PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

NATIONAL SECURITY BILL

First Sitting

Thursday 7 July 2022

(Morning)

CONTENTS

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

not later than

Monday 11 July 2022

The Committee consisted of the following Members:

Chairs: † Rushanara Ali, James Gray

† Bell, Aaron *(Newcastle-under-Lyme)* (Con)
† Eagle, Maria *(Garston and Halewood)* (Lab)
† Elmore, Chris *(Ogmore)* (Lab)
† Everitt, Ben *(Milton Keynes North)* (Con)
† Hart, Sally-Ann *(Hastings and Rye)* (Con)
† Higginbotham, Antony *(Burnley)* (Con)
† Hinds, Damian *(Minister for Security and Borders)*
† Hosie, Stewart *(Dundee East)* (SNP)
Jones, Mr Kevan *(North Durham)* (Lab)
† Jupp, Simon *(East Devon)* (Con)
† Lynch, Holly *(Halifax)* (Lab)
McDonald, Stuart C. *(Cumbernauld, Kilsyth and Kirkintilloch East)* (SNP)
† Mann, Scott *(North Cornwall)* (Con)
† Mohindra, Mr Gagan *(South West Hertfordshire)* (Con)
Mumby-Croft, Holly *(Scunthorpe)* (Con)
† Phillips, Jess *(Birmingham, Yardley)* (Lab)
† Sambrook, Gary *(Birmingham, Northfield)* (Con)

Huw Yardley, Bradley Albrow, Simon Armitage, *Committee Clerks*

† attended the Committee

Witnesses

Jonathan Hall QC, Independent Reviewer of Terrorism Legislation

Sir Alex Younger KCMG, Former Chief, SIS

Professor Sir David Omand GCB, Former Director, GCHQ

Paddy McGuinness CMG OBE, Former Deputy National Security Adviser

Public Bill Committee

Thursday 7 July 2022

(Morning)

[Rushanara Ali *in the Chair*]

National Security Bill

11.30 am

The Chair: Before we begin, I have a couple of preliminary announcements. *Hansard* colleagues would be grateful if hon. Members emailed their speaking notes to hansardnotes@parliament.uk. Please will you all switch your electronic devices to silent mode? I can see that you have not got teas and coffees, so that is good.

We will consider the programme motion on the amendment paper, followed by a motion to enable the reporting of written evidence for publication, and then a motion to allow us to deliberate in private about our questions before the oral evidence session. In view of the time available, I hope that we can deal with those matters formally, without debate. The programme motion was discussed on Tuesday by the Programming Sub-Committee for this Bill.

Ordered,

That—

1. the Committee shall (in addition to its first meeting at 11.30 am on Thursday 7 July) meet—

(a) at 2.00 pm on Thursday 7 July;

(b) at 9.25 am and 2.00 pm on Tuesday 12 July;

(c) at 11.30 am and 2.00 pm on Thursday 14 July;

(d) at 9.25 am and 2.00 pm on Tuesday 19 July;

(e) at 9.25 am and 2.00 pm on Tuesday 6 September;

(f) at 11.30 am and 2.00 pm on Thursday 8 September;

(g) at 9.25 am and 2.00 pm on Tuesday 13 September;

2. the Committee shall hear oral evidence in accordance with the following Table;

Date	Time	Witness
Thursday 7 July	Until no later than 12.00 noon	Jonathan Hall QC, Independent Reviewer of Terrorism Legislation
Thursday 7 July	Until no later than 12.40 pm	Sir Alex Younger, former Chief of the Secret Intelligence Service; Professor Sir David Omand, King's College London
Thursday 7 July	Until no later than 1.00 pm	Paddy McGuinness, former Deputy National Security Adviser
Thursday 7 July	Until no later than 2.40 pm	Demos; Henry Jackson Society
Thursday 7 July	Until no later than 3.00 pm	Electoral Commission
Thursday 7 July	Until no later than 3.20 pm	Professor Ciaran Martin, Blavatnik School of Government, University of Oxford
Thursday 7 July	Until no later than 4.00 pm	The Law Commission; the Law Society
Thursday 7 July	Until no later than 4.20 pm	Reset
Thursday 7 July	Until no later than 4.40 pm	Reprieve

3. proceedings on consideration of the Bill in Committee shall be taken in the following order: Clauses 1 to 14; Schedule 1; Clauses 15 to 20; Schedule 2; Clause 21; Schedule 3; Clauses 22 to 32; Schedule 4; Clauses 33 to 36; Schedule 5; Clauses 37 to 44; Schedule 6; Clauses 45 to 47; Schedule 7; Clauses 48 to 51; Schedule 8; Clause 52; Schedule 9; Clauses 53 to 61; Schedule 10; Clauses 62 to 65; Schedule 11; Clauses 66 to 73; new Clauses; new Schedules; remaining proceedings on the Bill;

4. the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 13 September.—*(Scott Mann.)*

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Scott Mann.)*

Resolved,

That, at this and any subsequent meeting at which oral evidence is to be heard, the Committee shall sit in private until the witnesses are admitted.—*(Scott Mann.)*

The Chair: Copies of the written evidence that the Committee receives will be made available in the Committee Room and circulated to Members by email. We will now go into private session to discuss lines of questioning.

11.32 am

The Committee deliberated in private.

11.34 am

On resuming—

The Chair: We are now sitting in public again and the proceedings are being broadcast. Before we start hearing from witnesses, do any Members want to make any declarations of interest in connection with the Bill? I take it that there are no declarations of interest.

Examination of Witness

Jonathan Hall QC gave evidence.

The Chair: We will now hear oral evidence from Jonathan Hall QC, independent reviewer of terrorism legislation. Before calling the first Member to ask questions, I should like to remind all Members that questions should be limited to matters within the scope of the Bill, and that we must stick to the timings in the programme motion that the Committee has agreed. For this panel we have until 12 noon. Could you please introduce yourself for the record?

Jonathan Hall: My name is Jonathan Hall and I am the independent reviewer of terrorism legislation, a position that I have held since 2019.

Q1 Scott Mann (North Cornwall) (Con): Mr Hall, thank you very much for giving up your time for us this morning. I understand that this is your first time giving evidence to Parliament, and this is my first time leading a Bill Committee, so we are in similar territory.

Do you agree that utilising the tools made available in the Bill will enhance our ability to deal with the current threats, and give us the flexibility to respond to the changing threat landscape?

Jonathan Hall: Yes, the measures in part 1 and part 2—I will talk about part 3 at some later stage—contain tools that are necessary. I am not a state threats specialist—I am terrorism specialist—but I have had a chance to interrogate officials, and it is clear that there are determined and well-resourced adversaries who will not be put off by a knock on the door to say, "We know what you are up to." The agencies and the police need measures to prosecute and PIMs—prevention and investigation measures—which are special measures.

Q2 Scott Mann: Following on from that, what should the proposed STPIMs regime—state threats prevention and investigation measures—learn from how terrorism prevention and investigation measures were administered and used?

Jonathan Hall: There are two things. First, the official who chairs the review group meetings, which are to decide whether to submit to the Secretary of State that a measure ought to be imposed, or the group which reviews whether they remain necessary and proportionate, needs to be really strong. This is what I have witnessed, I am glad to say, with terrorism prevention and investigation measures. That official has to be able to really hold the agencies in particular to account, and really test and probe what they are saying, both about the intelligence that is being given to the review group and about whether the measures remain appropriate. The first message from the TPIMs is that you need to have a strong chair of the TPIM review group, or the equivalent, the PIMs review group.

The second thing is that one of the experiences from TPIMs is that it is really difficult with connectedness. People who are under those measures can become very isolated, and I think that officials have struggled with whether to allow those people to have smartphones or access to the internet. These days it is very difficult to function as a normal member of society unless you have access to those. One of the lessons that will be learned from TPIMs is how to try to square the circle to ensure that people cannot do bad communications but while also allowing them to function normally in the world with access to normal communications technology.

Q3 Scott Mann: The Bill allows for oversight of STPIMs. In your view, what is the strength of the independent function of your office?

Jonathan Hall: First, it is being able to go to the room where it happens—the meetings where these decisions are taken. When I review TPIMs, I have a completely free hand. I am able to interrogate officials and able to see whatever I want. That is really important. I am not just looking at judgments in courts, or just reading documents; I am actually there able to interrogate, test and challenge. That is what I do. Also, I think it is important that Parliament and the public have a sense of what is going on. Regrettably, because legal aid has not been made available in all cases for TPIMs, there are now fewer court cases, so general information about how this important but serious power is being exercised is relatively cut off. The independent reviewer can provide a lot of transparency about how it is operating.

Q4 Holly Lynch (Halifax) (Lab): Thank you ever so much for your time this morning. May I take you to clause 49, which refers to an independent reviewer carrying out a review of part 2 of the Bill? If it is appropriate for you to say so, have you been approached by the Government to consider how appropriate it would be for your office to take on that review of part 2? What is your assessment of how appropriate that would be compared with setting up a new independent reviewer for state threats legislation?

Jonathan Hall: It has been tentatively mentioned. Obviously, because the legislation has not been passed, I have not been formally asked whether I would do it, but it has been tentatively asked. My answer is that I think it actually is quite a good fit for the reviewer's job, and I think it probably is right that the person who does the independent review of terrorism legislation should also do the state threats legislation. The reason is that this new legislation is really modelled on terrorism legislation. In crude terms, the concept of the foreign power condition sits in place of the purposes or acts of terrorism, and then there is the same framework in terms of very strong arrest power, detention up to 14 days, strong powers of cordons and search and investigations, and, of course, the PIMs. There are so many learning points between the two regimes that it does make sense.

Q5 Holly Lynch: In your experience, do you think that that level of review should apply to part 1 as well as part 2 of the Bill?

Jonathan Hall: Having thought about this, I do. I do not think that decisions on prosecution are going to be made other than in really strong and good cases. Where I think one needs particular care is with all the strong powers that come before prosecution, for example with arrest and detention, as well as the PIMs, which are based not on beyond reasonable doubt but on the balance of probabilities.

We have to acknowledge that we live in quite a polarised world at the moment and that citizens of individual countries, such as Russia and China, and those who associate with them, are bound to fall under suspicion. There is a parallel here, in the sense that people used to argue—I think wrongly, but they did argue—that counter-terrorism laws in England and Wales were anti-Muslim, and I think having a reviewer is one way of offering reassurance that that is not the case.

Q6 Holly Lynch: Thank you very much. Following the thread of the Minister's questions on the state threat PIMs and having read your most recent review specifically on TPIMs, may I ask how effective you envisage the state threat PIMs to be, given your understanding of the implementation of TPIMs?

Jonathan Hall: I expect that they will be effective because the agencies and the Home Secretary will only think about imposing one when they think it is going to work. There are many more subjects of interest who have terrorist intents than are currently on TPIMs, and I expect that the same will be true in relation to people who are foreign threats. There will be many more people who are identified as foreign threats who will actually go under PIMs. At the moment I think only two people are under TPIMs, so it is very few. I would have thought that the agencies and the Home Secretary will think very carefully before imposing them.

Q7 Holly Lynch: I noted your assessment of the introduction of polygraphs. Have you been able to consider their use in any ongoing cases?

Jonathan Hall: What I have been told is that polygraphs have not been used for TPIMs, as far as I am aware, but they have been used for released terrorist offenders and some disclosures have been made. Everyone always thought that the real utility of polygraphs and the clear reason for their use is the disclosures that people make when undergoing the process. I gather that some admissions have been made that have been valuable and have led to a recall. I do not have a huge amount of data, but they seem to have had some success in the context of terrorism offences.

Q8 Damian Hinds (East Hampshire) (Con): Mr Hall, thank you for being with us this morning. Coming back to STPIMs, you spoke with the shadow Minister a little bit about effectiveness but I want to ask for your thoughts about necessity. From your experience with the counter-terrorism regime, how do these sorts of devices get deployed and why? On transparency, I know there are sometimes concerns that these things may be used in large numbers. Will you say a word about how many TPIMs have typically been in operation at any one time?

Jonathan Hall: I cannot remember the total number of TPIMs. I think it is around 30, but I may be misremembering and that may also include—

Damian Hinds: That is over a number of years, of course.

Jonathan Hall: Yes. The maximum I remember in any year is up to six; at the moment it is down to about two. The authorities ran quite a successful campaign, using TPIMs against members or former members of al-Muhajiroun. Those have tended to drop off, and we are now looking at a very small clutch—I think it is only two now.

Q9 Damian Hinds: In terms of their usefulness in the suite of what is available in order to counter these threats in the terrorism field, which obviously is your primary area of expertise, can you say why one might elect to use a TPIM?

Jonathan Hall: First of all, where there is good intelligence that an individual is up to no good but it is impossible to prosecute them. There may be secret sources of intelligence—information coming from allies or from electronic means that could not be disclosed—that mean that the agencies know perfectly well that someone is a real risk. Having had the opportunity to read the intelligence, I know that there certainly are cases where people are very dangerous and are engaging in attack planning but could not be prosecuted. These measures allow a huge amount of control.

One of the key measures for the really serious people is moving them from their home location. They find it much harder to operate if they are outside their home location: they do not have the people around that they know, and they find it a more hostile operating environment. There will also be some people whose threat really comes from the propagation of terrorist propaganda, so the measure might be directed towards their use of electronic devices and the internet.

Q10 Damian Hinds: Given that there is obviously a lower burden of proof—there is no court case—and given the numbers of TPIMs that we have spoken about, are you satisfied that the proportionality is satisfactory?

Jonathan Hall: Up to a point. I have expressed my disappointment that because legal aid is not now available as of right for all TPIM subjects, there is a cohort of TPIM subjects who are not getting court reviews. In the absence of the court having the opportunity to test the proportionality, it is particularly important that the Home Office official who chairs the TPIM review group's meetings is really testing, and I also feel that I have to play that sort of role myself. I have certainly seen cases in which it has been debatable whether the measures have been too strong, particularly in relation to electronic devices, and whether enough attention is being given to allowing people to live a useful life without presenting a threat to the wider public.

The Chair: I am going to move on to our next question now, from shadow Minister Jess Phillips.

Q11 Jess Phillips (Birmingham, Yardley) (Lab): This is a convenient place to start, because I want to focus on part 3 of the Bill, which is obviously taken up with legal aid and civil remedies. You have already said that you are okay with parts 1 and 2 of the Bill in earlier statements, so I will just give you the floor to express your view on part 3 of the Bill.

Jonathan Hall: I have one thing to say about part 1, but we will come back to it. Part 3 is different from parts 1 and 2, because I believe that part 3 is not there to meet an operational need. Generally speaking, I think the reason why the public support terrorism legislation is that they believe that laws are being passed to improve their security—obviously, today is the anniversary of 7/7. Here, the changes are intended to be entirely symbolic. The first thing to do is to recognise that it is quite unusual in the context of terrorism legislation to enact a measure that is really symbolic, and therefore it needs to be justified with care.

My concern about the legal aid, beyond the symbolism aspect, is that the class of individuals who are going to be affected by this is very wide indeed. The justification for removing legal aid from convicted terrorists is that they have broken their links with society. Of course, we all understand that in the context of an Islamic State would-be suicide bomber or someone of that nature, but the same effect will be felt by children who are arrested for document offences—in other words, having a copy of "The Anarchist Cookbook" on their computer.

As you know, there are now many children who have been arrested and prosecuted for terrorism offences. It also catches people who do not get custodial sentences at all, so the cohort of people captured is very wide indeed, and I do not myself understand why the decision has been taken to include not just the most egregious examples of terrorism-convicted people, but also people who may never have gone to prison and may have very quickly—one hopes—gone back into normal life. That is my general point about aid. I have expressed further points about how it is possible that this measure could be counterproductive. Should I pause there?

Q12 Jess Phillips: I would agree with you. I feel it is counterproductive. You are an expert on terrorism; I am an expert on violence against women and girls, grooming and the link between people who perpetrate terrorism and a previous history of domestic abuse.

Could you see a situation arising—you may well have these cases; I have seen some—where a woman who is a victim of domestic abuse falls foul of this legislation, because of an association with her abuser who goes on to be convicted of terrorism, because she cannot access civil legal aid to go to family court and stop her children being taken by that terrorist?

Jonathan Hall: I do not think so, because legal aid is termed individually. In the example you are giving, the woman in question would not be a terrorist convict, so she would be able to apply for legal aid.

Q13 Jess Phillips: But what if she had been convicted because she shared some information? I am mindful of the fact that a high percentage of those women who are referred to the Prevent programme—it is over 50%—are found to be victims of domestic abuse.

Jonathan Hall: Then, yes. A woman who has previously been convicted of a terrorism offence would be forced to resort to what is known as exceptional case funding. As I think the Justice Committee has reported, it is very difficult to get solicitors to even apply for exceptional case funding and there are great difficulties in getting hold of it urgently. I suspect it will be said that, for the worst cases of domestic violence, it would be granted. I do not know if that is the case.

Jess Phillips: It is not the case.

The Chair: I am going to have to move on to the next questioner. I would appreciate it if colleagues could be succinct with their questions. I will allow a couple if you are succinct—otherwise it is just one question.

Q14 Ben Everitt (Milton Keynes North) (Con): I shall be succinct, then. Thank you for attending, Mr Hall. Are you comfortable with the change in language between the focus on non-state actors and state actors? I am thinking in particular from the perspective of your terrorism background.

Jonathan Hall: I think what you mean is, am I comfortable with the fact that legislation has now been passed that is dealing with state threats, when previously the focus had been on terrorism? If that is what you are saying, then I think I am comfortable, because I accept and recognise that we live in a contested and uncertain world. Focusing on state threats is now a very sound necessity.

Q15 Ben Everitt: This is the succinct follow-up: when it comes to the link between state actors and non-state actors—who are actually proxies for rogue states and other aggressive foreign powers—do you think we have got the balance right in being able to capture the intelligence we need to combat those threats?

Jonathan Hall: I think the two regimes—the terrorism regime and the state-threats regime—should be sufficient. There are obviously people operating in the grey zone at the moment who might be able to say, "We fall outside the remit of terrorism legislation," for example, the Wagner Group. If they are acting on the battlefield in support of Russia, we would have difficulty seeing them as terrorists. I think this legislation probably fills some gaps.

Q16 Stewart Hosie (Dundee East) (SNP): Mr Hall, you said that the agencies would think very carefully before using an STPIM. I think that is correct. You have also said that the evidential test for deploying an STPIM is self-evidently lower than securing a criminal conviction. Do you give any credence to the argument that the STPIMs might move from being measures of last resort to being used more frequently because they are easier to deploy? Do they therefore undermine some of the criminal provisions in the Bill?

Jonathan Hall: I do not think so, if the regime operates as it is intended to, because the Bill replicates the obligation for the Secretary of State to consider whether it is possible to prosecute in the first place. I do not think in practice that they will become a measure of first resort, just because they are so resource-intensive and complicated. I suppose it is possible that, unlike some of the terrorist TPIM subjects who are individuals without a huge amount of access to resources, some of the individuals who may be under an SPIM could be backed by a huge amount of resources, which means that there will be perhaps more significant litigation than there has been with TPIMs; I do not know.

The point is that you are dealing with people at a lower level than beyond reasonable doubt. Intelligence is fragmentary and it is possible to make a mistake. It is always important to bear that in mind, with a degree of modesty and humility, when these really strong measures are being imposed.

Q17 Stewart Hosie: On the point about beyond reasonable doubt, one of the conditions in clause 33 to deploy an STPIM is that the Secretary of State would reasonably believe that the individual is or has been involved in some activity. If we remove "beyond reasonable doubt", is "reasonably believes" sufficient, or should it be on the balance of probability?

Jonathan Hall: My view is that it is the same thing.

Q18 Holly Lynch: You said in response to my hon. Friend the Member for Birmingham, Yardley that you had a point to make about part 1. I want to give you the opportunity to make that point.

Jonathan Hall: I am slightly uncertain and concerned about the scope of clause 3(2), the foreign intelligence services offence. On the face of it, an offence could be committed inadvertently, and it does appear to cover quite a lot of lawful conduct. The example that I have been debating with officials is the example of someone who sells miniature cameras, which is undoubtedly conduct of a kind that could assist a foreign intelligence service. My concern with clause 3(2) is that it does not seem to have a sufficient mental element, either that the individual who commits the offence is deliberately acting prejudicially to the UK interest, or knows or ought to suspect that there is some foreign intelligence service involvement, so I have a concern about that particular clause.

Q19 Sally-Ann Hart (Hastings and Rye) (Con): You mentioned that restrictions to legal aid could be counterproductive and could harm rehabilitation efforts. Can you please expand on that?

Jonathan Hall: Not all terrorists are cold, calculating, ruthless killers who will go and commit terrorist acts whatever their circumstances. They may exist, but there

are also quite chaotic terrorist-risk offenders. I have certainly come across cases where the terrorist risk from the individual—the chance of their stabbing someone, for example—goes up if they are not taking their medication or if they are homeless.

My concern about the legal aid is that it will make it harder, for example, for a terrorist offender, maybe 10 years after they have been released and who is facing eviction, to get legal aid. That means that you might have less good decisions made and a sense of injustice or grievance on behalf of the terrorist offender, who will perhaps say to themselves, "Why can't I get legal aid when everyone else in my situation can?" My real concern is people becoming homeless or falling into debt when they might otherwise be able to get legal assistance.

The Chair: I am afraid that brings us to the end of the time allocated to the Committee to ask questions. On behalf of the Committee, I thank Mr Jonathan Hall QC for giving evidence in this session.

12 noon

Examination of Witnesses

Sir Alex Younger and Professor Sir David Omand gave evidence.

Q20 The Chair: We will now hear oral evidence from Sir Alex Younger, former chief of the Secret Intelligence Service, and Professor Sir David Omand from King's College London. For this session, we have until 12.40 pm. I would be very grateful if the witnesses could please introduce themselves for the record.

Sir Alex Younger: Hello, my name is Alex Younger and I was chief of SIS from 2014 to 2020.

Professor Sir David Omand: I am David Omand. I am currently at the King's College London war studies department as a professor. My previous career in the civil service involved being director of GCHQ, permanent secretary of the Home Office and UK security and intelligence co-ordinator.

Q21 Scott Mann: Thank you both for coming to give evidence today—we are very grateful—and for all you have done in the past to keep our country safe. My first question is to Sir Alex. Can you describe how the threat picture has changed across the UK in the time of your career?

Sir Alex Younger: Yes. That is a huge question. To keep it brief, though, I think the predominant fact that developed during my career was the erosion of boundaries. When I started, the difference between peace and war, domestic and international, covert and overt, and virtual and real was reasonably clear, and we were organised along those boundaries. The threats that eventuated most powerfully were the ones that recognised that those boundaries had eroded and crossed them. What I would call grey threats eventuated and often presented us with real challenges, particularly when actors or states felt themselves at war with us and we did not feel ourselves at war with them, for good reason.

My career saw less emphasis on conventional threats and more on grey space. Most of my career was devoted to counter-terrorism, which was the dominant example, but subsequently we saw state actors working in sub-threshold space—operations short of conventional war—to harm us. That is broadly the situation we are in now, even if we have a very 20th-century example of conflict happening on our continent.

Q22 Scott Mann: How do you think Russian aggression since before Salisbury has factored into security priorities for our intelligence services?

Sir Alex Younger: It has risen. During my career, we were broadly in a situation where we had to focus on state threats or terrorist threats. I think that all of us, societally, were hubristically convinced of the end of history and the fact that liberal democracy had triumphed. Perhaps another answer to your earlier question is that that was demonstrated to be false. In fact, we are in a geopolitically contested world, just as we always were. That led to the increasing dominance of the state threat over time as the world diverged ideologically. Of course, with Russia and the UK specifically, we had some really acute examples of that, in terms of services demonstrating complete contempt for us and our democracy by attempting to murder people on our soil. In a sense, that got us, particularly in the national security community, to the hard truth quicker than many.

Q23 Scott Mann: In terms of this Bill, much of the legislation we are looking to update is quite old. How much of a need do you think there is to upgrade our current legislation in the light of those threats?

Sir Alex Younger: I think it is pressing, not least because, as I have said, many of the threats are ambiguous. This legislation, in seeking to dispel ambiguity—daylight is the best disinfectant—has my support. The reality is that the act of using deception on behalf of a foreign power to undermine our democracy, cause our citizens harm, sap our strategic advantage and undermine our economic advantage is essentially not criminalised at the moment, and that is odd. As you would expect, our adversaries have tonnes of legislation outlawing spying. That is what they do; it is part of how they engineer unity. There is a sense of an external and pernicious threat.

I am more struck by the fact that many of our allies, particularly in the Five Eyes, have seen fit, for many years in some cases, to have such measures in place. To that extent, I regard them as basically uncontentious and overdue. If I may be permitted a professional observation as someone who has worked in this area for 30 years, they will definitely make it harder for people who mean us harm to operate, in a way that they would not like and the public would like.

Q24 Scott Mann: Just one final question for this witness, if I may. We have just had evidence from Jonathan Hall QC, who reflected that he did not think there was an operational need for part 3 of the Bill. Do you agree that it is legitimate for the Government to disrupt terrorist financing?

Sir Alex Younger: Yes.

Q25 Holly Lynch: Thank you both very much for your time. To echo the Minister's sentiments, we are grateful for your service to the country as well. Sir Alex, the measures in the Bill, particularly in clause 3 and some of the others on assisting a foreign intelligence

service, do not make any attempt to distinguish between countries that are our allies or that we have friendly relations with—you talked about the Five Eyes partners, for example—and those countries that would seek to undermine us or are hostile states. Do you think it should attempt to distinguish between the two?

Sir Alex Younger: First of all, I think it is a good idea, fundamentally, to require people to say if they are acting on behalf of a foreign power. I am supportive of that because I know how difficult it makes it for people intent on conducting operations against us to operate, and makes it much easier to prove. I am therefore instinctively supportive of that, and of a register, and I think that we should get on with that. I have talked to the Government about that; they are understandably cautious, given all the unintended consequences attached to it, and the fact that our adversaries use those techniques in a way that lacks good faith and is malicious. However, fundamentally, I am supportive of it.

I have to be honest; I am more ambivalent about the idea of distinguishing between nations. My view of legislation generally, but particularly when it comes to technology, is that it is a mistake to write things to the current circumstances. It is much better to write things to the principles that you are seeking to employ. I am not a lawyer or a member of the Government, but my recommendation would be that we go for a principles-based approach in so far as we can.

Q26 Holly Lynch: Thank you very much. May I ask you both about clause 23, which grants an extension of powers to the security services? It appears from speaking to other colleagues, particularly Members on the Intelligence and Security Committee, that the current legislation—the role of the Investigatory Powers Commissioner, the Fulford principles and the exemptions in the Serious Crime Act 2007—all works together quite well. Do you think that the extension in clause 23 is necessary and that it has the appropriate checks and balances that you would expect with such an extension of powers?

Sir Alex Younger: You are referring to the amendment to the Serious Crime Act?

Holly Lynch: That is right, yes.

Sir Alex Younger: I strongly believe that that is necessary. I am conscious of the concerns that you will have, and even the contentious nature of the assertion, so if you will forgive me, I briefly have to tell you why.

First, alongside our ability to uphold our values and not be terrorists, the other reason why we have been successful in stopping bombs going off has been international partnership. That is because no one state or intelligence service really ever has the full facts. They have to work together and combine their information to get the intelligence that is required, proactively, to disrupt terrorist events. That was true in the analogue world; it is really true in the digital world. It is the thing that works and keeps us safe.

That involves an unavoidable risk. That risk, through all the safeguards that you will be familiar with—but which I am happy to talk about—is managed down to the very lowest level possible. However, ultimately, we are dealing with sovereign actors—other states who we do not control—and ultimately, when we are exchanging large bulk datasets, notwithstanding all the scrutiny and risk management, there is a possibility that there will be data in that dataset whose significance we do not understand until it is compared with another dataset that we do not have. That is an unavoidable risk.

An issue that I think you have to consider is, who should be carrying that risk? My view is that there must be accountability, but where an SIS officer or any other UK intelligence community officer is acting in good faith, within their instructions, as authorised by Ministers, on behalf of you and the public, it should not be them carrying the risk. It is more appropriately carried by the Government more broadly. I feel that, as you can tell from my body language, very strongly, as a leader.

It was unavoidable that we sent our young men and women into harm's way when it came to physical risk. For instance, I served in Afghanistan. Our people were asked to go out on to the streets day in, day out. It involved physical risk that we mitigated down to the lowest level we could possibly manage, but it was part of the deal.

These risks are avoidable. Through this legislation and other measures, we can make sure that these risks are attached to the appropriate person or people or entity. I am much less comfortable as a leader about the idea that we therefore ask individual men and women in the UK intelligence community to suck it up. I do not think that is right.

Professor Sir David Omand: I very strongly agree with what Alex Younger has just said. I know from my own experience of GCHQ that information-sharing with our close allies and indeed more broadly is essential, and I think it is morally wrong to place that burden on the individual member of staff, who may be quite junior, who is simply following the policies and the instructions that they have had. In the end, the Government Ministers must account if something unexpectedly does go awry.

Q27 Holly Lynch: Would it not be fair to say that no cases have yet been brought against anybody acting in that way on behalf of the security services, and would that not be because the protections that are in place in law already give them the discretion to do some of the activities that we are talking about?

Professor Sir David Omand: My counter-argument would be that this is actually a question of principle—how Government works, particularly in relation to people whom we as a nation are asking to take some significant risks on our behalf. This is an additional risk. You may say that it is theoretical; they may not feel it that way, and I think that we owe it to them to protect them.

Sir Alex Younger: It does not feel theoretical. You know, you have to examine the motives of the staff of the UK IC, who are ordinary members of the public, just like you and me. They are not doing this for personal gain.

There is a very practical point that I think the Committee must consider, which is the incentive. Over time, what is going to motivate admittedly a very mission-orientated community if they see personal legal jeopardy in an area where there is an unavoidable level of ambiguity? I think that will inhibit people from the exercise of sharing. I hope I have been really clear that it is the exercise of sharing that allows us, as a team, to deal with the threats that we face. The risk may be theoretical, but it does not feel like that when you are stood in front of the person or the computer.

Q28 Stewart Hosie: Sir Alex, this Bill certainly addresses foreign powers and the actions that they will undertake, but it does not update the Official Secrets Act 1989. That leaves us, or may leave us, in the bizarre position where someone discloses something that may inadvertently help a foreign power, but we have ended up with two different legal regimes and two different sentencing regimes for something that may deliver the same negative impact. If we assume that the Government are not at this point going to redraft the 1989 OSA, and we take for granted that they will introduce a foreign agent registration scheme of some sort, is there any other aspect of the 1989 Act that should definitely be included by amendment in this legislation later?

The Chair: Just before we get the answer, I will just flag up that this may be outside of the scope of this Bill, but we will allow the discussion to proceed, because we have not made a precise ruling on it as the co-Chairs of this Committee. So please proceed, but there the potential for it not to be within the scope.

Sir Alex Younger: My answer is a less eloquent version of that, which is that I have talked about the Government about this. Essentially, they say that they think it is too complicated to work this issue through in the timescale that this Bill is operating in. I am not a lawyer; I apologise. I do not have a detailed answer to your question.

Professor Sir David Omand: I believe that the powers in the Bill are not only necessary, but urgent. In addition to everything that Alex was saying, we are living through a digital revolution. The digital harms are there. I would hate to see the powers in this Bill held up, and possibly even miss their legislative slot, while quite difficult work is done on the 1989 Act.

Q29 Maria Eagle (Garston and Halewood) (Lab): I have never heard anybody apologise for not being a lawyer before.

Sir Alex Younger: It is sincere.

Maria Eagle: It is novel for me—I speak as a lawyer.

I would like to come back to clause 23 and the changes proposed to the Serious Crime Act 2007. I could tell you are very strongly in favour of the changes, but I wonder whether this kind of complete carve-out from liability for the agencies is something you have come across before anywhere else. Is this totally novel, or have you seen it operate somewhere else, and you think it would work well in these instances? There are already defences in that legislation to protect the people you were expressing concern about. What is so wrong with the defences that are already there?

Sir Alex Younger: There are other examples. Australia is the clearest, but it goes much broader than this, actually. In our case, you are right, and it is really important to recognise that a large part of what is already there works. The SCA is, by the way, an Act that I absolutely support—I hate to see fat cats here helping people launder money overseas; it is really irritating. We need this stuff, but I am fairly sure that this aspect, the potential criminalisation of intelligence exchange, was unintentional. The reality is that the way the SCA is drawn, with its extraterritorial nature and its very broad conditions, captures things that would not be adequately addressed through the safeguards that were in place before.

Of course, as you allude to, there are defences in place, but to go back to the conversation we have just had, I do not think I as a counter-terrorist operator, which I was, would be particularly happy—even though I have faith in the justice system and the wisdom of juries—to know that what I did could be tested in a court of law with all the uncertainty that entails, when I am obeying a lawfully authorised instruction with all of the oversight that exists. I want to be really clear: when a UK intelligence community individual acts not in good faith or outside those instructions, they should absolutely be subject to all the considerations, including of secondary liability, that exist, but I think any ambiguity in the circumstances I just described is wrong and will have a chilling effect on our intelligence exchange.

Q30 Maria Eagle: Does not the ability to obtain a ministerial authorisation under the Intelligence Services Act 1994 deal with those concerns?

Sir Alex Younger: Again, I am not a lawyer, but I do not believe that it does, no, not entirely. In fact, that is the predicate for what I am saying.

Q31 Maria Eagle: Do you agree, Sir David?

Professor Sir David Omand: Yes, I would agree with that.

Q32 Damian Hinds: Sir David, you have a long sweep of history to look back at, with GCHQ and your role as the first security and intelligence co-ordinator, and now in academia. Sir Alex was speaking earlier about some of the long-term trends and the blurring of boundaries. I think you used the phrase "the digital revolution". I wondered if you might say a word about what you think are the biggest growing or evolving threats right now.

Professor Sir David Omand: From my experience, I would point to the consequences of the digitisation of every conceivable kind of information. That is proceeding apace. We have digital cities. Our infrastructure is now wholly dependent on IT.

In my recent book, I coined an acronym, CESSPIT—crime, espionage, sabotage and subversion perverting internet technology—and that perversion is going on as we speak. I will add one thought: I put "crime" in my acronym deliberately. If you take the activities of something like the North Korean Lazarus group, which was responsible for the WannaCry ransomware attack on our national health service, it is operating in order to obtain foreign exchange to pay for the North Korean nuclear programme and North Korean intelligence activity. In March, the group took more than $0.5 billion-worth of Ethereum currency from an exchange. This is large-scale larceny on behalf of a state.

My hope is that the powers in the Bill will help the police and agencies to deal with state-based criminal activity. I know that there are aggravated offences powers as well, which will help the police.

Q33 Damian Hinds: How do you see information operations working? How might foreign states seek to interfere in our democratic processes and public life?

Professor Sir David Omand: If you recall the statement made almost exactly two years ago in the House by Dominic Raab, he said that the Government had concluded that it was "almost certain" that "Russian actors" had

"sought to interfere" in our election in 2019; and we had the evidence from the American elections and the French presidential election in 2017. All the techniques were deployed. I do not know whether any members of the Committee have been watching the TV series showing on Channel 4, which is as good a primer as any on how such techniques can be used to pervert our political discourse as well as actually harm individuals. This is the world we are in, these are the harms we face and I think that this Bill is a good start in helping the agencies to address some of those harms.

Sir Alex Younger: On this issue, you are right to focus on the possibility of interference in our democratic process and the potential unintended consequences of what we are talking about here. Of course, one person's interference is another person's legitimate intervention. Perish the thought that it should be the Government's responsibility to say what is true and what is not. That is the difference between us and our opponents.

I can understand the scale of the problem; I have seen it. I had a long chat with the Government about this, and the thing that convinced me that this was an appropriate response was, first, the foreign powers condition—to be clear, that is about people acting on behalf of a foreign power—and, secondly, essentially the use of deception to achieve your aim. It seems to me that if someone is working on behalf of a foreign power, using deception, to distort our political process, we have a pretty clear basis for taking action. That, I think, is as it should be.

Q34 Sally-Ann Hart: I want to pick up on the foreign interference point in clause 13 of the Bill:

"A person commits an offence if…the person engages in conduct intending that the conduct, or a course of conduct…will have"

a negative "effect" on the UK for or on behalf of the foreign power in question. In other areas of law, in particular the criminal law, we have intent and recklessness. Do you think that clause 13 should be expanded to include recklessness?

Professor Sir David Omand: I looked at clause 24, "The foreign power condition", and there is quite a lot of scope in it for a successful prosecution to demonstrate that the individual who as, as you say, acted recklessly, could reasonably have been expected to know that their act would benefit a foreign power, for example, so I was not so concerned about that particular question.

Sally-Ann Hart: So you do not think that it should be included in clause 13?

Professor Sir David Omand: No, I had not concluded that.

Sally-Ann Hart: Sir Alex?

Sir Alex Younger: I do not have anything to add to that.

Q35 Stewart Hosie: I just want to press further on clause 23. You said that the absence of a carve-out to protect officers could have a chilling effect. Given that we have substantial data sharing, particularly with our closest partners, that the internal safeguards are very robust, and that there is already the defence of acting reasonably—you made the point that this would be on an order to do so—I am not clear yet why the carve-out in clause 23 is as necessary as you suggest it is.

Sir Alex Younger: First of all, "carve-out" means different things to different people, but there is a wild idea that this is a granting of immunity that means we can behave willy-nilly. You will know from your Committee experience that this is not true. I want to make that really clear. The reality at the end of all this—we have had the theoretical versus practical conversation already—is that there exists a risk that individual UK IC officers will face criminal sanction for doing their job. I do not think that risk should exist. That is fundamentally where I am. You can decide as politicians that it is better than what is being proposed by the Government, but I am saying that I do not think it is compatible with a healthy sharing regime of the sort that produces the security benefits I have outlined.

Q36 Ben Everitt: Sticking with that point, Sir Alex, in an earlier answer you referred to Australia having a much broader, greater carve-out for their intelligence officers to keep them safe and do their job legally. Could you expand on that?

Sir Alex Younger: I cannot. I am sorry, but it happened just at the end of my time. I know from conversations with my Australian colleagues that they are very satisfied with the legislation that exists, in so far as that it deals with this issue. I would recommend looking into that yourself or speaking to the Australians. I do know that it is broader than what we are proposing here today. I am sorry I cannot be more helpful.

Q37 Ben Everitt: I am sure the Clerks are listening. Speaking generally then, with Australia in particular being a close ally—there is Five Eyes and other joint initiatives—would you recommend more co-ordination legislatively with close allies such as Australia, to protect our frontline officers?

Sir Alex Younger: Yes. It is not something I have thought hard about, but the fundamental principle of operating as a team is probably our most powerful riposte, alongside our values, to the threat of authoritarianism. It is something I am completely signed up for, but alliances are a thing we have that our opponents generally speaking do not. I was very proud to operate in one of those—Five Eyes—which is a particularly effective version. If we, as a matter of principle, aimed for interoperability through legal alignment, that is something I would absolutely support. It is never going to be complete. The United States particularly has a very different legal process to us. Certainly as regards counter-terrorism, the extent that we manage to align legally massively boosts operational co-operation. I am wholly confident that the same would be true when it comes to state threats.

Ben Everitt: I think everybody here would agree that a team has to play by the same rules.

Q38 Holly Lynch: The Bill creates a new offence of preparatory conduct in part 1. To what extent do you think that was an omission in previous legislation? I have heard from former members of the security services that they feel quite strongly that this is welcome, but the definition of preparatory conduct is drawn quite broadly. I wonder if you could comment a little on that.

Professor Sir David Omand: I was pleased to see the power in the Bill because, particularly in the digital age, you can take the offensive and you can prepare, but

you may not have got to the stage of actually pressing the button. If you can demonstrate that a foreign state was engaged with help from inside the country in some serious espionage or sabotage activity, it seems to me that the very preparation is something that the prosecutors ought to be able to bring forward. In the terrorism example, the cases would be slightly different, but the offence of acts preparatory to terrorism has been extremely helpful to the prosecution authorities for good reason.

Sir Alex Younger: The bottom line is that we have to get in front of this stuff. Just speaking as a counter-terrorist practitioner, that is the additional discipline. It is not like solving the crime. We need to solve it before it has happened, and that raises a set of ethical and legal dilemmas where it is important to be striking the right balance, so I really welcome the proper treatment that we see of that in the Bill.

Q39 Holly Lynch: Sir David, following up on your points about the digitisation of information, Microsoft told me that a great deal of online state activity is around theft and access to data policy development, and think-tanks increasingly becoming a focus for attempts to have a look at and steal that type of work. Are those some of the things that you are seeing in terms of hostile state activity online, and do you think that the clauses in the Bill go far enough in protecting that type of policy work and data?

Professor Sir David Omand: Probably not, but on the other hand you have to balance that against the risk that legislation would inadvertently catch, for example, academic activity in think-tanks. Alex Younger has referred to transparency and covertness. Where a foreign power is taking covert acts and dirty tricks in order to access our institutions, think-tanks and universities, that would be criminalised by the Bill.

Where a member of the embassy of any foreign state represented here attends, quite openly, think-tank meetings and so on—everybody knows who they are and they know they are on the guest list—that does not pose a direct harm. It would be a mistake to start to try to confuse those categories too much. However, what it comes down to is that this is a probabilistic business; this is doing things that increase the chances that we all protect the citizens and the interests of the state. This Bill alone is not going to prevent states from attempting harm against us, and it probably will not catch all those harms either, but it is a good start.

Q40 Scott Mann: I did not get a chance to ask you a question at the start of the session, Sir David, so I feel I am slightly obligated to ask you a question at the end. In terms of the need for reform, some of the legislation that preceded this is very old. You have mentioned some of this already, but could you expand a little on how changing the legislation will address some of the current state threats? It is worth having that on the record again.

Professor Sir David Omand: Well, there is a lot in the Bill. The move away from having to identify states as enemies, for example. States have interests of their own and they will promote those interests. If they are doing so openly through diplomatic and academic means, that is one thing, but if they are doing it, as some are, covertly, then although you might not categorise them as enemies, they are none the less conducting themselves in a way that causes harm. That is one of the examples where I think the Bill takes a more up-to-date view. It is not just nations with which we are at war or potentially could be at war.

Scott Mann: That is very helpful. Thank you.

The Chair: We have a few more minutes. Does anyone else have any further questions?

Q41 Holly Lynch: I will pick up on a thread from the previous question, if that is okay. We talked about some of the physical engagement around think-tanks, universities and academia. Microsoft has done some work that shows the prevalence of targeting online, with Government, NGOs and think-tanks seen as emerging targets for hostile state activity. For understandable reasons, some of the limitations of the Bill would make it quite difficult to pursue and prosecute when theft takes place entirely online by somebody who is overseas. With that in mind, do you think there is anything further that we could do in legislation? Is what we have in the Bill enough to disincentivise, stop, disrupt and criminalise online theft of policy development and data, as opposed to trade secrets, which the Bill is quite explicit about in clause 2?

Professor Sir David Omand: My reading of the Bill is that trade secrets and theft of intellectual property are well covered. You probably also have to have in mind the Online Safety Bill, which has a whole different set of considerations but which is, again, intended to reduce the amount of harmful content that citizens are exposed to. It is quite easy to envisage cases where a foreign state is putting material online covertly and pretending to be someone else.

In the 2016 US presidential election, there were a number of egregious examples of that—for example, in order to stir up conflict within society by exaggerating an existing split in society, be it over race, inequality or any other issue. That is the nature of the threat that we currently face in all democracies. You cannot solve it all by creating criminal offences where a link cannot be established back to the foreign powers condition, but you may be able—by working with the companies, which will exercise their own terms and conditions—to get more of this stuff removed. You need that as well as the powers in the Bill.

Q42 Holly Lynch: Further to that, we intend to table an amendment that would put a requirement on the Government to commission an independent annual review of the prevalence of disinformation pushed online by hostile states—looking at it in its entirety, but also its specific impact on UK elections—to try to deliver the transparency piece alongside some of the new offences. Is that the sort of thing that you think would be helpful?

Professor Sir David Omand: Yes, and another important consideration is public education. I have argued before that we should start teaching critical thinking in schools and teaching kids how to be safe online when they come across deliberate and malicious misrepresentation.

The Chair: We have one minute left.

Q43 Damian Hinds: I realise that we have a tiny amount of time left. It is the curse of these things that we have to finish exactly on time, because we are just getting into this very interesting and important topic.

You mentioned the US elections in 2016. Do you think the word "disinformation" really covers what we are talking about? Sometimes, the most invidious and harmful activity is not necessarily saying something that is untrue; it is just winding people up to hate other people more than they did before, and to distrust the system, society and democracy more than they did before. I do not mean to lead the witness, Sir David.

Professor Sir David Omand: I recommend the use of the OECD's triplet of "misinformation", which is wrong, but innocently so, and should be corrected; "disinformation", which is deliberately and maliciously wrong; and "malinformation", which is information that is true but was never intended to enter the public domain, such as the personal emails of Members of Parliament.

Sir Alex Younger: Please hold that thought, because I spent years trying to work out whose side Vladimir Putin was on, as he was propagating all sorts of contradictory causes, and then I just realised that he wants an argument—he wants distrust and discord. I have not been to the OECD on the subject, but I entirely support that.

The Chair: That brings us to the end of the time allocated for this session. On behalf of the Committee, I thank our very distinguished witnesses for your time today.

Examination of Witness

Paddy McGuiness gave evidence.

12.40 pm

Q44 The Chair: We will now hear oral evidence from Mr Paddy McGuiness, former deputy national security adviser. For this session, we have until 1 pm. I would be very grateful if our witness could introduce himself for the record.

Paddy McGuinness: My name is Paddy McGuiness, and I am currently an adviser with a critical issues firm called Brunswick Group. I was previously a national security official, latterly as the deputy national security adviser for intelligence, security and resilience in the Cabinet Office from 2014 to 2018. In that role, I oversaw hazards and threats affecting the UK homeland, including some aspects of counter-terrorism, alongside Sir Alex, and cyber-security programmes, offensive and defensive. I began the work on hostile states, and I also dealt with questions of broader resilience to natural hazard. For much of that time, I was also the Government's chief security officer, overseeing matters of vetting, classification, investigation, and disciplinary and criminal proceedings to protect classified information.

Q45 Scott Mann: Thank you for your service to the country. Your recent service as national security adviser gave you a valuable perspective on the current threats. Can you describe the extent to which the UK has the tools to deal with hostile acts from foreign states and the nature of how those threats have changed in your time in your job?

Paddy McGuinness: I really welcome the way you framed that question, because when I thought to myself, "What am I going to say in front of this Committee?" that was absolutely at the centre of it. As the representative, in a policy sense, of the intelligence agency—Sir Alex and the others—and as a person trying to practise Government security and see through disciplinary and sometimes criminal investigations around compromise of classified material, my lived experience was that our legislation and regulations were, frankly, a Potemkin front, and that behind them there was not very much.

I would move in public or speak to Members of Parliament and Ministers, and they would say, "Ah, we have got the Official Secrets Act. We have got this and that," and they would look at the terrorism powers, which Jonathan Hall described so fully, and the way they interplay with the powers proposed in the Bill, and they would assume we have similar powers, but as you see we had almost nothing. Where there were powers, very few of them crossed the serious crime threshold to engage the full range of intrusive investigative techniques and police time to pursue them. That was very disturbing at a time, certainly when I was deputy National Security Adviser and previously, when the impact on the digital age, as described by Sir David and Sir Alex, came to the fore, and when many states were messing, within the United Kingdom, with our institutions, corporate life and communities, over which they thought they had some share because those people came from that country of origin.

The answer is that I was left very disturbed. That is why under the coalition Government, the Cameron Administration and the May Administration—I left during that—I was, if you like, an apolitical advocate of new powers to shore up what was a weakness or shortfall in our national security capability.

Q46 Scott Mann: That is really helpful. You mention cyber. From your perspective, what is the increasing relevance of cyber to state threats?

Paddy McGuinness: Yes, and this is illustrative. In the other areas, as Sir Alex described and did fantastic service in countering terrorism, we have not had as much terrorist pressure on our societies and values as there might have been, because of the suppressive effect we have been able to have with our partners. That is because we had capabilities and powers. In the case of hostile state threats, we have some capabilities but perhaps not enough powers, and that is true in cyber. So we have left in front of people who wish to have purchase over our decision making, or to be able to influence us or possibly attack us, free space.

Inevitably, we concentrate on those that are most egregious. Sir David referred to the Lazarus Group in North Korea, and we might look at Iranian behaviours. Indeed, we might look at Russian or Chinese behaviours, particularly around intellectual property and technology, which are all very serious, but I refer you to the number of advanced persistent threats that are now listed because that gives you a description of the number of states that, unconstrained, are beginning to use these techniques for their policy purposes, whatever they are.

For me, almost the best example of this was in the covid pandemic, when there were intrusions and potentially damaging activity in the networks of international healthcare organisations that we needed to help us deal with the pandemic, such as the World Health Organisation. The APT—advanced persistent threat—identified was Vietnamese. I refer you to that list. We do not need to

ask any former official to breach the confidentiality of high classification material to know that many states act in this space, and they have clear space in front of them in the cyber domain and in some of the techniques that are countered by the Bill.

Scott Mann: May I have one final question?

The Chair: I will bring you back in later. I call the shadow Minister.

Q47 Holly Lynch: Thank you, Mr McGuinness, for your service and for keeping us and our communities safe. The Bill creates a new offence of sabotage. Is that something that you felt had been missing from previous legislation?

Paddy McGuinness: It was quite extraordinary that we had a range of different possible offences that relate to the kinds of things that a hostile state would commit in order to sabotage, for instance, critical national infrastructure—a target entity in the UK—and that it was not coherent. What I would put in front of the Committee when you are thinking about this is: the most common thing that I find now in corporate life, but also in Government or in policy space—and in Parliament where I do a bit of advisory work—is stovepiping.

You say "cyber" or "cyber-security" and people immediately think of cyber-security issues, or you say "insider issues" and they say they will deal with that, or they think of physical attacks or physical disruption and they deal with that. They do not understand that this is a playbook, which, if you are a Russian commander, you put together, and you have a choice of what you do.

So you go in an escalation route from, "Can we access this remotely through the internet? Is there another way of accessing it electronically? Do we have a spy within it? Can I send someone from the embassy to go and get close to it and do something to it? Shall I send in Spetsnaz covertly—you know, go to Salisbury and poison some people? Or shall I go to war?" You have that whole range of things and they all relate to each other. And all of them relate to sabotage. We need to approach this by understanding what the adversary is doing and not having little bits of powers in some criminal damage legislation, or in the Computer Misuse Act. That will not do because that is not the purpose of the opponent.

I have described it for disruption and destruction in a sense of warfare, and I have used a kind of Gerasimov Russian example. It is very interesting when one looks at the way in which intellectual property has been stolen. There are a few cases where we see the end-to-end Chinese state effort, where you begin with remote cyber-attacks in close proximity—the case I am thinking of was in the United States—and an inability to get in by those means. Eventually, the subversion and recruitment of a member of staff operating in Switzerland provided them with the intellectual property, which they were not able to access using the cyber techniques. All the way through they were intervening in the networks and activities of that company.

One final thought on this: one of the difficulties with this grey space activity, as Sir Alex described it, is that if you have a presence for an intelligence purpose, you can flick it over and turn it into a disruptive or destructive attack. That is where that preparatory bit is quite important, too: understanding that the simple fact of engaging and being present quickly takes you towards sabotage. I think these are absolutely vital powers.

Q48 Holly Lynch: That is incredibly helpful and interesting; thank you very much for that insight. Can I take you from that to a slightly different issue? You heard the previous conversation with Sir Alex and Sir David about hostile state interference and making sure we have protected our democratic processes from that possible risk. How satisfied are you that UK elections are secure from foreign interference?

Paddy McGuinness: The Clerks may have told you, or it may be in my bio, I do not know, but after I left Government I was asked by the Oxford Internet Institute to join them in a thing called the Oxford Technology and Elections Committee, prior to the 2019 elections—with an urgency because of what had happened in the United States in 2016—to come up with some practical suggestions for what we might do to protect our elections. I refer you to it: it is a great bit of work, and the Oxford Internet Institute has gone on doing that work. I am no longer as involved, but there is good work there.

The way I would frame it is this: it is a bit like what I said about the powers that we have. Because we do not occupy the space, others step into it, so because there are not strong controls and real clarity about what is happening around our electoral processes, people mess about in that space. It is really important—this rather echoes something Sir Alex said—that we do not take messing about in the electoral space as being the same thing as delegitimising an election. We have a strong tradition in the United Kingdom of being able to make judgments about whether the way in which candidates have behaved or the way in which money has been spent in a given constituency makes an election void, and you possibly have to run it again. We are used to making that judgment.

One of the risks that I note in this space—again, this is a point Sir Alex made very nicely about Vladimir Putin's intent, which is to have us off balance—is that if the Russians do hack into a political party's servers and mess about within them, and maybe mess with the data or interfere, or if they play games with a technology platform that people rely on for information and put out information, and we decide as a result that we cannot trust a referendum or an election, they succeed. That is success for them, so I think what really matters in this space is the ability to measure the impact that state activity has on the democratic process we are looking at, and—as Sir Alex said—that there is bright transparency so we know who is doing what.

The Chair: I bring in Sally-Ann Hart.

Q49 Sally-Ann Hart: We heard from the previous witnesses about the challenges of online harm—sabotage and dis, mis and malinformation—and the Bill seeks to modernise the espionage regime to meet the challenge of the digital age. Do you think it will achieve that aim and where are the gaps, if any?

Paddy McGuinness: I would expect it to be a dynamic process. I think you will be looking at further legislation; let us hope you have a long life as an MP, but in your time as an MP I would expect you to have to look at this again.

To Sir David's point, I do not think we should delay for a moment fixing the things that the Bill fixes because of the fact that technologies develop dynamically. There is a lag. I can remember—I think I was actually working at GCHQ at the time—us thinking about what was happening with Facebook as it emerged as a widely used platform. Here we are with the Online Safety Bill, about 13 years later. There is a natural and quite proper lag between rapid technology innovation and slow and considered regulation and legislation, and we are going to have to live with that. I think this is good. It provides a basis, and I think the extraterritoriality is particularly important, as is the way in which sabotage is broadly defined to allow you to deal with the kind of range of things that I have been talking about, given that the opponent will move through those spaces.

Q50 Antony Higginbotham (Burnley) (Con): The other day the director-general of MI5 and the director of the FBI said that most of what is at risk by quantity is not what the state does, but the technology, research and development and commercial advantage developed by our businesses and academic institutions. Does the Bill do enough—I am thinking mainly about the offences part of it—to protect against that risk?

Paddy McGuinness: I think it does a very significant thing in the way in which it criminalises specifically the trade secrets aspect, which covers a very broad range. Again, we may have to return to this. This kind of legislation and the type of work that Sir Alex and his successors in MI5, MI6 and GCHQ are doing has Darwinian effect, so I have no doubt that as companies have got better at certain kinds of protection advised by the interaction with the CPNI and the National Cyber Security Centre, so the opponents have got better at it. And we will have to go on doing it.

It does not feel as though we have quite the same volume of opencast mining of our intellectual property and economic value that we had, as was described previously by General Keith Alexander, the head of the National Security Agency in the US. He described the enormous volume—trillions of value—taken out of our economies. There still is a very high level, though, so there is more work to do on this, and it is a significant challenge to the corporate sector to do the right thing in this space, because of the difficulty that it represents. The Bill provides a really solid basis for that discussion, because of the criminalisation of the trades secrets aspect.

Q51 Antony Higginbotham: That is really helpful. They also said in the same speech that our opponents have a whole-of-state approach to further their aims—you touched on this. Does the Bill do enough to join us up and ensure that we have got that whole-of-state view on how we defend against espionage, sabotage and so forth? Or is that not realistic because of the evolving threat?

Paddy McGuinness: One must constantly avoid complacency, but one of the strengths of the British state is the way in which institutions and agencies work together pragmatically and practically—within the bounds of law, obviously. That is how we have managed to get this far, with a lack of powers, without something going catastrophically wrong. It has felt really nerve-wracking doing it. As the person who had to represent it to Prime Ministers and the National Security Council, my word I was nervous about this. I was much more confident in other areas of my responsibilities, because there was a real shortfall. The Bill closes out quite a lot of that.

I would note something that I think reads across several of the points that have been made by the previous witnesses that I have heard today that it is important for the Committee to understand and for me to represent. When you are dealing with state threats, and in particular against really capable actors, that is a different task from dealing with terrorism or serious and organised crime, because we must work on the assumption that some of our communications, some of our computers and some of our people are under their control.

When I look at, for instance, the STPIM powers, I reflect that it is much more difficult still to bring prosecutions in this area than it is for terrorism and for serious and organised crime, where sometimes people have been suborned by the crime group. This is all together more serious, and it would be naive to think that no one spies for a foreign country, no communications are intercepted and no one is in any of our computers. That just raises the level of difficulty that we have got in this space.

The Chair: Thank you very much. That brings us to the end of the morning sitting and the time allocated. On behalf of the Committee, I thank Mr McGuinness for giving evidence today.

Ordered, That further consideration be now adjourned. —(*Scott Mann.*)

1 pm

Adjourned till this day at Two o'clock.