GCHQ: Intelligence and Cybersecurity Today

Chair: Julia Wheeler (JW)

Speaker(s): Jeremy Fleming (JF)

JW: Hello and welcome to the Cheltenham Science Festival @ Home, and in particular to this very special event. My name is Julia Wheeler and I'm absolutely delighted to be joined by the Director of GCHQ, Jeremy Fleming. Welcome Jeremy, and thank you for being here. Jeremy is the 16th person to hold that role and he's done so since 2017. Early in his career, he qualified as a chartered accountant before joining MI5 in the early 1990s. His work includes the areas of counterterrorism, espionage and cyber investigation, of course, and he was involved in both the response to the London terrorist attacks and in the preparations for the London Olympics. Jeremy joins us now from GCHQ in Cheltenham. As I say, welcome to the Science Festival @ Home, thank you for being here.

Let's begin, if we may, by perhaps you giving us an idea of how much the balance of threats has changed because of the situation we're in, because of this pandemic.

JF: Well hello, Julia. It's great to be part of this festival, even though it is remote. I'm joining you from our headquarters here in Cheltenham. I think this pandemic has given us all a chance to really think very carefully about our place, our place in our business lives, in our communities, how we work and how we interact. And, of course, the same goes for GCHQ. I'm really conscious that 100 years into our history that the symmetry of us starting our existence around the time of the last global pandemic, and now suffering this pandemic 100 years on gives us a chance, I think, to give a broader perspective on that. Of course, the reality of what we're seeing is that it is going to change the world, it's changing the world for us at many levels, and I hope we get a chance to explore some of that as we go on today. Probably one of the main differences from 1919 is just the extent to which technology, and particularly digital technology, is all pervasive in our societies in the way we interact as humans. So, it is the case that Covid is changing the balance of the threats as we see them. It's changing the way in which we work as an organisation, and it will change the way in which we'll have to respond in the future. It's a massive moment for us, as it is for everyone else.

JW: So, when you talk about the balance, then, what do you see are the main changes, or what have you seen so far have been the main changes?

JF: Well, I think the first thing is to refer back to my comments a few minutes ago, our dependence on technology and on digital communications means that the very fact that we're doing this Festival in this online way. The very fact that all of our businesses and our interactions are happening on these sorts of digital, means that the security of those systems is paramount. Of course, that's something that we all have a role to play in securing, whether that's the steps we take as individuals to secure ourselves, as simple as passwords, the steps we're taking at businesses to make sure our data is secure and our customers' data is secure, to backup. Or, whether the steps we're taking as nations to make sure that the things that are really critical for our existence and our economy are as secure as they can be. I think the reality of that, Julia, is that the balance of what is critical is changing. So at the moment, this is obvious, but I'll repeat it, our health security and our biosecurity is at a much, much greater prominence than it was even a few months ago. The steps we take to protect our health system, to protect our vaccine development, to protect those involved in delivering vital services right across the economy. The importance of those tasks is changing. It is, of course, the reality that others are interested in disturbing those, or in stealing secrets, or in otherwise disrupting our efforts in those areas.

JW: So, how does the work that you do at GCHQ, not just in Cheltenham, I know you have offices around the country, how does that feed into protecting those areas that you mention?

JF: Well, GCHQ has done, broadly, the same three sets of things since it started in 1919. So, we're charged with collecting intelligence against the highest priority threats, we're charged with protecting the nation's critical information, and for us, now, that manifests itself as cyber security, and we're home to the National Cyber Security Centre. We're also responsible for helping others to make use of that intelligence and investigation, to compete in cyberspace and, where necessary, to disrupt in cyberspace. So, those three areas of objective are as important today as they've ever been. Our primary responsibility, and the way in which the demands on us have moved over the last few weeks, have been in several key areas. So firstly, we have moved in to help support the health sector, and that's a cybersecurity ask. So, that's working very closely alongside the NHS and the more distributed health sector to try and protect everyone's critical information and their operations as far as we can, to enable them to improve and protect their cybersecurity. We lent in to advise and help around the creation of the NHS app around COVID, and that's to make sure that all of our information is as secure as possible, and that the architecture behind the system is really cutting-edge and is protecting the things that we need to do, so that the decisions taken from it are as effective as possible.

We've lent support and data science support more broadly across government. So, I'm blessed with nearly 10,000 people in GCHQ, all of them amazing people in their own right, and many of them with very strong technical backgrounds. They have a role to play more broadly in projecting our data science skills and our technology skills, including across government, where it's required. So, we've lent in to help on that. Also, we've been helping government and helping policing and the National Crime Agency in particular, cope with some of the spikes we've seen in serious and organised crime. As it is the case that hostile states can seek to do us harm, cyber criminals have spotted the opportunity from the pandemic. Today as I speak to you, and I appreciate this might be a little while before this airs, but as I speak to you, then we've seen them using Covid-related tactics as lures to try and defraud people, to mount their forms of criminality and cause people harm. So, we're leaning in to help on that, too.

So, right across the span, and I'm very conscious of that in talking about what we're doing on Covid, I wouldn't want to give the impression that perhaps some of our more traditional areas of business have been stopped, they haven't. Counterterrorism is still a very important business for us and we're working extremely closely with MI5 and policing on that. The activities of hostile states more broadly, remain of incredible relevance to us. So, we are doing the things we were doing in the past, we're having to do them differently, and Covid has added to the priorities there.

JW: Because there would be the potential for danger that, actually, if everybody's looking over there for Covid, that you're not looking at what's coming over here. So, you know, you must just have so much more to be thinking about and acting upon.

JF: Well, certainly there's no shortage of demand for the things that we can do as part of the broader national security community. That is ever the case, actually, Julia, so it's a priorities business, it's based on risk at a particular moment, and it's based on government's understanding of the priorities, and it's based on our national interest. Our national interest has changed a bit because of Covid, and we'll prioritise according to those demand signals. Actually, it's something I pride ourselves in doing. If we are to be a very relevant, 21st century intelligence and security organisation, then we've got to be very responsive, we've got to be fleet of foot, we have to respond to threats as they emerge.

JW: Let's come back to that NHS app, because there has been some concern in the media and with individuals more generally that that somehow threatens liberty. Yes, people want to do their part and they want to help in combating the virus, but at what price. So, I wonder what sort of reassurance you can give in terms of data protection for people and the way that that information will be used?

JF: Yes, and I am really very pleased that we are having this sort of national debate about these issues. I see it is an incredibly important principle for me and how I go about leading this organisation, but also for the UK as a liberal democracy. So, I think it's entirely healthy that we should have this sort of conversation. I mean, to reassure you, privacy, security, data protection has been absolutely at the heart of our approach and the NHS' approach to the development of the app right from the start. It has been built in as a fundamental principle, the way in which the app operates, the way in which, with the user's authority, it shares data so that clinical decisions can be taken, the way in which, long term, the interests of every individual in this country who downloads the app and the data that they provide is treated long term has been treated so seriously from the off, that I would like to provide significant reassurance on that. I think it's also equally important that we continue to be as transparent as we can be about that as a nation. I really want us to keep having a debate about all of that. Fundamental principles around necessity and proportionality underpin everything that happens in a secret intelligence organisation. I think it's really important, as it was when our legislation was last overhauled a couple of years ago, that Parliament has a decent chance to debate and understand the balances that are being made on behalf of the population as a whole. A final bit of reassurance, you know, none of the data from this comes to GCHQ, this is an NHS thing, we've advised on the design and the security around it, and I think I would take pride in the fact that we've been allowed voice around those issues, too.

JW: What sort of weighing up do you see in terms of contact tracing being a technological thing and being a human thing? Where do you think the balance, again, is there, in moving forward within this pandemic and helping to open up lockdown and move back to whatever becomes normalcy?

JF: I think it's clear to us all now as we move to the next stages of dealing with this pandemic, of living with, with Covid, that society is going to have to reach a new balance to enable a smarter form of lockdown. You know, when there are flares up in the virus, government, with citizens and with communities, are going to need to move to take whatever measures are necessary to monitor that and control it. Of course, technology has a role to play in all of that. I think it's really hard to answer your question with any great fidelity. The main step at the moment that has been taken is the development of this app, as I talk to you it hasn't yet rolled out. So, I don't have the benefit of knowing exactly what position we'll be in at the point at which this airs. The way in which that contact tracing app is designed to develop should give us, with a really good understanding for those people who've downloaded, on where the virus is moving, provided people take part. There's a broader picture there, and the Prime Minister has announced the creation of a giant biosecurity centre, where other aspects of data can come together, open source data, most of it, actually. Again, that's something that we'll play our part in, but we won't be involved in the analysis of the data. This is a broad, government-wide effort to try and make the efficacy of the testing and the tracking and the testing capability as good as it can be.

I mean, my previous answer around the balances that we reach here and the conversation we need to have with the public about the mix of that data, I think, refers. You know, we've got to keep debating this as an organisation. How much future technology is involved? I think that's still up for grabs.

JW: How does GCHQ, and you in particular, how do you feed into Whitehall? Are you at the COBRA meetings?

JF: Certainly, throughout my career I've attended a hell of a lot of COBRA meetings, probably more than I care to remember. COBRA, in a way, has this sort of mythical status. It is a meeting room in the bowels of the Cabinet Office, it's set up to communicate with a range of participants broadly, at classified levels and unclassified levels, and it convenes depending on the issue of the day. So, I would not expect routinely to be involved in a COBRA about the medical handling of the Covid epidemic, but in the event there is a terrorist incident, or when there's a cybersecurity incident, then of course I attend COBRA and I will answer questions and be involved in discussion with whichever ministers are involved in that particular area of government.

JW: One of the things that we are all having to get used to is working from home and different technology, and so on and so forth. What are the big things that people need to think about in terms of keeping themselves safe, keeping their companies safe, keeping their data safe?

JF: I was tempted to answer with a flippant answer about giving themselves enough room so the dog doesn't come in and destroy the picture, or children.

JW: You haven't got your dog with you today?

JF: No, not in this building, yet. I have had some requests, actually. I mean, the first thing is that we are all reaching a new balance here, aren't we? That's the same for an organisation like mine. Deeply secret, very covert in lots of aspects, but what we've seen through this crisis is an acceleration of the trends we've had for the last few years, where lots of my people are involved in work which is either public in itself, so can be done in a very open way and a transparent way, or involved in the development of capability where the focus of that is very public. You know, we develop source code in an open, transparent way, lots of it. We are involved in code sharing, we look for collaborative ways of developing capability. So, for large amounts of people involved in that, or in our cybersecurity work, or in our outreach work, then actually it's been quite seamless to accelerate the move of that outside of the office to work from home. Culturally, that's a big thing for us, of course. Welcomed by lots of people, it's a very different way of working and I've been experimenting with it too. At our heart, we have very sensitive capabilities and very sensitive information and that bit we will always fight to retain control over and secrecy over, and so we will have, always, an aspect that cannot be done from home. In a way, those sorts of balances about what can be done from home and what can only be done in an office environment are ones that companies and individuals up and down the land are making.

The guidance for that, and we have provided a lot of advice for this, and a quick plug, if you look on the NCSC website, you'll see guidance on things like video conferencing, as well as more broad advice around cybersecurity. The advice on how to do that, it's pretty common sense, really. You know, so what sort of technical capability do you have available, and how secure is that capability? Have you set it up in accordance with guidelines and our best advice? Are you sure of the credentials of people who are taking part, or with access to your systems? Have you set it up in a way in which their identities and the identities of those who want to take part are properly connected? All of those sorts of considerations are very common sense considerations. When you get into more sensitive areas, then what is it as a company that you really need to protect?

So, there are there are aspects of development, whether that's on the academic side or whether that's in the business side, that amount to commercial, or at least proprietary secrets, in their own right. You wouldn't go talking about those with a loud hailer on the top of the bus. You have to be

thinking about what it is you most care about, what it is you most need to protect, and what are the arrangements around those. Of course, the same questions relate to working from home. The reality is, you can do most things from home, for most people, you don't need to worry about it very much. But you do have to make sure that some pretty basic cyber hygiene disciplines are in place to protect your information. Then, you can fill your boots with everything that this technology can bring. It really is enabling, and our message in GCHQ and from the NCSC is that these technologies are here to enable us, they're brilliant at doing that, so let's do it, but let's try and do that as safely as we can.

JW: I think lots of people have a different head on when they've got their work laptop and, you know, they're dealing with colleagues. Anecdotally, there seemed to be a sort of rush to tech at the beginning of this, where people said, 'Oh, how are we going to keep in touch? Let's download Zoom, kids wanted Houseparty, and people weren't thinking, necessarily, with a sensible head, and I include myself in that. It's interesting that, I mean, for example, this conversation today, we're not having over Zoom. Is that something that is just because you haven't tested it, you're concerned about it as other people have been, of Zoom-bombing and all of these other things? If that's the case, should other people be more cautious around some of those really, relatively new tech potential?

JF: Well, we'd always advise you to think carefully about the tech you're using and how it's set up. As it happens, I'd be more than happy to have this conversation over Zoom. I mean, you're about to post it on YouTube. So, there's nothing in here that I'm saying that is deeply sensitive or that is going to be something that I would want to protect in a different way. If I was having a conversation with you about the next stages of my strategy, or where I thought Government should go on a particular aspect, then I wouldn't be doing over Zoom. I'd be thinking about what was the most effective medium for doing that. So, I think I'm illustrating the points I was making earlier here. When you're using technology, do it with your eyes wide open, treat it with the caution that that deserves. Don't do things on there that you probably wouldn't be prepared to do face-to-face. Certainly, if you're a business and you have things that you want to protect, then make sure you understand where those red lines are.

JW: Historically speaking, there have been great jumps forward during wars for medicine, because people have to deal with things, you know, it's all come bunched at once and there's been more of a priority of that. Do you see that being the same in this pandemic situation for technology? Will we be making leaps and bounds because we have to?

JF: Yes, I'm actually quite cautious about using the war analogies around a pandemic, just because of the messages that that sends. That said, I think it is a useful parallel to think about, you know, what are the advantages and the step forwards that could come from this? Whilst it's pretty early on in the grand scope of things to be concluding on those sorts of areas, there are probably a few things I'd like to say about it. The first is, and we've just touched on it, but I think it has accelerated some trends that we've seen in our society for some time about how we use technology in our working lives and how we get the balance right between our home and our business lives. I'm pretty sure that some of those are going to be long lasting. So, there's that sense of, you know, behavioural, almost cultural changes, about what it means to go to work and how we go to work and what sort of flexibilities we enjoy, and what sort of tools we need to support that, that I think will be long lived. Notwithstanding the, you know, the Zoom and Houseparty fatigue that you've already talked about.

The second area, well, it is, of course, already the case that we're seeing a massive acceleration in some of the medical and health responses around all of this. The global rush to a vaccine and to other sorts of therapeutic treatments and all of the tail around that. Which, of course, in itself is a

big technology and a science effort. You know, the ramifications from all of that, I think will be enormous. The third I think, and this is something that again, touches on some of our previous conversation, is just around data. So, I think we've all seen the way in which governments all over the world have had to think really hard about the sorts of data that are going to help them make the right decisions around all of this. So, from my perspective, you know, data-based policymaking, data-based governance, data-based protection, those are really positive steps forward. I think we will see further accelerations around data science, around the power of data. We'll see greater pressures, I think, to open up data. So then, again, that's back to that conversation about how do we manage that safely, and what sort of consent conversation do we need to have with the public to safeguard privacy? We'll definitely see an acceleration around all of that. There are some dangers for us, too, in that data space, but it'll already be clear that some states, some more autocratic states where they have more control of their populations, have approached this in a particular way. I like to think that there's a liberal Western democratic approach to that that will hold us in good stead when all of this technology is rolled out down the track. There's quite a lot to play for in that regard.

JW: So, let me take you back away from the technological side into the historical side, you mentioned that it was the centenary of a GCHQ last year. There was signals intelligence, wasn't there, during the First World War, but what do you see as the beginning of your organisation proper as it were?

JF: Well, it certainly came out of the end of the First World War when those sorts of early signals in intelligence efforts had paid their way during the war. Both the military and the government came out of it thinking that they wanted to make use of those sorts of capabilities in peacetime. Actually, it wasn't a completely done deal that that was going to be the case, there was very much a sense in some circles that that was a war effort and that we were beyond the war, and we wouldn't need to have that sort of organisation. The reality was that Whitehall and ministers and the Prime Minister agreed that something should be created, and Government Code and Cypher School came into being in 1919, 100 men and women, many of them who had served in the First World War, came together. Their efforts were initially mostly focused in the diplomatic space, as it happens, through most of the '20s. It wasn't really until we got into our second and, of course, third decade, that we got into the very famous war years, that were involved in that sort of broad military effort again.

JW: You touched earlier on talking about partnerships being important, and that was certainly the case, wasn't it, during the 1930s and the Second World War. I'm in particular thinking about the Poles and the French codebreakers. We think of Alan Turing, but there was plenty that went on before that and during his time with others.

JF: Yes. So, one of GCHQ's core values is teamwork. I really can point to aspects of teamwork, areas where teamwork has made the difference, for every year of the 100 years since. Of course, there are some very famous moments when that teamwork comes into sharp focus. You're right, during the war, some of those codebreaking efforts with the French, with the Polish, in particular are now quite celebrated. Equally, during the war with the Americans, very closely with the Canadians, and with other aspects of what became the Commonwealth afterwards. Deep and long lasting partnerships. Perhaps the most famous intelligence alliance in the world, the so-called Five Eyes, almost mythical status here. So, that's the UK and America, Canada, Australia, and New Zealand. That partnership came together in the aftermath of World War Two. The agreements that were forged over 75 years ago are still keeping our country safe all these decades later, but crucially, are also making a major contribution to keeping their countries safe. That sense of, you know, a deep, interdependent partnership, a lot of that, historically, was based on the power of the Signals Intelligence Partnership, which then became GCHQ.

More recently, I can point to a whole range of different partnerships. Of course, we're part of the UK intelligence community, we're very close to MI5 and MI6. We're deeply enmeshed with the military at every level, including, increasingly, on cyber matters. We work with the National Crime Agency in policing on organised serious crime. What's really interesting to me is how the partnerships are developing in different areas. So, our partnerships with academia to create things like the National Centre of Cyber Knowledge, to to make sure that we're protecting aspects of their research. Or our relationships with business. I can point to a whole range of partnerships from retail to critical national infrastructure, water, nuclear, and so on, where we are working hand in glove with them to make sure that they can provide the best possible service and the best protection to their service. Then, of course, partnerships with other countries. Brexit has made no difference to our cooperation with our European allies, and I'm confident that that will continue to be the case going forward. Our corporations in the Middle East or further afield, the Far East, there is a whole range of really different partnerships. It is the case that GCHQ can do nothing on its own nowadays, it's a very interconnected intelligence world as it is a business world, or indeed a personal and a social one.

JW: Let's take you back to that Five Eyes organisation. Is there a threat to that because of the disagreements over Huawei?

JF: No, I see no threat from that. No, Five Eyes isn't an organisation, it's a partnership, it's an alliance. It is, of course, the case that whilst we share basic principles, we share basic values and we are all liberal democracies, there are areas where, from time to time, our approaches differ. Of course, you've pointed to just one of those. Those are not fundamentally undermining the alliance. Indeed, I think it's the power of the alliance that, where we do differ, we can both understand why we're taking those decisions, but also make sure that we continue to cooperate across the broader piece. So no, I'm not worried about that.

JW: You don't see that there's the potential for issues between, if you like, the US on one hand and China on another, which has, kind of, grown up in different ways, right, at the moment, but actually, there's also some previous form on that? So, if the US don't want to have anything to do with Huawei and we are, then that puts us potentially in a tricky position?

JF: Of course, it is the case that China's rise, if it wasn't front and centre for everyone before this pandemic, it certainly is front and centre now. All of us as nations are working about how we work with China, where it is we disagree with China, how we disagree with China, and what it means for our economies and our relationships going forward. So, China's rise and its position in the world is a fact of life today, and all of us have to pay very close attention to that. That means, for the UK, we see China as an intelligence adversary, we see them as an economic partner, we work with them in some areas, we compete with them in others, and in still others, we call out their behaviours when we don't think they align with what we expect to see or with our values. So, it's a very complicated picture. Of course, China is something that we discuss with all of our allies, and the balance we reach is something for us as a nation and for ministers, ultimately, to decide on.

JW: I should imagine that you and your team are not strangers to conspiracy theories, in terms of what's heard, and so on, on the internet. Were you surprised at some people's reactions and protests towards these 5G masts, and the confusion that came in the current circumstances with the pandemic?

JF: Yes, I mean, my experience on conspiracy theories is the aim off heavily. I'm choosing my words carefully on this environment, I think mess up, rather than conspiracy. Of course, one of the side effects from the amazing interconnectivity that we now have, and the ubiquity of these sorts of communication tools and social media tools, is that voices can be amplified extremely easily. They

can, either because people are amused or interested, or perhaps haven't had the chance to look more deeply into something, they can be amplified in a way in which is, frankly, not very helpful. So, I think the 5G masts is a classic case in point. Absolutely no evidence to suggest, and in fact, little common sense, actually, if I can go as far as that, to suggest that those conspiracy theories were any way close to the reality of the situation. So, you know, I regret the way in which the technology work meant that those were amplified, and that that people felt they had to take action on that. I think that's quite hard for me to understand.

JW: I'm sure you're aware that Cheltenham Science, both for the Festival and actually the rest of the year round, is all about bringing youngsters into science and research and medicine, and so on. So, there will be people watching this who think, 'Oh, I quite fancy a career in the secret services, MI6, MI5, GCHQ.' Your personal career, is that fairly typical? I mean, I know that your degree was Economic and Social History, and I know that because it was also my degree, and we have to stick together because there are not too many of us around. You then went into, as I said earlier, accountancy, you were in MI5 before moving across to GCHQ. Is that fairly typical, or are you an outlier?

JF: I don't think anyone has a typical career nowadays, probably. Whilst I greatly enjoyed and benefited enormously from my degree, I very much took from my degree, as many people of my generation did, I think, a sense of intellectual curiosity, a way of learning, rather than the subject matter itself. So for me, the decisions I took about my career were quite serendipitous. I found myself in the right place, I went off and got a financial qualification because I thought that would hold me in good stead to take a whole range of choices. Then, I ended up in MI5 actually by mistake, it was still the time when people turned up more or less not knowing who they were going to go and work for. I thought I was going to work for the Ministry of Defence. So in a way, quite lazy decisions. Since then, of course, I've found myself involved in a national endeavour where I've felt that the things that I'm doing have made a difference, where I've worked with people whose values I have deeply shared, and frankly, where it's always passed the Monday morning test for me. You, know, do you want to get out of bed for this? So, I've had a deeply satisfying and very interesting career with lots of variety in it.

Those aspects, I think, that sense of being able to do a lot of things, being part of something that matters, I think that is actually fairly typical in the national security world. Sense of mission doesn't just come in our worlds, if anything, we've seen from the Covid crisis just how much of a sense of mission pervades so many parts of the United Kingdom. You definitely get it in the intelligence world, too. The reality is that that sense of mission, that sense of being able to have a career in our world, for much of our history, actually, hasn't been as open or transparent or as welcoming to large parts of our communities and our population as I would like it to be. So, for the last few years, probably for the last decade or so and certainly in the last five years or so, we've done everything we can to reach out to a different group of people in the United Kingdom, to help those people from different backgrounds and in different parts of the country feel that they could have a future and a career in my organisation or in our community's.

It is, on one level, a deeply specialist and a very technical organisation, but I am stacked full of people with a very wide range of skills. From people who underpin the technology to people who use their linguistic skills, to data scientists, to analysts more broadly, to the people who make the logistics run right across our organisation, to the people who make it welcoming for us and a nice workspace every day. There is a whole range of careers and opportunities in my organisation, and my hope is that we are demystifying it in a way where youngsters, where, frankly, more women, where more people from BAME backgrounds, where people from other parts of the United Kingdom

feel that they want to be a part of that future. The signs are, that's working. We've had over 30,000 girls now through the Cyber First Girls scheme. In the last two years I've had nearly 200 apprentices in through the doors. The amount of social media interest we had during our centenary year is enormous, because we're reaching out in different ways. The Instagram account approach, the way in which we're doing local recruitment efforts, every aspect of that means that I'm hoping we're demystifying what we do, and people will think, 'Ok, I've read Economic and Social History, but actually, I could be Head of GCHQ.'

JW: See, I've just diverged on a different path, I should have thought exactly that!

JF: We'll do a job swap, shall we, Julia?

JW: We've got some questions that have come in from members of the public, some of them I think we might have touched upon, but let's see. So, has the Covid-19 situation increased or decreased the cyber threat for the general public and for businesses? That's from Gethin.

JF: Yes, I think we've mostly touched on this, haven't we? So Gethin, I think the reality is that we're not seeing a big increase in overall volumes, but we are seeing a reshaping of the threat. That threat is to take advantage of this situation, as criminals always do. So, scams that use Covid as a lure, yes, we're definitely seeing increases in those. As a member of the public, you do need to watch out for those.

JW: Bert says, during these unprecedented times with many companies operating minimal staffing or massively increasing the numbers of people working from home, what's being done to protect businesses, or help businesses protect themselves from cyber attack?

JF: Yes, so this is a partnership, isn't it? So, if there is an individual or a business in the land that is thinking that they can passively wait to look after their cyber hygiene, then they're mistaken. This is something where government, where business, where individuals have to all meet halfway to make sure that we're doing the right things. Of course, to do that, you've got to have the right sort of advice. You've got to understand what the technology is capable of doing and where it is you need to protect it, and that's where the role of the National Cyber Security Centre is really important, I think, to the nation. I would encourage all of you and anyone who is listening who hasn't already connected with it, take a look there. See whether there is advice that could make a difference to you as an individual, see whether you're following best practice. That sense of easy to access, transparent guides in plain English, hopefully demystifying some of these things. It's not rocket science to get this stuff right, it's where we want to go.

On the other side, the big technology companies and the people who produce the technology, the telecommunications companies that operate here in the UK, they're doing their best to make sure that their network and that the way in which information is transmitted is as secure as possible, too. They provide advice and provide services. So, the point for me is you've got to be conscious about it, you've got to take these choices consciously. You've got to recognise personal responsibility to go out and look for advice, and then my side of the bargain is to provide the advice so that you can access it.

JW: Karen W has written in, there have been news reports that state actors are targeting laboratories that are researching coronavirus vaccines. Are these cyber attacks different to the types of attacks we've seen in the past, or has that focus changed, or do you think it's a combination of both?

JF: It probably is a combination of both, but the reality is that we are seeing attacks on the health infrastructure. We do know that, whether it's states or criminals, they are going after things which are sensitive to us in this regard. So, it's a high priority for us to protect the health sector, protect, particularly, the race to acquire a vaccine, and there has been quite a lot of publicity around all of that. They're not using particularly different techniques to do it, they're still looking for pretty basic vulnerabilities in our cybersecurity, they'll still try and use lures to get people to click on the wrong thing, or will look for vulnerabilities where people aren't backing up properly, or where they've got basic passwords and so on. There is a lot of low-hanging fruit, still, in cybersecurity. If we all did some of these basic things, then even quite sophisticated state actors would find it hard to come after us.

JW: I know you won't, because you're not able to give away secrets, I wonder, for you, personally, who has spent your life in this area, if you can give us a flavour of what you're excited about in terms of the technology and the changes that we're likely to see over the short to medium term, in your field?

JF: I'm massively excited by technology. As you've already pointed out, I'm not a technologist by training, but I have spent a lot of my career involved in technology and involved in data. I think the UK has a real opportunity here to be a major digital and cyber power. By that I mean, if we're world class at defending our digital homeland, making sure that our businesses and our citizens are as safe as possible, if we are able to foster the newest technologies, start-ups in technologies here, and provide the environment where those sorts of industries and technologies and science can grow, then we're going to provide a very, very firm platform for our economic resurgence after this pandemic. So, I think that's all really, really exciting. Wherever you look in the UK, there are world-leading technologists. Of course, in my own particular area, then that's around data science, and it's around how we're thinking about quantum going forward, it's about artificial intelligence, and before that, machine learning. Developments in those areas where the UK is leading in some aspects of it, have great promise, I think, for us all. They provide massive challenges, of course, but I think it's extremely exciting to see what is already happening in our country and what could happen. My real hope is that GCHQ can be part of that, will benefit from the skills spin-off from it, but also as we've done at points throughout our 100 years, where we have developed technologies and where we've shared them with the outside world, we can really be part of driving that future for the United Kingdom, too.

JW: Jeremy, thank you so much for being here and for being part of the Cheltenham Science Festival this year. It's been absolutely fascinating to be inside GCHQ, inside your mind and to hear what you're doing to keep us safe, and the plans for the future. Thanks so much for being here.

JF: It's been my pleasure, and it's always a pleasure to be part of this Festival, I think it's a really important endeavour and way of reaching out in an area that is critical to, not only GCHQ's future, but our broader communities and the nation as a whole, so thanks Julia.

JW: Thank you, and thanks to everybody for watching, do please keep watching, there is plenty more to come on the Cheltenham Science Festival @ Home. There are more details on the website, also details of how to donate to support the work that the Cheltenham Festivals does throughout the year in Cheltenham, in schools, in communities and beyond that. Thanks again Jeremy, and thanks again for watching.