PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

NATIONAL SECURITY BILL

Third Sitting

Tuesday 12 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

Saturday 16 July 2022

© Parliamentary Copyright House of Commons 2022
This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: 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)
Hosie, Stewart *(Dundee East)* (SNP)
† Jones, Mr Kevan *(North Durham)* (Lab)
† Jupp, Simon *(East Devon)* (Con)
† Lynch, Holly *(Halifax)* (Lab)
† McPartland, Stephen *(Minister for Security)*
† 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

Public Bill Committee

Tuesday 12 July 2022

(Morning)

[James Gray *in the Chair*]

National Security Bill

9.25 am

The Chair: I welcome the Committee to the line-by-line consideration of the Bill. Let us first have a few moments of parish notices. Many people here are old hands at this business, but some are not. Members will therefore forgive me if I talk them through the way in which the Committee ought to consider the Bill, from the beginning—forgive me if I am telling you things that you already know.

The Bill before you is the Bill as agreed, without Division, on Second Reading. The purpose of the Committee is to consider the Bill in detail and seek to improve it. That is done by any member of the Committee tabling amendments. Most often, amendments are tabled by Her Majesty's loyal Opposition, although anybody can do so. On this occasion, there is also a large number—perhaps larger than usual—of Government amendments. We talk through the amendments.

Amendments are grouped on the selection list before you and are linked together by subject. If there are amendments across the field on a similar subject, they are debated together in one group. Amendments are then voted on not at that time, but when we get to the relevant part of the Bill; amendments are debated together, but often we will vote on them two or three days later, as we come to them. That removes the confusion on that part. The Member who tabled the lead amendment in a group starts the debate. Others may then catch my eye. Members may speak as often as they like on each amendment, although we might seek to avoid overdoing it.

Behaviour, as it were, is identical here as to that in the main Chamber. Things such as eating and drinking are not allowed, and—to begin with, at least—gentlemen are wearing their coats. I am a very old-fashioned traditionalist and tend to start that way. However, if somebody at some stage wanted to make a point of order, I might be persuaded to change that particular rule—for the first time in my 25 years as a Chairman, mark you, but these are extreme conditions. I am sure that the Doorkeeper will kindly ensure that everyone has plenty of water, as we need to be aware of the heat today.

Clause 1

Obtaining or disclosing protected information

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): I beg to move amendment 46, in clause 1, page 1, line 10, leave out "prejudicial" and insert "damaging".

This amendment seeks to clarify the tests to be met before the offence of obtaining or disclosing protected information is committed.

The Chair: With this it will be convenient to consider the following:

Amendment 47, in clause 1, page 1, line 10, after "safety or" insert "critical".

This amendment seeks to clarify the tests to be met before the offence of obtaining or disclosing protected information is committed.

Amendment 48, in clause 27, page 21, line 4, at end insert

""critical interests" includes security and intelligence, defence, international relations and law and order".

This amendment seeks to clarify the tests to be met before the offence of obtaining or disclosing protected information is committed.

Clause stand part.

Stuart C. McDonald: It is a pleasure to serve under your chairmanship, Mr Gray. I welcome the new Minister to his place and wish him all the best in his new role. I certainly foresee this experience as being thrown in at the deep end, but it is a Bill on which there is broad consensus, so I hope that it is not too much of a baptism of fire and that he enjoys it.

It is nice to be able to join colleagues. I was sorry to miss the evidence session last Thursday, as I was indisposed, but I have read the transcript, and the session seemed to prove incredibly useful. I therefore did not miss the usual experience I have at around this time of a Bill Committee, when I think, "If only I had been able to hear or read that evidence before drafting my amendments, they might have been slightly different."

Let me reiterate our position: the vast majority of provisions in the Bill are welcome and probably long overdue. Clause 1, like clause 4, implements part of the Law Commission's review recommendations. The clauses are broadly welcome and should stand part of the Bill. Our amendments to clause 1, like most of the handful of other amendments we have tabled, are simply designed to probe whether the offences are drawn tightly enough. The crimes that we are talking about are serious—the offence in clause 1 can lead to life imprisonment. I do not think that anybody on the Committee would say that that is not appropriate when a person steals or hacks protected security information at the behest of a foreign Government and puts the lives of UK citizens at risk.

The amendments are simply designed to ask whether the offence might catch conduct that it was not intended to catch, particularly behaviour that might embarrass the Government but is not in any genuine sense prejudicial to our safety. The shadow Minister put that question to the Law Commission witnesses last Thursday. Professor Lewis responded that such questions are probably legitimate in relation to the Official Secrets Act 1989 and leaks, but the offence is different in this case because of the requirement to be acting for a foreign power. She said succinctly:

> I think we are in a slightly different realm here: the realm of espionage and not the realm of leaks.—[*Official Report, National Security Public Bill Committee,* 7 July 2022; c. 52, Q98.]

On the whole, I absolutely accept that point, and I fleetingly considered withdrawing some of the amendments, but there are questions about whether that distinction is 100% correct. There are legitimate concerns—they were raised on Second Reading and in the written briefings provided to MPs in advance of it—that the clause also catches behaviour that is more akin to a disclosure under the 1989 Act.

Article 19 and the Campaign For Freedom of Information argue that some of the broad concepts used in clause 1 combine in a way that puts civil society organisations and journalists at risk. I am grateful to those groups for their Second Reading briefings, which have largely prompted my remarks this morning. They point to several features of the clause that cause difficulty. First, it covers material that does not bear a security classification, and information is in scope even if it is not restricted but the person receiving it reasonably believes that it should have been.

Secondly, the concept of "safety or interests of the United Kingdom" is essentially determined by the Government of the day, so it is a policy of the state and, potentially, a broad concept. Thirdly, as well as not being confined to hostile states, the foreign power condition appears to be met simply by obtaining funding from a friendly Government who are pursuing perfectly reasonable aims.

That combination of factors gives rise to concerns for NGOs and journalists. I will give some hypothetical examples of each, which I have borrowed from Article 19. Let us say that an NGO in the UK has some general overseas funding from a friendly Government to campaign on climate change. The Government of the day decide that fracking or new coal are essential for UK interests—who knows where we might be in a few months' time? The NGO is provided with leaked information undermining that policy—perhaps about the safety record of the company being lined up to operate the plan—and publishes it. Has the NGO involved committed a criminal offence? The way the clause is worded suggest that it might have.

The right hon. Member for Haltemprice and Howden (Mr Davis) made the point that lots of excellent organisations receive funding from overseas foreign powers, as they are currently defined. In fact, a list would include ActionAid, Anti-Slavery International, Article 19, Client Earth, Global Witness, Index on Censorship, Media Defence, the Organised Crime and Corruption Reporting Project, Privacy International, Reprieve—from which we heard evidence last week—and Transparency International. The funders of those NGOs include organisations such as the Danish International Development Agency, IrishAid, New Zealand's Ministry of Foreign Affairs and Trade, the US State Department's Bureau of Democracy, Human Rights and Labour, and the US State Department's Office to Monitor and Combat Trafficking in Persons—there are many more in that vein. That is why we have concerns about the effect of clause 1 on NGOs.

In contrast, if a different NGO—one just across the road—had published that document online, it would not be committing an offence, not just because it does not receive any such foreign funding, but because the 1989 Act is more specifically about the subject matter or material that leads to an offence of disclosure—namely, it would have to relate to security and intelligence, defence, international relations and law enforcement. Environment or energy policy—or fracking, in my example—would not be covered. The punishment under the 1989 Act would be two years' imprisonment, not life, so there is real inconsistency between the disclosures caught by the Bill and those caught by that Act.

My second example relates to journalism. What happens if, rather than directly publishing the leak, the NGO passes it to a journalist who reports the leaked information as part of their story? If that journalist is employed by a UK news organisation, all is well, because the foreign power conditions are not met. However, if the journalist works for another Government state broadcaster—even a friendly one—the foreign power condition is adequately met. One reporter commits no offence at all; another reporter—who perhaps works for Danmarks Radio or any other state broadcaster—commits an offence that could mean life imprisonment.

Our amendments offer different ways of addressing that. Amendment 46 would reintroduce the test of damage. Interestingly, the Law Commission's proposals for reform of the 1989 Act recognise that damage can sometimes act as a public interest test, and that it is a concept worth keeping in relation to offences that could be committed by journalists or citizens generally, even if the Law Commission was arguing for removing it in relation to other disclosure offences.

Our amendments would also clarify what interests are protected by that serious offence, and would match the clause up with what is protected by the 1989 Act. Amendment 48 mentions simply "critical" interests—meaning security, intelligence, defence, international relations and law and order.

There is another alternative that I will come to later, which relates to fixing the foreign power clause so that NGOs are not caught if they get funding from benign foreign powers for perfectly reasonable purposes. Those are different alternatives, and I would be interested to know whether the Government accept that those two scenarios are caught by the clause. If so, what is their response?

The Minister for Security (Stephen McPartland): It is a pleasure to serve under your chairmanship, Mr Gray, and to be here in Committee. I will start with the clause and then deal with the amendments tabled by—let me see if I can get this right—the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East.

Stuart C. McDonald: Very good.

Stephen McPartland: Thank you.

I will quickly respond to some of the hon. Gentleman's points. There are a variety of protections throughout the Bill. One is that someone has to be doing activity designed to benefit or help a foreign power in order to commit an offence. Secondly, most of the offences in part 1 of the Bill need sign-off from the Attorney General. Thirdly, the Crown Prosecution Service has to be satisfied that prosecuting is in the public interest. Those are three very large protections that exist throughout the Bill. As we go through the Bill clause by clause, we must always remember those three big principles.

I will start by referring to the recent case of the individual working in the British embassy in Berlin who was extradited and charged, and to the conviction of a Ministry of Defence contractor in 2020 under the existing espionage legislation, which indicate the threat that is posed by those looking to harm the United Kingdom by committing espionage. Clauses 1 to 3 create four separate but overlapping offences to ensure that the Bill proportionately covers the wide range of threats and harms that constitute espionage, without capturing legitimate activity. The clauses are supported by other provisions in the Bill, including the "prohibited places" provisions, by building on and modernising our existing

[Stephen McPartland]

tools in the Official Secrets Acts 1911, 1920 and 1939. The new provisions continue to criminalise harmful activity while reducing the risk of loopholes that can be exploited by sophisticated state actors. I will speak later to clauses 2 and 3, and to the "prohibited places" regime.

Before I get into the detail of the offence set out in clause 1, it is important to flag that, along with other offences in the Bill, it will apply only in circumstances where there is a clear link between the activity and a foreign power. This is provided for by the foreign power condition, which we will discuss in more detail later. In essence, a person's conduct must be carried out for, on behalf of, or with the intention to benefit a foreign power. This responds to the recommendation, made by the Law Commission in its 2020 "Protection of Official Data" report, to move away from outdated concepts.

Stuart C. McDonald: The foreign power condition includes activities carried out with the financial or other assistance of a foreign power. The concern is that if an NGO gets regular funding for environmental or human rights work, it would be accidently caught by the foreign power condition. A journalist who works for a friendly state broadcaster would also be caught by the foreign power condition. We still think that such scenarios are a concern.

Stephen McPartland: As I said earlier, we have three huge protections. One is that activity must be for, or on behalf of, a foreign power. I understand the point the hon. Gentleman is making, but there are another two layers on top of that protection. The first is that the Attorney General's consent must be obtained. Secondly, the Crown Prosecution Service must be satisfied that prosecution would be in the public interest. Those are three very strong layers of protection that would help protect an NGO if it were to do something inadvertently.

Maria Eagle (Garston and Halewood) (Lab): I welcome the Minister to his place. Having such protections in place is all very well, but the real issue is the chilling effect this could have in the kinds of circumstances that the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East has set out. It is not right, is it, for us to criminalise activity that we do not really want to criminalise, but then say, "Well, the Attorney General will sort it out later in each individual case."? That is not really a very good way of legislating.

Stephen McPartland: We are not talking about legislating in that way. If the hon. Lady will forgive me, we are saying that there are three layers of protection. The first layer is that people would be deemed to be obtaining or disclosing protected information for, or on behalf of, a foreign power. The next layers would involve the Attorney General and the Crown Prosecution Service. The hon. Lady, as a lawyer, will be very well aware that the CPS always determines whether it feels it is in the public interest to prosecute. People will not be caught up by accident, and I think we are getting into theoretics by going further and further down that line.

Ben Everitt (Milton Keynes North) (Con): I am struck by the hypothetical example given by the hon. Member for Cumbernauld, Kilsyth and—

Stuart C. McDonald: Just go with Cumbernauld, if that helps.

Ben Everitt: Okay, we will just go with Cumbernauld. The hypothetical example referred to a Government of the day diversifying their energy sources so that, potentially, they were less reliant on fuel and power from a possibly hostile foreign state. The Minister has detailed the extra layers of defence that will act in the public interest. Does he agree that in the hypothetical example cited we would want some protection from foreign interference in Government policy—a democratically elected Government of the UK?

Stephen McPartland: My hon. Friend is correct. Three tests must be met for someone to be prosecuted: conducting harmful activity with regard to information that is protected effectively, knowingly prejudicing the safety or interests of the United Kingdom, and acting in a way that benefits a foreign power. Forgive me, but I do not believe that an NGO will accidentally fail all three of those tests.

Mr Kevan Jones (North Durham) (Lab): But it may, because subsection (1)(b) states that a person commits an offence if

"the person's conduct is for a purpose that they know, or ought reasonably to know, is prejudicial".

An NGO might think that putting something into the public domain is in the public interest. They may not even take into account that that disclosure may damage UK security. For example, in this morning's newspapers—

The Chair: Interventions should be brief.

Mr Jones: The story of alleged shootings by the SAS has clearly been put into the public domain. I would argue that disclosure is not in the public interest of the UK, but people are arguing that it should be in the public domain.

Stephen McPartland: That example demonstrates how important the Bill is, because it sets out that activities that are illegal will still be illegal if actors are acting in a particular manner. The Bill is trying to bring current provisions up to date to provide our intelligence services with the toolkits they need to keep our nation safe and secure. I believe that the three tests are strong enough to help provide those protections.

Mr Jones: I accept that, but just take this morning's example cited on the BBC of the alleged illegal acts by the SAS. Someone has got the information, put it in the public domain and may feel that it is in the public interest for it to be scrutinised. Will that damage our interests? Yes, it will. The Government might think that that disclosure will help a foreign power or damage our interests—and I would argue that possibly it will—but that is not to question the judgment of the individuals who have decided that the allegation should be in the public domain.

Stephen McPartland: I understand the right hon. Gentleman's point, but I believe that we have three very strong tests that must be applied: the information must benefit a foreign power, the Attorney General must consider the case, and the CPS must decide that it is in the public interest to prosecute. Those three tests and protections run throughout the Bill.

Jess Phillips (Birmingham, Yardley) (Lab): I recognise that the Minister is trying to make progress and I apologise for intervening, but does he have any concerns about the Attorney General test? Does he think that the Attorney General does not protect the Government from embarrassment? Does he think that the law always comes above with the Attorney General?

9.45 am

Stephen McPartland: Current events demonstrate that we never protect the Government from embarrassment!

Before I get into the detail of the offence itself, it is important to flag that, along with other offences in the Bill, it will apply only in circumstances where there is a clear link between the activity and a foreign power. That is provided for by the foreign power condition, which we will discuss in more detail later. It responds to recommendations in the Law Commission's 2020 "Protection of Official Data" report about moving from outdated concepts such as "enemy".

Clause 1 enhances our ability to tackle the threat of espionage by introducing a modern offence to capture those unlawfully obtaining, copying, recording, retaining, disclosing or providing access to protected information. Protected information is any information, document or other article that is or could reasonably be expected to be subject to a form of restriction of access in order to protect the safety or interests of the United Kingdom—for example, if the information is stored within a secure Government building or has a form of restricted classification. Protected information can cover a wide range of Government material, including information such as raw data, documents such as committee reports and other articles such as memory sticks.

Protected information includes, but is not limited to, classified material. That is important, given that serious harm can be caused by obtaining or disclosing seemingly non-sensitive information that, if used in a certain way by sophisticated state actors, could be capable of damaging the United Kingdom's national security. However, I want to be clear that the definition will not cover truly benign items such as the lunch menu of the Home Office canteen.

Like the existing espionage provisions, and as recommended by the Law Commission, clause 1 will require that a

"person's conduct is for a purpose…prejudicial to the safety or interests of the United Kingdom".

The term

"safety or interests of the United Kingdom"

has been interpreted in case law as meaning the objects of state policy determined by the Crown on the advice of Ministers, which includes national security. That enables the United Kingdom to respond to threats targeted against its wide range of interests.

Amendment 46 would require that a person's conduct be instead for a purpose that they know, or ought reasonably to know, is damaging to the safety or critical interests of the UK. That would create a higher evidential threshold to secure prosecution in an area that is often difficult to evidence due to the sensitive nature of the information that may have been obtained or disclosed. Put simply, we would have to explain why it caused damage, which may require evidence that compounds the damage. That would provide challenges to our law enforcement agencies and courts, and is likely to result in fewer prosecutions being pursued, offering further opportunities to those looking to harm our country through acts of espionage. The use of "prejudicial" mitigates some of that risk.

Maria Eagle: I am grateful to the Minister for setting out the difference between those two words, but can he give us an example? The hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East gave a theoretical example to illustrate why he tabled the amendments. Can the Minister give us an example of something that is prejudicial and not damaging?

Stephen McPartland: I will come on to that in a bit. I will provide an example shortly.

Maria Eagle: Thank you.

Stephen McPartland: You are very welcome. I would not want to get it wrong.

Amendments 47 and 48 would introduce and define the term "critical interests". In the amendments, "critical interests" is defined to include security, intelligence, defence, international relations and law and order. Although I recognise that the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East tabled the amendments to attempt to specify exactly what should fall under UK interests in order to add clarity, I must stress that it limits the scope and utility of the clause 1 offence and risks creating loopholes that could be exploited by those looking to harm the UK. There is also the risk that the offence would become quickly outdated as the UK's interests naturally and properly evolve. Notably, the list does not include economic interests or interests relating to public health, to name just two areas that would be overlooked by such a definition. Those are areas that are targeted by hostile actors and should rightly be protected.

The safety or interests of the UK test is used not only in clause 1, but in several other offences throughout part 1 of the Bill, such as sabotage or entering a prohibited place with a purpose prejudicial to the UK. There is a risk that creating a notably different test under the clause 1 offence would confuse the legal interpretation of the tests under those other offences and may have a significant impact on their operational utility.

Finally, I reiterate that the test of a person conducting activity

"prejudicial to the safety or interests"

of the UK already exists and is understood in the courts. Just last week at an oral evidence session, the law commissioner invested considerable time and effort in reviewing this area of law, outlining their support of the Government's decision to retain that term. They commented that the

"safety or interest of the state is consistent with a lot of the wording that already exists within the Official Secrets Act…and it avoids what might risk being an unduly narrow focus on national security."—[*Official Report, National Security Public Bill Committee,* 7 July 2022; c. 52, Q97.]

Moving away from the amendments, it should be noted that instead of using "enemy", as in the espionage provisions, the offence in clause 1 includes a foreign

[Stephen McPartland]

power condition. That moves the offence away from labelling countries as enemies, which is less relevant in the 21st century.

The hon. Member for Garston and Halewood asked about the difference between prejudicial and damaging. The damage requirement would require the court to demonstrate harm and explain why it is damaging, whereas prejudice is broader and could include reducing future opportunities. That will also mitigate some of the risks associated, as I have said. It provides a wider test so that we can intervene at an earlier stage of a plot or something else that would affect our national security.

I turn to the extent of the provisions under the 1911 Act. An activity that takes place wholly outside the UK would be an offence only if it is committed overseas by a UK national or officer, such as a Crown servant. Technological developments in a more global world mean that it is now more likely that information that warrants protection to safeguard the safety or interests of the UK may be vulnerable to activity that takes place outside the UK by a wider range of actors—for example, a locally engaged security guard working in a UK embassy stealing papers, or the theft of information held there digitally via cyber means.

To keep pace with the modern threat, the extraterritorial jurisdiction for the offence has been expanded so that the offence can be committed anywhere in the world and by anyone, regardless of their nationality. The extraterritorial jurisdiction is a critical reform within the offence as a better defence for the United Kingdom against a modern espionage threat, whose global nature is not reflected in the current provisions in the espionage offence of the Official Secrets Act 1911.

Another key difference from the existing offence is the increase in the maximum penalty available to life imprisonment. The emergence of modern vectors such as cyber means that espionage has the potential to cause a greater level of harm than was possible in 1911 when the United Kingdom's espionage offences and penalties were first drafted. In the most serious cases, an act of obtaining or disclosing protected information can result in the loss of life or can gravely undermine the United Kingdom's ability to defend itself from a range of threats. This demonstrates the United Kingdom's resolve to make it more difficult and detrimental for hostile actors to undermine our country's interests and safety by committing acts of espionage.

Although we will come to this in more detail later in Committee, I want to flag a key safeguard that applies to prosecutions to this and other serious offences in part 1. Given that state threat activity and the United Kingdom's response can have a significant impact on the safety and interests of our country and wider international relations, the Attorney General's consent, as I said earlier, must be obtained in the case of England and Wales before a prosecution is taken forward. In Northern Ireland, the consent of the Advocate General must be sought.

I stress the importance and need for reform of the espionage laws in the Official Secrets Acts 1911, 1920 and 1939. Recent and ongoing events make it clear that the threat from state threat activity, particularly acts of espionage, is of continuing concern and we must have robust protections in place. The introduction of the offence of obtaining or disclosing protected information as a core part of the Bill provides measures to tackle the harmful espionage activity that the United Kingdom faces. That is why clause 1 is so vital. I encourage my fellow Committee members to support it and I ask that the hon. Member withdraw his amendment to it.

The Chair: Before I call the shadow Minister, it might be helpful if I clarify the order of debate that I normally expect to see. The person who has proposed an amendment moves it. By and large, anybody else then takes part in the debate, including the shadow Minister. The Minister replies to the debate and then the proposer gets a short whack at the end. On this occasion, I will call the shadow Minister, and then the Minister will have an opportunity to reply before the proposer rounds up.

Holly Lynch (Halifax) (Lab): I am eternally grateful, Mr Gray. It is great to see you joining as Chair of this Committee on this particularly important piece of legislation. Thank you for the refresher on the order in which the Front-Bench spokespersons take part in proceedings.

We have had a highly unconventional start to this Bill Committee. I do not think anybody is more relieved to see the Minister in his place—perhaps the Government Whip. I really do welcome the Minister to his place and wish him all the very best. I know he has made every effort to get across the detail of the Bill in the incredibly short time he has had to prepare. I echo the sentiment we expressed on Second Reading and offer him the assurance that the Bill has our support. It is right, and increasingly urgent, that our laws are updated. We intend to be nothing but constructive in our scrutiny, deliberations and suggested additions, as we work together to ensure that the legislation is as effective as we all need it to be.

The Home Office's impact assessment is clear that:

"The threat from hostile activity by states is a growing, diversifying and evolving one, manifesting itself in several different forms including espionage, foreign interference in our political system, sabotage, disinformation, cyber operations, and even attempted assassinations."

I was struck by the testimony of Sir Alex Younger, the former chief of the Secret Intelligence Service, in last week's evidence session. In response to a question about how threats to the UK have changed, he said:

"What I would call grey threats…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 subthreshold space—operations short of conventional war—to harm us.—[*Official Report, National Security Public Bill Committee,* 7 July 2022; c. 11-12, Q21.]

Following detailed pieces of work such as the Intelligence and Security Committee's "Russia" report and the Law Commission's "Protection of Official Data" report, we have been calling for progress in this legislative area for many months, so we welcome the opportunity to work with the Government to get it right.

As the Minister has outlined, clauses 1 to 3 will introduce three new espionage offences: obtaining or disclosing protected information, obtaining or disclosing trade secrets, and assisting a foreign intelligence service.

As was highlighted by the Government's integrated review in 2021, state threats to Departments, national infrastructure, British businesses and private individuals are growing and becoming ever more complex. The situation in Ukraine and the ongoing Russian aggression have brought about an urgency to introduce new offences in this area, but make no mistake: this has been an emerging trend in contemporary national security threats for years.

The director general of MI5, Ken McCallum, in his joint address to UK businesses, journalists and academics with the director of the FBI last week, said that alongside the situation in Ukraine, the

"most game-changing challenge we face comes from the Chinese Communist Party. It's covertly applying pressure across the globe… We need to talk about it. We need to act."

I thank the director general and all those who are working so hard in our UK intelligence community for the work that they undertake around the clock to keep us safe. They have to respond to threats that most of us cannot begin to comprehend. We are grateful for their service, and it is at the forefront of our minds as we consider what they need from us in order to do their job. Therefore, these new offences, which reflect the changing dynamics of the challenges to our national security, very much have our support.

Clause 1 criminalises obtaining or disclosing protected information. Further to the Minister's introduction to the clause, we heard from the witnesses last week about the need for the clause. It is a particular focus of the Law Commission's "Protection of Official Data" report, and the commission confirmed that it was satisfied that the offences

"reflect well the recommendations that we made."—[*Official Report, National Security Public Bill Committee,* 7 July 2022; c. 50, Q94.]

In explaining why the offences are required, the "Microsoft Digital Defence Report", which was published in October last year, identified that Chinese actors engaged in this type of activity mostly targeted data and intellectual property exfiltration. A broad range of sectors has been targeted, including comms infrastructure, the defence industrial base, IT, education, law firms and medical research. Interestingly, the report said:

"In the last year, espionage, and more specifically, intelligence collection, has been a far more common goal than destructive attacks."

However, rather than commercial or industry targets, Microsoft's data shows that

"nearly 80% of those targeted were either in government, NGOs, or think tanks."

Its analysis suggested that,

"Think tanks often serve as policy incubators and implementers, with strong ties to current and former government officials and programs. Threat actors can and do exploit the connections between the more traditional NGO community and government organizations to position themselves to gain insights into national policy plans and intentions."

The theft of research, policy development and datasets has been the focus of hostile state actors in recent months, so we are satisfied that there is a need for the new offence created by clause 1.

10 am

On Scottish National party amendments 46, 47 and 48, tabled by the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East—this is the third Committee I have served on with him, and it has taken three Committees for me to be able to reference his constituency with any degree of certainty—we will also seek to probe some of the questions that he highlighted.

There are some recurring principles throughout the Bill, which manifest themselves in clause 1, and it would be useful to work through them in these early stages. The condition that

"the person's conduct is for a purpose that they know, or ought reasonably to know, is prejudicial to the safety or interests of the United Kingdom"

must be satisfied in order for the offence to have occurred. The principle of "ought reasonably to know" recurs in the offences created by clauses 1, 2 and 3, and later in the Bill, so I am keen to work through the notion, further to the conversation I have had with the intelligence community directly. In some of my discussions, there has been a sense that a clear and robust representation may be made in order to communicate to a person that their conduct, if it persists, will bring them within the scope of the offence.

One example is the security services interference alert, issued in January to Members of this House. One would expect that that would put it beyond any doubt that the conduct of someone continuing to engage or supply information to an individual named in that way is prejudicial to the safety or interests of the United Kingdom, removing any ability to plead ignorance. Is that type of formal intervention required for someone to commit an offence under the "ought reasonably to know" stipulation? If not, will the Minister provide further clarity about the other ways in which he envisages that condition being met?

Former members of the UK's intelligence community have put it to me that the combination of a relatively broad definition of "protected information" in clause 1, combined with a maximum sentence for these offences being imprisonment for life, a fine or both makes the clause quite a beast, in terms of what it does. I recognise the need for seriousness for all the reasons I have outlined, but I am mindful that "protected information" has a much broader definition than "classified information". It is not beyond the realms of possibility that a naive young person visiting the House of Commons comes across a misplaced hard copy of what should be a password-protected document, takes a photo and puts it on their Facebook page—if that is indeed what young people use for social media nowadays. For other potential scenarios, hon. Members are limited only by their imagination. I have no doubt that they will be relieved that I will leave it to just that one. As stupid and unhelpful as that is, has that person opened themselves up to life imprisonment?

The Minister said that the Home Office menu will not be captured by these offences, but there is a plethora of examples between the Home Office menu and very serious information, and that requires some working through. I am sure the Minister will assure me that there will be sliding scale of offences up to and including life imprisonment at the disposal of the judiciary, which will presumably be dealt with in the sentencing guidelines. Will he confirm that that will be the case? Can he remind Members of the process of the development of the sentencing guidelines, and the timeframe in which we might expect to see them alongside the Bill? An indication of the value of the fines available to the judiciary would also be incredibly helpful.

Stephen McPartland: It is a pleasure to follow the hon. Lady and I thank her for her kind words. She asked a number of questions, which I will do my utmost to answer.

Protected information is information, documents or other articles to which, for the purpose of protecting UK safety or interests, access is restricted, or it is reasonable to expect that access would be restricted. The hon. Lady's example of taking a photograph inside the House of Commons would not be considered that. Throughout the Bill there are three tests. First, would the activity assist a foreign power? Secondly, would the Attorney General give consent? Thirdly, would the Crown Prosecution Service consider it to be in the public interest to prosecute? Taking a photograph inside the House of Commons or of something a bit more restricted than the Home Office lunch menu would not come under the provision.

The hon. Lady referred to the director general of MI5; this is about giving the Home Office, the intelligence services and the intelligence community the tools they need to tackle the wider threat. The British public trust the UK intelligence community to do the job and to have the powers. People often worry when other agencies get wider powers, but that is not what is happening in the Bill.

On being able to intervene at an earlier stage, the provisions in the Bill provide a toolkit to allow the intelligence community to intervene earlier in some matters in order to work with people to stop them progressing into specific acts that would break the law. It will help people who may be going down the wrong path, as well as helping the intelligence community to act at a much earlier stage.

Stuart C. McDonald: I am grateful to everyone who has taken part in the debate and to the Minister for his response. As I say, I absolutely accept the case for a clause such as this one. However, the Minister's explanation of the protections in place in respect of the two scenarios that I outlined falls a long way short of what I would regard as satisfactory.

I outlined three solutions or protections. One was the foreign power condition; I have explained already why both the NGO and the journalist in those scenarios would meet the foreign power condition, so that does not work. Thereafter, we are left with the Attorney General and the Crown Prosecution Service. That offers no protection at all. From the point of view of the rule of law, people need to know whether they have broken the law or are committing an offence that is punishable by life imprisonment. We cannot leave that journalist or NGO in that position by saying it all depends on what the Attorney General or the Crown Prosecution Service thinks.

I have no idea whether the Attorney General or the Crown Prosecution Service would regard that NGO and journalist as having committed an offence that they would want to prosecute. As Members have said, that leaves a big chilling effect on that NGO and journalist. They have no certainty that they will not be prosecuted for the activities they undertake. They open themselves up to the possibility of life imprisonment for what, on the face of it, has all the characteristics of a disclosure of information, which should be dealt with, if at all, under the Official Secrets Act 1989 rather than in this Bill.

Mr Jones: I have been told that this may be outside the scope of the Bill, but it seems to me that what is missing from it is a public interest defence for those individuals. That protection not being in the Bill opens people up to what the hon. Gentleman describes.

Stuart C. McDonald: That is a fair point. In the light of the lack of satisfactory safeguards we have heard this morning, we may have to revisit that question. There is an issue of scope in relation to sticking that into the 1989 Act, but I do not see any reason why we could not include it in some of the offences in this Bill. Unless the Government can come up with better safeguards than have been offered this morning, we are going to have to revisit that.

I urge the Minister to go away and think about this issue. I am actually more worried about those two scenarios now than I was at the start of the day. I am not absolutely sure that the amendments that I tabled are the right ones, so we will revisit the issue on Report. In the meantime, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 1 ordered to stand part of the Bill.

Clause 2

Obtaining or disclosing trade secrets

Question proposed, That the clause stand part of the Bill.

Stephen McPartland: Clause 2 provides for an offence of obtaining or disclosing trade secrets. It will be an important tool for law enforcement and the intelligence agencies to detect, deter and protect modern espionage activity. It will introduce an offence to criminalise the illicit acquisition, retention or disclosure of sensitive information with a commercial, industrial or economic value linked to its secrecy for, on behalf of or to benefit foreign states.

There is an inherent link between economic prosperity and our national security; we cannot ignore one and expect the other not to suffer as a result. We must respond to the fact that our adversaries and competitors are already acting in a more consolidated way, taking a whole-state approach to state threat activity. It is crucial that we ensure our legislation covers the wide range of threats and harms that constitute modern espionage.

For the purposes of this legislation, a person commits an offence if they obtain, copy, record, retain, disclose or provide access to a trade secret; additionally, the person's conduct must be unauthorised and they must know or ought reasonably to know that their conduct is unauthorised. As with clause 1 and a number of other provisions in the Bill, there must also be a link to a foreign power, such as an intention to benefit that power or to direct tasking by that power.

The clause provides for a maximum penalty of 14 years' imprisonment or a fine, or both. That reflects the severity of the conduct and the potential damage to the UK, its businesses and our economy, as well as being comparable to existing similar legislation.

Mr Jones: The Minister said that there must be a direct link to a foreign power. May I give an example? Suppose that somebody obtains information and gives or sells it not to a foreign power but to a competitor business. Is that covered under the legislation?

Stephen McPartland: The legislation takes civil offences and makes some of them criminal. That case would remain a civil offence. What we are doing is providing the intelligence services with the tools they need to prosecute people who hand over trade secrets in the criminal system. For example, MBDA in my constituency builds Brimstone missiles, which are currently being used in action. If some of those secrets were to be removed and handed over, that would be difficult for the people using those missiles and for the country. There are clear examples of how the loss of trade secrets threatens the country and our allies' lives.

Mr Jones: I agree, but is it the case that to prosecute under the Bill there will need to be a causal link from the individual to a foreign power and not necessarily to a competitor in the UK?

Stephen McPartland: My understanding is that the action would have to be done on behalf of or for the purposes of a foreign power. If it was done unknowingly, it would be for the lawyers and the Crown Prosecution Service to decide how to proceed.

Maria Eagle: In the example that my right hon. Friend the Member for North Durham gave of a person obtaining information and trade secrets and selling them to a competitor business, if that business had a complex ownership structure that led back to, say, China, would that be enough for the person to fall foul of the legislation?

Stephen McPartland: I appreciate the question and understand the spirit in which it was asked. However, one thing that we must be careful of is laying out exactly what someone must do to fall foul of the legislation. If we did, in that example, the Chinese would create that structure and be in a position to use it ensure that anybody acting on their behalf would not fall under that power. We must provide the intelligence agencies with the tools that they need to interdict and decide whether such people can be pursued and taken to court. As we have seen, it is difficult to get anybody on espionage. However, as we have said throughout proceedings, we do need the foreign power condition, or to reasonably know, and reasonableness is a huge test within English law, so a person would have to reasonably know that what they are doing would benefit a foreign power.

The offence under the clause is first and foremost a national security offence. We have created a definition of "trade secret", found in subsection (2), which is intended for use in the state threats context. The introduction of the definition in the offence will help to address the increasingly diverse set of tactics employed by state actors to undermine the UK's national and economic security and target a wide range of information.

There is no specific criminal offence in UK law that directly criminalises the threat to trade secrets by or for the benefit of foreign states. We have trade secrets regulations that transpose European law, but they serve a different purpose. We have therefore modified the definition of "trade secret" to ensure that it is suitable for our specific purposes. For example, as well as requiring that protections are in place that would limit the utility and potentially impose obligations on businesses, the definition in the Trade Secrets (Enforcement, etc.) Regulations 2018 does not account for information with a potential value. We are seeking to capture early-stage ideas such as research as well as established ideas that are more likely to be subject to protective measures.

Subsections (1)(b) and (3) set out in the instances in which a person's conduct is unauthorised and what that means. The clause uses the term "unauthorised" because it focuses on the consent of the person with the power to give that consent. We want to make it absolutely clear that legitimate conduct is not captured by this offence. For the purposes of this offence, a person's conduct is unauthorised if they are not entitled to determine whether they are able to carry out the conduct in question—for example, if they disclose a trade secret to a foreign power and they do not have the permission of the person who does have the power to make that decision. An example of where someone is not captured by the offence could be a team of researchers who are working with a foreign power, but although the information they control amounts to a trade secret, their research partnership authorises them to share that information with the foreign power.

10.15 am

Technological developments have enabled espionage and information acquisition to be conducted from a foreign state with greater ease. United Kingdom business interests are often targeted. Implementing an offence with extraterritorial jurisdictions is necessary to defend the United Kingdom against threats posed by foreign powers. The clause applies overseas where the conduct takes place wholly outside the UK, but only where the trade secret is in the possession or control of a UK person.

Stuart C. McDonald: That is one of a couple of issues that I have. I would like the full information on why the offence can take place only outside the United Kingdom if it is in respect of possession by a United Kingdom national, as opposed to a UK resident or any other description of persons. I do not know whether the Minister can answer that now, but it would be useful to understand it.

Stephen McPartland: I will come back to the hon. Member on that point.

The clause applies overseas where the conduct takes place outside the UK. That includes both a UK national overseas and a UK company based overseas, provided that it is incorporated or was formed, if unincorporated, under domestic law. The clause brings forward an important offence that will form part of a modernised toolkit for our world-class intelligence agencies and law enforcement. It is proportionate to the threat posed by this activity, and imposes no restrictions or obligations on UK businesses, but offers further protections for them, and the UK as a whole, against modern espionage activity. We cannot promote economic prosperity without enhancing our national security and responding to the modern threat posed by espionage.

Holly Lynch: As the Minister just outlined, the clause creates an offence in relation to obtaining or disclosing trade secrets. The former deputy National Security Adviser, Paddy McGuinness, set the scene for this new offence when he gave evidence last week. On the trade secrets element, he said that it does "a very significant thing", and continued:

"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."

He said:

"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."

He also said:

"The Bill provides a really solid basis for that discussion, because of the criminalisation of the trades secrets aspect."—[*Official Report, National Security Public Bill Committee,* 7 July 2022; c. 25, Q50.]

All that provides an incredibly sobering outlook on the scale of the challenge that we face as a country.

Let me work through some of the detail further. We have some queries about this clause, as we did for clause 1. The seriousness of the clause is underlined by the fact that it creates an offence for which, if someone was found guilty of committing it, they would find themselves with a jail term not exceeding 14 years imprisonment, or a fine, or both. The Minister did not give us that extra bit of detail about the sentencing guidelines in the discussion about clause 1. I wonder if he might be able to return to that point in the discussion on clause 2.

Further to that, I confess that on my first reading and several subsequent readings of the clause, and having listened carefully to the Minister explain the detail of who can be prosecuted and where, it seems to suggest that this offence could be committed only by a UK national. I asked a former member of the intelligence community to have a look at it, and they felt that subsections (4) to (7) on who can commit the offence only seem to refer to a UK person, a United Kingdom national or a British citizen. Only on seeking a legal opinion was it judged that it could be interpreted to apply to non-UK nationals, but only if their criminal activity takes place in the UK. It does not apply where this activity is wholly outside the UK. That same legal opinion queried what it means to be "wholly" outside the UK, as that is unclear in this online age. It is also unclear why obtaining UK-related trade secrets unlawfully is not criminalised for non-UK nationals operating entirely from abroad, as is the nature of a lot of this type of activity.

We are not naive to the additional barriers to bringing someone to justice in these circumstances, yet such activity is no less wrongful because of nationality or where the criminal act takes place. With that in mind, I would be grateful if the Minister could confirm, first, for absolute clarity, that this crime can be committed by non-UK nationals when acting in the UK and we could prosecute them using this clause on that basis. Secondly, why does the clause not extend to criminalising non-UK nationals when they commit this offence in the theft of UK intellectual property and trade secrets outside the UK? Will the Minister clarify those points?

Again, we have the principle of "ought reasonably to know", which warrants further consideration and clarity. On the "ought reasonably to know" threshold, I have it on good authority from former members of the intelligence community that the duping of individuals by nation states into doing the bidding of that nation state is not uncommon tradecraft. Are we satisfied that we have the right balance in that regard? Any clarity that the Minister can provide on the sentencing guidelines would be enormously welcome.

Simon Jupp (East Devon) (Con): On a point of order, Mr Gray. Would you mind awfully if Members were to take their jackets off?

The Chair: I will not be taking my jacket off, but hon. Gentlemen and hon. Ladies may take their jackets off if they wish, as it is very hot.

Stuart C. McDonald: I have three short points building on what Members have already raised in relation to this clause.

First, as raised by esteemed colleagues from the Intelligence and Security Committee, there is a question mark over what happens if somebody recklessly starts dishing out trade secrets, not directly to somebody in way that meets the foreign power condition but in a way that makes that inevitable or very likely. That does not seem to be caught by the clause at the moment, so that is something for the Minister to think about.

Secondly, as I have already asked, I want to understand why the offence is only committed "wholly" abroad if the trade secret is in the possession of a UK national, not, for example, a UK resident who is not a national. The Government have made a conscious choice about that drafting and I am interested to know why.

Finally, the clause states that the offence is committed if

"the person's conduct is unauthorised".

Do we need to be a little more explicit about what we mean by authorisation and authorised by whom? I can imagine situations where, for example, the person who we want to prosecute might say, "Actually, my conduct is authorised. It is authorised by the laws of my country," which may be considerably different from the laws of this country. Does that need to be clarified? That might be implied in the phrase

"the person's conduct is unauthorised"

but it may be something the Government want to look at.

Stephen McPartland: Earlier, we talked about sentencing guidelines. My understanding is that we are not in a position to give more detail on that yet. That is something I have discussed with the Ministry of Justice, as we will come to later.

With regard to the offence, one issue we have is the offence is designed to catch overseas activity with a strong link to the UK. It has been set at the threshold of a UK offence, so if we extend who it will to apply to, that will end up extending the scope of the offence. It is

almost as if we have tried to put a safeguard in place to protect and control it, and the more we extend it, the more it will extend the scope of the offence and bring more and more within its scope, so that is the position we are in.

Jess Phillips: As a point of clarification, how will it apply to somebody who has indefinite leave to remain, who is not a lawful British citizen in the United Kingdom but very much operating here?

Stephen McPartland: It applies in the sense that if that person were to commit murder, they would be prosecuted in this country under the laws applying to murder.

Jess Phillips: The Minister would be surprised.

Stephen McPartland: Effectively, it would apply in the same way. As I have said, with all these offences the Advocate General has to sign them off, and the Crown Prosecution Service as well.

Jess Phillips: In actual fact, on a number of occasions I have handled cases where someone with ILR in the UK has committed murder abroad and there was absolutely nothing that could be done about it.

The Chair: That is well beyond the scope of the Bill.

Jess Phillips: But it is not beyond the scope of what—

The Chair: It is beyond the scope of the Bill.

Stephen McPartland: I have nothing further to add.

Question put and agreed to.

Clause 2 accordingly ordered to stand part of the Bill.

Clause 3

Assisting a foreign intelligence service

Stuart C. McDonald: I beg to move, amendment 49, in clause 3, page 3, line 30, leave out paragraphs (a) and (b) and insert

"activities which are prejudicial to the safety or interests of the United Kingdom."

The Chair: With this it will be convenient to consider the following:

Government amendments 1 to 4.

Clause stand part.

Stuart C. McDonald: On the face of it, the offence of assisting a foreign intelligence service in the UK or, in the case of UK persons, anywhere else is long overdue. Under the Bill, the offence is rightly a serious one and is capable of seeing a person in prison for 14 years.

We have tabled the amendment to push the Government on whether they have got the scope of the offence right, to ensure that we do not catch people who were not intended to be caught. In particular, is there not a danger that, as drafted, the offence punishes behaviour that might actually be consistent with, or even positively beneficial to, UK interests? That may come about because, as the Minister explained, we no longer have the concept of enemy services and also because of the very limited scope of the prejudice test.

What does "assisting" mean? It means assisting a foreign intelligence service in carrying out "UK-related activities". Where those activities are outside the UK, it is only an offence to assist that service as a UK person if those activities are

"prejudicial to the safety or interests of the United Kingdom".

However, where those activities are in the UK, there is no need for those activities to be prejudicial at all—any conduct which assists those activities is very likely criminal. I can well understand that a clear ban on assisting any conduct that supports Foreign Intelligence Service activities is attractive, but I will give another hypothetical example, which is much more dangerous than my earlier one, because it does not come from any briefing—I have had to make it up myself, so let us see how it goes.

What if the Estonian intelligence services, for example, believe that a member of their embassy staff in London is providing information to the Russians? They ask an Estonian student who lives in the same apartment block as that staff member to allow access to her apartment to undertake eavesdropping, or they ask her to undertake some monitoring, such as noting times of arrival or departure. That activity by the Estonian intelligence services, or by that student on their behalf, seems positively consistent with UK interests, but as drafted, it would amount to a serious criminal offence under clause 3.

The clause is so widely drafted that I worry that lots of people involved in setting up and facilitating a future meeting between the head of MI6 and the CIA might be in danger of committing an offence, whether they pick him up at the airport, provide him with a hotel room or serve him breakfast. I very much look forward to being reassured that that is not the case.

The amendment would ensure that, as with activities outside the UK, conduct here would have to be intended to support activities adverse to UK interests, or to be such that a person ought reasonably to know that it would possibly assist activities adverse to UK interests. There might be different ways of fixing this potential problem—perhaps a different hurdle can be used to assess "in the UK" activities, such as "inconsistent with UK interests."

On the Government's amendments, why do the Government intend to turn the relevant provision into a defence, which then puts the burden on the person accused? The explanatory notes talk of clarifying that it is a defence, but that seems a very deliberate change of mind by the Government, especially if one reads the explanatory notes, which say that clause 3(7)

"sets out exceptions to the offence to ensure that legitimate conduct that is within the UK's interests is not caught withing the offence."

That is what the explanatory notes say about the original drafting of the Bill, so it is not clear why the Government have had a change of heart, and I look forward to hearing the Minister's explanation.

10.30 am

Mr Kevan Jones: I understand the thrust of the clause, but I would like some clarification on the definition of assisting a foreign power. I have one historical example, although I think it might not work. Eddie Chapman—

[Mr Kevan Jones]

Agent Zigzag from the second world war—was working for both sides. He was a UK agent and a Nazi agent. He got an Iron Cross for his misinformation work. In that case, he was not assisting a foreign power, because he was given dud information, but what about the case of a UK-based foreign diplomat who is working against us and supporting his or her nation, but is also then feeding information to us? It could be argued that that individual is working against our interests, because they are working on behalf of that other nation, but separately they might be the source of information. What would happen to that individual?

Gordievsky is a good example; he was in the Russian embassy in London for many years, feeding a lot of vital information to the UK, but his daily activities would have been prejudicial to the UK's interests. How would the clause apply to individuals like that? Would they be separated out because of their benefit to us, although certain activities they are conducting would not be of benefit? I give just two historical examples, but there might be others in the future. Where would those individuals fall under the provisions in the clause?

Holly Lynch: As we have heard, the clause introduces a new espionage offence of assisting a foreign intelligence service. A person commits an offence if that person

"engages in conduct of any kind, and…intends that conduct to materially assist a foreign intelligence service in carrying out UK-related activities."

Once again, we are broadly supportive of the clause. As highlighted by the Government's own integrated review in 2021, threats to Government Departments, national infrastructure, British business and private individuals are growing and becoming ever more complex as states become more assertive in advancing their aims. The clause goes a long way towards updating the threat posed by modern-day espionage and the changes are long overdue. The Intelligence and Security Committee's 2020 Russia report stated:

"The current legislation enabling action against foreign spies is acknowledged to be weak. In particular, the Official Secrets Acts are out of date—crucially, it is not illegal to be a foreign agent in this country."

Nevertheless, it is important that the Government clarify a number of different aspects of the clause. I highlight two recommendations from the Law Commission's 2020 review of the Official Secrets Act. Recommendation 12.5 stated:

"In any new statute to replace the Official Secrets Act 1911, the requirement that the defendant's conduct was capable of benefitting a foreign power should continue to be objectively determined. There should be no requirement to prove that the defendant personally knew or believed that his or her conduct had such capability."

Will the Minister confirm that that requirement is compatible with the new offence established in clause 3?

The Law Commission also highlighted the danger of an individual unknowingly assisting a foreign intelligence service and then still being charged and convicted with the same offence as an individual who actively sought to assist a foreign intelligence service. This defence is currently accounted for in the Official Secrets Act 1989, as my right hon. Friend the Member for North Durham discussed. I appreciate that that Act is not being updated by this legislation, but the principle still stands. The Law Commission's recommendation 12.24 stated:

"The 'defence', currently contained in section 1(5) of the Official Secrets Act 1989, of not knowing and having no reasonable grounds to believe that the material disclosed related to security or intelligence, should continue to apply."

It is naive to think that foreign intelligence services advertise who they are and what they are planning to do with any information they are given by someone or in any engagement they may have. The duping of individuals is a somewhat common tool in espionage tradecraft. Let us say that an overseas business research company commissions a UK national to explain how the UK's parliamentary processes work, but it transpires that the business research company was working for a foreign intelligence service. Under clause 3, could the UK national still be tried for assisting a foreign intelligence service?

We welcome the exemptions in subsection (7) that create an appropriate space for democratic obligations and diplomacy to take place, especially as the Bill makes no distinction between countries that are our allies and those that are hostile and seek to undermine the UK's interests. However, I also note that the offence is explicit about the definition of a foreign intelligence service. On first reading, I had concerns that where someone is sharing information with a former member of intelligence services, the definition might not extend to criminalising that conduct. As the old saying goes, once a KGB officer, always a KGB officer.

However, given that the definition included in subsection (9) outlines that "foreign intelligence service" means

"any person whose functions include carrying out intelligence activities for or on behalf of a foreign power",

I understand that anyone sharing information with former KGB officers, for example, would be committing an offence. I would be grateful if the Minister could confirm that that is the case.

Stephen McPartland: That was a range of great examples, and I will do my best to address them. The whole purpose of the clause is to provide our world-class intelligence agencies and law enforcement with the tools to respond appropriately to activity conducted in and against the UK by foreign intelligence services that wish to cause us harm. Although the Government understand and appreciate the intention behind the amendment, we propose to reject it.

The distinction between activities taking place inside the UK and those taking place overseas was deliberate. For activity taking place overseas, clause 3(4) requires the conduct to be

"prejudicial to the safety or interests of the United Kingdom."

That is to ensure that we target the most harmful activity overseas that has an appropriate link to the UK. For activity taking place inside the UK, there is currently no requirement for the activity to be prejudicial to the safety or interests of the UK. However, taking into account the defence in clause 3(7), foreign intelligence service activity carried out in the UK without even informal agreement or assent is inherently prejudicial to the UK's safety or interests. Having to prove beyond a reasonable doubt why that activity is prejudicial risks creating a high evidential threshold that could, as we try to meet it, potentially compound the damage caused.

Clause 3(4)(a) has been drafted to ensure that the offence can prevent a wide range of activities from occurring and prevent threats from developing. Any legitimate activity would be covered by the three elements of the defence in clause 3(7), so there are appropriate safeguards in place. If a foreign intelligence service carried out activity in the UK and its conduct did not fall under clause 3(7), we must be able to call it out for what it is and prevent further harm from being caused. The current construction of clause 3(4) allow us to do exactly that, and the amendment risks reducing the operational utility of the clause as a whole.

We cannot allow the UK to become a hotbed for foreign intelligence services running covert and deceptive operations. I understand the examples that have been given, and I am looking into some of them, but the reality is that we need to be in a position to protect the intelligence services and give them an opportunity to go out there and deal with these people and the threats we face. As I have said, we have three protections throughout the whole Bill. We are coming up with lots of examples, but by answering each of them specifically, we will just provide our enemies and state threats with ways to work around the offence.

Stuart C. McDonald: I am grateful to the Minister for his response, but it is important to work through hypothetical examples so that we can understand the scope of the Bill. I absolutely get his explanation as to why there is a distinction between activity inside and outside the UK, and he briefly mentioned the idea of a friendly foreign intelligence service—in my example, the Estonian intelligence service—having permission to engage in the activities that I described. That may well be the solution. I will take away what the Minister has said. In the meantime, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Stephen McPartland: I beg to move Government amendment 1, in clause 3, page 4, leave out line 1 and insert—

"In proceedings for an offence under this section it is a defence to show that the person engaged".

The Chair: With this it will be convenient to discuss Government amendments 2 to 4.

Stephen McPartland: The amendment clarifies that clause 3(7) contains a defence, rather than an exception, because it may be unclear which of the two it is as currently drafted. In doing so, two changes must be made to the clause. One will insert new wording to show that clause 3(7) is a defence, and the other will insert subsection (7A), which states that the defendant must adduce some evidence to establish that a matter in clause 3(7) is satisfied. The prosecution will then be required to prove that it is not met beyond a reasonable doubt.

We tabled the amendments to provide clarity to the operational community and to make absolutely clear the intention behind the offence. Clarifying that clause 3(7) is a defence places an evidential burden on the defendant to adduce evidence that one of the three conditions in subsection (7) applies to them. If someone raises a defence under subsection (7), the prosecution will need to prove beyond all reasonable doubt that the defence does not apply.

There are three separate elements to subsection (7). If it is an exception, the prosecution would be required to prove in all cases beyond reasonable doubt that none of the three elements applies. That would potentially be challenging to evidence, given the wide range of circumstances under which the matters in the clause may arise. In effect, the prosecution would have to prove a negative. Where an offence is believed to have been committed and a prosecution is pursued, subsection (7) being an exception would mean that all three conditions would need to be shown not to apply in each case that is brought forward for prosecution. That is not our intention, and the amendment will mean that defendants must raise a defence under subsection (7), and the prosecution must then prove beyond all reasonable doubt that it does not apply.

We have worked closely with our operational partners, law enforcement and the Crown Prosecution Service on this amendment to provide greater clarity about the scope of clause 3. By tabling this amendment to subsection (7), we can more clearly represent the policy intention behind clause 3 as a whole.

Holly Lynch: I have the Minister's explanation. We considered the implications of Government amendments 1 to 4 earlier, and on that basis we are satisfied.

Amendment 1 agreed to.

Amendments made: 2, in clause 3, page 4, line 8, leave out "is" and insert "was".

This amendment is consequential on Amendment 1.

Amendment 3, in clause 3, page 4, line 10, leave out "is" and insert "was".

This amendment is consequential on Amendment 1.

Amendment 4, in clause 3, page 4, line 10, at end insert—

"(7A) A person is taken to have shown a matter mentioned in subsection (7) if—

(a) sufficient evidence of the matter is adduced to raise an issue with respect to it, and

(b) the contrary is not proved beyond reasonable doubt." *—(Stephen McPartland.)*

This amendment provides that a defendant bears an evidential burden in relation to the defence in clause 3(7).

Clause 3, as amended, ordered to stand part of the Bill.

Clause 4

Entering etc a prohibited place for a purpose prejudicial to the UK

Stuart C. McDonald: I beg to move amendment 50, in clause 4, page 5, line 9, at end insert—

"(7) No offence is committed under subsection (1) if the conduct is for the purposes of protest unless the conduct is prejudicial to the safety of the United Kingdom."

This amendment would restrict the circumstances in which access to a prohibited place for the purposes of protest would amount to an offence under this section.

The Chair: With this it will be convenient to consider the following:

Clause stand part.

Clause 5 stand part.

Stuart C. McDonald: It is obvious what the amendment is getting at: it is about protest rights, which were raised by my right hon. Friend the Member for Dundee East, who unfortunately cannot be with us today.

[Stuart C. McDonald]

We all broadly see what the Government are trying to achieve. Clause 4 builds on the Law Commission recommendations. It protects prohibited places against entry etc. for purposes prejudicial to the UK. Clause 5 criminalises entry etc. where there is no purpose prejudicial but where there is actual unauthorised entry. I will come back to why that is necessary.

However, as before, given that a person can receive a hefty 14-year penalty if they are found guilty of an offence under clause 4, we want to be clear about whether it has been drafted tightly enough. As with clause 1, issues are created by the breadth of some of the concepts, such as the safety or interests of the UK. Crucially, if a person even approaches or is in the vicinity of a prohibited place, they are at risk of committing this very grave offence if they have a purpose that they ought to know is prejudicial to the safety or interests of the UK. We must bear in mind that clause 8 allows for additional sites to become prohibited, not necessarily for the safety of the UK but to protect its nebulous interests. Again, there is that very broad concept.

In Chandler *v.* Director of Public Prosecutions, the plan of the folk being prosecuted was to enter a prohibited RAF station and prevent access to others, thus preventing aircraft from taking off. Unsurprisingly, it was held that, objectively, it was access for purposes prejudicial, even if the protesters themselves believed it to be in the interests of the state to get rid of nuclear weapons. It was decided that the interests of the state are not for the jury to decide on, but for the Government of the day.

Of course, many more protesters will approach or be in the vicinity of a prohibited place for peaceful protest with no intention of inhibiting its operations. Others want to cause a degree of nuisance—for example, in minor blockades, chaining themselves to plant pots—with no real risk to safety. The amendment simply asks what the new provisions mean for them. What is the Government's intention? Is a protest against nuclear weapons in the vicinity of Faslane, which the state currently believes to be in its interest, prejudicial to the interests of the United Kingdom? Would a minor blockade causing temporary inconvenience be in contravention of the clause? Surely these people are not to be convicted of such a serious offence, which carries up to 14 years in prison.

10.45 am

Our amendment would therefore exclude protesters from the scope of the provision unless they put safety at risk. If they do not, why not simply leave the issue to the policing and protest Bills that already exist? I have some problems with how the Government go about dealing with protests and policing, but that is for another day.

Finally, it is not clear to me what clause 5 adds to the current trespass offences, including under the Serious Organised Crime and Police Act 2005 and in particular the section 128 offence of trespassing on a designated site. Why do we need another trespass law? Why a longer punishment? What is the justification for that, and why are we seeking to punish people who simply did not know, but made a mistake?

Mr Jones: I sympathise with the amendment. In terms of legitimate protest, I may disagree with, for example, the peace camp at Faslane, but does it fall within the remit of the clause? Is that proportionate in an open and free society? I may disagree with what the protesters call for, but I would defend their right to make their opinions known.

We need clarity and to get the balance right between legitimate protest in the public interest and protecting security. The clause is detailed on access to prohibited areas. The clause states that a person commits an offence if they cause

"an unmanned vehicle or device to access"

an area. That is very clear. A drone, for example, would be prohibited. But what happens in the case of a trained eagle wearing a camera? I think that is covered by "device to access" an area. Will the Minister confirm that if someone strapped a camera to an eagle and sent it over a prohibited site, that would be covered by the Bill?

The clause is clear about inspecting

"photographs, videos or other recordings",

but how wide is the area? It would cover someone standing with equipment that had access from 20 miles away, but what about somebody just observing through binoculars? Would that be covered? How big is the prohibited area? If we are not careful, the points that the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East has raised could fall within the scope of the Bill, or be used by the Government to stop legitimate protest or people who have an interest in opposing activities taking place at a certain site.

Holly Lynch: The SNP spokesperson, the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East, and my right hon. Friend the Member for North Durham have outlined their thoughts on amendment 50. I will speak to clauses 4 and 5 more broadly.

Clause 4 establishes a new offence of entering a prohibited place for a purpose prejudicial to the UK. We welcome the measure, and the protection it will offer to sites and places that are vital to our national security. It has been a long time coming, and we have been falling back on somewhat antiquated legislation in the absence of such provisions. Giving evidence to the Intelligence and Security Committee in January 2019, the director general of MI5 said,

"The purpose of [a potential new Espionage Act] is to be able to tighten up on the powers that have become, you know, dusty and largely ineffective since the days of the Official Secrets Act, half of which was drafted for First World War days and was about sketches of naval dockyards, etc."

In his evidence on behalf of the Law Commission last week, Dr Nicholas Hoggard said

"One of our concerns about the existing offences in the 1911 Act was that the existing prohibited places—though extensive; it is an extensive and complicated piece of drafting—have a strong military focus, and they do not necessarily reflect the way that critical national infrastructure, for example, or sensitive information is held by the Government."—[*Official Report, National Security Public Bill Committee,* 7 July 2022; c. 51, Q96.]

Clause 4(2) sets out that,

"a reference to inspecting a prohibited place includes—

(a) taking, or procuring the taking of, photographs, videos or other recordings of the prohibited place;

(b) inspecting photographs, videos or other recordings of the prohibited place."

We heard some more innovative examples, as my right hon. Friend the Member for North Durham likes to think outside the box, and as those acting on behalf of hostile states will continue to evolve and adapt to the legislation that we progress through this place.

Clause 4(3) explicitly states that the offence applies if the person inspects a prohibited place

"by electronic or remote means",

and clause 4(4) states that the offence applies

"whether the person's conduct takes place in the United Kingdom or elsewhere."

The use of drones has been an asset in many ways, but inevitably a headache in others. I have raised concerns previously on behalf of constituents that it is at the extremes of distaste and disrespect for drone footage of serious or even fatal accidents to be taken by members of the public and shared on social media, or published by news outlets. It is with urgency that we need to update the laws that ensure national security is not compromised in the absence of up-to-date legislation, but for the reasons I have highlighted I hope this might also be the start of a conversation about drones, beyond their national security implications.

Clause 5 establishes that

"A person commits an offence if—

(a) the person—

(i) accesses, enters, inspects or passes over or under a prohibited place, or

(ii) causes an unmanned vehicle or device to access, enter, inspect 15 or pass over or under a prohibited place,

(b) that conduct is unauthorised, and

(c) the person knows, or ought reasonably to know, that their conduct is unauthorised."

The Opposition welcome this provision, and see it as a necessary step to protect sites that are vital to our national security. I would like to probe the Minister on the stipulation that a person who commits an offence "ought reasonably to know" that their conduct is unauthorised. There is a concern that an individual may unknowingly stumble on a prohibited place, and then be prosecuted in the same way as someone actively seeking to undermine UK national security. Further detail on the sentencing guidelines might allow us to work through that uncertainty, but we have to work with what we have in primary legislation. The chances of that occurring are made more likely by the fact that this stand-alone offence does not need the foreign power condition to be met.

Let me provide some rare light relief in today's proceedings. In 2016, civilians began to wander on to the grounds of several restricted air force and military bases in Canada while playing Pokémon GO, which is an augmented reality game where characters spawn randomly in the proximity of a user's location—it was all the rage at the time. Documents released on request to the Canadian Broadcasting Corporation revealed the military's confusion about what was happening at the time. One email from a major read,

"Please advise the Commissionaires, that apparently Fort Frontenac is both a PokéGym and a PokéStop".

He went on to say,

"I will be completely honest in that I have no idea what that is."

Just three days after the app's release, two men drove a van on to an air force base near Toronto just before midnight. A corporal confronted the occupants and found them playing with their smartphones. In another incident, one woman was found at the Borden base playing the game, while her three children climbed over tanks. In their attempts to get on top of what was going on, the documents revealed that one colonel wrote,

"There's a game out there taking off like gangbusters, and it requires people to move to digitally cached locations to get points".

I do not know what "gangbusters" means. Another security expert recommended they hire a 12-year-old to help them out with the problem.

As part of the military response, at least three officers at different bases were assigned the task of playing Pokémon GO on site, and logging the appearance of every gym, PokéStop, and wild monster. In what I thought was a particularly enterprising spirit, in my constituency of Halifax's namesake, they instead recommended that the PokéStop be relocated nearer to the museum, in the hope that it would increase footfall in a helpful rather than unhelpful way. I intended to share those examples by way of demonstrating that innocent players of Pokémon GO should be protected from the harshest of sentences, but on reflection, having read out the details, I am not so sure.

Back to the serious—I could not find specific examples here in the UK, but I can only imagine that there were some. We cannot afford to create carve-outs for Pokémon GO players that could be exploited by those acting on behalf of hostile states. The example outlines the need for appropriate consideration of such mitigations in the sentencing guidelines for such offences.

I note that the Law Commission proposed that in any reform of the Official Secrets Acts, a safeguard similar to that contained in section 131 of the Serious Organised Crime and Police Act 2005 should be introduced, requiring the Secretary of State to take such steps as he or she considers appropriate to inform the public of the effect of any designation order, including, in particular, by displaying notices on or near the site to which the order relates. That would ensure that an individual is given fair warning that he or she is approaching a location that is given enhanced protection by the criminal law. If I am not mistaken, that point was made by the right hon. Member for Dundee East on Second Reading. I hope that the Government will recognise the merit of doing so.

Maria Eagle: I have a short point of clarification for the Minister, if he would be so kind. It is about what is covered by the offence.

I am looking at clause 5(1)(a)(i), which states:

"A person commits an offence if…the person…accesses, enters, inspects or passes over or under a prohibited place".

Clause 5(3) clarifies further:

"In subsection (1)(a) a reference to inspecting a prohibited place includes taking, or procuring the taking of, photographs, videos or other recordings of the prohibited place."

Does that include someone who is off the premises with binoculars or some device to enable them to look closely at the prohibited place, without being under or over it? Does that include the old-fashioned spy looking through binoculars and taking notes, rather than taking photographs, or is that not covered by the clause? It does not seem that it is, but I might have missed something. I will be grateful for clarification.

Stephen McPartland: I may dwell on this clause slightly longer than others, because it is the first of a number of clauses regarding a regime to protect sensitive sites in the UK. There has been a range of examples and questions. To the hon. Member for Garston and Halewood, the simple answer is yes.

With regards to the Pokémon examples of the hon. Member for Halifax, the answers again are about—this very much determines the whole scope of the clause—prejudicial interest and people doing something accidentally. To fall foul of the clause, someone needs to have prejudicial interest against the UK. In the examples, people have wandered in and done something accidentally; they would not be prosecuted under the clause.

The right hon. Member for North Durham gave the example of strapping a camera to an eagle; if that is something that someone can do, fair play to them. However, if that camera strapped to the eagle were then to record activity in the place, and that was prejudicial to the UK, the person would be prosecuted. If they just wanted to strap a camera to an eagle to see what happened, the intelligence services have the opportunity not to prosecute someone, because, given the protections throughout the Bill, the Attorney General would have to sign off on whether to prosecute, and the Crown Prosecution Service on whether that was in the public interest.

I understand the point made by the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East on ability to have lawful protest, and for lawful protest not to be restricted. It has been reflected by other Members and I raised it with the Department last week.

Sally-Ann Hart (Hastings and Rye) (Con): It is absolutely right that people have the right to protest, but the attention of the Minister and that of the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East to the recent cases in which, for example, Extinction Rebellion protestors were found not guilty of criminal damage, despite the judge directing jurors that there was no defence in law. Likewise, the protestors who toppled the Colston statue were found not guilty. We have to be careful: jurors might find people not guilty, but we have to protect the ambitions of the Bill.

11 am

Stephen McPartland: I understand my hon. Friend's point, which is that we have to be careful to provide the intelligence services with the tools they need to protect our protected sites. I may not agree with the purpose of protest, but I agree with the ability of everybody to protest lawfully. People will start to fall foul of this clause when they try to scale the walls of a restricted site and to impede lawful activity going on at the restricted site—when they start to move from protest towards criminal activity. That will be captured.

Mr Jones: I am not sure it will. Let us take the Faslane peace camp as an example. I totally disagree with what those people are arguing for, but if somebody there took a photograph and put it out on social media to make a political point, would they be caught under the Bill? Is not that prohibited under the Bill?

Stephen McPartland: No, because they would not be doing something designed to prejudice the United Kingdom.

Stuart C. McDonald: That is useful and it might answer my question. The offence is committed if somebody approaches or is

"in the vicinity of a prohibited place".

That obviously covers the peace camp. Is the Minister saying that at that stage there is nothing prejudicial to the UK's safety and interests, and that such action only becomes prejudicial to UK safety and interests when people take further action, along the lines that he suggested?

Stephen McPartland: Yes. The intention is that people have to do something prejudicial to the UK's interests to fall foul of the clause.

Prohibited places are inherently sensitive sites that are likely to be the target of state threat activity. Unauthorised access to such sites could be a precursor to harmful acts such as espionage or sabotage, and it is important that we have the tools and powers we need to adequately protect those sites.

Mr Jones: I think the Minister just said yes to my question and the question of my hon. Friend the Member for Garston and Halewood about a person with binoculars. Does that fall under clause 5(1)(a)(i), which refers to an offence being committed if a person

"accesses, enters, inspects or passes over or under a prohibited place"?

Would somebody on a hill several miles away with a pair of binoculars be classed as inspecting an area? Is that why the Minister says that is covered in the Bill?

Stephen McPartland: Yes, that is the intention. Remember that the Official Secrets Act 1911 refers to sketches. We are trying to reform that Act and the others to get to a point at which we help our intelligence services to come up with ways of dealing with some stuff that could technically be considered out of scope. The idea behind the clause is that we will be able to give the intelligence community the tools they need to deal with somebody inspecting a site or doing something prejudicial to the UK's interests.

Mr Jones: I come back to the fact that if we looked at the Official Secrets Act 1989 and had one big Bill, it would have been far better than this one. Will the Minister clarify that somebody with binoculars would be classified as "inspection"? My hon. Friend the Member for Garston and Halewood asked whether a person looking at a site through binoculars would be captured by this offence, or whether they would have to be writing something down. What is the situation with the old-fashioned sketches mentioned in the 1911 Act? Would they be covered?

Stephen McPartland: The purpose is to cover activity that is prejudicial to the United Kingdom's interests. For example, if someone were bird watching and they looked at the site through their binoculars, they would not be captured by the offence because they would not be doing anything prejudicial to the United Kingdom's interests. However, if they were sketching a site to identify how they could break into it or to record activity going on there, that would be prejudicial to the United Kingdom's interests, so the clause covers that. It is a case-by-case situation.

The current prohibited places provisions fall under the espionage offence within section 1 of the Official Secrets Act 1911.

Mr Jones: The Bill is specific about procuring "photographs, videos or other". I understand why they are included: they are modern. If we pass the Bill, will sketches still be covered? Would it not be better to repeat that bit of the 1911 Act?

Sally-Ann Hart *rose—*

Stephen McPartland: I thank the right hon. Gentleman for his intervention and am happy to give way to my hon. Friend the Member for Hastings and Rye.

Sally-Ann Hart: Does my hon. Friend not agree that "other recordings" would include a sketch?

Stephen McPartland: Sketches are included, because a sketch would have to be inspected. The question was: are sketches included? The answer is yes.

Mr Jones: Where?

Stephen McPartland: Because a sketch would have to be inspected.

The Chair: Order. This really must not become a conversation. Minister, you might perhaps wish to conclude your remarks. We cannot have a conversation backwards and forwards across the Chamber.

Stephen McPartland: I agree.

Maria Eagle: Will the Minister give way on this point?

Stephen McPartland: A final time.

Maria Eagle: I regret having to ask more than once, but I am just not quite clear from the Minister's answers. Perhaps he could write to the Committee if it is not totally clear; that would not be a problem. In subsection (1)(a)(i), does inspecting include looking from a distance—not over or under—say through binoculars that magnify, if someone is doing that with a malign intent, so they are caught by subsection (1)(b), which are the other requirements of the offence?

Would just looking through binoculars from a distance—not taking videos or photographs—and just doing notes or a sketch still be covered, or are we creating a lacuna? That is the only question I seek an answer to. I am afraid the Minister has not been totally clear on how looking through binoculars is covered. We are not inspecting the sketch—we are inspecting the site through the binoculars. Is that not right? In which case, is it still okay for this person to do a sketch? It is not clear.

Stephen McPartland: I am grateful for the intervention and shall try to clarify. It is clear that the provision is not exhaustive, but the reality is someone has to inspect the site, whether that is through binoculars or making a sketch, and the purpose of that activity—that inspection—is to be prejudicial to the interests of the United Kingdom.

Maria Eagle: That is clear.

Stephen McPartland: I will move on to amendment 50. The condition inserted through amendment 50 removes the term "safety or interests of the United Kingdom" in the context of protests. It is the Government's view that this is detrimental to the offence under clause 4 as it limits the range of conduct that would be considered prejudicial to the UK and risks creating loopholes that hostile actors could use to exploit using protest as a tool to disrupt sensitive sites in the UK. It is also likely to mean that sites that are not directly involved in the safety of the UK would not be afforded any protection where protests are being inappropriately used to disrupt the lawful functioning of the site. It is crucial that we retain the existing term if we are able to effectively protect the UK's most sensitive areas from harmful activity.

In addition, the effect of amendment 50 would be that no offence would be committed by protesters if their conduct were not, as a matter of fact, prejudicial. In practice, this would not have any further effect on safeguarding protest activity because if the activity were not in fact prejudicial, a person cannot know, or be in a position where they ought reasonably to know, that that is the case. The amendment may be designed to ensure that no offence is committed unless actual damage results from the conduct, but it would not have that effect and the Government would not support a narrowing of the offence along those lines. While I understand the intention of the amendment, I do not see any requirement for it, given the fact that sufficient safeguards for legitimate protesting activity are already in place.

It is important to say that we will work with the police and the College of Policing ahead of commencement of the provisions to ensure that those implementing these clauses have the appropriate training and guidance to use these powers proportionately. I do not support the amendment and ask that the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East withdraws it.

Finally, clause 5 provides a second offence to capture harmful activity within the reformed prohibited places regime. A person commits this offence if, without authorisation, they engage in conduct at a prohibited place and they know, or reasonably ought to know, that their conduct is unauthorised. A person's conduct is unauthorised if the person is not entitled to determine whether they may engage in the conduct, or if they do not have consent to engage in the conduct from a person entitled to give it—for example, if they walk past signage stating that access to the site is prohibited without authorisation, or if they take pictures from outside the site in spite of clear signage that that is not permitted.

Holly Lynch: This is a question I asked members of the UK intelligence community because I could not answer it: does a list of prohibited places exist in the public domain? Such a list might equip someone with the information prior to arriving at a site and enable them to determine whether a place is prohibited. It is not clear to me whether a list exists. Can the Minister clarify?

Stephen McPartland: I am grateful to the hon. Lady for her intervention, and I will certainly look at that. A number of sites will be prohibited in law, and some sites will not want people to know exactly where they are and

[Stephen McPartland]

what they are doing because they will become targets. Once again, there is a balance to be struck in relation to provision for the intelligence community.

Holly Lynch: I completely accept the sensitive nature of the subject and why we might not want to put such information in the public domain, but with respect to the "ought reasonably to have known" defence, I wonder whether we should ensure that people are equipped with the information that a site is indeed prohibited before they find themselves, perhaps accidentally, in a compromising position. How can we ensure that all that is communicated appropriately and sensitively so as to protect people from accidentally falling foul of these stipulations?

Stephen McPartland: It goes back to the reasonableness test: is the person conducting a reasonable activity, or is the activity prejudicial to the United Kingdom's national security interests?

For a person to be guilty of the offence, the prosecution must prove beyond reasonable doubt that the person knew, or reasonably ought to have known, that their conduct—for example, in entering the prohibited place—was unauthorised, which provides protections. Unlike the clause 4 offence, there is no requirement that the person have a purpose prejudicial to the safety or interests of the United Kingdom to commit this offence. That ensures that action can be taken in cases when a person has knowingly carried out unauthorised conduct at a prohibited place, such as trespassing, without having to consider whether that person has a purpose prejudicial to the United Kingdom's safety or interests, which requires a higher threshold of potential harm to be demonstrated.

To take account of the fact that a purpose prejudicial to the safety or interests of the United Kingdom does not need to be proven, there are differences between the conduct caught under the offence under this clause and the offence under clause 4. For example, this offence does not criminalise the inspection of photographs of prohibited places, and it is not capable of capturing conduct in the vicinity of a prohibited place.

The Government do not consider it proportionate or necessary to capture the inspection of photographs under this offence, given that inspecting a photograph that has already been taken of a prohibited place cannot be classed as inherently unauthorised activity. Given the wide range of legitimate activities that could be undertaken in the vicinity of a prohibited place, and given that there is no inherent need for walking past a prohibited place to be authorised, the offence under clause 5 does not capture activity in the vicinity of a prohibited place.

The second prohibited places offence under clause 5 is a crucial addition to the tools our law enforcement agencies and courts can use to capture the full range of harmful activity that can take place at prohibited places. Even though this offence is not aimed at capturing the most damaging activity around those places, as clause 4 does, and attracts lower penalties, it is equally important that we introduce an offence that can capture activity that may seem less severe, but is still capable of interfering with and damaging the operations and security of the United Kingdom's most sensitive sites.

This offence should be seen as part of a tiered approach alongside the new police powers to protect those sites, which I will come to, and it will ensure that law enforcement has a range of tools and powers at its disposal to protect those sites.

Stuart C. McDonald: The debate has been useful, particularly in relation to protestors, and it is useful to know that, apparently, the Minister's view is that protestors approaching or being in the vicinity of a prohibited place will not necessarily engage the clause because, at that stage, the activity is not prejudicial to the interests of the United Kingdom. Something more is required before that part of the test is engaged. We might need to explore that further on Report, but for now it is important that we say protestors are not so interested in the Pokémon players. We can revisit that on Report. In the meantime, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 4 ordered to stand part of the Bill.

Clause 5 ordered to stand part of the Bill.

Clause 6

Powers of police officers in relation to a prohibited place

Question proposed, That the clause stand part of the Bill.

11.15 am

Stephen McPartland: The powers set out in clause 6 allow for a police officer to exercise specific powers in order to protect prohibited places. A person commits an offence if they fail to comply with an order imposed under the police powers in relation to a prohibited place. Those powers include the ability to order a person who has accessed or entered a prohibited place or is in the vicinity of one to leave it immediately. Under these powers, a police officer may also arrange for the removal or movement of a vehicle or device from a prohibited place or an area adjacent to a prohibited place.

Alongside the police powers, the clause provides that is an offence to fail to comply with an order given by a constable under those provisions. As an example, if a person is circling the perimeter of a prohibited place and taking detailed photographs of the infrastructure and activities within, the police may order this person to cease to engage in that activity and leave the area immediately, given that they are carrying out an inspection of the site and their activity is in an area adjacent to the prohibited place.

In order to exercise any of those powers, a constable must reasonably believe that doing so is necessary to protect the safety or interests of the United Kingdom. For example, exercise of the powers may be necessary for the prevention of activity that could harm or disrupt the operations or functioning of a prohibited place. In most instances, we consider that the use of these powers will be intelligence-led and that the police will be called to prohibited places where there is a concern identified from the site itself.

The aim of the police powers in relation to prohibited places is not to impede legitimate activity, such as lawful protest, but rather to catch and deter activity around prohibited places that is prejudicial to the safety or interests of the UK. That includes activity that is harmful

to and disrupts or impedes the functioning or operations of a prohibited place, such as scaling fences, blocking access points or wider disruption to the critical and sensitive work being conducted at these sites. Ahead of implementation, my officials will work with the police and the College of Policing to ensure that clear guidance and training are in place to ensure that the powers are used reasonably and proportionately to protect these sites.

The additional powers are a critical part of the reformed prohibited places regime and provide significant operational utility, given that they enable law enforcement to prevent harmful activity from taking place at these sensitive sites—activity that could be a precursor to state-threat offences such as espionage or sabotage. Without their inclusion, the UK will be less equipped to counter hostile activity as it happens, which will leave these sites more vulnerable to state-threat activity or wider threats that do not have a state link.

Holly Lynch: Subsections (1) and (2) set out the powers that police constables can exercise to protect a prohibited place, which include ordering a person to cease their activity or move away from the site. Subsection (3) provides that a constable must reasonably believe the use of those powers to be

"necessary to protect the safety or interests of the United Kingdom."

This includes prevention of activity that could harm or disrupt the operations or functioning of a prohibited place in a way that could jeopardise the safety or interests of the United Kingdom.

The clause gives the police powers to direct people to stop using devices and leave the area, but when I discussed its detail with a recently retired senior police officer he observed that the clause seemingly does not confer on the constable the power to seize the device or any video or images or, indeed, sketches or footage off the back of an eagle taken by the device. Can the Minister explain whether that is the case? If so, would the clause not benefit from an addition to prevent any such sensitive material from leaving the scene with a person instructed to take it with them?

I find it curious that all police officers tend to be referred to as "constable" in legislation, despite the fact that constable is just one of several possible ranks. Indeed, there is some variety in the responsibilities for keeping sites defined as prohibited places safe. The Civil Nuclear Constabulary, overseen by the Civil Nuclear Police Authority, is the armed police force in charge of protecting civil nuclear sites and nuclear materials in England and Scotland. The Ministry of Defence police is responsible for law enforcement and security of military bases in the UK; as it says on the tin, it reports into the Ministry of Defence.

Will the Minister confirm that the powers conferred in clause 6 extend beyond those officers serving in regular police forces that report to the Home Office? It is the specialist forces sitting outside of those structures that tend to pick up the lion's share of the responsibility for protecting prohibited places. Could he confirm that the powers apply to all officers, regardless of rank, and where the military also provide defences at their own sites, or are at least partnering in that work? Could the Minister explain whether the powers extend to the military, or are exclusively for police officers?

Finally, the powers conferred will also allow a constable to arrange for the removal of a vehicle from a prohibited place "or an area adjacent" to it. Does the Minister envisage any further guidance on what constitutes "adjacent to a prohibited place" to assist a constable in determining distance, proximity, and so on, in making those judgments and communicating those clearly in a reasonable way to members of the public?

Stephen McPartland: I am grateful to the hon. Lady for the very good points she has raised. My understanding is that the powers currently apply only to police officers, not to members of the military. It is very clear throughout the clause that it refers to "a constable", and it is referenced as "Powers of police officers".

Mr Jones: Is that not a hole in the legislation? We are coming on to Cyprus next, where it is not civilian police that do security there, and I can think of a few others around the world where it is done by the military. Therefore, should those powers not also be given to the military?

Stephen McPartland: When we talk about military, MOD police will have those powers.

Mr Jones: Yes, but a number of sites are not guarded by MOD police—although there are some—but are the responsibility of the UK armed forces, which are not police.

Stephen McPartland: Both the right hon. Member for North Durham and the hon. Member for Halifax made a very good point. We will take that away and look at it. If they want to strengthen the Bill, we are happy to work with them to do that.

Antony Higginbotham (Burnley) (Con): Would my hon. Friend agree that there is a difference between providing force protection for a site and providing constabulary and law enforcement duties?

Stephen McPartland: My hon. Friend makes a good point. We must also bear in mind that it is not our intention to introduce search-and-seize powers under these police powers. This is part of the tiered approach we referred to earlier, with the police being able to warn people to go away before they fall foul of the law. There is the opportunity to give them that warning before any arrest.

Mr Jones: I agree with the hon. Member for Burnley, but there are also sites that are benign, so it is not a force protection point but a constabulary duty that is carried out by members of the armed forces. Therefore, I think they need these powers if this is a comprehensive suite of powers.

Stephen McPartland: I am grateful to the right hon. Member. As I said, that is certainly something that we will look at and come back to.

Maria Eagle *rose—*

The Chair: The Minister has concluded his remarks, unless I am much mistaken.

Question put and agreed to.

Clause accordingly ordered to stand part of the Bill.

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

11.23 am

Adjourned till this day at Two o'clock.