HOUSE OF COMMONS

Science, Innovation and Technology Committee

Oral evidence: Science diplomacy, HC 838

Tuesday 15 July 2025

Ordered by the House of Commons to be published on 15 July 2025.

Watch the meeting

Members present: Dame Chi Onwurah (Chair); Emily Darlington; George Freeman; Dr Allison Gardner; Jon Pearce; Steve Race; Dr Lauren Sullivan; Adam Thompson.

Questions 35 - 54

Witnesses

II: Dr Pia Hüsch, Research Fellow in Cyber, Technology and National Security, Royal United Services Institute; and James Black, Deputy Director, Defence and Security, European Lead, Space, RAND.

Examination of witnesses

Witnesses: Dr Hüsch and James Black.

Q35 **Chair:** Welcome to the second panel in the first evidence session of the Science, Innovation and Technology Committee's science diplomacy inquiry. I welcome our excellent and well-informed second panel. Could each of you introduce yourself as you answer the first question? Earlier, we were looking at some of the soft threats and opportunities that science diplomacy raises. Now we are looking very much at the hard end of science diplomacy. I would like you briefly to give me your thoughts on what threats the UK faces from hostile actors investing in technologies with dual use—civilian and military—purposes.

Dr Hüsch: Thank you very much for having me. My name is Dr Pia Hüsch. I am a research fellow at RUSI, the security and defence thinktank. I sit within the science and tech team. We research cyber and technology policy here in the UK. My research focuses on science, tech and innovation policy at the intersection of national security. I am happy to come back to some of the themes on which we just ended.

There are a number of threats facing the UK science and tech community. How do we know that? There have been repeated warnings from the UK intelligence community, whether MI5 or GCHQ, that we are seeing increasing hard threats through cyber-attacks: insider threats; talent recruitment of UK-trained scientists who return to their home countries, perhaps with sensitive information and knowledge of our IP that they take with them; and espionage or disinformation operations threatening or undermining UK research. There are a number of threats.

Intelligence services have warned against them. Perhaps a few flagship speeches have been made. Other than that, a few people have come forward anonymously perhaps illustrating what they have experienced in the science and tech community, but, on the whole, there remain a lot of unknowns, particularly in the more public domain.

Q36 **Chair:** Thank you. It sounds like you think that threats have been identified and raised, but not addressed. Could you specify a couple of those?

Dr Hüsch: One example, which I looked up again before coming here in preparation for this session, is what happens if you look up threats to the UK research community. There was a prominent warning from MI5 in April 2024, but that is quite a long time ago in terms of how technology develops and how much staff turnaround there is at UK universities in the research community. There are some warnings and some prominent cases.

Q37 **Chair:** To be clear, was that a general warning about research threats, or was it a specific warning about specific areas of research?

Dr Hüsch: Both. It is universities more generally and specific areas of AI, quantum and similarly sensitive dual-use technologies. If I am a researcher and I see that, it seems like an awfully long time ago. A number of other measures have been enacted since, but they primarily impose administrative hurdles for researchers. If that is the position I am in as a UK researcher and I google that and see that, I think there could be specific warnings given more regularly that are discussed more publicly. Some researchers, like one researcher from Chatham House, have come forward. That is very laudable and is a strong warning to other researchers in this area.

James Black: Good morning, Committee. I am James Black, deputy director of the defence, security and justice team at RAND Europe, which is the European arm of RAND, the world's largest policy research organisation. I come to this as somebody who has done a lot of work particularly in the hard defence space, looking at strategic competition over S&T, but we do work for DSIT, FCDO and across Government on these sorts of issues. I also try to channel my well-informed colleagues.

Specifically on the question of dual-use S&T, to put it in context, the locus and direction of innovation has changed over the past decade. If you go back to the '40s, '50s and '60s, the general trend when talking about dual-use technologies started in the military and public sector and then moved into civil commercial applications in the private sector. Think of things like computing, jet engines, GPS, the internet, whatever. Broadly, that is no longer the world we live in. We now live in a world in which private companies, not necessarily those considered to be world-leading innovators, but for example Samsung making TVs, spend more on R&D than UK Government military labs. They are trying to make their TVs 0.1% better looking; we are trying to make the country safer.

Equally, there has been an eastward shift away from the US and Europe towards China and particularly Japan, India and emerging economies. It is important not to overstate that. Many of those countries, China in particular, are very good at quantity, but quality is still patchy. Quantity has a quality all its own, to quote a certain Georgian statesman, so that clearly is a challenge. In that context, when we look at what our adversaries and competitors are doing, they are trying simultaneously to develop themselves and undermine and subvert us—both sides of the equation of competition on dual-use tech.

In developing themselves, countries like China pour huge amounts into their military and, more broadly, their scientific and industrial bases. They benefit from economies of scale and large domestic markets; they benefit from stronger Government ability to compel action from private institutions. I am sure we will come back to that sort of military-civil fusion topic, but we shouldn't overstate it. We should recognise that the grass is not always greener and China has its own challenges, but they have a number of inherent advantages: an authoritarian regime, a large

country, lots of bright people, and very loose planning regimes. With all these sorts of things they can obviously push through change.

The flip side of that is the attempt to undermine and subvert the UK and its allies. We are talking about a broadening attack surface. It is not just going after universities; it is going after SMEs, industry, supply chains or raw materials. There are different threat vectors. We heard a little bit in the first session about some of the research security challenges around collaboration, but there is also more direct intellectual property theft; there are cyber-attacks across universities and companies; there are questions of data poisoning, not just extracting data but fiddling with our data so that, for example, our AI models do not give the results they should. There is the insider threat around personnel. There are all sorts of challenges.

Conscious that we are talking about science diplomacy, there is also the diplomatic side of that. How are these countries trying to shape international governance, discussions, regulations, standards and norms around some of these technologies in their favour through organisations like the International Telecommunications Union or the newer fora that exist around things on AI? A lot of the dual-use technology often overlaps with under-governed spaces; cyber-space, outer space, the Arctic and AI are areas where there is some governance in place—it is not none—but it is not robust. If you start talking about how you regulate those dual-use technologies, it is not the same as traditional arms control for nuclear weapons or stuff that is overtly military. That is the really complicated space as you get into the trade between geopolitics, economic growth, scientific collaboration and all the sorts of incentive structures that we talked about in the first panel.

Q38 **Chair:** You have painted quite a disturbing picture of the lack of appropriate warnings being addressed in terms of the threats posed by dual-use technology, together with the range of challenges and examples that you have given us, always remembering that part of the purpose of science diplomacy is to support deterrence so that we deter hostile actors from carrying out some of the threats you mentioned. Could you tell me how many different Government Departments—you have brought a number to mind—need to collaborate on addressing this? Could you also say a little about the most effective deterrence? You have talked about a broad range of threats. What is the most effective way of deterring them?

Dr Hüsch: The challenge is that there are so many different Government Departments. Perhaps the obvious are DSIT, the intelligence community and Education, but also any Government Department that effectively funds research, like the FCDO or others. That interconnection makes it really difficult because there are so many different stakeholders involved.

Something that was alluded to in the previous panel was the challenge in communicating perhaps with the national security community. The national security community has increasingly ramped up its efforts in communicating with academia and researchers in this area, whether that

is through university briefings or guidelines from the National Cyber Security Centre on how to enhance research security, but the challenge remains that the national security community is a very insular Government body. Transparency and open communication do not come naturally to them, despite best efforts.

On the other hand, there is perhaps a lack of understanding of what drives individual researchers. There might have been a briefing to a high-level university employee, but individual researchers are motivated by things like the REF cycle. How many publications can I get out? Will I get a promotion if I secure additional research funding from somewhere? That is what drives the individual. There still needs to be more communication from the national security community at the individual level, and understanding what drives the individual researcher, and perhaps those universities beyond the few universities that we can all think of right now where we openly know that they are doing security-sensitive research. This is not just a topic for the London bubble, or perhaps those who already have established links to the Ministry of Defence or similar. Particularly with dual-use technologies widening the threat surface, it is a topic that affects all universities and researchers in the UK.

Q39 **Chair:** Thank you very much. That is a very clear recommendation. We like that. James Black, perhaps you could talk a little about deterrence as well.

James Black: For those not familiar with it, deterrence theory came out of RAND in the '50s and '60s. If you have seen "Doctor Strangelove", who works for BLAND, which is Stanley Kubrick's not so subtle rip-off, you know that game theory and all the sorts of things invented around it is beaten into us each morning in the ritual calisthenics that we do.

To break that down into its constituent parts, first you are trying to influence your adversary's decision making. Deterrence is one way of doing that. There are other ways, like persuasion, and I will come back to that in a second. If you break down deterrence, you are trying to have a cognitive effect; you are trying to affect their decision calculus, their cost-benefit calculus. If I do this hostile act, for example to subvert part of the UK's S&T capability or industrial base, are the benefits worth the costs and the risks? You can play with both sides of that equation. You can either do deterrence by denial and make it harder to achieve their goals in the first place, or at least increase the cost of doing so, or you can do deterrence by punishment: "If you poke me in the eye, I will punch you back." In the world of science and technology and science diplomacy, what that means in practice is that there is a whole range of things that can be done across Government. To your question on cross-government, it absolutely has to be done cross-government, because there are inherent tensions between different national strategic objectives and, therefore, different departmental objectives, say security, growth, scientific advancement and influence. These things sit in tension at times,

so it is a real challenge for any one Department to try to navigate that faithfully. It has to be across Government.

There are tactical things we can do, for example, to improve research security and strengthen the dialogue with research-intensive universities, publishing houses for journals and funders, around those research security threats. It does not eliminate the problem, but you can raise the costs for adversaries. To link back to the previous panel, I emphasise that those sorts of tactical actions, while sensible and prudent, are not necessarily sufficient on their own. They are necessary but not sufficient. That is because, as has been discussed, there are some broader structural, systemic challenges facing UK S&T around things like funding, access to talent, access to infrastructure, energy cost or whatever that fundamentally affect the incentive structures for academics to be secure, or to pursue other goals. There is no security solution to this that does not also include addressing those more structural challenges in S&T.

There are two other things we have to consider. One is that it is not just about how we protect ourselves and build a bigger fence; it is about how we innovate quicker and acknowledge that there will always be some degree of technology leakage, effectively, to our adversaries, but we need to keep up by developing the next thing quicker and quicker. That speaks more to an innovation and absorption challenge. The UK is famously good at science, less good at commercialisation, which will not surprise any of you.

The final point is that we need to start thinking seriously about scenarios in which it is our adversaries who have better science and technology than us, so we have to think about either mitigation and seeking ways to have an advantage with lower tech, which is completely alien to us as a society—we have not had to think about that for a few hundred years—or start to think offensively about how to subvert the S&T bases of others and steal their intellectual property one way or another. These are very uncomfortable conversations to have, but we are still locked in the mentality of thinking it is all about protecting what we have and stopping others getting it. The reality is that what other people have nowadays might be as good as, if not better than, what we have.

Q40 **Chair:** You mentioned a number of Departments and that it has to be across Departments. Who should be leading on this in the Government? Should it be Defence? Should it be the Cabinet Office? Should it be DSIT? No. 10?

James Black: I am hesitant to get into organograms too much. If it is the whole of Government, there is a case for any of those three organisations, but I think it would require the clear backing ultimately from No. 10 that, "I have chosen this lead because this is where we are optimising the trades between security, growth and collaboration." We need real clarity on that strategy, not just aspirations but hard trade-offs around who we are going to work with and under what conditions. It may well be that for countries like China we absolutely can and should be

working with them in certain technology areas, because it is in our mutual interest and the global interest—health, climate change—but in other areas we say that there is a tiered approach and they fall into a different kind of risk tier.

Q41 **Chair:** Dr Hüsch, the previous Government said they were going to do a consultation on research security. My understanding is that nothing ever came of that. Is that your understanding?

Dr Hüsch: I am not aware of the latest developments on that front. I would not want to make a decisive statement on that. I know that measures have been taken through the NCSC and others that are active in this space. It is not that nothing has happened; a few other measures have been taken—for example, more guidance to academics under the foreign influence scheme.

The National Security and Investment Act imposes regulation or obligations on academics to make risk assessments. That links to the previous question about who makes the decision. Should this come from Government or academia? At the moment, many of the policy levers impose obligations on academics to make assessments, flag risky scientific collaboration perhaps or foreign investment. The challenge with that is that it puts the ball into the academics' court without them having the full information that a national security community would hold. Why would the assessment prioritise national security requirements if I am an academic who doesn't have that kind of information? We cannot expect academics to prioritise national security concerns without adequate knowledge.

There has been an announcement to increase things like national security clearances for specific academics in this area. I don't know the details. It is a good measure to share information; otherwise, you cannot expect academics to make those challenging recommendations. They can seek help, for example, from the Research Collaboration Advice Team—RCAT—at DSIT, but we know that is fairly poorly staffed to comply with the amount of requests and administrative needs for support that academics have. Ramping up the efforts and resources of RCAT, if you want academics to comply with this and seek help, would be advisable.

Chair: Excellent. We can certainly look at what the resources are and how they are being used.

Q42 **Dr Gardner:** I want to put a couple of follow-up questions before I address cyber-security. You mentioned a couple of risk areas: quantum and AI. Quantum computation is very relevant to encryption and we are due to see it having its AI moment in about four to five years' time, but if another country gets to that point before us we will have real issues. Do you feel that there are particular areas within universities that are being targeted for attack, such as quantum, and what do we need to do to mitigate that, because if a country gets there first we have problems?

James Black: If you look at the stated priority areas in S&T for the UK, China or most countries, you see the same sort of things cropping up. It is relative—different balance of investment, or whatever, based on the national strengths—but there is a sort of bingo card of emerging technologies; it is going to be synthetic biology, quantum, AI and those sorts of things. From a strategic competition perspective, what is materially different with things like AI, quantum and advance compute is that they are not just potential technological breakthroughs in their own right; they are things that could in turn accelerate your ability to innovate further. If you have an advancement in AI that enables you reflexively to improve other models, you can get yourself into an intelligence explosion-type scenario with artificial intelligence. That is why we see such heightened geopolitical interest in these sorts of technologies, because, as you say, potentially—I emphasise "potentially" because it is a theory and is not proven—there is significant first-move advantage to those countries that get there first.

The challenge, equally, is that framing it as an arms race in those terms can itself be very destabilising, and can disincentivise countries like the US, China or Europe from working together on things like AI safety and security or quantum governance and regulation. That is unfortunately the needle we are trying to thread at the moment. I would add on top of that the challenge that so many of the advancements in quantum, AI and other things are being driven, again, not by the public sector particularly but by large private companies, often American in practice but some in the UK, and certain universities. Often, they have a better understanding of the state of the art technologically than Government might have. They obviously have lots of lawyers and lobbyists and other things. They clearly have commitments to things like safety and security as well as commercial pressures, and the challenge there is building up the requisite understanding in government to be able to be an intelligent customer, an intelligent regulator and an intelligent collaborator around governance norms. To be clear, we cannot do everything in quantum and AI, but we need to work out the necessary UK sovereign role in that tech stack for those technologies, and then mitigate those areas that we cannot do on a sovereign level through our alliances, our partnerships or whatever means.

Dr Hüsch: We have seen some targeted operations and cyber-threats against universities that have NCSC cyber-security certified courses. There has been some element of that. The challenge I see with the specific focus on quantum technologies is similar. Yes, it is a threat, but if I am a researcher at a UK university working on quantum encryption, for example, there is a good chance that I am already aware that this is a national security-relevant technology or scientific research that I am conducting. However, with dual-use technologies and cyber-attacks targeting other students to use their credentials and then escalate to other parts of the university network, it is not just about the niche technologies or niche research areas that are interesting to foreign actors. Those actors can also target way beyond one specific lab at a

university. It is important that we do not just focus on cyber-security for a handful of researchers but across the broader spectrum.

Q43 **Dr Gardner:** How well protected against cyber-attacks are UK scientific research institutions? Do they have the infrastructure underpinning the key technologies that they need?

Dr Hüsch: No. There are a number of good measures that have been taken. In particular, the NCSC has been very active in this field, publishing very valuable advice to researchers in the AI field. We have just heard extensively about the funding challenges that universities have, and that includes cyber-security measures that require quite significant budgets. A lot of university networks grow organically, are pretty patchy and depend on legacy systems that are not updated regularly enough because the resources are not there. Yes, there has been some good work from Government in this area, but of course that comes in direct competition to funding cuts and resource restraints.

James Black: I agree with what has been said. It is not just universities and so on; it is also SMEs and the private sector. There is a repeatedly stated ambition from UK Government, no matter who is in charge, around a greater role for SMEs in delivering innovation to the military, the emergency services or the broader economy. It is those SMEs that are often the least well equipped to deal with some of the challenges, because they are two men in a shed and there are, clearly, capacity constraints. How we secure the entire supply chain, the entire technology stack—not just those bits that are dominated by bigger players, either universities or private companies, that have the resources to deploy proper cyber-security—is a real challenge.

We can look at what is happening in a couple of dual-use areas like space and AI. In space, we have the new draft EU Space Act. There is a big emphasis in that on trying to raise the level of cyber-security across research and industry organisations in space because there is a recognition that it is not as good as it could be, and those services are now critical to so much of the economy. Equally, with things like AI, there is a lot of concern about data poisoning, which I mentioned, and things like extracting model weights. This is where some of the AI security and AI safety issues start to bleed together.

A lot of the most concerning scenarios around loss of control of an artificial general intelligence are not that we necessarily lose control ourselves, but that there is a cyber-attack by someone else seeking to take those model weights for their own advantage—scientific, commercial or whatever—and they house that AI in a less secure environment in their own country, which then gets out and causes problems. There are similar concerns about some of the biotech stuff. It is a real challenge. You cannot secure everything to within an inch of its life because then you cannot innovate, but we definitely need to find a balance that is much more reflective of the cyber-threats that we face nowadays, which are pervasive and moving quickly.

Q44 **Dr Gardner:** My second question was about whether hostile actors were trying to access UK research areas and what we are doing to stop them. Clearly, they are trying to. One of the comments you made earlier was that a lot of these attacks focus on areas where we have poor governance. You mentioned AI and data poisoning a number of times. As well as having the infrastructure and the technologies, do you feel that the governance by Government or universities themselves to protect against things such as data poisoning is in place? Do they need support there with understanding how to govern this and mitigate the threats?

James Black: To stick with AI as an example for a moment, on the positive side, an area where the UK has been very active, and arguably leading, is around ethics, law, regulation, norms, governance standards and best practice guidance. You have the Alan Turing Institute. You have different bits of UK Government. You have an AI Safety Institute and an AI Security Institute. In many ways, the UK is at the forefront, relative to a lot of countries. The challenge is that being at the forefront of something is a relative assessment. It is how we are doing versus everyone else. It is not an absolute assessment.

The reality is that no country has figured these things out yet because the technology is moving so quickly, and the geopolitics are so toxic at the moment that achieving consensus on anything is tough. On the positive side, we are doing a lot in that space to understand both at the domestic level and internationally what the governance should look like. The challenge is just keeping up with implementation when the technology is moving forward exponentially rather than in a linear fashion. Academic institutions think in academic years; they don't think in six-week tech cycles. Governments think in Parliaments or in the news cycle, or a bit of both. It is the challenge of how we keep pace.

Q45 **Dr Gardner:** Do you have a solution, an idea or a suggestion?

James Black: On the international level, it is very difficult to achieve any meaningful consensus on the governance of things like AI or space or "Insert emerging tech here" without addressing some of the broader tensions between particularly the US and China. When we talk about achieving consensus on these issues, we really mean can we get those two in some level of mutual trust, mutual vulnerability and mutual acceptance on this issue—not on all issues—and then how can the UK and other players slot in around that and influence that, and try to bring the global south and others with them? That is very hard to do.

There are concrete specific little things you can do around transparency and confidence-building measures, so that if we are doing certain things with AI or space, we publish what we are doing, we explain what we are doing, we explain why it is safe, and we try to reduce the concerns of other countries that we have malicious intent as a way of inducing them to more positive intentions themselves; but those things take time. The regulation, the governance, of nuclear weapons, which are unequivocally military, not dual-use, and unequivocally bad for the planet if we all use

them, still took several decades of negotiations to achieve. Also, that was in a world that was bipolar; it was, effectively, the US and the Soviet Union. It was not the multipolar world that we have today. I don't think there are any quick fixes, but my point is that we can build momentum.

Chair: That is very helpful. Thank you very much.

Q46 **George Freeman:** As you probably both know, I should declare I am very concerned about this. We are witnessing an industrial scale haemorrhaging of value from the UK science and tech landscape, and, as a Minister, I raised the issue of broader research security at three G7s and two G20s. I want to ask about two Ps: principles and policing. On principles, when I returned to Government in October '21, I was told that our policy on research security was "as open as possible and as secure as necessary", which I think is a joke. If you ran an airline on the basis of "as convenient as possible and as safe as necessary", I wouldn't want to fly on it. I am really worried that the scale of the global race, the chase for sovereign advantage and the new cold war getting pretty hot is a whole new landscape and that we have not really put in place a suitable principle. I would be interested in both of your views on what an adequate principle for the pace of today's global race is.

On policing, to the question we asked in the earlier session, we can have conversations about it, but these are pretty here-and-now urgent dual-use questions. Who should police it? Of course, we need to get academics and the security services together, but in the end someone has to decide. The academic community has traditionally, rightly, jealously guarded academic freedom from political interference, but it seems to me that we are in a new world where, as Ministers and a Parliament responsible for £20 billion a year, we have to reassure the public that we are protecting properly. Two questions: first, principles, and then policing. Which other countries are doing this well? Where would you put us on the scale? Are we mid-pack, are we falling behind, or are we ahead?

Dr Hüsch: Generally speaking, the UK is doing relatively well in this area. We previously heard reference to the Science and Technology Network. There are a number of initiatives, bilateral or with more than one other country facing pretty similar issues. A number of European countries also have a strong academic sector and need to protect their research—Denmark, Germany and the Netherlands. Through that network, there is a lot of work on collaborative efforts for research security. The UK is definitely in conversation with other countries and trying to identify best practice. It is not a task that is particularly easy to solve or one where it is easy either to come up with a catchy principle that I am afraid I cannot deliver on the spot or to make final assessments on who is policing it.

My main message in this context is that I would like to see more national security community influence or warnings in the conversation and a more strategic approach to some of the questions through prioritising specific technology areas with a national security backing, as well as not

expecting that one academic in an office somewhere in the basement of a Scottish university can make that assessment for the UK, in the absence of a comprehensive China policy and other questions. To put the pressure on an individual researcher to make that call would be the wrong thing to do.

Q47 **George Freeman:** James, how would you rate us internationally on this? Who is doing it really well?

James Black: The UK faces some sorts of acute policy choices more than certain countries. If you are the US or China, you can sort of afford to do everything. If you are Austria or Slovakia, you can pick two or three things, get really good at them, and it is very easy to mobilise public/private partnerships around that. The UK is caught in that hinterland. It is a nice situation, depending on what sort of index you look at, being the third, fourth or fifth biggest science and tech player in the world. That is obviously a good thing. Equally, it means we have some real challenges there. Linking to your point about principles, we have to ask ourselves whether we are serious about some of that rhetoric and the scale of the challenge it implies.

If we genuinely want to be a science superpower, as the previous Government did, or if we want science to drive growth and the various other missions that this Government have, the reality is that it is not just about spending money; it is a wholesale relook at government. Government is an 18th, 19th, 20th-century institution that is now trying to deal with 21st-century problems, and it is simply not structured in a way that would genuinely deliver on that mission. That means looking across both domestic and foreign policy. It is things that DSIT can do. It is also the security aspect. It is the talent, the infrastructure, the planning, the energy costs, and all the sorts of things that enable the UK to be a competitive part of the tech stack. We need to recognise that we are not going to have sovereign control of most technologies—that is simply not going to happen—but what we can do, and is a realistic goal, is to say, "As the third or fourth biggest player in this, we are going to be an indispensable part of the global tech stack, but we need to recognise where that is and insert ourselves into that and then cling on." There are some countries that are very good at that, such as the Netherlands with things like lithography machines. They have a clear national strategy: "We can't do all of AI, but we are going to do this one thing that makes that one thing that makes this one thing that makes AI, and that will make us an indispensable part of the conversation." I think we can do that.

Equally, in terms of the principles, it is a tiered approach. It is the "own, collaborate, access" that we talked about earlier. Certain technologies are absolutely going to be driven far more by collaboration and openness. For others, it is going to be a much higher fence. A competitive advantage and comparative advantage that we have over countries like Russia and China is our allies and our partners. That is the other element. We need

to be clear-eyed about how we get the most for the UK out of those alliances and partnerships, be they military, governmental, business to business, or academic.

Dr Hüsch: I believe that the UK has some significant strengths in that ecosystem, but I am afraid relying on third position in a number of rankings would be a fallacy, from my perspective. It doesn't matter that much whether you are third, fourth or fifth if the gap to No. 2 is so significant. Unlike the Netherlands or Denmark, the UK has not strategically positioned itself in a way that accepts that UK resources are more limited compared to the US or China. If we compare ourselves to other countries, we look to the US and China, but the lessons learnt from those ecosystems with such vast resources just—

Q48 **George Freeman:** I am intrigued as to whether there is—I do not think there is yet—an index of research security. My fear is that the UK is very open, hugely collaborative, does not police and is haemorrhaging value. As a Minister responsible for making sure that we are getting public value and as a Committee charged with making sure that the Government do, I think this is a new landscape for us. James, is there an index? Is there any measurement?

James Black: No. One of the challenges is that it is compounded by the innovation and commercialisation problems that we have in this country. It is not just that the UK, because we are a relative leader in lots of areas of science, is an attractive destination for those seeking to steal some science; it is also that we are underperforming in turning that new knowledge into tech that we exploit ourselves, commercially, militarily or whatever. You put those two things together and it is not just that we perhaps leak scientific knowledge, IP and all those things; it is also that we are not exploiting it ourselves. That is the other side of the equation.

George Freeman: The threat, as I see it, is also acquisitions. We cheer ourselves on for having sold a company. Other countries cannot believe we have sold it so cheaply. There are a lot of dark China investment funds that are in disguise. There is a whole landscape, not just cyber-security. Can we turn to space, or do you want to finish?

Chair: We need to go on to Emily. We will try to come back to space.

Q49 **Emily Darlington:** One of our previous strengths in science, science diplomacy and science soft power was our strength in regulation and standards, being able to influence ISO standards. It goes right back to when we drew up the oceans and decided who was responsible and what was territorial to whom, which has obviously had a huge impact right the way through, on our security and on how the seas are policed and other things. Is that still a strength of the UK? Is it still something where we have any authority in trying to drive it? I am going to link it to space because I know we want to go on to space. Do we need a seas-type global agreement in terms of space, given its strategic opportunity and commercial essentiality for future development?

James Black: I will talk broadly and then use space as an example. Yes, the UK has outsized strengths in regulation, law, insurance, which is always relevant, and finance, and it obviously brings them to bear. We have advantageous positions in a number of international institutions as a UN P5 member or whatever.

To use space as an example, space is an area where, in the space security/space defence domain, the UK is a relatively small player. We have fewer sovereign military space capabilities than the French. The Germans and Italians spend a lot more than we do. We benefit from a close relationship with the US, but there is also therefore a level of dependency. We have been a leading player in the last five years in the discussion about dealing with space security issues and space governance issues. Indirectly representing the UK, I was one of the people who briefed the United Nations open-ended working group in Geneva on responsible space behaviours, which the UK initiated. That ended up being blocked by the usual suspects—Russia, China and Iran—from achieving a consensus report, and we now have the slightly strange situation in Geneva where there are two rival efforts, from us and the others.

None the less, the UK achieved some influence in that space. It clearly brought a lot of the emerging spacefaring nations along. It raised capacity and awareness in countries where they may only have one or two people working on space policy or space regulation. The UK was able to go in and, in a non-lecturing, non-hectoring way, explain some of the problems, explain what good might look like and try to shift the debate. Those things can be good. I emphasise though that that soft power has to come from some level of credibility on hard power, ultimately. I don't necessarily mean military power, but you need the science and the technology as a country. Then you need the understanding within government, and the scalable companies to continue to exert that influence. It is a wasting asset. It has to be constantly replenished and repaired.

Dr Hüsch: I agree. Our research has demonstrated that indeed the UK is still a leading voice when it comes to standards, particularly in the AI safety and standards world. The AISI has done an incredibly good job that has been internationally acknowledged. The UK generally is well represented in working group meetings, standard-setting bodies and similar. The UK should leverage its position to make sure that other European partners adequately resource and staff standard-setting bodies, working groups and efforts. The UK could do with a little bit more diversity in its standard-setting work. That of course can come with some support from the private sector, but particularly when it comes to academics and researchers, the talent pipeline is not looking particularly prosperous. Raising more awareness among researchers that the standard-setting work is important, by providing travel funding or similar incentives for younger researchers coming into this space, is important as well.

Q50 **Jon Pearce:** I want to look at the strategic defence review briefly. The SDR highlighted several technologies that are redefining warfare, including AI, robotics, directed energy weapons, space-based capabilities and quantum. We have touched on many of those this morning. James, from your perspective, which of the technologies that are identified in the SDR presents the biggest risk to the UK?

James Black: To be clear, overall the list is the right one. There is a lot of good stuff in the SDR. The challenge, as with every SDR or SDR equivalent over the years, is the implementation in terms of the investment, because the level of investment at 2.5%, or 3%, is not adequate to deliver on all the things in the SDR, bluntly.

There are two sides to which are most threatening. One is what is most threatening in terms of what our adversaries might employ against us, and some of it is more about what is most threatening if we fail to deliver on our side. On what is most threatening from our adversaries, as we have discussed, if there are meaningful advances in AI for things like strategic decision making, targeting and links to autonomy and autonomous systems, any of that can be really destabilising, and I don't just mean as a direct military threat but as an economic threat to us, which then affects the ability to spend money on defence and therefore the relative balance of power, or the ability to project power around the world in other ways. Countries like China are thinking very hard about how they use AI and digital technologies as part of their broader belt and road initiative and outreach to countries. All those things affect us in a security sense, not just on the battlefield.

Absolutely, there are advances in things like AI, long-range precision weapons, hypersonics, cyber and space that can affect the basic enablers of our western and UK way of warfare. We have a networked focus on precision. We link up small but high-quality exquisite forces, and then through a bunch of techno-wizardry they are able to deliver an outsized qualitative effect. We do not have quantitative advantage. We need qualitative advantage. The reality is that, in Russia and China, both their military doctrines now emphasise versions of systems warfare—going after key nodes or linkages, be they satellites or networks, taking those out and then paralysing our forces, paralysing our society and paralysing our alliances and ability to respond. I am most worried about those kinetic/non-kinetic ways of taking out our digital-networked way of fighting and indeed our digital-networked way of living.

On our side, the reality is that we will not be able to do all those things to the extent we would like. We will have to specialise and make some hard choices. That necessitates reliance on our allies, so there are broader questions at the moment about the robustness of our alliances that it is hard to take that away from, because clearly there are big tech bets you could place with the US or AUKUS. There are tech bets you could place with the French and the Germans. You probably can't do all of them, so some of those choices are really challenging on our side.

Dr Hüsch: What I think is most threatening is another list of technologies that lists all of them without any specificity or recognition of the intersection of those technologies. No one wants to come forward with a list of technologies that are not a priority, including the team behind the SDR. In some ways, that would be a step forward. It is relatively easy to come up with a very long list of technologies that are all a priority to the UK. What would really move the dial is a more specific set of technologies or use cases. Yes, AI is a priority, but what kind? What use cases are you looking at? What intersections are important to the UK and link back to existing strengths that the UK already has? The follow-up question on that, as James has already mentioned, is: what are the technologies where we want to partner with others? That is the realistic approach that is a little bit missing. If everything is a priority, nothing is. That is where more work needs to be done.

James Black: The big phrase is "bureaucracy, culture and peacetime mindset" against an adversary that is on a wartime mindset.

Chair: Thank you. That is an important reference.

Q51 **Steve Race:** You just mentioned AUKUS, and I want to talk about some of the big programmes. AUKUS is pretty deep and broad in science and technology collaboration. We have GCAP on a smaller scale. What is your assessment of the importance and impact of these agreements in the global environment and particularly for our science diplomacy?

James Black: RAND in the US, Europe and Australia is working on both pillar 1 and pillar 2. We are doing a piece of work at the moment looking at lessons learnt from pillar 2, which is not published, but I am sure once it is we can share it with the Committee. There are huge opportunities—genuine generational opportunities—from AUKUS. The original statement of intent from it is to try to do, effectively, 50-plus years of working together between three countries. It is not just to deepen collaboration on specific programmes like pillar 1 and the submarines, but more broadly to integrate the industrial and innovation ecosystems of three allied countries with broadly similar threat assessments and cultures. That is a huge undertaking and genuinely strategic. There are lots of things that are being done on the pillar 1 side not just to invest in the submarines but to build up Barrow, the industrial base, the infrastructure and the people in the UK, Australia and elsewhere. Those things are great. In terms of level of intent, it is a national endeavour.

With pillar 2, the challenge has been that, unlike pillar 1, it has not had the same clarity of purpose and desired outcome. There have been divergent levels of funding, risk appetite and prioritisation between the different technology working groups from the different countries. There are different political and budgetary cycles, bureaucracy and all those sorts of things. Although there is an ambition for pillar 2 to be very focused on nearer-term operational problems for which there might be a tangible, concrete, technical solution, the reality is that a lot of it so far has been low-level discussions and a bit of experimentation. It has not

actually led to tangible capability that we can now say we have developed between the three countries and we have filled it, and it is solving this particular operational problem. There are questions about the funding, the information sharing and the clarity for industry on whether they should invest in AUKUS. It has been a few years, and many of those companies have not really seen a return yet, so there is a question about patience. We have seen in the US discussions on pillar 2 very recently in the public domain about losing patience with it and not delivering hard outputs, so there is a desire.

I will finish by saying that there are ancillary benefits that probably are not obviously captured. We have seen the ITAR reform in the US and the defence export reforms across the three countries. There are examples from talking to companies where that has enabled them to do something where their Australian business unit and their British business unit can now work together on a technology and do something without duplicating costs that they could not do before, but that is not necessarily tagged to an AUKUS-badged programme. There is not an obvious AUKUS flag slapped on that product or technology to say, "This is an AUKUS benefit." Some of those benefits are there, but they are not necessarily pulling through into pillar 2 explicitly. They are almost an implicit pillar 3. If pillar 2 wants to deliver in the way that pillar 1 does, there needs to be some seriousness of funding and intent, and communication of that to industry.

Dr Hüsch: I have nothing to add on AUKUS.

Q52 **Steve Race:** There has been some question in the US about AUKUS generally and pillar 2 specifically. What is the likelihood that the US at some point might pull out of AUKUS? It is unlikely to survive without the US, right?

James Black: Yes. It is hard to comment on US politics at the best of times, but probably particularly at the moment. Their direction of travel can change. AUKUS in many ways is very clearly lined up with prioritising many of the US strategic interests in the Indo-Pacific, countering China, deterrence in that region, reassurance of allies in that region, and helping shore up the US industrial base around submarines, for example, which has its own challenges. There is investment from the Australians and others to help with that. There are questions about how you balance the US navy's requirements for submarines versus the Australian navy's requirements for submarines, which is a challenging question for some in the current US Administration

If you look more broadly, there are huge returns to the US, as, to be clear, there are to the UK and Australia. It is a positive on something. This is, one would hope, something that can be solved relatively well with the current US Administration. It is something that has so far survived changes of Government in all three countries involved. There seems to be broad bipartisan acceptance that it is in the strategic interest of those countries, but, absolutely, political interest and political will is contingent on delivery and continuing delivery. If the industrial base from pillar 1

cannot deliver submarines quickly enough at the right cost, and if Australia cannot get up to speed with building them themselves, and if on pillar 2 it is not delivering tangible outputs, just talking shops, that political will may sap.

Q53 **Chair:** Thanks very much for the picture that you are painting. I want to try to end with a concrete example. The strategic defence review talks about the digital targeting web, also called the "kill web", which will connect a target to the defence military capability and decision making. The tech stack for that is going to be complex. It will involve AI decision making. It will involve communications. It will involve data. Does that tech stack need to be entirely sovereign capability? I think the answer to that has to be no, because it can't be. It will involve different country collaborations—the US, Australia and the European Union. It will also involve private sector collaborations, some with tech companies that may be run by people whose values we may not agree with or indeed understand at times. Is it possible to have a security process and a security assessment for a tech stack of that complexity? What should this Committee be looking at in terms of science diplomacy to identify the key issues and the key challenges that we would face in realising that specific ambition from the strategic defence review?

Dr Hüsch: That is quite a comprehensive question. For a project like this, there is no easy supply chain mapping. It is incredibly complex. There cannot be a supply chain that really is sovereign. That is something about which most people share an assessment. It is good that we are having these conversations and that we are raising awareness of supply chain complexities, and that we do not just look one layer deep. In your conversations, you look beyond and you peel away the layers and go to the bottom of some of the supply chains. Yes, it is an incredibly complex undertaking, but if you look from a threat perspective, cyber-security and similar, that is what is needed. On the specific supply chain, I don't have any further comments.

James Black: Regarding the digital targeting web, we have been involved in all the work around future command and control, multi-domain operations, all the acronyms and abbreviations and the alphabet salad that is thrown around these things. It comes back to that own, collaborate, access discussion. We did a study for the MOD space directorate looking at how you navigate and operationalise those own-collaborate-access decisions. I can share that with the Committee. It was, effectively, a flowchart of questions and yes/no arrows going to different places. The reality is that so much of this has a temporal dimension. There is a time dimension to it. Building a digital targeting web in the next couple of years is the ambition. That is partly as a forcing function to show that the MOD can innovate and absorb that tech at pace. It is also a recognition that the threat we face is potentially war in the late 2020s and early 2030s and we want to get ahead of it. If that is the time horizon you are optimising for, your choices around sovereignty are

driven more by expediency and getting stuff working and out the door than perhaps having full control over it in the way you would like.

An obvious example is Ukraine. Ukraine has gone from a very old-school, Soviet-style, poorly equipped military to one that now has systems like Delta, which is their command and control software that does a lot of that, and things like Avengers, which is an AI tool that helps with targeting. They have built a lot of that on the move as a country with far fewer resources than us, but they have done it because they have a wartime requirement and have accepted certain trade-offs around sovereignty. Certain bits they do themselves and they rely on others for certain bits, and then try to mitigate those things as best they can.

The reality in our case is that if we are facing a threat in the late 2020s you cannot build that entire tech stack as fully sovereign, as you say. To be clear, we already rely on countries like the US and others for many of these elements. Command and control is already not sovereign in the technology sense in many areas. Absolutely, there are things you can do that would give you prudent risk mitigations across that: looking at avoiding vendor lock-in in your contracts, looking at making sure you have control of the underlying data and understand where that is going, making sure you have freedom of use configuration and upgrade and those sorts of things. We cannot own and develop all of it, nor should we—it would be calamitously expensive—but there are absolutely things you can do with smart contracting and the like to boost your resilience.

The final thing is thinking through what the mitigations are. If I cannot rely on a system any more because it is reliant on a foreign company and that company withholds access, what is my back-up? What is my reversion mode? What is my redundancy? That is something we need to more generally get better at training the military in. How do you operate when you don't have access to space services? How do you operate when all your networks have gone down, and how do you operate when you cannot get anyone on the radio because everything is jammed? That is procedural. It is training. It is education. It is not tech, but it is as important. We can either win advantage by having the best tech or win advantage by being the best country at fighting even when we don't have the best tech.

Chair: Very good point. A final question from Emily.

Q54 **Emily Darlington:** It flows really well from the question Chi just asked you. I want to bring you back to space. Space command is probably the least developed chapter in the SDR. I have had the pleasure of seeing much of our capacity in that area. There seem to be two schools of thought. One is that we are behind, so we will just rely on others. The other school of thought is that given where warfare is going we absolutely have to accelerate. Where do you guys sit in that discussion? Do you think that the UK needs to play catch-up and put a lot more investment into that near-space function for defence reasons—you could

put commercial and economic reasons into that—or do we say, "We've missed the boat on this one. We'll start looking to develop in other areas and rely on others"?

Dr Hüsch: I am sitting next to a space expert.

James Black: Yes, I wear a second hat, or a fascinator, as the head of our space hub at RAND Europe. I gave testimony to the UK Engagement with Space Committee a couple of months ago. We have done a lot of work with the space directorate, Space Command, and others in the US and the European Commission.

Absolutely, there is a need for more investment. The UK has over the last five years with the national space strategy and defence space strategy signalled a level of intent. There is increasing concern from industry, allies and partners that the stated intent is not matched by the investment. We have lots of strengths in the UK in our space science base and the industrial base, but we equally have challenges. We obviously do not have the scale of the US. We do not have the commercialisation trends of the US around space. We are outside the EU, which increasingly has an outsized influence with things like the European Space Agency. Something like 75% of the UK Space Agency's investment goes into ESA, so we do not really have a strong national programme. We have lots of good contributions to international programmes. We have improved our geo-return from ESA recently, which has been great, but, again, we do not have a sovereign base that we are building on.

The same applies in the military where we have had outsized access to Five Eyes and functionally American space capabilities for decades, which has meant we have not invested as much as the French, the Germans or the Italians. We are not spending the proportion of GDP on those things that we probably could and should. We are now in a situation, even predating the current Trump Administration, where the UK wants to increase its offering in those partnerships. We are never going to be a 50:50 partner on military space issues with the US, obviously, but can we be 70:30, 80:20 rather than 90:10 or whatever the number is? That is about us having sovereign capability and offering resilience and services to others, like our allies in Europe and the US and further afield.

Yes, you have to invest more. We are doing lots of great interesting things at Space Command at the moment in building up the capability of that command with people and investing in and innovating a new orbital asset, but they are not at scale. If we look at the numbers we are putting in orbit versus the numbers the Chinese are putting in, it is a huge gap.

Chair: I think the answer was yes. That's brilliant. Thanks so much. Thank you very much, Dr Pia Hüsch and James Black, for your contributions. It has been absolutely fascinating, if somewhat disturbing.