

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

NATIONAL SECURITY AND INVESTMENT BILL

Third Sitting

Thursday 26 November 2020

(Morning)

CONTENTS

Examination of witnesses.
Adjourned till this day at Two o'clock.

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Monday 30 November 2020

© Parliamentary Copyright House of Commons 2020

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: † SIR GRAHAM BRADY, DEREK TWIGG

† Aiken, Nickie (<i>Cities of London and Westminster</i>) (Con)	† Onwurah, Chi (<i>Newcastle upon Tyne Central</i>) (Lab)
† Baynes, Simon (<i>Clwyd South</i>) (Con)	† Tarry, Sam (<i>Iford South</i>) (Lab)
† Bowie, Andrew (<i>West Aberdeenshire and Kincardine</i>) (Con)	† Tomlinson, Michael (<i>Lord Commissioner of Her Majesty's Treasury</i>)
Fletcher, Katherine (<i>South Ribble</i>) (Con)	† Western, Matt (<i>Warwick and Leamington</i>) (Lab)
Flynn, Stephen (<i>Aberdeen South</i>) (SNP)	Whitehead, Dr Alan (<i>Southampton, Test</i>) (Lab)
† Garnier, Mark (<i>Wyre Forest</i>) (Con)	† Wild, James (<i>North West Norfolk</i>) (Con)
† Gideon, Jo (<i>Stoke-on-Trent Central</i>) (Con)	† Zahawi, Nadhim (<i>Parliamentary Under-Secretary of State for Business, Energy and Industrial Strategy</i>)
† Grant, Peter (<i>Glenrothes</i>) (SNP)	Rob Page, Yohanna Sallberg, <i>Committee Clerks</i>
Griffith, Andrew (<i>Arundel and South Downs</i>) (Con)	
† Kinnock, Stephen (<i>Aberavon</i>) (Lab)	† attended the Committee

Witnesses

Lisa Wright, partner, Slaughter and May

Christian Boney, partner, Slaughter and May

Professor Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government, University of Oxford

Public Bill Committee

Thursday 26 November 2020

(Morning)

[SIR GRAHAM BRADY *in the Chair*]

National Security and Investment Bill

11.30 am

The Committee deliberated in private.

Examination of Witnesses

Lisa Wright and Christian Boney gave evidence

Q80 The Chair: Before calling the first Member to ask a question, I should like to remind all Members that questions should be limited to matters within the scope of the Bill and that we must stick to the timings in the programme motion that the Committee has agreed. For this session, we have until 12.15 pm.

I welcome the two witnesses from Slaughter and May. Can I ask you to introduce yourselves for the record, please?

Lisa Wright: Hi, my name is Lisa Wright and I am a partner in the competition group at Slaughter and May.

Christian Boney: Good morning. I am Christian Boney and I am a partner in the corporate mergers and acquisitions group at Slaughter and May.

Q81 Chi Onwurah (Newcastle upon Tyne Central) (Lab): Thank you very much, Ms Wright and Mr Boney, for sharing your expertise and time with the Committee. It is indeed extensive experience of mergers and acquisitions.

I am sure you are aware that many countries—the US and Canada are just two—give some sense of the factors that might be considered under a national security assessment. Do you think it would be helpful for market participants to have greater clarity about the types of factors that would be considered? How could we give that clarity while retaining the sensitivity and discretion that are needed on those matters?

Joined to that, there are cases such as Arm and DeepMind where economic security became national security over time. When considering what national security is, what links do you see between national security and economic security or sovereign capability? Can they better be reflected in the Bill?

Christian Boney: Lisa, shall I have a go at that first?

Lisa Wright: Yes, go for it.

Christian Boney: Starting with the need for factors to help inform market participants' decisions about whether, for example, their potential transaction presents risks, yes—in short, the more guidance that can be given about the kinds of factors that the Government will consider in determining whether a transaction presents a national security concern, the better. The statement of policy intent is very helpful in framing that, but clearly the more detail that can be included, the better.

The other thing that will be important in giving people a sense of whether their transaction should be notified or whether it falls within a mandatory notification sector is the interaction that will take place through informal engagement through the investment security unit. It is very important that the process for getting informal guidance from that unit is as streamlined, interactive and responsive as it can be. That will go some way to giving practitioners realtime guidance on potential concerns.

Lisa Wright: Can I just add a point to the idea of the desire for more certainty around what national security means? I think it is worth recognising that that is particularly important if you look at where we have come from. With the existing regime under the Enterprise Act 2002, there have only ever been a dozen or so interventions on national security grounds. There is not a widespread understanding of what it means and the circumstances in which the Government would intervene. That is the historical position, but we all know that this is constantly evolving.

When you take that and add to it the fact that the prediction now is that there will be, as it says in the papers, between 70 and 90 call-ins a year, that is obviously a huge increase against the 12 since the Enterprise Act. Any greater clarity that can be given around the circumstances in which the Government would be looking to, for instance, exercise the call-in powers would be beneficial, particularly at the beginning of the regime when everybody is trying to learn the ropes.

Q82 Chi Onwurah: You mentioned, and I think it is absolutely right, the issue about going from a standing start to such an increase in the number of callings but also in the number of notifications—the impact assessment estimates 1,830 notifications. That is on the acquirer and does not take into account the fact that almost every start-up seeks capital investment at some point and I imagine would, therefore, as a consequence have to think about this regime. What impact do you foresee on the UK's investment climate and especially on capital sources for small and medium-sized enterprises? How could that impact be mitigated or encouraged to be as positive as possible?

Christian Boney: I think this question really divides into two. In terms of larger corporates, investment by, and in, larger corporates is very likely to be unimpacted in any meaningful way by this legislation, because large corporates and their advisers are very used to going through regulatory clearance processes. This will just be another thing that needs to be added to the list.

I think you make a very valid point in the context of start-up and early-stage companies. The concern I would have principally is with those companies that are in that phase of their corporate life and fall within the mandatory notification sectors. Given the kinds of companies that this country is trying to encourage to flourish—those that are active in areas like artificial intelligence, advanced robotics and quantum technologies—a reasonable number of start-ups, I would expect, would fall within those mandatory notification sectors. For them, this regime is going to make the process of getting investment more time-consuming and more complex.

Anything that can be done in the process of consulting on the mandatory sectors, and anything that can be done to pair back the regime to make it more workable

for companies in that stage of life, the better. An example might be some form of de minimis threshold, which is included, such that really early-stage companies do not fall within the mandatory notification regime, but the Government can nevertheless rely on their call-in power down the track, should that early-stage company become successful and more strategically important within the UK. Those are my principal thoughts. Lisa, do you have anything to add?

Lisa Wright: Not on that point, no

Q83 The Parliamentary Under-Secretary of State for Business, Energy and Industrial Strategy (Nadhim Zahawi):

May I return to the national security issue—as opposed to the wider public interest test, which is an important question—and get your view as to the Bill’s scope, which is very much focused on national security, versus the wider public interest, to which I think my colleague’s first question alluded?

Chi Onwurah: To clarify, my question was this: how would you distinguish between national and economic security?

Nadhim Zahawi: My question is more about your reflections on the Bill being narrow in its purpose to deal with national security versus the wider public interest.

Lisa Wright: It is already a very broad regime; it catches a lot of transactions, as we have just discussed. I therefore think it is important and right that it is limited, in terms of the substantive concerns that it is catching, to national security. That is already a necessarily, I think, uncertain or undefined concept. Corporates and investors can make it work as long as other aspects of the regime work efficiently. That may be subject to some of the points that Christian just made about the impact on start-ups.

I think that once you broaden the regime out from national security into other considerations, you do risk introducing quite a degree of unpredictability, which possibly would impact on people’s assessment of the investment climate in the UK. My understanding is that the existing intervention regime under the Enterprise Act is planned to remain in force, so the national security considerations will come out of that and will be dealt with under this new regime. But there will still be the ability for—[*Inaudible.*]

The Chair: Mr Boney, do you have any observations while we are waiting for the tech to work?

Christian Boney: I agree entirely with what Lisa has been saying. I think the scope of the Bill is already broad, so to my mind, broadening it further to take account of other areas is likely to introduce the uncertainty that Lisa was referring to and, as a consequence, have a potentially negative impact on the investment climate in the UK.

The Chair: Lisa, it looks like we have got you back now. Would you like to add anything?

Lisa Wright: I am not sure at what point you lost me, but I think I was saying—

Nadhim Zahawi: We lost you while you were talking about a “degree of unpredictability”, Lisa.

Lisa Wright: Okay. In my view, if you were to broaden the regime out from national security to take into account other considerations, that would introduce quite a degree of unpredictability and would, I think, potentially impact negatively on people’s assessment of the investment climate in the UK—I am sorry if I am repeating myself. However, my understanding is that the existing intervention regime will remain, so national security will come out of it, but the Government will still be able to intervene in transactions on other public interest grounds under the Enterprise Act. That regime has some limitations, but those powers will still be there.

Q84 Stephen Kinnock (Aberavon) (Lab): Thank you very much for the really excellent evidence you have already given us. I want to go back to what Mr Boney said about de minimis thresholds and whether you might look at introducing de minimis thresholds for particular areas, sectors or industries that I guess you would say are considered to be low risk from a security point of view and highly beneficial to the UK economy, which should therefore affect our thinking about how you might filter this whole process. But are there not other considerations on filtering as well? In essence, this is a risk management process and you have to identify the highest risks. Surely issues of critical national infrastructure would place a type of acquisition into the high-risk quadrant. If the acquirer is close to a state or Government—particularly a hostile Government—that would place it in the high-risk quadrant. Therefore, on having a more filtered process, is the de minimis threshold the right way to go, or would it not be better to have a strategic approach based on a hierarchy of risks?

Christian Boney: I think the de minimis concept is potentially relevant and helpful in the context of thinking about what needs to be subject to mandatory notification. If you are not within the mandatory notification regime, that does not mean that the Government cannot exercise the call-in power so long as the relevant tests in the legislation are satisfied; it just means that the relevant company does not have to make a notification. There are elements of the mandatory sectors where some form of de minimis has already been included. Energy is a good example of that, and that makes sense in the context of energy.

I think it is worth exploring whether, within any of the other sectors, where we are more likely to see start-up, early-stage companies operating, there is benefit in introducing some form of de minimis regime solely in respect of the mandatory notification requirement. As I say, if a small-scale company operating in critical artificial intelligence is receiving investment from somebody who we view as a hostile actor, that transaction might escape mandatory notification, but that does not mean it escapes voluntary call-in by the Government at the point they become aware of it. That is something that might be worth exploring.

Stephen Kinnock: Thanks very much. Does Ms Wright want to add anything?

Lisa Wright: No.

Q85 Stephen Kinnock: I want to explore a bit further the issue of critical national infrastructure, which is defined by the Intelligence and Security Committee as

[Stephen Kinnock]

the Government's 13 sectors ranging from energy to transport infrastructure and anything that relates to public health. With covid, we have seen the massive importance of how we have been overexposed in certain supply chains, and that might have an effect on our thinking about critical national infrastructure. To what extent does that influence your work on mergers and acquisitions and your thinking about whether such mergers and acquisitions in areas of our critical national infrastructure are in the national interest?

Christian Boney: If I am following the question correctly, I think it is the correct balance to strike to say that people pursuing significant M and A activity involving the UK's critical national infrastructure should expect to go through a notification process and should expect their transaction to be at potential risk of examination and call-in. From my experience, corporates undertaking transactions in the spheres of national infrastructure and so on expect that. It is what they see in other countries and jurisdictions, so it is something they come to accept as part of doing deals in top-tier democratic nations.

Lisa Wright: I agree with all that. I guess I would also add that people are well aware that these considerations change over time. This year has shown that more than ever. People have an eye on what might not have been an issue yesterday; today, it might be different. We saw the amendments coming through to the Enterprise Act earlier in the autumn to bring in the power to allow the Government to intervene on public health grounds. People are very conscious of the fact that this changes, and they keep an eye on it from that perspective.

Q86 Simon Baynes (Clwyd South) (Con): Thank you both for your submissions this morning. I want to go further into the issue of how you, the Government or the agency it sets up to do this makes a judgment about whether a small or start-up company really falls within being a threat to national security. I imagine that that might be quite a difficult judgment to make. I am putting to one side the issue of mandatory notification, which Mr Kinnock has looked at in more detail. I am saying that once it has been notified, how do you make the judgment about whether it is a threat to national security?

I would have thought that there are two aspects to that. One is the nature of the acquirer, which is partly what you have already alluded to. The second part is that I would have thought that it is quite difficult to ascertain whether something at the cutting edge of technology is or is not a threat. I would have thought that that is a really difficult judgment to make in practice. Do you have any thoughts on that, and what experience do you have of other regimes trying to make that kind of judgment?

Lisa Wright: I think there are probably a number of ways to tackle that question. I guess that an answer is that it is ultimately a question for the Government. They are the ones who understand the threats and the intelligence. As advisers, we can look at the guidance and cases that have happened in the past, and we can speak to the unit, which, as we understand it, will be open for engagement and will welcome that. We can guide clients through the process, using the touch points

and information that is available to us, but ultimately it is the Government that are in possession of the full set of facts and considerations that go into the decisions about whether that particular transaction is a problem or not. I guess what that speaks to is having the right people in the unit and getting them plugged into the right people elsewhere in Government to arm them with the ability to make these assessments.

Christian Boney: To pick up on that, I agree entirely with what Lisa said. It is not necessarily an easy thing for the advisory community or clients themselves to make a judgment about whether they are presenting risk to national security. That is why this concept of real-time, interactive engagement with the unit that is set up to police this regime is going to be so important.

In the world I operate in, one of the regulators we deal with is the Takeover Panel, which is fantastic at being responsive, with real-time engagement. It results in a dialogue and an interaction that helps advisers navigate their clients through a regime that is not straightforward at times. That is the kind of practice that could usefully be learned from in the context of the investment security unit, because that kind of real-time feedback and informal advice will be very helpful in helping companies make the judgment about which side of the line they fall.

Q87 Peter Grant (Glenrothes) (SNP): Good morning, Ms Wright and Mr Boney. I want to look in more detail at the kind of information that might be included in the Secretary of State's clause 3 statement, which will set out the kind of factors that they will take into account in deciding whether they needed to intervene.

There is a fair amount of information in the Bill and the documents published alongside it about the kinds of businesses being acquired or taken over that might give rise to concern. There are quite clear definitions of what constitutes a trigger event, whether it is a purchase of shares or whatever, but there is very little detail about how the Secretary of State will decide which potential acquirers pose a threat. There are clearly good reasons why that information cannot be made public in too much detail, but is the fact that there is so little on the face of the Bill about how that decision is arrived at a problem? Does it make it less certain and therefore more likely to result in legal challenge?

Christian Boney: Acquirer risk is one of the points picked up in the statement of policy intent that is going to be looked at when determining the level of risk that a transaction presents. When looking at and explaining acquirer risk, I think that helpful additional guidance could be added to it to, for example, make clearer how the Government will consider acquirer risk in the context of things such as private equity funds and other funds that may be looking to invest in the UK. By that, I mean in particular whether the Government will be willing to disregard the identity of limited partners and other investors in funds that sit above the particular acquisition vehicle that is doing the relevant transaction. That is the kind of thing that I think there would be real benefit in trying to make clearer in the statement of policy intent.

Q88 Peter Grant: Thank you. I will focus a bit more on the definition of a trigger event, and in particular the catch-all provisions that define when somebody becomes a person with significant influence or control over a company.

The Companies Act 2006 has similar requirements for a company to notify Companies House if certain things happen that put someone in a position of significant influence. From a lay person's point of view, such as my own, some of those provisions are almost word for word the same in the Companies Act and the Bill. Some appear to have the same effect but the wording is different, and therefore there will potentially be occasions when the definition is different. Would there be benefits in completely aligning both pieces of legislation so that a particular event either has to be notified or does not have to be notified? Otherwise, there is the possibility that some events will have to be notified under the Bill, and other events will have to be notified under the Companies Act but not the Bill.

Christian Boney: In short, I think there would be benefit in having as much alignment as there can be. Clearly, the two pieces of legislation are not necessarily designed with the same intent and focus in mind. Yes, I think there is merit in having as much alignment between the two as there can be.

If I may, there is just one point about the trigger events that is worth considering. One of the points in the statement of policy intent in the context of trigger events is the Government considering the risk of espionage. That seems to me to be something that is worth thinking about in the context of this regime. At the moment, the trigger events are focused, as you were saying, on the ability to influence a particular company, but there are certainly circumstances where, without acquiring a level of shareholding that enables a person to influence the company, the person can nevertheless gain very significant access to information—for example, through a board seat, which might come at a shareholding of lower than, for example, 15%. That would give that person considerable access to information within the company. If they were a hostile actor and they wanted to act in a nefarious manner, it would enable them to feed that information back to another hostile party. We have spoken about narrowing the scope of the regime, and I appreciate that that would be an amplification of it, but I think that is a point that is worth considering.

Q89 Mark Garnier (Wyre Forest) (Con): I will carry on with the line you took just now about an investor's potential influence over or access to a company. A little earlier, you were talking about start-ups who sought to get staged financing in order to try to build their businesses. Of course, there are more ways of getting investment than just getting equity. We know that if a business has a relatively small amount of equity but a huge amount of debt, the provider of the debt has much more influence over the company than perhaps the shareholders do. We saw that on the banking commission when we looked at the role of bondholders in influencing banks, compared with equity holders. Clearly the bondholders, in effect, had much more influence.

The other thing is that a start-up company can raise money in other ways. The Bill tries to make sure that we are not losing intellectual property, but a business can raise finance by licensing the intellectual property that we are trying to protect—I am not sure that that would come within the scope of this Bill—or even sell the intellectual property and license it back again. There are various other ways in which a company can raise finance, over and above equity, where there is a huge

amount of influence or it falls outside the Bill. Clearly, crucial national infrastructure is a very different thing, but intellectual property is something that is very difficult to grab hold of; it is like trying to grasp a handful of sand. Given the objectives, I wonder how the Bill tackles those other areas, which seem to allow malign investors a way through.

Christian Boney: I think an important aspect of the Bill—this is one of the reasons why Lisa and I have described it as a broad regime—is that it does allow policing of the acquisition and control of assets, including intellectual property. In my experience, at least, that is quite different from what you see in other international regimes. Clearly, the acquisition of control of assets does not fall within the mandatory notification regime; nevertheless, it is helpful that the Government have the power potentially to exercise a voluntary call-in in respect of, for example, an acquisition or a licence of intellectual property.

Q90 Mark Garnier: And the debt issue—the fact that debt holders can be more influential over businesses than equity holders?

Christian Boney: That is certainly fair. I think the level of influence and control that a debt provider will typically get in what I will call the ordinary courts means that it is less likely—I am certainly not saying it is impossible—to be at the level of getting such granular, sensitive, let us call it operational information, which is the kind of thing we would really be concerned about. It would more be focused on getting access to financial projections, financial performance and that kind of information, which, although it can still be sensitive, is probably less sensitive than operational data. A balance needs to be struck, it seems to me, in the context of this legislation. Not having debt providers obviously within scope does limit the legislation, but does it strike an acceptable balance? My personal view is that, on balance, it probably does.

Q91 Nickie Aiken (Cities of London and Westminster) (Con): From your professional point of view and experience to date, what could be the long-term impact of the Bill on UK business and investors? Will the Bill help or hinder the global position on investing into the United Kingdom?

Lisa Wright: In many ways, the regime just brings the UK into line with major international peers. From that perspective, for people doing deals around the world who have already experienced those other regimes, it ought not to have any real negative impact at all, provided that BEIS can deliver on the aspiration set out of a slick and efficient regime, turning around notifications within sensible deal timeframes and providing the kind of informal advice and early engagement promised. That will be critical, particularly in the early stages of the regime. From that perspective, I do not think this should have a long-term negative impact on people wanting to do deals in the UK. As Christian was mentioning earlier, it may be a slightly different picture for the start-ups and the smaller companies where they are caught up in the mandatory sectors, but overall I think it is right that this can be viewed as the UK bringing itself into line with what else is going on around the world.

Christian Boney: I agree with that. That is the right assessment.

Q92 Sam Tarry (Ilford South) (Lab): Picking up the idea of bringing us into line with global peers and equivalent countries, there are many different regimes and you both have incredible global experience legally. If you have experience of dealing with companies and transactions, mergers and so on, particularly in the US, you will know that it has the Committee on Foreign Investment in the United States, with its white list of almost green-lighted countries, which they can deal with slightly differently. Should we consider something like the US does with its more established regime and having not necessarily an approved list but different layers for our regime, from the most hostile countries through to those who are our closest allies?

Lisa Wright: It is certainly worth considering. I would imagine that those sorts of considerations will be going through the mind of the officials and the Secretary of State tasked with making these assessments and issuing the decisions. I can see there may be some sensitivities and a desire perhaps not to make that all transparent in terms of public documents. Perhaps they think they will deal with it over time through this engagement and, with advisers and parties coming to talk to them, you will get a sense of who is okay and who is not that. But I can see that perhaps they will not want to put that down in very great detail on a public piece of paper, not least because one might imagine it could change over time. I guess there needs to be a degree of flexibility to recognise that.

Christian Boney: I agree. I am certainly not a CFIUS expert, but my understanding of the exempt list of countries is that actually the practical impact is quite tightly drawn. I do agree with Lisa. I think we are likely to get the best sense of those countries that are viewed as more risky than others through the engagement process and as people's experience of the regime develops.

The Chair: We are almost at the end of the time available for this session, so there will be no further questions for these witnesses, but thank you, Ms Wright and Mr Boney, for being so generous with your time and assisting the Committee so much. We will now move on to the next witness—either we will suspend the sitting briefly until everything is sorted out or we will move seamlessly on—but thank you both very much.

Examination of Witness

Professor Ciaran Martin gave evidence.

12.10 pm

Q93 The Chair: Would you mind, Professor Martin, just introducing yourself for the record and for the benefit of the Committee?

Professor Martin: Thank you. My name is Ciaran Martin. I am currently a professor of practice at the Blavatnik School of Government at the University of Oxford, but until August of this year I was the founding chief executive of the National Cyber Security Centre and a member of the executive board of GCHQ, within the Government. I should also declare for these purposes,

although I am not sure it is relevant, that I serve on the advisory board of a US venture capital company called Paladin.

Q94 Chi Onwurah: Welcome, Ciaran; it is great to see you here. Thank you so much for sharing your expertise: as the founder of the National Cyber Security Centre, you have a great deal of expertise. I want to ask you to talk about a question that I have raised a number of times and that your expertise should be able to give us a real view on, which is about understanding the distinction, if there is a distinction, between national security and economic security concerns. You will be familiar with a number of cases, such as Arm and DeepMind, to name just two, that involved an economic security issue, you could argue—in terms of sovereign capability in artificial intelligence in the case of DeepMind, and of mobile silicon in the case of Arm—but that pretty swiftly turned into national security concerns. This Bill identifies a number of different sectors or areas—up to 17, I think—where a notification will be mandatory. How can we look at understanding or reflecting a distinction between evolving economic security and, ultimately, our national security?

Professor Martin: Thank you for your comments, Ms Onwurah; it is nice to see you again. I speak as someone who thinks that the Government have broadly got this issue correct, in terms of their proposals in this Bill. That is not to underestimate the sheer complexity of dealing with the core, fundamental question that you rightly identify of balancing economic security and national security and of where one stops and the other begins. That is a very complicated and difficult thing to do. I think one starts with an attempt to define a core principle, which is essentially around the freedom to act. I think that if you look at something such as Arm—I would say this probably more in the case of Arm than DeepMind—and its potential ultimate sale to Nvidia, you see that the UK has less freedom of choice in a key strategic technology, which undermines its own ability.

I think there is an analogy with the little known but quite long-standing—for more than a century—work on sovereign cryptography. That is one of the areas that has long been covered by national sovereignty requirements. There are things in information security, as we used to call it, cyber-security, as we do call it, that have always needed to be fully sovereign, entirely British-made—they are not very many areas. The problem has been that as technology and communications have changed, it has been quite hard to keep up, and there are always pressures to expand that in a way that is economically harmful to competition and so on. So it needs a clever buyer within Government to identify what will be the strategic areas and what will not be.

In the area of sovereign cryptography, we end up trying to keep, depending on the era, around half a dozen or a dozen companies viable, because it is not a lucrative market. You can see the problem, but the key issue is whether there is enough, first, sovereign, but if not sovereign, friendly capability that allows us the freedom of choice to adopt key technologies. That means identifying the key technologies in the first place, evolving them over time and then having a very difficult to achieve but necessary intelligent function within Government that can evaluate the notifications that it

gets. Of course, at the moment we do not have the power to do that, and that is what this Bill correctly seeks to remedy.

Q95 Chi Onwurah: Thank you. I am very taken by your definition of sovereign and friendly capability. Indeed, that is exactly what we do not have in our 5G networks, hence the mess with Huawei.

Moving on slightly, a comment made numerous times on Second Reading was about the role of the intelligence services. Indeed, my right hon. Friend the Member for North Durham (Mr Jones) asked for more intelligence in the process. How can the Bill better ensure that the intelligence services, including the National Cyber Security Centre, have input and scrutiny and, indeed, provide their expertise as part of the process so that the appropriate decisions are taken?

Professor Martin: I think the essential, principal requirement is not the intelligence services' involvement—although that is important and I will come to that in a minute—but the understanding of technology and technological developments within Government. These are fundamentally economic issues as well. Apart from anything else, if you look at some of the reasons why the Bill has come about, you will see that, in strategically important technologies, the Government have invested heavily in university-sponsored research and in private sector research, only to see the fruits of that research sold off. Even if that did not impact on national security, which in most cases it does, it is not a good return for the taxpayer in terms of long-term UK involvement if the intellectual property ends up being monetised elsewhere.

I have enormous respect for Mr Jones and I think he is on to something in terms of involving the national security and intelligence services, but I do not think this should be intelligence-led. In my experience—obviously, I cannot go into detail on this particular aspect of it—secret intelligence adds relatively little to your knowledge of intent. If we take Russia and China, the two big strategic threats to the UK, Russia does not have a strategy in this space. We have to worry about Russia and cyber-security because it attacks us, but it attacks us on the internet that the west has built.

China is very different. China has a technological, strategic dominance aim, but it is not a secret. It is published and has been translated into English in the Made in China 2025 strategy, as you know. Our knowledge about the precise, intricate details of how that is implemented gains relatively little from secret intelligence.

What secret intelligence does have, particularly in GCHQ and the NCSC within it, is a knowledge of how technology works in terms of the national security threat space. I think the UK has a head start on other countries, because the National Security Council innovations of the 2010s gave the intelligence services a much bigger voice at the table, and that is reflected in the structures that we have now. The UK should be well placed to be able to listen to the intelligence services, but I would encourage—not least to make sure that in this very delicate balance of trying to show that we still have an open economy and are not shutting the doors to investment—as much transparency as possible on the decision taking. It will not always be possible because GCHQ technologists will know about things—exploitations of particular bits of technology—that they cannot reveal.

They will be able to tell that to secret forums within Government for consideration—I am quite confident about that: there will be a seat at the table for them.

My recommendation would be that, as far as can safely be done, the Government should be relatively open about why they make the judgements they make about strategic areas of technology and the interventions they will make once this Bill is passed—assuming that both Houses wish to pass it.

Q96 Nadhim Zahawi: Professor, that was excellent and I am very grateful for it. I will follow on from that thought and ask about the proposed powers within the regime for the Secretary of State to gather that information, which, as you quite rightly remind us, is not necessarily secret but about understanding the technology, or a particular piece of the technology, within the sector. What are your thoughts on the regime for the Secretary of State to be able to gather that information to inform a decision or to call in witnesses, so that they are able to really understand that particular issue and therefore make a decision on it?

Professor Martin: I suppose the mantra, if I had one, would be, “Broad powers, sparingly used, with accountability mechanisms”. It is incredibly hard to be specific about this, for two reasons: one is that new areas of technology crop up, as they invariably do, and the other is that sweeping categorisations are needed on the face of legislation.

I am not a deep technical expert—although others are available from my former organisation—but if you take sweeping, umbrella titles like “quantum” or “artificial intelligence”, there are huge swathes of that where, actually, not a lot of these powers in the Bill will be used. There will be companies that will be doing very interesting things—10 interesting things—of which only one would be caught by this Bill.

If you take areas like specialist quantum computing and so forth, I think the community of interest and expertise is actually relatively small and has relatively good relations with Government—not least because, again, while it is not perfect, the whole system of research council funding and Government investment in funding technological research is pretty good, by international standards—so you end up knowing these people. One of the reasons that this sort of policy evolution came about, which has led to the publication of the Bill before you—I remember this from discussions within Government—is that people were volunteering to come to us. World-leading experts, people who had been funded by the Government—I will not go into individual cases because it is commercially sensitive and possibly security sensitive—would come to Government and say, “Look, we’ve had this inquiry from a Chinese behemoth,” or even, “We’ve had this inquiry from a US company,” and so forth: “What do you guys think about this?” and, invariably, we would have to have an informal influencing discussion.

I do not think that some of the businesses to which this will apply will be screaming that this is horrible Government regulation and intervention in areas where that should not be made. There was already a dialogue; there was just no legislative framework. Of course, that meant that companies that felt a loyalty to the UK and so forth but that also had to look after their commercial interests were sometimes in a real bind.

To try to answer your question, I think that the powers should be fairly broad. I think there should be accountability and transparency mechanisms, so that there is assurance that they are being fairly and sparingly applied.

Q97 Stephen Kinnock: This is very interesting evidence. I want to ask you a little bit more about China. As you rightly pointed out, much of this is in the public domain, and the Made in China 2025 strategy is very clear about the objective, which is to achieve global technological dominance. Given your experience at the National Cyber Security Centre, can you share with us a little bit more about how that would manifest itself in practice? What do you see as China's next moves, in terms of rewriting the rules on technology and on creating that dominant position that you have talked about? How do you see that manifesting itself?

Professor Martin: I think there are broadly two or three areas in which China is very interested in doing that. I can make some comments on motivations, because I think they are very important, and then I will finish with how that manifests itself in UK casework.

Clearly, China has set out a stall, which it published in Made in China 2025, in which it said it wants to be the world's pre-eminent leader in a number of key areas of technology. It mentioned artificial intelligence and quantum, and it is throwing vast sums of state money and long-term strategies at them, unencumbered by the need to seek re-election and popular consent, so it is a very powerful movement. That is the first thing: it is trying to build up its capability.

China is also trying to change, at least for itself—we will come to that in a minute—the way the internet works. It was reported earlier this year that Huawei and other major companies in these international standards bodies are looking at something called new IP protocols, among many other things. To give you a sense of what the motivations behind that are, at the minute when traffic flows around the internet, despite some popular impressions to the contrary, it is actually pretty hard to work out what is going through it. Therefore, it is relatively difficult to censor, although China has managed it in some ways. The new IP protocol will make it much easier to work out what sort of traffic is going through and being rerouted, so it makes it much easier to control. China is trying to dominate and essentially get a lead in the strategic technology, and also to change the character and culture of the technological age from one that started off fairly anarchic to one that is much easier to control. That is what it is trying to do.

Why is China trying to do that? A lot of this is about the assertion of its own power for itself—the regime, power, Chinese nationalism and so forth. I think it does intend to extend its sphere of influence, but I have never seen that as the primary motivation. One of the interesting things, post the pushback from the Trump Administration and the US sanctions on Huawei, is the extent to which China will now accelerate its desire for self-sufficiency, and the extent to which that leads to a separate pole of technological influence that may become less interested in countries such as the UK, European Union countries and North America.

To date, how has that manifested itself in cases in the UK? Ms Onwurah has already mentioned the Huawei controversy. If you take Huawei as a company, I think it

shows the different ways in which this can manifest. The Huawei 5G controversy is going to be dealt with by a Bill that I believe is coming to the House next week, not this one. The 5G controversy was not about investment; it was about selling to British companies to build stuff. Obviously, that case has been very heavily analysed.

I think that the more interesting case in the last 10 years involving Huawei was its acquisition in 2012 of the Centre for Integrated Photonics—a world-leading British firm in a really key area of technology. That, in my view, was pretty strategically damaging. If we had our time over again, that is the sort of thing that the Bill might well notify. I know you have taken evidence from the likes of Charles Parton and people with huge China expertise. The fact that the acquisition of the Centre for Integrated Photonics did down Britain's technological development was probably a by-product. The point is that Huawei could buy world-leading research, which China could then take and appropriate for itself very cheaply. That is what it will continue to do to build up its own capabilities.

Q98 Stephen Kinnock: Given what you just said about the nature of the threat, how should that inform the composition of the investment security unit, which is going to be placed in BEIS and will be the primary locus for the screening of acquisitions? Would you say that it needs to have absolutely leading expertise in technology in the issues that you mentioned—quantum and so on? Should it also have China experts and people who speak Mandarin?

Professor Martin: One of the reasons that this is so difficult, as I said in my first answer to Ms Onwurah, is that I can think of at least three areas of expertise that the unit is going to need to draw on. Technological, yes, because of what technologies will matter. Geopolitical, yes, and I do not have a strong view on whether it needs Mandarin speakers because the UK has a strong and intelligent foreign service mission in country in China and all over the place that can provide input. But the third thing is actually quite a lot of commercial nous—patent laws and so forth.

This is where there is a distinction. This is not all about China. It is layered, and there will be things that we would not want to see going even to quite friendly countries. Arm is a case in point, with the concentration of power in a couple of US companies—particularly when one of them is derived from UK technology. That is not comparable as a strategic threat to Chinese dominance—I hope the Committee does not think I am saying that—but there are times when it would be a damaging foreclosure, if you like, of UK freedom of action and freedom of choice. We know that the US has a strong and sometimes aggressively used extraterritorial legal system in which it can use the power of US companies and block trading with US companies and so on, so we need people who understand those areas where we think, “We are not sure we would want that to leave the country at all” as well as people who understand Chinese. That involves a lot of expertise in things like patents, international law, US commercial law, sanctions and so on.

Q99 Andrew Bowie (West Aberdeenshire and Kincardine) (Con): Professor Martin, I have been listening with interest—it has been fascinating—especially when you were talking about the need to balance national security,

the national interest and economic security. I have been reading the very good briefing by the Law Society of England and Wales, which suggests that the Bill could be improved by the insertion of a definition of national security. Do you agree?

Professor Martin: I do not vehemently disagree with that suggestion, but I am not persuaded by it. It is not a new issue. I remember cases—they have nothing to do with this—going back to the aftermath of the so-called global war on terror, with demands during inquiries for definitions of national security. I am not sure what that would achieve other than it would be heavily litigated. In terms of both definitions of national security and the categories of technology, a better answer is a drumbeat of reviewable activity, which is by definition transparent, about how the Government interpret the scope of the Bill, if it becomes an Act, and the sort of cases it applies to so that, over time, you build up a broadly accepted framework—of course, not everyone will accept it—that is seen to be fair and rational.

Q100 Peter Grant: I understand the reluctance to have an explicit legal definition of national security, but would there be a benefit in having an “except for” clause that makes it clear that certain activities do not come under the category of a threat to national security? Would that help to allay fears about infringements of rights of democratic participation—the right to protest and so on?

Professor Martin: I certainly would not be against things like that, if it could be done in a way that did not compromise the wider use of the Bill, because I do not think there is intent to interfere in the democratic process. I think the intelligence services take that pretty seriously. I remember in other contexts, when asked to co-operate on cyber-security with other countries, given that some cyber-security capabilities—by no means all—can be intrusive, that a lot of due diligence is always done on whether they could be turned by more authoritarian regimes against their own people. I would not object to that in principle. I do not know whether you have a case in mind when you say that might be necessary, but I have an open mind on that.

Q101 Peter Grant: There has been some discussion of whether the investment security unit is best placed within BEIS, the business Department. Do you have a view on that? Does it matter where in government it is based? If it does, would BEIS be your preferred location, or do you think it should be based elsewhere?

Professor Martin: In general terms—this is a personal view, for what it is worth—I do not think the location of most government functions matters a great deal. Perhaps I am just a bit of a contrarian on that point, and always have been. The Government is the Government. Institutions do have cultures. I do not know whether the Government or the intelligence services have offered a formal view, but personally I would be reluctant to put it within the national security estate, first, because it has to be economically literate, and secondly, because it has to justify its existence and use. A strong national security input is important, but I would not leave it in the national security community.

I am sorry to sound like a broken record on this point, but I think the more important force in function is some form of reviewable transparency requirement.

If you set it up and let it go away, first, you take away pressure to perform well, and secondly, you take away pressure to justify the decisions that are made.

This is a really hard problem. When I was still in government and there were discussions around it, this was not the sort of Bill that most Ministers and politicians came into Government to want to pass. It is a necessity of a bunch of case work that we have become concerned about that has required us to do this. It is sort of the least bad option. The country wants to be open to investment—we are all mindful of the impression it may give that it is trying to deter investment—so it is probably the least bad option, as I say.

I do not think there is any arrogance in government or belief that a bunch of civil servants assembled in BEIS or another Department will make infallible judgments on individual cases, but what is the alternative way to stop the sort of things we have seen happening—world-class taxpayer-funded research in key strategic technologies that are going to be vital for national security being sold for a song to potentially hostile regimes?

Peter Grant: I will leave it there, Sir Graham. I may want to come back later, but I will let someone else in now.

Q102 Simon Baynes: Thank you for your excellent evidence, Professor Martin. You said, if I understood you correctly, that the process needs to be relatively open about why it is making decisions, but I foresee problems, particularly where there are issues of confidentiality and national security. Would you explore that a little? I note that within the terms of the Bill, decisions will be subject to judicial review or appeal, and the Government will be able to apply for a closed material procedure to protect sensitive matters in such proceedings. It seems to me that there is a potential problem there in relation to commercial and national security information sensitivity, so the “openness” of the system might be fairly limited and it might not be as respected as it could be.

Professor Martin: I get that completely. I do not think 100% transparency will be possible in this case. Obviously, it will be judicially reviewable, but I am entirely unsurprised that there is an explicit provision for closed material procedures. It will be a minority, but there will be cases in which the reason why a particular aspect of a particular piece of technology is really sensitive—it will probably be highly specialised, and there might be a dozen people, of whom four serve in government, who actually understand why—cannot be published. Then, of course, there will be commercial sensitivities.

Having said all that, if you take, for example—these are real examples—the current debate around the potential use of offensive cyber, or the sort of allegations Edward Snowden made against Five Eyes countries in 2013, or some of the defences that the Government had to use in the 2000s about their role in the aftermath of 9/11 and Iraq and co-operating with US forces, in my view there is a clear distinction between being able to describe the operating environment and the sorts of thematic issues that you are dealing with, versus individual cases, which often contain extremely sensitive detail. National security organisations can say much more about the former than historically they have been willing to do.

In something like this, where we are talking about business confidence and how the country looks to potentially very friendly and helpful outside investors who like the UK, want to come here, want to put money here and like the high-quality research and the brilliant innovators and individuals, it should be possible to give them something that says, “In the course of the last year, we have looked at quantum resistant cryptography and here are the types of aspects of this that we are reserving and here are the bits that are more open” or that sort of thing, without disclosing anything sensitive. That is all you need to be able to say—these are the judgments. Let us say that the Bill becomes law in the middle of 2021, for sake of argument. By 2025 and the beginning of the next Parliament, the tech landscape will look very different. You will not want investors to be looking back at the debates you are having in the House now as a guide to the latest way in which the Government are applying this, or looking at drip feeds of information. You will want something official. It should be possible to do that.

Q103 Mark Garnier: I want to refer back to some earlier questions about the skills within the investigatory unit that would be within BEIS. With your knowledge of Government, do you see any sort of experiences that can be carried over from the export control joint unit within the Department for International Trade? They do not have all the skills there, but they draw on skills from other Departments, particularly when it comes to arms export control and the eight consolidated criteria. Do you think there is potentially an opportunity in the day-to-day structure of the investigations unit for some lessons to be learned and carried across from the ECJU? Or do you think that is irrelevant?

Professor Martin: I do not know the ECJU that well, but it is relevant. I remember, although it was some time ago, being asked for specific inputs into that sort of point. The important thing is that the unit achieves a prominence and reach across the Government, because bits of Government will have to be involved occasionally and there will be bits that will be embedded. It needs a home—in our system of government, every organisation needs a home with a responsible Minister and an accounting officer and all that. However, I do think this needs to be broadly based and multidisciplinary. Export controls are one of the few areas where we have had to do that consistently for a number of years, so I agree that it is well worth a look.

Q104 Mark Garnier: Do you think it should be formalised or do you think an informal relationship with other Government Departments will be adequate?

Professor Martin: I think it should be formal. The Government are not new to this. There should be some sort of review board to make sure that it has the right resources, the right performance, the right skillset and so forth. I would encourage ministerial interest. It may be something that the National Security Council wants to periodically review. In my time in national security, there were standing issues that the Government would come back to twice a year, whether there was anything interesting happening on them or not, just to take stock. That might be an issue. In answer to the previous question about transparency, there may be a case for a formal presentation, secret detail and all, to the National

Security Council every year, which would include all the potentially covert and sensitive stuff. It really needs to work with the grain of ministerial thinking as well. That will need to be done collectively, at some point, so there may be a role for the NSC.

Q105 Peter Grant: Good afternoon, Professor Martin. As part of the provisions for transparency and parliamentary oversight of the way the powers in the Bill would be used, the Bill would require the Secretary of State to have a statement approved by Parliament and then reviewed at least once every five years. Does that time period seem reasonable to you? Is there an argument for a shorter review period, especially in the early days when everybody will be feeling their way as to how the Bill works?

Professor Martin: There is a reasonable case for a more frequently reviewable point. There is also a cultural point about the way in which the political processes work. There are aspects of government about which questions are not routinely asked in Parliament, because they seem to be too secret. Again, it is a point about casework versus framework.

To my mind, there is no reason why the Secretary of State for BEIS could not be asked from time to time to update on this or why questions in the House should not be asked. I do not think technology changes fast enough that the whole framework of categories of regulated activity and so forth have to be updated more than every five years, but there will be a possibility of more frequent updates on working, approving listings and that sort of thing.

Peter Grant: To be fair, there is nothing to stop MPs from asking questions about international security, but the chances of us ever getting an answer may be somewhat less.

Q106 Chi Onwurah: You have placed a lot of emphasis on the right technological skills and said that they should be forward looking, for a number of reasons, including identifying new technologies, but also giving clarity and certainty to businesses. Where do you see those tech skills being located? How can the Bill ensure adequate appropriate access to them?

Professor Martin: I am not sure if the Bill will get in the way or help, one way or the other. I think Government technological nous across the civil service needs to be invested in properly. There is a deep, fairly sizeable reservoir in GCHQ. Again, without going into too much detail, more and more people are being transferred and seconded from there into other areas. That is a good thing, and we should welcome that rather than cast aspersions on this being all secret state stuff. It should be permeating normal Government activity.

There will be issues about how to pay for some of the specialists that are needed. I do not think we will ever compete with the big tech companies, but there may be scope for paying some specialists a bit more and bringing them in here. There is something about creating a career path for technologists in Government. There are big issues for the heads of the civil service and the permanent secretaries. If I were heading it, I would want an immediate infusion of seconded talent and private sector buy-ins relatively quickly. Government can do that quite well sometimes, and sometimes not so well. There also needs to be a long-term strategy for technologists in Government.

The Chair: I will now thank you very much, Professor Martin, for giving your time so generously and being of such assistance to the Committee. Given that the next witness is not due to give evidence until 2 pm, I invite the Government Whip to propose the adjournment.

Ordered, That further consideration be now adjourned.
—(*Michael Tomlinson.*)

12.49 pm

Adjourned till this day at Two o'clock.

