HOUSE OF COMMONS

Defence Committee

Oral evidence: The Integrated Review – Threats, Capabilities and Concepts, HC 834

Tuesday 10 November 2020

Ordered by the House of Commons to be published on 10 November 2020.

Watch the meeting

Members present: Mr Tobias Ellwood (Chair); Stuart Anderson; Richard Drax; Mrs Emma Lewell-Buck; Gavin Robinson; John Spellar; Derek Twigg.

Questions 52-89

Witnesses

I: Dr James Lewis, Senior Vice President and Director, Strategic Technologies Program, CSIS, and Distinguished Visiting Professor of Cyber Studies, United States Naval Academy, and Dr Beyza Unal, Deputy Director, International Security Programme, Chatham House

Examination of witnesses

Witnesses: Dr James Lewis and Dr Beyza Unal.

Chair: Welcome to this Defence Committee hearing, which will focus on the integrated review. I am delighted to welcome Dr James Lewis, who is the senior vice-president and director of the strategic technologies programme at the CSIS and a distinguished visiting professor of cyber-studies at the United States Naval Academy. We also have Dr Beyza Unal, the deputy director of the international security programme at Chatham House. Thank you both for joining us this afternoon. Our focus on the integrated review will very much look at cyber-threats and cyber-security, and at both civil and military aspects.

Q52 **John Spellar:** I will first apologise to our guests if I have to walk out not long after asking my questions. It has nothing to do with the argument; it is because I have to be in the Chamber. To start off with a scene-setter, how have cyber-threats to the UK evolved since the last Strategic Defence and Security Review in 2015?

Dr Unal: We still have similar issues to those we had in 2015, when the last national Strategic Defence and Security Review was published, but what we see today is a larger scale of operations. Also, the type of operations and the method of operations have changed. In cyber-threats, for instance, we see attacks on businesses and companies. We see different types of attacks, in general. Attacks on the UK's critical national infrastructure are happening.

What we see today is more sophisticated in nature than it was in 2015. The attackers might have exploited security vulnerabilities within the critical infrastructure. There are insider threat problems. There are problems that come with the exploitation of design vulnerabilities, and so on. The third level of threat that was probably not described in 2015 is cyber-threats to military systems and weapons systems themselves. That is what we are seeing—exploitation of the space infrastructure, for instance. The types and the scale of the threat have changed.

Q53 **John Spellar:** So in both qualitative and quantitative terms there has been an exponential increase in the threat.

Dr Unal: I would definitely say that. In terms of the actors involved, we see the same actors, such as Russia, China and Iran, being involved in certain types of activities. There are also state-sponsored actors, of course. The third level, which I think is a trend that is coming up, is the nexus between organised crime groups and hacker communities, for instance. The dark web started to be a place for those two groups to meet up. There were some incidents that happened in 2017, for instance. South American drug smugglers worked with hackers to infiltrate Belgian port systems. The aim was drug smuggling, but we know that in the defence sector there is more and more digitalisation going on for borders, port systems and so on. That will lie as a threat in the future that we also need to be looking at.

Dr Lewis: I used to work at the UN. That means I still have Russian and Chinese friends, or at least acquaintances. In discussions with them we have generally concluded that the nature of the cyber-threat has changed. Whereas we once focused on critical infrastructure protection, they agree that the greatest threat is from espionage and influence operations.

For the purposes of this Committee, I would add that interfering with military operations and systems has become a goal for all major powers. On any given day, Russia and China at a minimum will be trying to hack into your defence systems, both to interfere with decision making and to reduce the performance of any technology that you may rely on.

What have we seen since 2015? A much higher pace of activity and much greater agility on the part of our opponents. They are exploring combinations of technology. One that I think the Committee has looked at in the past is the combination of electronic warfare and cyber-operations. That will be the future of warfare in many ways.

We also see that our opponents are much less constrained than they used to be. In 2015, I was one of the people who negotiated the global agreement on norms. We could not get that deal today. At that point, Russia and China were interested in finding ways that we could work together to improve stability and decrease risk. They no longer feel that way, so it is a much more difficult and a much more hostile environment—one where I would say that espionage, influence operations and interference with military systems are your principal concerns.

Q54 **John Spellar:** With that, you are clearly looking right the way across the board, including most countries. How would you compare the threat faced by the UK with those being faced by other countries? Conversely, how would you evaluate the UK's capability to respond?

Dr Lewis: For some reason, the Russians really do not like you. I still have not quite figured that out; it may be some historical artefact.

John Spellar: The Russian revolution.

Dr Lewis: It goes back a way, and they have a special regard—perhaps it is the desirability of living in London. I think that for you the primary threat is Russia, because the Russians have shown themselves in other areas to be unconstrained and undeterred. They are in a much more aggressive campaign against the UK than they are against the US. They are very aggressive against the US, but that is primarily influence operations; we don't see assassinations, we don't see as many penetrations of airspace, and we don't see the naval probes that you see. So Russia is your primary opponent.

The Chinese have a global campaign to steal technology, and the UK is a primary target because of the strength of your R&D and the strength of your defence industry. Again, the Chinese are less of a threat on the influence side; they studied what the Russians did in 2016, but they have not yet been able to duplicate it. So with the Chinese the threat is espionage; with the Russians it appears to be everything.

I do not know if my colleague agrees, but when we list the cyber powers—the countries with advanced cyber capabilities—the UK is always at the top, but that is more GCHQ than your MoD. One of the issues, which I think you are rightly looking at, is this: how do you bring the MoD and GCHQ into operational alignment?

There has been some success. Task Force ARES in the US, which you may have seen, was a joint effort against ISIS's internet and online activity, and it was successful. From that we learned of the need to combine NSA and Cyber Command, and I think that you have a similar issue. You have made progress, but that is what I would look at. The UK is at the top of this list with its capabilities, but I am not sure whether you are yet at the top when it comes to military application.

Dr Unal: I would agree with that assessment, in a way. When it comes to cyber-threats, it is really Russia and China that are leading in the UK's threat landscape.

There is a reason why Russia is not following a similar course of activities in the UK and the US, and it is mainly because the Russian strategy is completely different from the Chinese strategy or the Western strategy in general. It relies on non-traditional, non-kinetic approaches in different countries, and it does testing and probing of systems in different ways. So where it conducts information operations in one country, it conducts a different type of operations in another—cyber operations to military systems, cyber operations to critical infrastructure, election meddling and so on. That is actually part of the Russian strategy, so that is what we are seeing.

When it comes to China, I think the major threat is really the theft of intellectual property and related issues. Of course, we can also talk about critical national infrastructure and so on, which we have already mentioned.

John Spellar: Thank you very much.

Q55 **Chair:** You mentioned the phrase "the dark web". It is used as a general phrase as this place, for something in the ether that anybody can go to and that is unpoliced. For the uninitiated, given that the web is man-made, why do we not have greater control over what happens in the dark web? Why is it seen as a place where there is no authority and where anything goes?

Dr Unal: Thank you for that question. There is a certain level of authority; I know that the FBI and others are working to try to understand who is in the dark web, but the problem is that there is a lot of anonymity. It is a place that you cannot access from your regular internet engine. For you to be in the dark web, you want to have anonymity and that anonymity is, in a way, provided in that web environment. There are methods whereby organised crime groups, and even terrorist organisations or hackers, find ways to disguise themselves from the authorities. That it is why it is very challenging.

Dr Lewis: I think the dark web is important in relation to criminal activity, but one question to ask yourself is this: if Russia and China actually enforced their own laws when it comes to foreign hacking, how much would the threat go down? The majority of malicious activity—and certainly the most dangerous malicious activity in cyber-space—comes from these two states; they are the most active. Private sector actors do not have the full range of capabilities. That is changing, but very slowly. We have been hearing about this now for about 20 years. I would say, the dark web is interesting as a criminal activity, but the source of the problem is two nation states—Russia and China. It is worth asking about Iran, because it is improving. If you compare where the Iranians where 10 years ago with where they are now, they are much better, but they are still not very good. It is those two countries that are your principal opponents, and they are active against you as we speak.

Chair: Thank you.

Q56 **Richard Drax:** Good afternoon to you both. What role, if any, should the UK Military play in enhancing the cyber-resilience of the UK's critical national infrastructure?

Dr Lewis: I use the UK as an example of a country that has actually done pretty well when it comes to these things, with your National Cyber Security Centre, the work of GCHQ and of other Ministries. I would say that Ciaran Martin, who has just left, did a stellar job. You are in good shape when it comes to critical infrastructure. It is difficult because the threat is omnipresent, agile, dynamic and it evolves rapidly. Where does the Ministry of Defence fit in? Of course, at the core, a strong defence is essential for cyber-security, because there will always be vulnerabilities. You need opponents to think and calculate what the risk is of taking action against you. I would probably suggest focusing more on that: what can the MoD do to change the attitudes and expectations of foreign opponents, rather than directly working with the private sector to secure critical infrastructure?

Dr Unal: I would add that, when it comes to resilience, I see it in four realms. You can create resilience by focusing on cyber-defence. I think the MoD is already doing that by thinking about protecting the systems and networks of the Military. I think that is really hard to do, because we are talking about complex and integrated systems, so mapping needs to be completely done on understanding the levels of risk and vulnerabilities that exist in order to protect these systems. It is a certain level in the MoD that has been coming along.

The second way of creating resilience for some people is through cyber-offence. The claim on the cyber-offence side is that if you hunt for systems and try to find threats in different systems and networks, you can then come back to the UK network and protect it before the adversary attacks your system. They say you are preventing an attack before it takes place and making your system resilient. That is a bit controversial at the moment in the UK. GCHQ generally holds the cyber-offence capabilities more than the MoD itself, and then there is the question of how much

cyber-offence capability the MoD should have. Of course, there has been the establishment of the National Cyber Force—I think it was established in June or July—which it is a joint structure between the MoD and GCHQ that is looking at these issues.

The third way to create resilience is by looking at deterrence itself—how can we make sure cyber-deterrence works? The way it works in my mind is by denying the adversary the ability to attack the MoD structures or the UK itself. That is particularly important for creating resilience structures.

Q57 **Richard Drax:** You make a very interesting point, Dr Beyza, and I have heard it before. I wonder whether you can clarify the divide between the MoD and GCHQ. We have visited the MoD, and it seems to take a more defensive role and to shy away from a proactive, more aggressive role, leaving that to GCHQ. Why is that, when the MoD represents our Armed Forces? My view, as an ex-soldier, is that the best form of defence is attack.

Dr Unal: I do not know why that division took place at the very beginning, but in 2013 the UK decided to establish a big force in the cyber space. The realisation was, "Okay, who is going to be at the forefront of the activities?" GCHQ, as the main organisation, together with the National Cyber Security Centre, has been the one generally doing either the attribution side or conducting the offence side. I think that has actually been changing a bit. For instance, I have been told that within the Army there is a small regiment looking at issues relating to cyber-offence, but it is very small—compared with what GCHQ does, it is nothing; that is what they say.

The National Cyber Force that is now established is a really interesting initiative, because it is a joint initiative between the MoD and GCHQ. The whole idea is that it is not only defence, because there is also an offence component, but there needs to be some clarity about what the National Cyber Force is going to do. There is not much transparency when it comes to the cyber-offence operations. The UK actually wants to keep these things a bit quiet, and that is probably because they do not want to put much classified information, or any type of information, in the hands of the adversary. We need to learn a bit more about how we should be clearer about the objectives of cyber-offensive operations. That is really critical.

Q58 **Richard Drax:** Dr James, what should the Military not be responsible for?

Dr Lewis: The debate at the moment in cyber-security is about the fact that we have state actors that are unconstrained. While we have agreed norms, they do not pay any attention to them, so how do you impose consequences on them that will get them to recalculate their behaviour?

There is an implicit threshold in cyber activities, above which countries have been reluctant to go. That threshold is roughly the use of force. Things that cause deaths, damage or casualties are generally avoided. There have just been a handful of episodes, largely by the Russians, to

some extent by the Iranians and the Israelis, and in at least one instance by the US. The UK has been active in other ways.

One of the first questions for you to ask is this: how do you decide where offensive operations make sense? I note that there is a great concern in the academic community about escalation, yet in more than 20 years of cyber-operations, we have never seen inadvertent escalation, so I think that fear is overrated. The most important thing that the MoD can do is signal the UK policy to opponents and show that the UK has the capability of taking punitive or retaliatory action for some kind of cyber episode. Through working with the civilian infrastructure, I am not sure there is any need there.

One of the things that we found—I did a lot of work with the UK when it set up the National Cyber Security Centre—was that private companies prefer to work with civilian agencies. Although the Military has an important role, it may not be in working directly with the companies, which is one of the key elements of success for the UK—sitting down with your big companies and talking to them seriously about cyber-security. The MoD's role is probably on the other side of that divide. That is not to say it is not a crucial role. It is one that many countries have wrestled with, because it is a little frightening to see offensive cyber-operations. But it is one that you will need to work through.

Q59 **Richard Drax:** Dr Beyza, do you have anything to add on what the Military should not be responsible for?

Dr Unal: I think the Military should not be responsible for protecting the networks and systems within the overall UK infrastructure. The Military is responsible for protecting its own networks. If we do that greatly and in a good way, I think we would be even better off than we are today. That responsibility needs to be clearly defined.

Richard Drax: Thank you.

Chair: Thank you, Richard. Let's go to Stuart Anderson.

Q60 **Stuart Anderson:** At the outset, Dr James, you spoke about how the nature of cyber threats is changing from CNI to espionage and influence. How vulnerable is the defence industry compared with other CNI sectors?

Dr Lewis: It is of course a central target for opponents—both the Russians and the Chinese—because there is a desire to understand how British weapons work, to understand British defence R&D and to borrow the fruits of your labours when possible. The Russians are less effective when it comes to the theft of intellectual property. I sometimes wonder whether that is because they have so many industrial and economic problems now. Unfortunately, the same is not true for China, so I would say the biggest single threat to the UK defence industry and cyber-space is Chinese espionage. I am sure that you have already been briefed that this is a regular occurrence. In some ways, that makes the defence industry a little unique, because it is related to defence. But it also makes

them a very high-priority target, so it is a much more difficult environment.

People know that if you were to turn off the electrical power in the UK, it would probably generate some sort of very nasty response. The Russians or the Chinese could do it if they wanted to, but they won't unless they get into much greater conflict with you. But stealing your defence property—that is just par for the course. Remember that part of this is about understanding that software now makes up a significant proportion of every weapons system. Understanding how it works gives you the ability, in a conflict, to interfere with it. The defence industry is in some ways a unique target.

Dr Unal: You particularly asked about the difference between the defence sector and the other critical infrastructure. There are a lot of similarities in terms of vulnerability, but one difference I see between the two is actually the vulnerability of the supply chain. Within the defence sector, it is way higher than the other critical infrastructure within the UK systems. The reason I am saying this is because, as far as I am aware, the MoD is focusing mainly on the defence companies within the tier 1 structure, in order to create a protection for the tier 1 defence companies. These are companies that are big defence companies that the MoD does dealings with. But these big companies generally subcontract to small and medium enterprises, or to other companies. The way that I know is that the MoD defers the responsibility on cyber-actions by subcontracting to the tier 1 companies. That poses great danger, risk and vulnerability, in the sense that we should be aware of the level of maturity—cyber-maturity—in the supply chain. That is the biggest risk that I see.

Dr Lewis: May I add a note of caution? I agree completely, the primes are protected, so their opponent goes down the food chain until they find a vulnerability. But one unexpected consequence that we found is that some of our suppliers say, "It's not worth it, so I'm exiting the defence market. You have put all these requirements on me, and I don't have to—if I make commercial products, it's easier." We found that through efforts like the cyber-maturity model and other requirements, you have the risk that the smaller suppliers will exit the defence market. That is just something to think about. It is a manageable problem, but it is a problem.

Q61 **Stuart Anderson:** That is an interesting point. Yesterday, in a Sub-Committee, we discussed that very point with my friend Mr Drax.

Looking at the supply chain, having identified some vulnerabilities within that, what are the implications of those vulnerabilities? Dr Unal, will you start us off, please?

Dr Unal: I guess there are a number of implications. The first implication is probably that there would be an advantage in stealing data—sensitive information, classified information and so on—and that is important to the MoD for many reasons. The MoD tries to secure this type of information. With remote working, for instance, this risk is increased as well, so we need to understand what covid-19 brought forward for us.

What is also important is that sometimes the equipment itself might come flawed from the design stage. If it is designed by a subcontractor company, not the contractor company itself, and if the equipment is flawed at the design stage and that is not recognised, it is implemented within the other military systems, and you will see consequences, even mission-related or mission failure-type consequences down the line in the long run. We need to understand that. The implications we see today are peacetime ones, but we need to think about the conflict or crisis time—the implications happening today will probably be higher when conflict or crisis starts.

Stuart Anderson: Dr Lewis, may I get your views on that as well, please?

Dr Lewis: I agree with everything that my colleague has said. I would add two points. One concern is that access to software by an opponent allows them to contaminate it. Given that these are programmes that involve millions of lines of code, we might not know. We might be able to detect the entry. One of the rumours about why the F-35 is so expensive is that, at some point, going through a sub-tier supplier, the Chinese were able to gain access to its software. Rather than say, "Oh, we think we found all the problems", it had to be replaced. Contaminating the software is a crucial risk.

The other one is going back to the American experience—I apologise, but it is what I am more familiar with. We did a study some years ago of the provenance of software in weapon systems—provenance is an important point. We did the initial study about a decade ago. One of the big primes makes a product, and it contracts out to a sub-prime to do the software. The sub-prime will often go to a specialist firm to do it, and then there is the specialist firm—by the time we got to the end of the chain, it turned out to be Uncle Vinny in Mumbai who was writing the code.

Plus, there was a reliance on open source software that was a bit of a surprise. My impression was that, to some extent, the reason the primes were reluctant to share provenance was that they were reusing code and selling it twice. That is just a guess. But you need to ask yourself, has my software been contaminated? Where did it come from? What is it made of? You should particularly ask the question about third-party open source software that goes into the actual code. I do not know whether you need rules for this beyond transparency, but it is useful to have some insight into where the code came from and who wrote it.

Q62 **Derek Twigg:** Dr James, following on from your last answer, my question is about how cyber-threats to military systems differ from those to civilian critical and national infrastructure. Perhaps you could say a bit more about that.

Dr Lewis: The threat is in many ways similar. I think you have heard that from both of us. The goal is to gain access to software, control systems and the software that actually provides operational capabilities. In that, there is a difference with critical infrastructure. You can hack the power grid and get an understanding of the operating system that creates the

electrical power, the operational technology, but this is much more focused in the defence sphere. The threat of stealing intellectual property is the same.

In critical infrastructure it is the ability to understand weapons performance, to manipulate that weapons performance and degrade it, and to understand the role of IT in decision making by commanders and degrade that decision making. One great benefit of cyber-conflict is that it allows you to expand the fog of war exponentially. That is what opponents are often looking for. How do I confuse the other side? How do I make them make mistakes? How do I get them to slow down in their decision making? That is where you will get an advantage as an attacker. That is a difference here: the more intense scrutiny of operational activities and the desire to build in much greater ability to interfere in those operational activities. For me, that is the difference between regular critical infrastructure and defence critical infrastructure.

Q63 **Derek Twigg:** I think I heard you say in an earlier answer that the Russians and Chinese could, if they wanted to, turn off our power supply or our grid. On what basis do you make that comment and do we not have defences against that?

Dr Lewis: You do, but as we know from other military activities, no defence is perfect. Were the Russians to decide that that was a useful move for them to make—I think it is unlikely, but they could—they could devote an immense quantity of skilled resources to look for vulnerabilities. As we have discussed, those vulnerabilities might be in the people who supply the electrical power or in the people who support them. There is a famous incident where the penetration was made through the company that managed the air conditioning systems, which was not the primary target. One thing we have learned is that there are thousands of potential vulnerabilities and an aggressive opponent who is willing to devote the resources is likely to eventually find them.

Q64 **Derek Twigg:** Dr Beyza, do you want to add anything to that?

Dr Unal: I would add that we need to protect not only the software, but the hardware and the network. There are different levels of protection and vulnerability that exist. I did research of nuclear command and control systems in relation to cyber-threats, as well as strategic weapons systems and cyber-threats to conventional systems. I would say that vulnerability exists both in the conventional and in the nuclear enterprise in general. You will see vulnerabilities that result from human error. These systems are operated by humans, so we need to be aware of that. There are vulnerabilities that result from system failure. There are the vulnerabilities that come from the design vulnerabilities that we mentioned. Sometimes there is reliance on open-source, commercial software, off-the-shelf software. That could also be part of the vulnerability that comes to the command and control structure—or maybe not command and control itself, but a system that is indirectly linked to the command and control structure.

I would also say that the operations are actually a bit different when it comes to the weapons systems themselves. This is not only on the cyber-side; we are also seeing electronic warfare activities. We see, for instance, jamming and spoofing. These two terms go hand in hand when we talk about weapons systems. Spoofing is a co-ordinated attack where the adversary, the attacker, changes the information but the recipient country does not realise that the information has changed. A good example of spoofing activity is that Russia spoofed the GPS systems of the US ships in the Black Sea and those ships ended up in locations that they did not initially mean to be in. The navigation system itself was spoofed and they didn't even realise that it was spoofed.

Therefore I would say that, in terms of the types of operation that we are seeing, it is probable that spoofing is really important, and we need to be addressing how to prevent spoofing. We focus a lot on jamming, but if your system is jammed, that means that you are not getting the signal, and automatically the Military will realise that something is going on—something is jammed. When you are spoofed, you don't even know that you are spoofed, and that is particularly worrying.

Q65 **Derek Twigg:** To follow up the point about command, control and communication systems for both conventional and nuclear weapons, could I ask you to say how the threats might be different in terms of the various structures that we have in place to try to protect them? Is the risk to nuclear different from that to conventional?

Dr Unal: There are definitely different levels of threat to nuclear and conventional, but I would be cautious, because there is more and more integration—what we call entanglement—of conventional systems with the nuclear systems. For early warning, for instance, we use conventional systems as well as the nuclear systems; there is this entanglement of the two. Then the question becomes: if the early warning system is attacked or infiltrated, how will that correspond to the nuclear weapons system itself? Because these systems are complex systems, the level of integration and entanglement within the systems is not yet known as much as we would like. I think we should be really careful not to overestimate what we know. It is much better to say that we need to be looking at this; we need to be doing a better job at this, and hence we need to be looking at both conventional and nuclear weapons systems.

Derek Twigg: Dr Lewis, do you want to add anything?

Dr Lewis: Sure. One of my son's friends is in naval aviator school, and they are forcing them to learn how to use a sextant. I could never get the darned thing to work, but the theory is that you can no longer rely on GPS, and that's interesting—I pity the poor kids who are having to learn how to do 17th-century technology.

You have a bit of an advantage on the nuclear side, in that your arsenal is submarine-based. That imposes an additional level of difficulty for an opponent—it's not impossible—but this is something that people know. It is very dangerous to interfere with another state's nuclear weapon. So

there are several degrees of security not related to cyber per se. The things to look at are, how could you interfere with command and control or how could you interfere with air defence or naval operations? One of the things that I have always thought would be a lot of fun would be, there is something called Blue Force Tracker, where you are a commander and you have a screen. There are little blue dots on it that are your people and red dots on it that are their people. Suppose I could switch the dots so you shot at your own people? That would be great for a number of reasons, not because of the actual damage, but because it would make you hesitant.

That is the thing to focus on in this. It is not the nuclear weapons per se; it is the ability to inject uncertainty into commanders' decisions, including the decisions of political leaderships. Uncertainly in information is the unexpected battlefront that we have now.

Q66 **Derek Twigg:** Are there particular vulnerabilities around legacy systems?

Dr Lewis: I used to feel that legacy systems actually had a slight advantage, because the people who knew how to run them, at least in the US, were two people in their 70s who had retired to Florida, and it was difficult for a new generation of hackers to figure out how to get into them. Unfortunately, that is no longer true. To the extent that you rely on commercial software—this was the earlier point—which might be outdated, that does increase the level of vulnerability.

I once asked friends of mine who work at Microsoft, "Why do you change Windows every few years?" and they said that part of it was marketing, of course, but part of it was that after three or four years, hackers had discovered every vulnerability and they could no longer guarantee the security of those legacy systems. Legacy is probably a source of increased vulnerability, unless you take extraordinary measures.

Q67 **Chair:** Can I go back to a couple of points that have been raised? Dr James, I think you mentioned the F-35 and that China gained access to the software. Can you elaborate on that and where that went to? Was it stopped or is it something that we are having to live with?

Dr Lewis: Lockheed Martin did a great job of protecting its systems, but, as we heard from the earlier discussion, as you go down the level of contracting, not everyone is perhaps as secure as we might want. That is the allegation—that going through a subcontractor, the Chinese were able to gain access. What they were able to do, we do not know. The vulnerability was closed, and the software was largely rewritten to ensure that it did not contain unwanted surprises.

Q68 **Chair:** Okay, that is the assurance that we probably wanted, given that we are purchasing these aeroplanes: that that is no longer a concern. On the spoofing, if I can turn to Dr Beyza, you mentioned GPS systems in the Black sea. The Americans pride themselves on GPS being hacker-proof, if you like. The general public are perhaps not aware of how over-reliant our world has become on GPS. You buy a cup of coffee and it requires three satellites to make that contract when you tap your credit

card on the payment system.

Dr Beyza, can you expand on what happened with the spoofing of the GPS systems? I think it was Dr James, or maybe it was yourself, who said that our CASD is not reliant on any form of constellation of satellites, and that is a good thing, but everything else that we have is—all forms of communication. Indeed, our two main air-to-ground missiles, Brimstone and Storm Shadow, absolutely require GPS. Therefore our entire defence capabilities would be vulnerable if the Russians had succeeded in spoofing the GPS constellation of satellites over the Black sea.

Dr Unal: That is a really important point. I actually did studies on that looking at the cyber-security of space-based systems, and GPS is part of that infrastructure in a way. The Black sea is just one example. There was another example of GPS spoofing, for instance, just recently, during the Trident Juncture exercise in 2018-19 in Finland. We also saw jamming when the GPS signals were jammed by Russia. That was a civilian activity, but the outcome was seen by the Trident Juncture exercise as well.

There are things happening. The threat in this area is that we are over-reliant, as you have said, on GPS. That is the position, navigation and timing data that we use for almost everything, from our daily activities to critical national infrastructure, weapons systems and so on. That over-reliance and dependence need to be addressed in a careful way. I know that the UK Space Agency has actually been doing some work on understanding the space dependency within critical infrastructure, not only for GPS but for the Earth observation technology that we rely on or the weather information technology that the Military relies on, which all comes through space. That is probably why space is extremely important for military operations. We need to understand and realise how to create redundant structures for GPS or GNSS systems. That redundancy does not have to be on the satellite itself; local redundancy structures could be established as well—that needs to be looked at. Diversity is key.

Dr Lewis: To build on that, there are disputes over the Russian activities against US naval vessels in the Black sea—the Russians can be a bit boastful. I completely agree on the need to think about redundancy, particularly for merchant shipping. When you think of the channel, if you were to interfere with GPS, it may not be the Navy that suffers, but it could easily be the merchant ships. That could be damaging in ways that we would not want. There was an old system called LORAN, which was ground based and used radio, and we largely dismantled it as GPS came online. Now, people are thinking about the need to reconstruct those ground-based radio systems. Redundancy, as you have heard, is the key point, but do not always take everything that the Russians say at face value. I know that comes as a newsflash to you.

Chair: I know that a lot of the merchant navy watch our discussions on the Parliament channel, and I am sure that they will be rushing to antiques shops to buy sextants just in case this all comes true. Let us turn to offensive cyber-operations.

Q69 **Gavin Robinson:** Good afternoon to you both. I am going to ask about offensive cyber-operations in support of military objectives. Perhaps I can come to you first, Dr Unal, given your comments about Russia and spoofing. How have the UK's likely adversaries conducted offensive cyber-operations in support of military objectives? Do you see Russia's approach changing or evolving following the campaigns in Georgia, Ukraine and Syria?

Dr Unal: I think Russia is really taking the bat on this. As you have just mentioned, in Georgia, Ukraine and Syria, they have done a lot of testing of what types of cyber-operation they can do during crisis and conflict. In Western countries, we do not test those things in real time; the Military utilises an operational experimentation phase. Unfortunately, with Russia that is not the case; they really used Georgia or Ukraine as a test bed for those operations. That actually goes hand in hand with their military objective, which is really to rely on conducting grey zone activities and under-the-threshold activities. Those are hybrid activities that have the benefit of deniability—they come with a certain level of deniability. It achieves the objectives of war without actually going for war, and that is particularly important. We need to be thinking of how we can counter those grey zone activities and think about countering them. How do they conduct these activities? I do not know much about the Chinese side, but I can talk about the Russian side.

In terms of actors, Russia generally relies on GRU, which is the military intelligence organisation within Russia, and if you look at the operations that they have taken, there has been some attribution from the United Kingdom and the United States on some of these issues. They have done activities, for instance, on campaigns, collecting information on Hillary Clinton's emails back in the previous election; they have attacked the US Democratic National Committee and conducted attacks on the Ukrainian power grid, for instance, to go back to your example on Ukraine.

In the UK, for instance, in 2018, they attempted to attach attack DSTL, the technology and scientific lab within the UK, and they also did a cyber-attack on the FCO servers. I think 2018 is the key timing here, because it corresponds to the poisoning of Yulia Skripal and Sergei Skripal in the United Kingdom. The Russian activities are asymmetrical; they would follow these activities for the purpose of coming with the military objectives themselves.

In Syria, it is a bit different. They had done cyber-activities in Syria as well. For instance, I have seen that they did cyber-offensive activities on the Turkish communications systems in order to prevent the opposition forces from communicating with their Turkish counterparts back in 2015. They have also created these A2/D2 bubbles in Syria, which also helped with the cyber-activities. I see a merging of things coming up.

One last thing: Georgia is probably the start of all these things in terms of dominating the information space. I would say that Georgia was more about information operations and information domination, and Ukraine is more about test bedding on the critical national infrastructure how to

probe the systems and see the impacts of those systems. Syria is another level, adding up to the military stage with the A2/D2 systems and so on.

Q70 **Gavin Robinson:** Dr James, I don't wish to preclude your ability to respond to what we have just heard, but perhaps I could shift you on towards China. May I ask how China has deployed cyber-capabilities in pursuit of strategic objectives in the Indo-Pacific region?

Dr Lewis: One of the things we want to do is distinguish cyber-operations in support of larger military operations. That will be interfering with weapons, sensors and decision making, but that only occurs in actual armed conflict. All our opponents have developed some capability in this area. The second issue is political; this is a political contest, and that gets left out sometimes. The Russian goal is to create civil unrest, and to do that they need to manipulate public opinion. They have a theory called reflexive action, which has been part of Russian strategy for years, using misinformation and manipulating opinion. The defence there is largely political. On the military side, yes, you need to have the ability to defend your systems and interfere with the opponent's systems, but on the influence operations side, it is a political question. Do your citizens perceive the structure of government as legitimate? Do they believe in conspiracy theories?

The Chinese are less advanced at that. I have always thought it was funny that at one point we published a list of all the weapons systems we would use in what was then called, I think, the air-sea battle in the Pacific. That was a big mistake, because for every weapons system we listed, the Chinese immediately turned to try to hack it, sometimes with success. That was air defence, fighter aircraft, sensors and naval operations. China has a military capability that is focused on interfering with the operations of its opponents—communications centres and weapons. They are not as far along as the Russians; they are not as good, but of course they improve rapidly.

For China, the primary concern is their own population, and so much of their cyber-activity is focused on political control of their own population—massive propaganda campaigns and control of social media to squelch any dissent. So, the Chinese haven't been as effective in the kind of influence operations of foreign opponents as the Russians have been. They have other tools; they use money. You know, how many people thought for a long time that China was winning the 5G race. That turned out to be completely false. When I would talk to my Government colleagues, I would say, "If we get one thing out of Huawei, we should get their PR firm, because they're really good."

So, the Chinese have a blend of economic, military and espionage activities. The Russians have a greater sense both of the military capabilities but also of the ability to manipulate Western politics, and I think that is the key difference.

Q71 **Gavin Robinson:** You have already talked about the ability of China to evolve rapidly, but could we see China deploying cyber-capabilities in

support of kinetic operations in the future?

Dr Lewis: Oh, they already have. One of the things that is worth noting is that cyber-operations are increasingly blended with electronic warfare and with the electromagnetic operations in the electromagnetic spectrum. You know, ships are mobile, aircraft are mobile and weapons are mobile, and it is the ability to interfere with the communications that depend on radio signals that depend on spectrum. The Chinese have put a lot of effort into this.

The Chinese are not as far along in jamming; they have tried some very coarse jamming activities. The easiest way to think of them is that they are not as advanced when it comes to the warfare elements of this as the Russians. There are places where they have particular strengths. So, they probably have better missiles than anyone in the West—anti-ship missiles, certainly.

However, I think their doctrine is largely to avoid conflict—armed conflict—for the next few years. That is not to say they will avoid it for ever and there is always a chance that they will miscalculate, in India or in the South China sea. But they would prefer to bide their time, build their strength and avoid military confrontation.

Q72 **Gavin Robinson:** Thank you very much, sir. Dr Beyza, do you agree, or is there anything you wish to add to that?

Dr Unal: I would probably add that we cannot be certain that this is because China does not have the advanced capability; it is probably because we have not seen it. This doesn't mean they don't have it. Russia uses it and Russia tests it, but China doesn't do that. However, when we look at China's policy in other areas, it is really in line with its offensive cyber-operations as well. If you are not seeing what is happening, that just doesn't mean they do not have the capability itself.

I would again say that at the moment China is really focused on intellectual property and stealing intellectual property—at least that is what we are seeing from the US and the claim from the United States. Also, they are doing, as my colleague just mentioned, a lot of disinformation campaigns. That is a little different from a regular cyber-operation, I would say. So, those two things are a bit different, although they use the same medium as the cyber-space.

Gavin Robinson: Okay. Thank you both, and thank you, Chair.

Q73 **Mrs Lewell-Buck:** Afternoon both. I wonder if I could direct my question first to yourself, Dr Lewis. It has already been touched on in both your responses to my colleague Gavin's questions, but in what ways are our adversaries combining cyber-operations and information campaigns in support of their military objectives?

Dr Lewis: The initial Russian effort began with hacking, and it's interesting as an indicator—you can see the Putin regime using the tactics they have ultimately turned against Western countries. They used them first against their domestic opponents. That would include hacking

databases, emails and webcams—there was a famous incident where they hacked the webcam of an opposition politician in his bedroom—and then leaking this embarrassing material. One of their early episodes was not attributed fully. If you remember Climategate, which was more than a decade ago, someone hacked into climate scientists, found a number of embarrassing emails and then leaked them. The linkage is using cyber for traditional espionage purposes, to gain information that can then be deployed in the information campaigns and influence operations. That is the primary activity. The groups that do these are not always the same. One group will acquire the information through hacking; another group will then use it in information operations.

Dr Unal: On the disinformation campaigns, what we are seeing from China has shifted a little after covid. Before covid, on the disinformation side, China was portraying an image of how great China is. That is what they were doing and sending as a disinformation campaign. Inside their country, the whole idea is to control the community and control the country. They were doing two types of operation—one domestic, one outside. After covid, this has shifted a little.

With covid, there has been a lot of pushback on where this whole thing started, and it has been traced back to China. What we have seen is the emergence of Chinese Ministry of Foreign Affairs officials on Twitter, and a lot of new accounts have been established to diffuse information that this was not the case. We should remember that Twitter is banned in China, so they are even using Western sources to diffuse that information forward. That is something that we need to be aware of. China, and probably Russia, is using our openness and transparency—the two assets of being a democratic country—against the Western countries by taking such actions. That is something that we need to be working on.

Q74 **Mrs Lewell-Buck:** In terms of our Armed Forces, how should we be responding to this threat? Should we be responding to it in isolation, or should we be doing it alongside our allies?

Dr Unal: These types of threat are really hard to respond to, but we need to remember how the UK responded after the poisoning of Sergei and Yulia Skripal. That should be at least the baseline of what we should be doing. There was an immediate action in terms of attribution, whereby we started to gather information and track and trace what actually happened. This did not take one day, of course. It took several days or weeks for attribution to take place, but it was an important step for the United Kingdom. Afterwards, the UK pushed the allies together within the OPCW to create that attribution through the international stage. We have seen the UK pushing that forward, and it is extremely important. It is where we rely on allies and allied powers. These are the two things that are incremental and really important.

The other thing is that we need to start doing indictments. The US is really good at this. They just started doing it. I think they indicted six GRU officials just recently on cyber-operations. They are not only attributing to the nation or the state; they are attributing to the individual. That is

extremely important. Of course, these people are not going to travel to the US, probably—that is not going to take place—but the indictment shows the ability of a country and how well it can attribute to the level of the individual.

Apart from that, I think the last thing is about sanctions and working with allied countries to create a sanctions regime. Those are the points that I would add.

Dr Lewis: In working against both countries, the role of Allies is crucial. A collective response is much more effective, and it is perhaps the only effective response, particularly for the Chinese. The Chinese will try to brush off individual countries, no matter how big they are, but when it is London, Tokyo, Berlin, Washington and others, they are forced to pay attention. Collective response is crucial.

One of the things that we have been slow to do in the West is develop the appropriate responses to these activities. Our opponents have come up with a new form of inter-state conflict. It is not the conflicts of the 20th century. We need to rethink what our strategies are and what our operational efforts are in these areas, against things that will very often be below the level of the use of the force. It is nice that the Russians can't get through the Fulda gap, but that is not the battle any more.

Developing those appropriate responses is a key task for the Military. What are the right responses there? Part of that would be: where is an action by Military forces appropriate? That does not necessarily mean the use of force, but there are potential roles for the Military if we develop a new suite of responses to the aggressive behaviour of our opponents.

I will just mention that I love sanctions. I do talk to Russians and Chinese relatively frequently. The reason I love sanctions and indictments is because the Russians and Chinese hate them. They hate this because, for the Russians, it means no more vacations to the Maldives. They warn their citizens and their hacker community about the risk of being arrested, should they travel abroad after indictment. The Chinese hate them because it is embarrassing.

That is one of the things to think about. People sometimes talk about naming and shaming. That's worthless; you are not going to shame Vladimir Putin—give it up; it is just not going to happen—but this sort of attribution demonstrates your own capabilities and the UK has among the best capabilities in the world at attribution. It also puts your opponents on notice that you know who they are and you will take action against them should they come within range. It has to be part of a larger strategy of developing responses to this new form of inter-state conflict.

Mrs Lewell-Buck: Thank you.

Q75 **Chair:** Can I probe that a bit further? You talk about sanctions and indictments and so forth. Would you not agree that there is no set of international rules now? There is no Bretton Woods moment, to bring us

all up to agree a set of parameters. Where is the Geneva convention that we can point to, if we are able to apportion blame for a cyber-attack? With all these reactions, such as sanctions of individuals and so forth, are we not pursuing the wrong level of enforcement? Do we not need to update the global standards from which we operate, given how we are pivoting to a world where data is taking over terrain as an asset?

Dr Lewis: This will be a complicated answer, so I apologise. In 2015, all UN member states agreed on norms for responsible state behaviour. People say, "Well, the norms are non-binding." That was intentional, and the fact that a norm is non-binding does not mean that it does not have effect. When you think of the missile technology control regime, it is not binding. What is required for the norm to be effective is a political commitment to observe it. These things such as sovereignty, the UN charter and international law apply. States agree not to attack critical infrastructure contrary to their international obligations, which are under the Geneva conventions and international humanitarian law.

We have a framework of norms to guide state behaviour. The problem is that the Russians and the Chinese have decided that they can simply ignore them without cost. One thing that is interesting here is that late last year, again at the UN General Assembly, the UK, the US and 25 other countries agreed that they had the right to take action against a state that violated 2015 agreed norms.

What those actions were was not defined and could range from a démarche at the low end to some sort of military operation at the high end, but that is the core of a new approach, a new alliance with those 26 countries—which do not align perfectly with NATO, by the way—saying, "If you violate the agreed norms, we reserve the right to take action against you." Now we have to define what that action is.

I agree with you that it would be useful to have a Geneva convention. I worry that we only got the Geneva and Hague conventions after a catastrophe. That seems to be the history of arms control—something bad has to happen, and then we all say, "Ah, we don't want that to happen again, so let's come to an agreement." There has not been the catastrophe yet, so we are probably years from achieving any sort of binding international agreement.

I say that in part because the Chinese have decided that there is simply no agreement that would serve their interests, so we will not get the Chinese to agree. Tomorrow, I think, the French are holding the Paris peace conference again. When they did it last year, they came up with a statement about cyber-peace. I thought that was not useful, because China, Russia, the US, India and a number of other large countries refused to sign it. If the key actors will not play by the rules, there is no sense in getting an agreement.

Ultimately, we will need agreement, but what we need now is a coalition of states that share democratic values and that have agreed on potential

punitive consequences for malicious cyber-action. That is the task for the next few years.

Dr Unal: I primarily agree with that assessment. I would only add that the reason why the UN norms have not been going through, why Russia and China are not abiding by the norms agreed by the UN Group of Governmental Experts, the GGE on cyber, is mainly that what we in the Western world think the rules-based order is, is not the same as what Russia and China think it is.

The rules have changed from Russia and China's end—the way they see it is that the rules are not the same. That goes further than cyber, because it is really about the rules-based order. How are we going to define the rules-based order with Russia and China, or how can we get them back to the table of the same order that we had previously? That is the question that we need to be addressing, which goes beyond cyber. Even with space, the UN GGE on space has stalled as well. There is not much going on with that.

There are different levels at which we need to be engaging with Russia and China. But within that engagement, the problem that we have been seeing is how to make accountability an action. Responsible state behaviour means that you will not take certain actions, but if you do not do that, what will you face as a state? That has not yet been defined. That is why we see indictments, sanctions and so on.

Chair: Thank you.

Q76 **Stuart Anderson:** We have dipped in and out of this question but, before we go on to the next section, it would be good to clarify how the UK Military operates in the cyber-domain. Dr Lewis, will you start us off, please?

Dr Lewis: It is a new activity for the UK. One area for improvement would be better or more clearly defining the relationship with GCHQ. Another would be to identify the operational activities, or the menu of options, that the Military could undertake at the request of the political leadership in response to a cyber-activity. There is a third element. First, GCHQ; secondly, menu of options; and thirdly, defence infrastructure and weapons systems and networks. Those are all things that would be useful to pursue.

I don't know whether there is a role for critical infrastructure outside of what defence itself uses. I think the focus should be on that menu of options, which includes offensive operations. I don't understand the authorities well enough. In the US, authorities is always a problem. In the intelligence community you can do one set of things and the DoD can do another. Finding a way to make sure that the two are closely integrated has been a challenge, but it is something that there has been some success on.

There was talk a few years ago about splitting NSA and Cyber Command. That has all gone now. It was decided that it was beneficial to have them

dual-hatted, led by the same person. I don't think that is the right answer for the UK, but figuring out what the answer is for ensuring closer integration would be important. The main thing is coming up with the list of actions that the Military could undertake in the defence of the realm and ensuring that you have the capabilities to carry them out. We have all struggled with that, but when the Russians do x or y, do you do it jointly? Do you inform other people? What are the actions you are going to take?

Q77 **Stuart Anderson:** Just on that point, before I go to Dr Beyza, you have talked throughout about how the cyber-domain has changed. How time-sensitive is it for us to establish this? You had a list of options. At the moment it is not clear what we have in place. How time-critical is it to get it in place, or to get something right in place?

Dr Lewis: What is probably more important is to get in place a process within the MoD to make these decisions, and to ensure that you have an ability to dynamically adjust your strategies and operations as opponent activities change, and as technologies change. So this is a place where ensuring that you have an adequate, capable and dynamic process for identifying the necessary measures is probably more important than identifying one set of measures. You will need to adjust. The world is different from how it was five years ago, and I expect it will be more different five years from now. So getting those strategic planning processes and an operational doctrine in place is probably the key area.

Q78 **Stuart Anderson:** Thank you. Would you like to add any different points to that, Dr Beyza?

Dr Unal: I would just say that, on James's comment about cyber having the same head, he said that probably it is not the solution for the UK. Actually, the National Cyber Force is a joint Military and civilian force, which is, I believe, very similar to the structure that the United States has. On the cyber comment, it is both civilian and Military headed. I think the Military is heading it up and the deputy head is a civilian from GCHQ. We need to figure out the legal implications of that because civilian staff might become legal targets in conflict, in warfare, and what does that mean for the UK? How can we think about the legal challenges? That is one that we would be thinking of.

Again, on the cyber-operations, information-operations side, the 77th Brigade in the Army conducts the information operations. Also, within the Army there is the Cyber Security Operations Centre, which specifically provides secure communication information. The Military comes within the Army.

I should also mention—we have not actually discussed this today—the whole idea of multi-domain integration, which the UK Military is now pushing forward. That is an area that we also need to be thinking of: how will that concept actually be operationalised with cyber being included in that multi-domain thinking? It relies on collaborative efforts across the different domains, but there will probably be some challenges that we will see down the road, in the long run.

Stuart Anderson: Thank you.

Q79 **Chair:** Can I just probe those two points a little further? In the UK, we have had cyber-attacks on Parliament and on the NHS. Indeed, if we listen to some of the speeches made by senior representatives of the clandestine services—some of them still in situ, rather than retired—there are at least 500 attacks in any year, and those are only increasing. Our vulnerability to that will only grow as we become ever more reliant on the internet in every aspect of our lives. Are you aware of Britain or America formally announcing and confirming that they have launched a cyber-attack on an adversary?

Dr Lewis: The head of Cyber Command, Paul Nakasone announced two sets of actions against Russia because of electoral interference—one in 2018 and one now, in 2020—intending to degrade the ability of the Russians to interfere with our elections. Prior to that, there was a joint operation with the UK—the American name for it was Task Force ARES—which was an anti-ISIS operation. Those were announced somewhat indirectly.

So, in three instances, the US has confirmed that it has taken action against opponents in cyber-space. This is separate from the actions taken by the Department of Justice in indicting Chinese and Russian intelligence officials.

Chair: I am focusing on actual aggressive kinetic cyber-attacks, done by either Britain or the United States, in retaliation for being on the receiving end of something proportionately similar.

Dr Lewis: That is a great question, because I do not believe there has been enough of that, if any. It is important that the concept of retaliation is established to begin to change opponent risk calculations. There have been operations to interfere with opponents, but not necessarily in retaliation. This is a debate in the US at the moment; Cyber Command said that we took action against the Russians, and some of us argued that that was nice but certainly not sufficient. So one of the questions would be this: how much further do we need to push this for it to actually have an effect?

Q80 **Chair:** Where I am taking this is that this is now going to become, I think, more of a commonality, given that this is where the character of conflict is moving. Yet at the moment the legislature, and indeed the Executive, is bypassing any form of accountability that would come from being transparent about how and when this utility is used. Would that be fair to say?

Dr Lewis: I would say yes, in general. I don't know if Beyza has more views on this—I see her holding up her hand.

Dr Unal: I was just going to say exactly that. There is an accountability issue because we do not know in the UK specifically what type of offensive cyber-operations exist. We know that there was a cyber-operation against

ISIS but, back to your question, was there a kinetic operation? We do not have an answer to that.

That comes down to the accountability issue, because the question then comes to the legalisation. How far can the UK conduct cyber-offensive operations, and what are the legalities that come with that?

On the US side, there is actually an example that I can think of. Iran shot down a US drone a few years ago, or maybe in 2019. The Trump Administration retaliated with cyber-attacks on the computer systems of Iran's rocket and missile launchers. As I remember, that either happened or Trump said that he was going to take that action. I guess it happened, but it would be good to have a look at it before taking it for granted.

Chair: We might take what Trump said with a pinch of salt, given his track record in this area. Emma, I think you wanted to come back on this point.

Q81 **Mrs Lewell-Buck:** Dr Unal, you have touched on the integrated operating concept, which said our forces need to be integrated across all five operational domains in relation to cyber. Apart from that being a massive organisational and cultural change, what are the challenges that you think we will encounter in integrating these five operational domains?

Dr Unal: That is a great question. We know that the aspiration exists within the UK Military to create their multi-domain integration. The concept has been established, but I do not think it has yet set out how the Military will do this and achieve this. There are challenges in the way that the Army, Navy and RAF currently operate. The operation of these commands differs, so there needs to be an integration of that operating structure.

From the cyber side, there is a challenge, because I understand that the whole idea of multi-domain integration is to fuse together the information that comes from different domains and to be able to transmit information almost in real time to all UK forces. It prompts the question of whether we will have a single force or a single system where the information will be collected. If the information will be collected on a single cloud-based system, we are again going back to the question of vulnerability, because that system might be vulnerable to cyber-attacks and hacking. If it will not be a single-sourced, cloud-based system, it will be a decentralised system. Will you actually be able to have nearly real-time information sharing, as desired? I think that is the biggest challenge.

Q82 **Mrs Lewell-Buck:** I do not know whether you are able to answer this question. Bearing in mind that the previous SDSR, back in 2015, identified cyber-attacks as an increasing threat to us, and we now have the integrated operating concept, are we a bit late in the day to be doing some of this? Should we have moved a bit quicker, and does that make us more vulnerable?

Dr Unal: I was actually talking about this with a colleague recently, and she was the one saying, "Can you believe that we are doing this in 2020?" I think that answers your question. We are a bit late, but it is not bad. The

important thing is that we need to put these forward and understand how these things work. Multi-domain integration is something that the United States has been working on, and I know there has been work on this in NATO. We need to grab the lessons from them and understand how to do better.

Q83 **Mrs Lewell-Buck:** That is helpful. Dr Lewis, would you like to come in with any comments on that?

Dr Lewis: You need to look at the structure. One way to do this is to have the individual Services train and equip your forces. It makes sense still to have a Navy, an Air Force and an Army, and not to blend them all. But when you get into operations—think about Joint Command and about command and control—you need to merge cyber into that. If you think of the defence of the UK perimeter, that would be a naval task, an air task and a cyber task. You do not want to have separate Services doing them independently. How do you organise them jointly? Is there some sort of central command that does that? The same would be true for operations in other areas. So, I would say, train and equip by Service, but then think how to command jointly.

Mrs Lewell-Buck: That is really helpful. Thank you both very much.

Q84 **Derek Twigg:** Dr Beyza, in your answers to Stuart, you talked about co-ordinating civilian and military cyber co-operation. Where do you think we are in this country in terms of co-operation between the Military and civilian cyber? Maybe, after you have answered, Dr James could give us a view from the US in terms of lessons to be learned, or not, from there.

Dr Unal: I would say that there is more work coming along with the civilian and military infrastructure coming together. I think it was General Patrick Sanders who said in his speech a few months ago—in September, I think—that Strategic Command is working on a full-spectrum cyber-power operation to deny, deter and disrupt enemy or adversarial activities, and to attack the critical infrastructure of the adversary with GCHQ. That statement came, in a way, from the Military itself, so I think there is that ambition and understanding that that needs to be done.

Where are we with that? I am not completely sure; I do not know. Mainly, that is because there are certain things that are cloaked in secrecy in the UK, which is why we need to learn from the United States, and I look to James's comment on this. The United States is really open and clear about its operations, even the offensive operations. It says that we need to hunt for the threats in different adversarial systems. That is not something that we are comfortable with in the United Kingdom yet. That secrecy, in a way, is not helpful for moving forward.

Dr Lewis: I note that the Australians have also made a decision in the last year to be very open about their offensive capabilities, so it might also be useful to look at the Australian experience. They decided that it was important, as a way to warn opponents and to provide accountability to their citizens, that they should be very open on their offensive doctrine

and capabilities. The US has followed the Australian example to some degree, and even perhaps was a precedent for it in some ways.

The one thing that we have learned here is that cyber is a cross-cutting activity. In some ways, the lessons that you might get from anti-terrorism could be useful. We found that you needed to have central co-ordination. You needed it to be co-ordinated by the White House, because you have law enforcement activities, intelligence activities, defence activities and what we would call homeland security activities. Left to their own devices, they all go off in different directions and do not necessarily talk to each other.

The most important change that we made was to establish a series of Executive orders—presidential decrees—and an organisation within the National Security Council that provided this inter-agency co-ordination. I am not as familiar with the UK, but I think a precedent might be the JIC. Think about how you co-ordinate among the different activities and different authorities.

The Trump Administration, of course, dismantled that in part, which was an unwise move. I think you will see the Biden Administration reassemble it once it is in office. That central co-ordination by the political authorities—by the Prime Minister's office—is probably one of the most important steps that you can take to ensure a full-spectrum cyber-defence.

Q85 **Gavin Robinson:** I was going to ask about the capabilities, infrastructure and organisation to conduct offensive and defensive cyber-operations. Both of you reflected on elements of that in your earlier contributions. In asking you generally that question, for your reflections, what are the risks of blowback from offensive cyber-operations, and how can they be managed? Dr Lewis, we will go for you first, since you gave a big smile.

Dr Lewis: I was thinking that I am the wrong person to ask. As an aside, I have been reading a history of Parliament's thinking in the 1930s on air defence. In some ways, it is an unhappy precedent.

Two things are going on. First, we tend to overrate the risk. Democracies are risk-averse. Democracies don't generally like warfare—even the United States does not, and that is one of the reasons that Trump was elected. Democracies are slow to move to offensive operations. We prefer defence. Democracies do not like admitting that the world has changed. We have both touched on this. China intends to reshape the world. Russia may not want to reshape the world, but it does intend to damage the West. We are in a period of conflict, which means that the way we calculate risk—about responses—needs to take that into account.

There has been a slow movement in the US to being a bit more assertive in responding. You see this in the military doctrines of Defend Forward and Persistent Engagement. Defend Forward just means that you are on your opponents' networks taking action against them, rather than sitting around waiting for them to come and then taking action. Persistent

Engagement is just a recognition of reality. We are in hostile contact with our opponents every day. It is not the traditional kind of warfare, but that is what people will need to think through: we are now in a situation of conflict.

My assessment is that the Chinese in particular are not interested in reaching a peaceful settlement, unless that settlement is on China's terms. The Russians are a bit different. I think that the Russians might be amenable to some kind of deal, if it was linked to arms control issues, but it is not always clear how serious they are.

We are entering a period of increased conflict, which means that the responses that were appropriate five or 10 years ago no longer work. For me, that means that we might have to accept more risk. We might have to think about what a strategy to defend sovereignty looks like. Will it include retaliatory offensive operations? They create some risk, but this is not an environment in which we can live without risk any more.

We have done Persistent Engagement and Defend Forward in a very low-key manner, which is partly because there is a fear that we do not want to provoke our opponents, but that might be a luxury that we will not be able to afford in future. The same goes for the UK. Increased risk is sort of inevitable.

Q86 **Gavin Robinson:** That was not bad, for someone who said that they had nothing to answer or say on the question. Let me take you to this angle of it, sir, which I think you have an interest in, which is managing the risk of creating cyber-mercenaries. Is that a risk that can be managed? Do you see a fear of people with skills being taken to and fro between Western democracies and other countries, and put into potentially more fragile states to engage in cyber-warfare?

Dr Lewis: Beyza, do you want to go first?

Dr Unal: On the skills side, it is really important to create the skillset. At the moment, within the Military, I believe that there is this three-year hosting schedule that takes place, and that does not allow people to specialise in certain issues. The retention of staff is not there, so we need to think about this in a forward manner—not only on cyber-issues, but on emerging technology in general. How can we incorporate those skills within the UK military?

Also on the skills side, tactical units need to have a certain level of skills to operate and adapt in security environments, on the operational side, when, for instance, GPS is down or when information is spoofed, as we have mentioned. That adaptation is really important, and I am not sure whether that people skill—the human skill—is there yet.

I believe that the staff also need to educate themselves to protect themselves. The protection starts from us ourselves—even in information operations. If we are on Twitter and seeing certain activity, we need to be reporting those things, but we are not doing it as individuals. This goes

beyond the Military; I think the public—everyone—needs to have a fair share in understanding these issues.

I would say that the main blowback from taking forward cyber-operations is really about escalation and deterrence. Currently, our deterrence strategy relies on conventional deterrence and nuclear deterrence, but the adversary uses activities that are not covered by the way we structure our deterrence policies. I think that is the biggest blowback that we are seeing with cyber-operations in general.

Dr Lewis: I think you also asked about the use of mercenaries. Russia, China and Iran do use civilian proxies, and their recruitment pattern is pretty simple. I actually talked to a couple of the Chinese proxy forces, and they said basically they were called to their local police station and told, "Work for us or go to jail."

What's interesting is that the Russians, the Chinese and the Iranians keep fairly tight control of their proxy forces. The Russians, of course, allow them to engage in cyber-crime. There are more than 20 Russian cyber-criminal groups that are probably better than most countries when it comes to cyber-operations. But you don't see them being hired out or going around and offering their services to others. So, there is great use of proxies by Russia, China and Iran, but so far this seems relatively tightly controlled to ensure that it is done for state purposes.

This does lead into the workforce questions. One of the issues that we have struggled with, and I think is true for all militaries, is going into the offensive cyber-force. The question used to be, if you went into Cyber Command, what happened after that? You did your two years and maybe acquired some skills, then you were assigned to be the systems administrator at a missile base in Minot, North Dakota. Many did not regard this as a good progression, so we saw an outflow. You are competing with the private sector, which will easily double the salaries of the people you want to get. Whereas the Russians and the Chinese have fewer opportunities for their hackers and have a degree of law enforcement control that we cannot match, the issue on this side is, how do you make this an attractive career so that someone who comes in as, say, a second lieutenant can feel reasonably confident that they will be able to follow a progression up to lieutenant colonel or colonel? That was hard to construct, but we found it was essential for developing a cyber-force.

Gavin Robinson: Thank you both very much.

Chair: We are now going to take a step back. This is all part of the integrated review. We are waiting patiently—I don't know whether you have heard anything—for this publication to emerge. Let's explore this a bit further. Stuart, do you want to take it forward?

Q87 **Stuart Anderson:** Prevention is always better than cure. We have discussed different ways to respond to the threats—what we should be doing—but we would be very keen to know how the UK should develop a

deterrence strategy for the cyber-domain. We will hear first from Dr Unal, please.

Dr Unal: I think a cyber-deterrence strategy really relies on resilience itself. I don't think it's only on the offensive side. Yes, we can look at the offensive side, but resilience is extremely important. What we have seen with covid-19, within the world, is that we are not resilient. We were not resilient to an unexpected event, and we did not have a structure of resilience for covid-19—we need to understand that we don't have that in different areas, in systems resilience, people's resilience, organisational resilience. All those fit into the cyber-deterrence infrastructure and understanding, in a way.

We need to deny an adversary's ability to infiltrate these systems, and the best way to do this is protecting those systems, creating resilience and redundancy measures within the systems themselves. That means we need to be putting some budget in, to actually be able to create that redundancy. That is the challenge that we are seeing.

The other part of deterrence is offence, and we have discussed that—that we need to be clearer on how we are taking offensive actions and so on. I would say these two things are equally important. And, of course, cyber-defence, but that has already been going on within the Military.

Q88 **Stuart Anderson:** Thank you. Dr James, your views please?

Dr Lewis: Sure. Deterrence as we understand it now has largely failed. I believe this is in some of your own publications—that our opponents have spent a long time studying how to circumvent Western deterrent capabilities. One of the reasons they have these new tactics, or this new kind of warfare, is because we have not developed adequate responses to them, or that falls along the seams of our legal authorities and our protection of fundamental rights.

Deterrence as we have thought of it until recently has failed. What have we been able to deter? In cyber-space, yes you've been able to deter gigantic kinetic attacks, or attacks that would have effects similar to kinetic weapons, but if you're an opponent and you can achieve your goals without the cyber equivalent of launching a volley of cruise missiles, why would you change?

A lot of the concepts we inherited from the 20th century, such as stability, escalation and deterrence, don't make sense any more and need to be re-thought, and that will be a difficult task. But when you look at deterrence, defence is of limited value because if there is a target, with very few exceptions, highly skilled opponents will be successful against it. You cannot rely on defence, particularly in the private sector. There are several things you would want to think about, then. First, you have to demonstrate that you have the capabilities. That is one of the reasons that both the US and Australia have been public about their offensive capabilities. We want people to know what we can do. You have to demonstrate those capabilities.

Secondly, you have to rebuild credibility. If there has been a series of incidents over a period of more than a decade to which there has really been no response, or at best ineffective responses, your opponents don't fear you. So, how do you make those credible threats? You want them to think, "I don't want to do this because what will happen to me in response is not worth the game."

Finally, you need to think about a public strategy. One way to think about this is declaratory policy, which is an old nuclear term, just saying, "If this happens, we will do the following in response." One of the problems we have in NATO and in the US is that we actually have a declaratory policy that no one know about, because it's incredibly long and filled with all these lawyerly caveats—when the moon is full, and when the President is in a bad mood, and when x or y… the US reserves the right, etc.

You need a very clear public statement, saying "We have the capability, we have demonstrated our willingness to use it, and if you take these actions we will respond." That's the core of deterrence. I would say that sets some good goals for you. There is a debate within the Pentagon. I would say the minority view is that we need to escape the gravitational pull of the cold war and strategic nuclear concepts, but this will go on for years. For you, build and demonstrate the capabilities and then let the public, including your international audience, know what you are willing to do with them.

Stuart Anderson: On that point, I am conscious of time, Mr Ellwood.

Q89 **Chair:** Just to conclude and advance that question itself, if you were advising this Government on its integrated review, would you like to see, as I think this Committee would, a final recognition that China is a hostile competitor; that it is pursuing a very different geopolitical long-term outlook, which will clash with what we believe in in the West; and that there needs to be a Sputnik moment, if you like, where we wake up and recognise that China is not going away, but, as you put it in your last answer, that we do need to have a more collective and stronger response? Added to that, would you also like to see us, the United Kingdom, leverage the opportunity that a Biden Administration presents, when he has already committed his Administration to being far more collegiate, to build alliances and to stand up and upgrade the international rules-based order? Should Britain be front and centre participating with the United States? Dr James, would you like to go first?

Dr Lewis: Certainly. The UK needs to figure out how to leverage its opportunities and strengths. When you look at the exporters of cyber-security goods and services, the UK is in the top three. GCHQ, as we have discussed, is among the premier cyber-operational entities. You have real strengths that you can build on that very few other countries can match—probably another four including the US.

How do you take advantage of that both nationally and multilaterally? I think there is recognition in the people who will likely staff the Biden Administration that we are not going back to the old world—that the rules-

based order has been damaged. It needs to be rebuilt more than repaired. It would be useful to get the UK's thinking on what a post-Middle-East-adventure international order looks like. This is a discussion that many will have to have, so I think it is something to think about.

Multilateral action is the only way to respond to these things. You can make arguments for a more nationalistic American foreign policy, and some of them make sense, but unilateralism does not make sense in security. That is where partners are crucial, particularly strong partners like the UK. We need to think about how we work with you in responding to some of these things. This will require some political decisions on your part about the direction that UK foreign policy will take.

On China, have some fun—read translations of Xi Jinping's speeches. There should be no doubt about his intent. It was not a fluke that he started wearing those Mao jackets again; that is a hint of where he would like to go. I do not think that there should be any doubt that China is an opponent, with a very different world view and no respect for the rule of law, both domestically and internationally, and one that will be hostile to Western interests, albeit not in the forums of the 20th century. There should not be any doubt on that score. What we do about that is something that we will need to rebuild after the Trump experience.

Chair: Thank you for that, Dr Lewis. Dr Unal, you get the final word in today's session.

Dr Unal: Thank you very much—I appreciate that. I will just build on what James mentioned about multilateral actions being the way forward. I truly believe in that. The UK has a few spaces to use for its benefit. The G7 presidency is important, and we need to use it to our advantage this year. The UK is in Five Eyes as well, which is important for signal intelligence. They have also been pushing for some actions on the covid-19 disinformation campaigns and so on. That is another area to tap on.

The third area that I see is the Commonwealth. How can we use the Commonwealth to our advantage, to bring allies in the Commonwealth together in this endeavour? Also, I believe that now that Brexit is going ahead, the EU sanctions regime is important to tap on. The role of the UK and the EU, working together on these issues as partners, is an area that we should also be looking at in detail.

Lastly, I would say, because I come from a NATO background, that NATO is critical. NATO established cyber-domain in 2018. They do not have offensive capability, and I think the UK and NATO could work together in understanding who can do what, in a way, in this area.

Chair: Thank you for that. That is a more positive note to end on—the importance of alliances and perhaps the opportunity that Britain has. There are a lot of plates spinning in No. 10 at the moment. I hope that they are listening. I know that they are regular listeners to our debates and our discussions. It is so important that we take advantage of this new opportunity and make our mark, because the world is changing fast, as we

have discovered today.

Dr James Lewis and Dr Beyza Unal, thank you very much indeed. This has been a fascinating discussion. I very much appreciate your insights in helping us to understand more about the cyber-security world in relation to the integrated review. Thank you to Committee members as well, and to the Clerks and the team here.