resilient, affordable, and sustainable, and avoids overly concentrated supply where possible.

In recent months, Chinese involvement in the United Kingdom's civil nuclear sector has reduced significantly: the government has taken ownership of CGN's stake in the Sizewell C nuclear power project. Chinese state-owned nuclear energy corporations will have no further role in the project. The Department for Energy Security and Net Zero was created through a machinery of government change in 2023 and will focus on this and related issues, working closely with industry and other government departments to maintain a detailed picture of foreign involvement in energy infrastructure.

On the committee's recommendation SSS, and in line with its advisory role, NPSA will continue to engage with relevant parties on the security arrangements for Hinkley Point C as a priority. The specific scrutiny role proposed by the committee is not one that NPSA can or should perform; the government will, however, consider whether there is another organisation better suited to this role.

The government will continuously review measures to ensure that economic security and critical national infrastructure is protected. All investment involving critical infrastructure is subject to thorough scrutiny and needs to satisfy strong legal,

regulatory, and national security requirements. Any future projects beyond Hinkley Point C, and Sizewell C, including for any project brought forward for Bradwell B, will be subject to these individual assessments, i.e. a one step at a time approach. The United Kingdom plays a leading role in setting international standards and has a robust and effective regulatory regime for all British energy projects. This regime is overseen and enforced by the independent Office of Nuclear Regulation (ONR), which has robust enforcement powers. The ONR sets out its assessments in published Annual Reports, and on its website.

All employees and contractors working in the civil nuclear sector are subject to stringent pre-employment screening. Individuals with access to sensitive information, systems, materials and facilities are also subject to National Security Vetting which considers a range of factors, including nationality and period of residence in the United Kingdom. It is a statutory requirement for the civil nuclear industry to manage personnel security risks effectively. These arrangements are overseen and enforced by the ONR.

The National Security & Investment Act 2021 gives government powers that can be used to scrutinise and intervene when there has been a change in control of an energy asset. This can include changes in control of new energy projects that pose a current or future threat to national security, if relevant tests in the Act are met.

d. Technology and Data

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.

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.

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.

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.

The government agrees with the committee's conclusion that the United Kingdom's future success and security will depend on its ability to build on existing strengths in science, technology, finance and innovation. IR2023 reaffirms that strategic advantage in S&T remains a core national priority. The government will further strengthen national security protections in those areas where the actions of any foreign government poses a threat to the United Kingdom's people, prosperity and security, including protecting the United Kingdom's ability to generate strategic advantage through S&T.

The government recognises that China's significant expansion of military, economic and technological power makes it both more important and more difficult to maintain the United Kingdom's advantages in S&T. The government has therefore taken further steps to protect sensitive and public data, reduce dependencies in critical technological supply chains and promote innovation in British industry.

The United Kingdom has strong safeguards and world-leading investigation and enforcement to ensure that data is collected and handled responsibly and securely. All companies registered in the United Kingdom are subject to its legal framework and regulatory jurisdiction, and personal data transfers abroad are subject to a high level of legal protection. In 2022, the Department for Digital, Culture, Media and Sport published a Code of Practice on App Security and Privacy which helps to ensure that apps are more secure and resilient to cyber-attack and better protect individuals privacy.

The government actively monitors threats to data and will not hesitate to take further action, if necessary, to protect national security. In November 2022, government departments were instructed to cease deployment of visual surveillance systems produced by Chinese companies onto sensitive sites. In June 2023, the government committed to bringing a timeline to Parliament for when all Chinese surveillance equipment will have been replaced on sensitive government sites. In March 2023, TikTok was banned from all government devices in England and in Parliament,

except in a small number of special use cases, following a review which identified risks around how sensitive information could be accessed and used by some platforms. The Scottish and Welsh Governments have imposed equivalent bans.

Additional measures have been implemented to protect supply chains and technologies of strategic importance. In 2021, Parliament passed the Telecommunications (Security) Act to bolster the security of public telecoms networks and create one of the toughest telecoms security regimes in the world. Huawei was considered a vendor of concern, and therefore the United Kingdom is on a path toward complete removal of Huawei from its 5G networks by the end of 2027. As previously mentioned, the National Security and Investment Act, RCAT and ATAS also act to prevent the transfer of sensitive material and knowledge relating to S&T.

The government is committed to ensuring that export controls keep pace with new and emerging technologies and address evolving threats. In May 2022, it expanded the scope of the Military End-Use Control and added China to the list of countries to which it applies. This resulted in more than doubling the number of export licence refusals for China in 2022. The government is reviewing implementation of that control to understand better its overall impact and to determine whether its effectiveness can be improved further.

The government is also reviewing how controls apply to emerging technologies in a range of sectors and will consult on updating the export control regime to better tackle sensitive technology transfers, as set out in IR2023. It will also consider how to tackle the challenge of intangible transfers of technology and how to target end-uses, and end-users of concern, working with international partners to make multilateral controls more effective.

Alongside measures to protect the economy, the government has taken robust action to protect and promote innovation. New governmental structures, including DSIT, bring together core S&T functions across government. The National Science and Technology Council (NSTC), a cabinet committee chaired by the Prime Minister, has been established to address matters relating to strategic advantage through S&T. In March 2023, DSIT published the United Kingdom's new S&T Framework which sets out 10 cross-cutting system interventions to create the right ecosystem for S&T to flourish in the United Kingdom. Delivery of this framework is underway through an initial raft of projects worth around £500 million in new and existing funding. Government has dedicated £250 million to 'technology missions' that exploit and sustain the United Kingdom's global leadership in three critical technologies: artificial intelligence, quantum technologies and engineering biology.

The government has supported businesses to engage with China in a way that reflects the United Kingdom's security, prosperity and values, promoting safe and appropriate United Kingdom–China collaboration in the digital and technology space.

This includes the introduction of the Overseas Business Risk guidance mentioned above, that makes clear to British businesses the need to consider the risks of exposure to entities that may be providing or developing surveillance technologies when operating overseas. In 2022, in recognition of the threats to national security posed by the targeting of sensitive, cutting-edge technology, at the early commercialisation stage, NPSA and NCSC launched a "Secure Innovation" campaign. This follows the "Trusted Research" campaign and aims to provide guidance to start-ups and spinouts in the emerging and critical technology sectors. This year, the government is focused on increasing awareness of "Secure Innovation" across the technology sector, working with the venture capital community to explore mutual interest between protecting investments and securing businesses.

The government recognises that there is further work to be done. The whole of government will continue work to ensure progress against the S&T Framework, driving delivery through the National Science and Technology Council (NSTC). By the end of 2023, the government will publish an update setting out progress made, and further action required to achieve S&T Superpower status by 2030.

e. Intelligence and Effects

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" ***.**

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 ***. ***.**

The prioritisation of intelligence and effects is described above. The level of resource that the United Kingdom's security and intelligence agencies dedicate to China has increased significantly in recent years. SIS and GCHQ's effort must be constantly balanced to reflect the relative importance of each area to national security and prosperity and it should be noted that proportion of effort is not indicative of total size or effectiveness. The NSC decides on any necessary trade-offs as threats emerge and evolve, and the government is confident that SIS and GCHQ's priorities are commensurate with the risks faced and appropriately reviewed, and that MI5's operationally independent prioritisation reflects wider government strategy.

The Principal Accounting Officer (PAO) of the Intelligence Agencies is responsible for overseeing the Agencies' performance, and assuring Parliament of high standards of probity in their management of public funds. The Cabinet Secretary fulfils the role of the PAO, and is supported by officials that specialise in strategy, governance, policy development, programme appraisal, and financial management. The PAO uses regular senior meetings to monitor and scrutinise the Agencies' performance and return on investment. The government agrees with the Committee that it is essential that the Cabinet Office evaluates SIS and GCHQ's progress in meeting their targets, and can confirm that this is already underway. The Cabinet Office, in partnership with other departments, collects and analyses data on SIS and GCHQ delivery against requirements.

Ways Of Working And Machinery Of Government

a. Flexible working

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.

The government joins the committee in its praise of those civil servants who attended their usual places of work to perform essential functions during the pandemic (including the committee's own secretariat and the many other crown and civil servants who continued their work through Covid-secure measures) often in difficult professional and personal circumstances, both at home and overseas.

Throughout the pandemic, it was important for the organisations and government departments of the intelligence community to balance the need for staff to access classified IT systems with the need to stop the spread of COVID-19.

The intelligence community learned many important lessons about the benefits of hybrid working during the pandemic, and will continue to provide opportunities for staff to work from a wider range of locations where it is still possible for them to fulfil their roles. Much of the work involved with running such complex organisations can be done in a variety of ways, and providing flexibility allows relevant organisations to recruit and support a wide variety of staff and build a fully diverse and inclusive set of organisations.

b. Oversight

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.

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.

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.

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.

The government values the scrutiny the ISC provides and will continue to engage constructively with the committee to make sure that it is able to provide effective oversight, in line with its powers in statute and its memorandum of understanding (MoU). The government will continue to work closely with the committee to ensure that this essential scrutiny and accountability function works in such a way that protects the operating capabilities of the intelligence community.

The government notes the committee's comments about the provision of sensitive information to parliamentary select committees. There is existing guidance establishing that a protective marking is not sufficient reason for the government to withhold information from parliamentary select committees and there is an agreed process in place to provide sensitive information to any committee as needed.

The government is committed to the appropriate oversight of the operation of the National Security and Investment Act and the Investment Security Unit (ISU). In March this year, the government agreed a Memorandum of Understanding with the BEIS Select Committee—now transferred to the Business and Trade Select Committee—setting out arrangements for parliamentary scrutiny of the operation of the NSI Act and the ISU. This establishes arrangements to ensure the committee can access the information it needs to fulfil its scrutiny role, including setting out key principles on how and when the government and the committee expect information to be shared and protected. Separate arrangements are now being made for the ISU to deliver a classified briefing to the Business and Trade Committee about this area of work, in line with the MoU now in place.

This arrangement acknowledges the BEIS Select Committee's wealth of experience in scrutinising the NSI Act and complements the committee's oversight of the government's approach to business and investment more widely. The ISC is responsible for scrutinising the work of the intelligence community where it falls within their MoU with the government. It does not directly cover the work of the Investment Security Unit, as the unit does not provide an intelligence function. The

committee is able to scrutinise the work of the ISU where there is overlap with the work of the United Kingdom's intelligence community. This applies to other committees, such as the Foreign Affairs Committee, where the work of the ISU may touch on areas within its remit.

The government agrees with the committee that it is important that civil servants across the whole breadth of departments have access to vetting and facilities appropriate to their roles. As part of the recent machinery of government changes, there are a number of in-progress physical moves and specification of appropriate IT and other facilities. The number of cleared personnel does not, in and of itself, provide a meaningful measure of effectiveness, especially in wide-ranging policy areas such as China. We will continue to engage constructively with the committee on this point to determine the best and most proportionate measures for its purposes.

A robust personnel vetting regime is in place to identify and manage risks arising from staff with access to sensitive government assets and intelligence. Those with security clearance have their vetting reviewed throughout their careers, ensuring those who may be susceptible to pressure, improper influence or may even actively seek to act on behalf of a foreign intelligence service are identified.

As mentioned above, civil servants are also educated on the risks posed by hostile intelligence services. and a strong security culture is ingrained across the civil service to ensure sensitive material is protected.

COVID-19

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.

The government welcomes the committee's recognition of the complexities concerning the origin and spread of Covid-19. There are clearly questions that still need to be answered so the United Kingdom is better prepared for future pandemics. It is important not to draw any definitive conclusions or rule anything out until the WHO-led independent, science-led review has concluded. However, the United Kingdom's assessment is that it is highly likely that SARS-CoV-2 (the virus that causes COVID-19) is naturally occurring. It is unlikely that COVID-19 originated from a laboratory-acquired infection or accidental release from a laboratory.

COVID-19 reminded us that the United Kingdom, as a global trading and tourism hub, is vulnerable to biological threats with catastrophic impacts. As devastating as COVID-19 was, there is a reasonable likelihood that another serious pandemic could occur soon, possibly within the next decade. In response, the Biological Security

Strategy was published on 12 June setting out a renewed vision, mission, outcomes and plans to protect the United Kingdom and its interests from significant biological risks, no matter how these occur and no matter who or what they affect. The government's vision is that, by 2030, the United Kingdom is resilient to a spectrum of biological threats, and a world leader in responsible innovation, making a positive impact on global health, economic and security outcomes. This includes ensuring preparedness against future pandemics.

E02979899

978-1-5286-4437-2