PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

NATIONAL SECURITY BILL

Second Sitting

Thursday 7 July 2022

(Afternoon)

CONTENTS

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

not later than

Monday 11 July 2022

The Committee consisted of the following Members:

Chairs: † Rushanara Ali, James Gray

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

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

† attended the Committee

Witnesses

Carl Miller, Research Director of the Centre for the Analysis of Social Media, Demos

Sam Armstrong, Director of Communications, Henry Jackson Society

Louise Edwards, Director of Regulation, Electoral Commission

Professor Ciaran Martin, Professor of Practice in the Management of Public

Organisations, Blavatnik School of Government, University of Oxford

Dr Nicholas Hoggard, lead lawyer for the Law Commission's Protection of Official

Data project, Law Commission

Professor Penney Lewis, Commissioner for Criminal Law, Law Commission

Rich Owen, Access to Justice Committee Chair, Law Society

Poppy Wood, UK Director, Reset.Tech

Dan Dolan, Director of Policy and Advocacy, Reprieve

Public Bill Committee

Thursday 7 July 2022

(Afternoon)

[Rushanara Ali *in the Chair*]

National Security Bill

Examination of Witnesses

Carl Miller and Sam Armstrong gave evidence.

2 pm

The Chair: We will now hear from Carl Miller, research director of the Centre for the Analysis of Social Media at Demos, and Sam Armstrong, director of communications at the Henry Jackson Society. We have until 2.40 pm for this panel. Will the witnesses please introduce themselves for the record?

Carl Miller: Hi everyone. My name is Carl Miller. I am the research director for the Centre for the Analysis of Social Media at Demos. That means that my day job is trying both to build and then use technology to research the internet in different ways. I have been doing that for about 13 or 14 years now. I suppose most pertinent to the issues being discussed now would be the work that we have been doing for quite a long time trying to pull apart and understand illicit influence operations online and how they affect various aspects of British public life.

Sam Armstrong: I am Sam Armstrong. I am the director of communications at the Henry Jackson Society. I look after our work on China and I also serve as the director of strategy and communications at the Inter-Parliamentary Alliance on China, which I know a couple of members of the Committee are members of as well.

The Chair: Thank you. I call the Minister.

Q52 Scott Mann (North Cornwall) (Con): Welcome. Do you agree that the UK's ability to deter, detect and disrupt state threats will improve with the passage of the Bill?

Sam Armstrong: My fundamental answer is yes. There are a number of good powers in the Bill. It does not address every issue that some of our allies have wrestled with, but in so far as there are powers in it, all of them are in my view good and helpful powers, which will greatly aid the security services in their important work keeping us all safe.

Carl Miller: I will restrict myself from any broad observations and will keep to the one area that I actually know something about, which is to do with information warfare and influence operations, especially over the internet and social media, and how that might impact things. In so far as that is the case—I am sure we will dig into this more in a second—I do not see the Bill as doing any harm. In fact, strangely, as a centre-left think-tank, we have long been calling for more direct state activity in this area. We have deferred far too much and far too often to the tech giants to try to sort these kinds of problems out for us. My fear, though, is about how the Bill will be enforced and deployed. I do not think that in and of itself, as it stands, it alone will be enough to secure—digitally secure—elections and quite a lot of other important moments, themes and aspects of life against the kinds of online influence that we have seen.

Q53 Scott Mann: Could you expand a little more on the cyber-nature of those threats? What do we see and what do you need?

Carl Miller: If there is one thing to take away from any of my evidence it is probably this: we have completely misconceived—the Bill slightly, but generally in Government at the moment—the problem as one of disinformation. The problem is not overwhelmingly or primarily one of disinformation. When we pull apart these campaigns, ones that we know or highly suspect of being in one way or another sponsored or driven by, or of having interacted with, a foreign, usually autocratic state, we notice that disinformation is only one of a whole array of different methods that can be used to influence people. You can paint an extremely distorted picture of the world simply by amplifying some truths over others.

If we look at what is happening in Ukraine at the moment, it is as much about "Putin riding bear" memes as it is about explicit disinformation. Much of this interacts at the level of identity, belonging, kinship, friendship, reasons for getting up in the morning and the problems that people see in the world—hugely subtle. Even at the level of lying, it is less to do with the overt falsehood circulating on the internet and much more to do with the harnessing of false identities and false reasons for being involved in debates. I tend to view this as the emergence of a kind of shadowy tradecraft. It is one that can wrap together, yes, some disinformation, but also some black-hat search engine manipulation, the harnessing of outrage, things to do with identity, as I have been saying, and humour and comedy—all that is influential in different ways.

The way we often set up this problem is through a hyper-rationalist idea that there is this thing called disinformation that propagates online, people lacking digital literacy believe it, and that influences their behaviour and attitudes. I will shut up in a second. I rarely interview people, but I have interviewed some of the perpetrators that actually do these operations and they tell me one thing, time and time again. They say, "Carl, we don't lie about the world to get people to change their minds. We tell people things they already think are true about the world and then guide that in a particular direction."

The current influence operation in Ukraine is a brilliant example of that. What we are seeing is Russia or pro-invasion-linked influence operations targeting the global south, trying to portray the invasion as essentially being an anti-colonial gesture and tapping into deep-seated anti-western and anti-colonial attitudes within the audiences they are addressing.

Q54 Scott Mann: Sam, could you briefly describe the nature of the hostile threats that we see, how they have changed over the years and how you see them changing?

Sam Armstrong: Yes. In a sense, the threat is changing less so than our recognition of the change. Increasingly, we are waking up to the threat of the more all-encompassing nature of interference launched or directed by branches

of the Chinese Communist party. Unlike traditional Russian or Soviet Union espionage, this is not 100 or 200 individuals in the UK at any time running a network of agents in a very organised way. This is something more full-throated and all-encompassing—they call it the united front—in which people who would not ordinarily be, or who would not see themselves as being, operatives of a foreign intelligence state are being brought into it or are acting in it.

In addition, the nature of the way that we have woken up to this threat means that there are individuals acting on behalf of the Chinese state quite explicitly and openly who are also employed concurrently, and declaredly so, by public authorities in the United Kingdom, most particularly at British universities, where we have Confucius centres. That is one well known example. They are a branch of the Chinese state and they often take money directly from the Chinese state for their operations. People are double-hatting in roles in the academy there and in the university. That means there is the bizarre case of the British Government—not the British Government as in Her Majesty's Government, but public authorities at their largest—employing Chinese spies. The British state is certainly knowingly employing agents of the Chinese state.

Q55 Scott Mann: Will this Bill allow us to deal with that?

Sam Armstrong: This Bill will do an awful lot to deal with it. There are some offences in the Bill that are drawn extremely broadly and will allow the security services to take a knife to whichever problems they would like.

The Bill does not do certain things that other countries have done. For example, Australia introduced the Foreign Relations Act, which allowed the central Government to terminate relationships that public authorities had entered into with foreign states where they were undermining Australia's foreign policy position. That is a power that I know Australian officials have been keen to encourage the British Government to replicate.

In terms of assisting foreign intelligence services, which I think is by far and away the most broadly applicable offence in the Bill, and the trade secrets offence, there are broad powers there and the Government deserve commendation for bringing those powers before Parliament, although not before time. The security services have been keenly pushing for them and they will appreciate them in doing their work.

Q56 Holly Lynch (Halifax) (Lab): Carl Miller, you painted quite a distressing picture of the complexity and volume of the information that is being pushed online by foreign states. If it is not so much about disinformation or misinformation, but about the amplification of uncomfortable truths in a country, which then has a destabilising effect on society, how do we disrupt it?

Carl Miller: That is a great question. We can start by cleaning up the grubby world of spam. Often, when talking about online influence operations and disinformation, we descend into this kind of rarefied world of grand geopolitics, but it has as much to do with a very wide array of services and companies. If anyone googles "buy retweets now", you will be able to see what I am talking about.

There are a tonne of companies that operate in plain sight, selling social media manipulation as "social media services". You can buy fake followers; you can buy fake engagement. I looked it up on the way here; as of about 10 minutes ago, there was a company selling positive comments in Ukrainian on Instagram—mostly, they claim, by users from Ukraine—for $78 per 1,000. That is on the light net; we are not even talking about the services that are cryptographically secured or anonymised.

There is an array of these kinds of operations. An almost shadowy grey-area marketplace has emerged, which radically lowers the barriers to entry into doing those kinds of activities. That has always been there, but the consensus has emerged among researchers like me that, over the last year or two, the actual number, sophistication and variety of those services has increased quite dramatically. To be honest, if we were to really try to genuinely start increasing the cost and penalties for the actors that do that kind of thing, we would have to target that entire industry as participants in it.

Lastly, in pulling apart some of the operations regarding Ukraine, our hunch is that state-backed activities have likely made use of those exact same services. We will see states maybe rolling out capability outside of state, setting up as private companies, and selling those capabilities back into state.

Q57 Holly Lynch: Do you think social media companies are doing enough to identify the overseas networks that are pushing such content in the UK?

Carl Miller: I have spent 10 years saying the social media companies have not been doing enough on just about every matter of importance that I can possibly think of. They are doing a tremendous amount more now than before, but that has a couple of implications.

First, we have dramatically overfocused on Facebook and Twitter. There are reasons for that, and a lot of them are the fault of researchers like me. We research Facebook because it is big, and Twitter because it is easy to research. If you have a look at the journalistic stories that drive the awareness and debate, they are very often furnished by exposés and revelations about those two platforms.

If I were to point to one part of the internet that I am genuinely afraid about, it would be Wikipedia. If I were an information operation officer, I would have no idea why I was mucking around with Twitter. In Wikipedia, we have an open platform that is protected and serviced by an open community of people who can freely join. If I were a state, I would employ a phalanx of people to contribute completely legitimate edits to Wikipedia and build up their standing in the community, and then they could run for office within Wikipedia and start using the powers they would gain to change what is on Wikipedia and the policies that govern it.

There are lots of other such open-source communities, many of which, including Wikipedia, inform and drive the decisions that the tech giants make. They have not managed to build the kind of internal defensive teams that a Facebook or a Twitter can to try—often in the shadows and in secret; we do not know enough about what happens—to clear that kind of stuff off at scale.

Q58 Holly Lynch: Sam Armstrong, on China specifically, what types of activities should we be most concerned about here in the UK?

Sam Armstrong: The problem is that it is so broad, in that there are problems even in this building. The security services will tell you privately that—far beyond Christine Lee, who obviously was named—there are agents of the Chinese state here who are known to the security services and in whom they have taken an active interest.

There are huge problems in academia; China has made no secret of its interest in academia. When the Zhenhua database leak happened a couple of years ago—this was a database that China was using to identify potential targets of intelligence activity—it was no surprise that they had targeted think-tanks and academics very carefully.

The third and final area that China is very, very interested in is anything related to technology, and to the areas that it would like to obtain and that it set out in its "Made in China 2025" programme. Those areas are twofold. The first is universities and open research. There are researchers in the UK right now who are, frankly, working with branches of the Chinese navy to come up with devices to track nuclear submarines around the world. That is as dangerous as it comes to our national security, and that work is going on in the open. I am also aware of British companies that are making engines—or casings for engines in this case—that they have admitted are good for nothing other than for engines in tanks. There are grievous concerns about the whole level.

Where do you start first? Well, that is a choice between those that are dangerously undermining our national security and tech, and those that are dangerously undermining our democracy in accessing this building and in terms of the influence and space in which they are influencing our democratic process.

Q59 Damian Hinds (East Hampshire) (Con): Mr Miller, to come back to information ops, what do we know about scale of state-enacted or state-sponsored information operations specifically?

Carl Miller: One suggestion that I was going to make today was that we have nothing like a comprehensive picture. This is often extremely sporadic project-based research, and it is usually platform-specific, even though we know that, in all likelihood, that is not how the campaigns work—they will work across tonnes of platforms all at once. We will see only certain kinds of campaigns. We are broadly better at seeing broad-based campaigns addressing quite large slices of a population, but again, if we were to put ourselves in the mind of an influence operator, there would be much more targeted campaigns directed towards—if you will—higher-value targets as well.

What we know about scale is that many more countries than those we talk about are doing it. I understand that in the last Indian election, accounts attributable to every single mainstream political party were taken down by Facebook during that campaign. It has emerged as an almost mainstream campaigning tactic.

Q60 Damian Hinds: Sorry, but are you talking about domestic actors—domestic political parties in their engagement in domestic politics—rather than foreign state involvement?

Carl Miller: Yes. One of the reasons that I am hesitating is that, for researchers like me, clear and guaranteed attribution—outside the platforms—is unbelievably difficult, and I do not want to overstate. I can tell you that there are dozens upon dozens upon dozens of incidences, scenarios and narratives that we regard—reading the tea leaves of machine-learning patterns as we do—as suspicious. With the open data that is available to me, I cannot definitively link that back to a state. However, Twitter and Facebook, for example, have both disclosed dozens of campaigns that were—at least in part—likely targeting the UK, and linked them back to what they believe to be state actors.

Q61 Damian Hinds: When we talk specifically about foreign-interference information operations in countries such as the UK, we tend to focus on elections times, big democratic events, referendums and so on, but is there any reason to believe that something of a moderately comparable scale does not go on the rest of the time?

Carl Miller: No, there is not. In fact, I am sure it does, and that is one of the big trends we are seeing. We ran an effort over COP26, and we saw that there were certainly various kinds of organised attempts to manipulate big global thematic conversations about climate action, for instance. Given the barriers of entry into this world, I also do not think that it will be national elections; it might be quite small and local events that see some level of manipulation happening, too.

I will also point out one reality about how these work. One of the difficulties in seeing how the Bill—I am sorry if I have misunderstood this—might apply is its requirement that the actors involved have to be conscious that they are working on behalf of a foreign power.

Quite often, my suspicion is that you would have a state agency with various kinds of links with online actors, and there might be a whole chain, from a PR company to another more specialist digital consultant to a much spammier consultant, and that person might be the person reaching in and actually gathering together various kinds of functionalities, capabilities or services to do overtly illegitimate and malign forms of manipulation online. It might be very difficult; they might never know that a state is at the other end of the trail. With the companies that I mention—the ones selling large amounts of digital manipulation—I cannot believe that they do any kind of "know your customer" activity. I do not think that they have any idea who is employing them.

Q62 Damian Hinds: You talked earlier about what we might call the falsehood versus division distinction, and we had a good conversation about this with a previous panel of witnesses. This question is for you both: will you say something about how the use of those techniques varies between states, and what trends we are seeing?

Carl Miller: I cannot create a profile for how each state would approach information operations, to be honest. I do think that there is quite a high degree of heterogeneity among the actors involved. You have all kinds of different intelligence agencies, and military-based and political PR comms-based actors. One of the truisms is that it is a bit of a scattergun approach at the moment, where lots of things have been tried and they are attempting to evaluate them, and they do not really know which ones are succeeding and which are not. I am not quite sure if that is true or not.

The actual nitty-gritty of the techniques and technologies involved is probably the shadowiest part of this whole area. If the Bill were to be effective, something we need in parallel to it would be almost a digital influence version of the national risk register, where we have state support to pull apart and lay out where we think the genuine threats are and the genuine bodies of capability and technology that have been built to do this kind of stuff. It is very difficult for researchers in the open to do this by ourselves.

Q63 Damian Hinds: Mr Armstrong, with your China speciality, can you say anything about how that country's approach to information ops has changed or is changing?

Sam Armstrong: Yes. China initially began—there is some really interesting stuff that has only happened in the UK in this space. We had a university that for a very long time rather openly advertised itself as providing services and specialist media training to officers of the Chinese propaganda Ministry, among others—various branches of the Chinese state—right here in London, metres away from the BBC. You also have the Confucius centre picture, which is important.

Where China has actually done very poorly is in its direct Government-to-Government disinformation. Some of the stuff that you saw around "Wolf Warrior" or that the *Global Times*—its state international newspaper—puts out is very ineffective. What China is incredibly effective at is not really that disinformation or misinformation public communications picture, but identifying individuals of influence within academia, business or wherever, and building up close relations with them. They are invariably people of influence, who in turn use their own networks to say, "Well, look, I'd be careful of all this talk about China. They are the biggest-growing economy on Earth, we really need to trade with them and we shouldn't do anything to upset them at any point." In so far as I have seen, that is where the Chinese influence picture has been focused.

Q64 Maria Eagle (Garston and Halewood) (Lab): I have a couple of questions. My first is for both of you. You have said slightly different things about the Bill, but is there anything that is not in the Bill that you think ought to be there and that would make a difference in the field in which you are doing research?

Sam Armstrong: Yes, there are two things. The first is the foreign influence transparency register system. I note that there has been a promise that it is to come, but the devil will be in the detail on that because there is a series of policy judgments that have to be made—whether it is expansive, where the teeth bite and so on. It is incredibly important that it is seen quickly.

Secondly, there should be an ability for the Secretary of State, either of the Home Office or the Foreign, Commonwealth and Development Office, to intervene in known problematic institutional relations. There are excellent powers here, such as the individual prevention and investigation measures, but there is very little capacity when that is done more corporately—to go in and say not just to universities but to companies, which would be an expansion of the Australian power, "This arrangement is not in the UK's interest, and we are ordering you to terminate it." To say that is a glaring omission is perhaps overstating it, but those are the two powers I would really like to see.

Maria Eagle: Mr Miller?

Carl Miller: There is nothing I dislike in the Bill. It makes a lot of sense to criminalise conscious influence activities linked to foreign states, but we should not think that it will have an appreciable impact on the kind of illicit influence operations that we know are happening.

Q65 Maria Eagle: My second question is about the foreign influence registration scheme, which the Government promised they would introduce during the passage of the Bill through the Commons. However, we do not quite have a Minister at the moment, apart from Mr Mann, who probably has not been deeply involved in the policy decision making thus far. I may be doing him wrong, but as a former Minister I know that it takes a bit of time to get up to scratch in a new brief.

Mr Armstrong, you obviously think the foreign influence registration scheme would help a very great deal. Mr Miller, would it make any difference to some of the issues that you have been discussing if it were clearer that some of the actors that work in social media that you have been talking about had to register?

Carl Miller: No, it will not. Identity is being hijacked and used at a very great scale, so we do not know who these actors are. To be honest with you, the way to start to reduce this activity is to try to create some cost and penalties for the people who do it. They are not doing it from the UK. The nature of the internet is that crime on the internet, like anything, passes unbelievably easily across borders, almost without being noticed. The way forward will be for us to create ways of reaching beyond our own borders and increase the costs. This might sound strange for a think-tanker to say, but we need to increase cyber-offensive activity against the criminal architectures that allow this kind of work to happen.

Q66 Maria Eagle: Are there powers that you would like to see in the Bill that are not in it and might help with some of this?

Carl Miller: It is difficult, because the web of powers that the intelligence agencies have to use cyber-offensive activity—various kinds of online action, such as device interference—is spread out across a number of different pieces of legislation.

One of the difficulties is that online influence operations are so widespread and common that most of them would probably not pass the thresholds for the intelligence agencies to become interested and engaged in them. That is one of the difficulties that we have with cyber-crime in general. A tremendous amount of it happens, but so much of the capability to do something about it is concentrated within GCHQ, and not in the police services that have to handle most of it. Sorry, that was a slightly amorphous and broad answer.

Q67 Maria Eagle: That is fine. Finally, Mr Armstrong, is there a foreign influence registration scheme out there that you think would be particularly helpful to import into this legislation? What is the best example?

Sam Armstrong: The Australian scheme is by far and away the best example—in my view, the US FARA system is not a good comparator—and it is a shame that we have not taken the opportunity to bring it in sooner. The Australian high commissioner in London was George Brandis, who was the Attorney General

who wrote that very Bill, and I know he was keen wherever possible to impress on the Government that he was there and ready to help. I am sure that offer has not dissipated.

Q68 Sally-Ann Hart (Hastings and Rye) (Con): I have two questions, if there is time. First, Mr Miller, you mentioned people who are employed online and you said that you do not think those people have any idea who is employing them. Clauses 13 and 24 state that

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

and

"the foreign power condition is met…if… the person knows, or ought reasonably to know, that"

it is a foreign power. Do you think that should be widened to include an element of recklessness or recklessness?

Carl Miller: I think doing anything that might compel any of the services involved to do any kind of due diligence on the people who are employing them can only be a good thing, although the general point I am making is that I don't think criminalising activity within domestic legislation has been a particularly effective way of changing what people do on the internet, especially when those people are largely concentrated in jurisdictions that do not have any co-operative relationship with British law enforcement.

I remember I spent time with a number of cyber-crime teams across the UK and, in the words of one cyber-crime police officer, "If you are in Russia, the cost or penalty of doing cyber-crimes against British citizens is basically nil." This is not going to be an effective way of reaching beyond our borders and addressing where we believe a large number of actors doing this kind of thing are; they are not doing this from the UK.

Q69 Sally-Ann Hart: On that point and the concerns you mentioned earlier about enforcement and deployment, and that the Bill is not enough alone, what would you propose? Will you expand on that point?

Carl Miller: Sure. First, we need to change the intelligence picture slightly. We should integrate SOCMINT—social media intelligence—within the national strategic intelligence picture. We overlooked open-source intelligence—

Sally-Ann Hart: But that is not to do with this Bill, is it?

Carl Miller: Sorry, I thought you asked me— Would you like to hear what I think?

Sally-Ann Hart: Yes, carry on.

Carl Miller: Partly it is to do with changing our national knowledge of where these threats are and who is doing them, so the integration of intelligence. Then, as I said, there should be a national risk register and possibly the creation of powers for parts of the intelligence establishment to undertake direct activity against some of the technical architectures that allow this to happen.

Sorry to delve into the technicalities for a second, but for instance residential proxy IP addresses are a very important way in which this stuff happens. Residential proxy IPs are toasters and fridges and stuff. Basically, they each have an IP address and many of them are hijacked. They are the kind of things you that you use if you want to fool a social media platform into thinking that you are 10,000 people from around the planet when you are not—you are one operator sitting in a particular country. These are criminal architectures that have been amassed and rented out and sold to people, and I am sure they are rented out by some of the actors who seek to do influence operations. These are the kinds of things that we need to target. Putting pressure on that kind of asset is the kind of thing that will probably not get rid of them, but will meaningfully increase the costs of this kind of activity.

Q70 Gary Sambrook (Birmingham, Northfield) (Con): The Government tabled an amendment to the Bill to make "foreign interference" a priority offence in the Online Safety Bill. Do you think that will go some way towards addressing the concerns you have raised today?

Sam Armstrong: Yes, I think so. Imposing a duty on the social media companies is one of the only immediate tools and levers we can pull. I take Carl's point; I do not think it is going to be sufficient to deal with the hordes of people overseas who are, frankly, conducting quasi-military-type activities against the UK through cyber means here, because criminal law is not the tool for that. Should they exist and are they necessary? Yes. Are they sufficient? Probably not.

Carl Miller: It is just massively insufficient. The reason why is that the platforms, however rich, clever or large they are, cannot reach beyond the platforms themselves. That is the problem. The way we have tried to respond to this problem so far is to have Facebook take down accounts, but take-down is a very weak response. That is essentially being priced in to those kinds of activities. They have developed methodologies for setting up or acquiring new accounts as they go. In principle, I am not hostile to platform regulation across a range of online threats, but for those problems where we are dealing with a set number of actors who have specific capabilities and tap into a specific and constantly evolving tradecraft, I do not think it is going to be the tool to make much difference.

Q71 Ben Everitt (Milton Keynes North) (Con): We have covered a lot of the ground that I wanted to talk about. Several times in your answers, Karl, you have alluded to the fact that whatever we do the pitch is so complex that we cannot deter. What is it in the Bill, which you said you have no problems with, that you like about detecting and prosecuting—if deterrence is not contained in the Bill?

Carl Miller: The main thing I would say that the state can step in to help with is around attribution. That is something that we cannot do without state powers. It is something that, at the moment, only the tech giants do, and that is only linked to take-down. If we were to have any prospect of either taking direct cyber-action, or actually bringing criminal prosecution, it would be something that we need. One big thing here is around data access—I am sure you have had other panellists talk to you about that before. To foreground that, I have come here as a researcher whose job it is to do that kind of research, and one of my main things is that we know so little. We know nothing about TikTok—it makes none of its data available. Facebook makes some of its data available, and that is why we have some picture of it. Twitter makes a lot of its data available, and that is why we have a bigger picture.

TikTok is enormous, likely very influential, anecdotally there is tonnes of Ukraine-invasion activity happening on it now, and it has absolutely no application programming interface available for researchers in any way, whatsoever. By the way, there are also rumours that Facebook is withdrawing some of the data access that it currently gives researchers. I am sorry; I know this is ranging far beyond the scope of the Bill. However, to put this on your radars, I think that legislators may have to step in sooner or later to compel platforms to maintain data availability. Otherwise, even the very small window we currently get is going to continually shrink.

Q72 Ben Everitt: The Online Safety Bill can cover those points as well. Sam, have you got any comments on that?

Sam Armstrong: Yes, I would say that we should actually open this up. One of the best things about the Ukrainian war—there is not much to take solace in—is that defence intelligence has been publishing daily information that has been countering many of those problems. That is a really good thing; we have seen it work and it is wonderful.

We saw a foreign intelligence asset, Christine Lee, regularly making use of this place and having worrying relations with Members of this House. That continued right up until MI5 published a foreign interference alert about her. She is not alone; a number of countries have foreign intelligence and influence assets operating in and around here. There are a number more from the country that sent Christine Lee.

It has been a few months now. If you want to deal with this problem, the fastest way is some sunlight and disinfectant. Let us see a routine publication of those individuals that lengthy, hugely expensive but necessary investigations launched by MI5 have established—beyond MI5's doubt, at least—are engaged in foreign interference.

The Chair: Order. That brings us to the end of the allocated time. I thank our witnesses for coming in today.

Examination of Witness

Louise Edwards gave evidence.

The Chair: We will now hear, via Zoom, from Louise Edwards, director of regulation at the Electoral Commission. We have until 3 o'clock for this session. I would be grateful, Louise, if you could introduce yourself for the record.

Louise Edwards: Thank you. My name is Louise Edwards. I am the director of regulation at the Electoral Commission.

The Chair: Thank you. I call the Minister.

Q73 Scott Mann: May I ask you about—it might be interesting for the Committee to understand—the Electoral Commission's key functions in relation to the threats of foreign interference?

Louise Edwards: Of course. We are, fundamentally, an organisation that oversees the running of elections in the UK. We also have a role as the civil enforcement and regulator body for political finance in the UK. For foreign interference, that means that we are the experts on electoral law, electoral finance and the running of elections, and we offer that advice to law enforcement and indeed to the security services, on request. We are not a national security body per se. We do not have an intelligence function per se. It is really a question of working with the intelligence services or law enforcement where we can to offer them that advice.

Q74 Scott Mann: Can you describe the threat of foreign interference in our elections, as understood by the commission?

Louise Edwards: As I said, we are not a national security body, so our knowledge of the threat of foreign interference in the UK is very much based on what law enforcement and the police tell us, essentially. If you think about elections in the UK, we have not been notified by the security services of any successful attempts at foreign interference in UK elections, and I think we take some confidence from that.

On the political finance side—the money that is going in and out of political parties, campaigners and others involved in our democracy—I caught the end of the previous session and there was reference to one notification from MI5 in that area. That is the only one that we are aware of. However, I would say that it is not a matter to be complacent about. There are things that could be done, particularly on the political finance side, to really modernise and improve the safeguards in the system, not just for foreign interference but for any kind of abuse or interference in the political finance regime.

Q75 Scott Mann: I have one more question, if I may. The Bill introduces a new offence of foreign interference, which will criminalise interference in the UK political process. Do you see value in increasing prosecuting options in that area?

Louise Edwards: There is a key principle here, which is that you could hope there is a link between increasing the penalty that can be imposed for an offence and therefore disincentivising or deterring people from committing that offence. That seems like an in-principle link that you would want to see made. That is what perhaps the Bill is aimed at creating.

The measures in the Bill—the offences relevant to elections that are in it—are offences that the police will have to investigate and that will then go through the courts for prosecutions, so really key to making the provisions work effectively is to ensure that the police have the capability and capacity to take them forward, investigating them and passing them on to prosecutors when appropriate.

Q76 Holly Lynch: May I probe a little further to get a better understanding of the role of the commission sitting alongside enforcement agencies in this area? If you were to be made aware of a potential problem, where would the referral to you usually come from?

Louise Edwards: Do you mean a potential problem in the sense of a foreign state interference issue?

Holly Lynch: Yes, foreign interference.

Louise Edwards: Okay. If we were made aware of that, it is likely that it would be from the intelligence community or the police, because they are likely to be the ones that would have that information.

If we think about the sorts of offences that are being considered in the Bill, they are broadly around, if we look at the political finance ones, for example, the people who put money into the political system. In political finance, you have the people who are making donations and the people who are receiving the donations, that being the political parties, campaigners and candidates. For donors—the people putting the money into the system—the regime as it currently stands has a set of criminal offences that broadly sit with law enforcement rather than with the commission.

We, as a civil regulatory body, have a set of sanctioning powers for political parties and campaigners, so if we were to be notified of an instance of foreign interference—money coming into the political system from a foreign state power, say—our first response would be to discuss the matter with law enforcement, which would then decide whether to pursue it.

Q77 Holly Lynch: Have there been instances when you have referred something for further investigation to the enforcement agencies?

Louise Edwards: That is how the process would work. It is very common for civil regulators to have a route into law enforcement for anything that is a criminal matter. In fact, a number of offences in electoral law are both civil and criminal, so even now, before the Bill goes through, we would hand anything involving a foreign state power over to law enforcement to take forward. If the Bill goes through, we will have to hand that over to law enforcement anyway, because the offences listed in it will be investigated only by law enforcement, not by us.

We have a good, established process to notify police forces around the UK if we think that a matter is for them to look at and decide whether to investigate. We have very strong links with police around the UK through which we can do that.

Q78 Holly Lynch: Can you give us any sense of the volume of cases you are looking at in this space? As we anticipate this problem increasing, would it be to the commission's advantage to have any further resources to assist you?

Louise Edwards: The answer to your first question is quite simple: we are not looking at any instances of foreign interference at the moment.

The second question is a very good one. If I may be so bold, I do have an ask. One of the challenges when working with law enforcement is that we do not have effective information-sharing powers. One of the things that the Bill would achieve is to bring the police in particular further into the political finance enforcement regime by making the listed offences matters for them only, rather than for us at all. We need a more effective information-sharing power under which we can just hand evidence straight over to the police, unlike at the moment. Currently, it is like we have to say to the police, "Can you please ask us for the evidence information that we want to give you?" If we could cut through that with some decent information-sharing powers, it would make the process an awful lot more straightforward.

Holly Lynch: Thank you. There is an awful lot for us to look at closely there.

Q79 Damian Hinds: You mentioned a moment ago that we know of no examples of successful interference in elections. Can you unpack what you mean by "successful"? Do you mean changing the outcome?

Louise Edwards: The intelligence community have not notified us of any successful attempts to interfere in UK elections. As I mentioned, the Electoral Commission is not a national security body—we do not have intelligence functions—so when it comes those matters, we receive the information rather than creating it or analysing exactly what it means.

Q80 Damian Hinds: I realise that this is not your end of the business, but I do not think anybody would claim that there has been no small "s" successful interference in the democratic process in the sense of—I do not know if you heard our earlier session—winding people up, making them think they have less in common than they really do with others in society, and all those sorts of things. I do not want to put words in your mouth, but I think what you mean is actually changing the outcome of an electoral process. Is that right?

Louise Edwards: That is my understanding of what the intelligence community mean when they tell us that, yes.

Q81 Damian Hinds: I have questions about a couple of things that you have been talking about. I suppose that money coming into the political system depends on our definition of "political system". A lot of the activity we are talking about probably involves a lot of money in one way or another, but it never actually penetrates the boundaries of what we call our political system.

We talk in other contexts about regulating political advertising—meaning adverts placed by political parties that are registered under the Political Parties, Elections and Referendums Act 2000—but in reality, political parties' advertising is a very small fraction of the total online influencing that goes on in the run-up to elections. What is your expert assessment of how the whole political arena is changing? How do our institutions and our legislative approach need to change to keep up?

Louise Edwards: That is a very interesting question—how long do I have? The political finance side of the regime—I will unpack what I mean by that in a moment—is very much focused on the concept of regular and routine transparency that is enhanced significantly around an electoral event—an election, essentially.

When we talk about the political finance regime, we are talking about a defined set of actors: registered political parties, third-party campaigners, candidates or other members of political parties, and those who have specific responsibilities under law, including regular donation-reporting obligations. For example, political parties have to tell us about their substantial donations on a quarterly basis, and we then publish all that information.

When it comes to elections, as I am sure you know, there is a period in the run-up to elections called the regulated period. Any spending on campaigning that happens during that period—obviously, it gets more intense the closer you get to polling day—also has to be reported to us and gets published so that people can see it.

However, you are right that that is only one side of the nature of influencing or of the wider concept of political campaigning in the UK. There are some really

interesting questions there around whether it is sustainable to look only at detailed spending in the run-up to an election, when you might well argue that political campaigning these days is year-round rather than in the run-up to particular polls.

There is also another side to it: how do you define regulated political campaigning and the spending that has to be reported? Back in 2018, we did some work with voters looking at what they thought about online campaigning specifically. One thing we found was that quite often voters did not realise that something they saw online was actually trying to influence their vote, because it was not immediately obvious on the face of the piece of literature that that was what was happening.

In terms of how things might change or develop in the future, there was a bit of thinking done about this in the Elections Act 2022, which introduced what we call "digital imprints". They are a little bit of text that goes on a message online and says, "This was produced by this person, on behalf of this person, paid for by this person," so you can see that it is a political advertisement. It is that level of detail and transparency that now needs to be applied.

Q82 Damian Hinds: To be clear, to which actors does the digital imprint requirement apply?

Louise Edwards: It applies to anybody who is putting out regulated political material, so it would be political parties, third-party campaigners and candidates. The regime is fairly comprehensive, although not entirely comprehensive. I realise I am going slightly outside the scope of this Bill, but there is opportunity to make it more comprehensive and to really make it clear to voters every time they see a little bit of campaign material online who is paying for it. So it is those established actors who are—

Q83 Damian Hinds: Exactly, as long as they are part of our regulatory framework.

Louise Edwards: Yes.

Q84 Maria Eagle: We seem to have fairly decent regulation for participants in elections. We all know what imprints are, let us put it that way—anybody who has been elected knows what an imprint is. Some of the effort to perpetrate disinformation—to use a blanket term—whether that is successful or not, does not come from people who want to abide by the rules or who are keen to get their imprint on their material; that is precisely what they are not doing. Do you have any views about how we make it clear what is going on? In that respect, do you think that the foreign influence registration scheme that we are promised will be brought in during the Commons stages of the legislation will have a positive impact on identifying people who are trying to do this, or not?

Louise Edwards: You have hit upon one of the hardest issues here. Broadly speaking, people who are within the regime already—the established actors we have been talking about—comply with the law. Many of them, in fact, already put digital imprints on their online material, even though it is not yet a legal requirement to do so. The challenge is those who are perhaps based overseas or who do not want to play by the rules, basically. There are real enforcement challenges there, particularly when you are thinking about organisations or individuals based overseas.

If I go back to the recent Elections Act, one of the provisions that the Government brought in at that point was to lower the spending threshold in elections for people who are based overseas to £700: if you are an overseas entity, you can spend up to £700 campaigning in our elections, then that is it—that is your spending threshold. The problem is that, from our point of view, that can only really be symbolic, because it is virtually impossible to enforce spending at that low level. Even if we were to identify an overseas organisation spending in UK elections, they are overseas, so we have no enforcement powers that we can use to try to stop them.

I am painting a fairly awful picture, but there are some ways to tackle it from a slightly different perspective. For example, we have recently started launching a campaign before elections that is helping voters to look at online material with perhaps a more critical eye, to try to assess whether they should let it affect their vote and to give them a place to find out how to express concerns about that material, with the hope then being that we can perhaps raise confidence in legitimate digital campaigning while at the same time giving people an outlet if they see something they think is illegitimate. There is also a fair amount of work that you could do around political literacy at a very young age with voters, to help them to have that kind of critical perspective.

You mentioned the registration schemes. As a civil political finance regulator, our remit does not extend to matters of lobbying and influence, but one thing I would say, if I may, is that when it comes to the integrity of our democracy and voter confidence in it, transparency is key. Any registration scheme that brings more transparency around who is seeking to influence those involved in our democracy can only be to the benefit of the confidence of voters.

The Chair: Are there any other questions? Okay. I thank our witness for joining this Zoom call and for giving evidence. We will move on to the next panel.

2.58 pm

Sitting suspended.

Examination of Witness

Professor Ciaran Martin gave evidence.

3.1 pm

The Chair: We will now start our next session and hear from Professor Ciaran Martin, professor of practice in the management of public organisations at the Blavatnik School of Government at the University of Oxford. We have until 3.20 pm, so if colleagues could keep the questions succinct, I would be very grateful—then we can get in as many of you as possible. Could you introduce yourself for our records, Professor?

Professor Ciaran Martin: Thanks very much, Chair. My name is Ciaran Martin. As you say, I work at the Blavatnik School of Government at the University of Oxford. From 2014 to 2020, I served on the board of GCHQ, and I was the first chief executive of its National Cyber Security Centre.

Q85 Scott Mann: Professor Martin, thank you very much for appearing in front of us today. You are credited with being a significant proponent of transforming

[Scott Mann]

the UK's approach to cyber-security. Do you welcome the approach taken in this field to tackle all factors of hostile activity by foreign states?

Professor Ciaran Martin: Thank you for your kind words. I broadly welcome this Bill. There are a serious of fairly antiquated pieces of legislation that—sometimes at the margin, sometimes a little more profoundly—inhibit the pursuit of hostile-state threats, because they are, in effect, pre-digital legislative frameworks, very simply. With some of the language, you are replacing words like "maps" with words like "data", or at least adding words like "data" to words like "maps". You are dealing with things such as the flying of unmanned drones over sensitive sites. Despite my previous experience on the inside of the national security side of Government, when I read the explanatory notes, it was a bit of a double-take to be reminded that we had to explicitly criminalise assisting a foreign intelligence service in this country.

I think it is a very sensible piece of legislation, with the modernisation and some of the tidying up. From listening to your exchanges with the Electoral Commission, I think the provisions around disinformation and interference in political and democratic processes are really difficult to get right, so I welcome this sort of process. I think the intent is obviously cross-party and commands widespread support. The intent and basic provisions should be uncontentious, but I think some of the detail is going to be quite tricky.

Q86 Scott Mann: With your extensive knowledge in this space, it would be really interesting to have an understanding of how the threat has changed since you have been in your position.

Professor Ciaran Martin: When I say scale, I actually mean scale in its very precise meaning about volume. Digital espionage involves the extraction of information on a scale that was hitherto inconceivable, and that has, therefore, extended the scope of that. For example, there are specific references in the legislation to commercial and trade; we have seen that.

One of the changes that digitisation has brought, in terms of hostile foreign intelligence, is that it is possible to inflict large-scale strategic damage on the UK remotely, but it is not always done remotely. There are hybrid elements—there can be activity on the ground in the UK that assists digital espionage and digital penetration of the UK. Our existing legislative framework does not allow for that to be prosecuted. Even when it is done entirely remotely—for example, the People's Republic of China has done some of its operations entirely remotely—we have seen from the United States that, although it is not transformative, it is a useful policy lever to have a framework of criminal law that criminalises activity even in eventualities where you will not realistically be able to apprehend a named human being.

To be a bit more succinct, the large-scale extraction of and interference with data is essentially the risk. The willingness of nation states—principally Russia and China, to a lesser extent Iran, previously but not so much recently North Korea, and a bunch of up-and-coming potentially hostile states—to do that has been a very significant feature of the national security landscape over the past decade, as the head of MI5 and so forth emphasised.

Q87 Scott Mann: How big is the risk to the UK of disinformation?

Professor Ciaran Martin: One sees only the tip of the iceberg when there are major breaches. I will use a well-known example from the United States—a close ally that is perhaps easier to talk about because it does not involve disclosing sensitive things about the UK.

The hybrid operation against the United States in 2015, which the US Government at the time acknowledged formally was undertaken by the People's Republic of China, involved the extraction of more than 20 million security clearance records from the United States Office of Personnel Management—effectively the civil service department of the US Federal Government. It was the security clearance application forms of everyone who had applied for security clearance from the US Federal Government in the first 14 years of the century. As a dataset, it is incredibly rich. For example, if you are part of a commercial data breach, it is likely to be just your name and email address—possibly a password, although perhaps not even that, and possibly the last four digits of a credit card. If you go through a Government security clearance process, it is everything.

Think of the current politics of the US and China, and think about the established fact that the Chinese Government have this dataset of US Government personnel, with lots of information about them. You can see the strategic impact that that can have. To the best of my knowledge, based on public scholarship and disclosures relating to that incident, it was a largely remote operation, but it did include some activity on the ground. You can see how the sort of legislation we are talking about here might be useful in at least deterring or being able to deal with that.

Q88 Holly Lynch: Further to some of the points that you were making, I think it was the Russia report that identified that, as this hybrid activity becomes an emerging threat, we could be doing more internally and in Government to streamline Departments' responsibilities for different areas of the response to cyber—whether it is policy development or offensive or defensive cyber—alongside some of the powers here. Do you think there is more we can do internally to try to get a grip and pull all that together?

Professor Ciaran Martin: I would say this, wouldn't I, but there has been a reasonably decent trajectory of controlling it.

There is a challenge for defenders. If you are attacking—if you are Russia and you have a programme of destabilisation of the UK through these sorts of means—it is all the same programme to you. But if you are defending against it, the defence of the networks of a privately owned critical infrastructure company, such as the energy grid, is one problem, and the protection of sensitive Government networks—diplomatic cables and intelligence services—requires you to do something slightly different.

Disinformation is a different problem again, because historically under our laws, quite rightly, it has not been an offence to make up a lie and put it on the internet. That is different from a cyber-attack. Putting it under a single organisation is really quite hard.

Things were starting to get better around the time of the end of my Government service in 2020, although there is probably some way to go, on the synthesis of operational cohesion—the sharing of information—across these different parts. It is better than it is in quite a lot of other countries—it is less siloed—but I am sure, Ms Lynch, that there is plenty more that could be done to improve it.

Q89 Holly Lynch: Given some of the conversations we have had with the prior witness panels, are there other examples of best practice from around the world in respect of the influence of foreign states, particularly online? Have other countries—other legislatures—got some of the answers that we perhaps do not have in this legislation?

Professor Ciaran Martin: A lot of countries have struggled with it, and it goes beyond just legislation, if I am honest. In terms of things like disinformation, quite interesting were some of the things that the French did in 2017, when there was the Russian attempt to do something and they deliberately sort of cast doubt on the integrity of it. They knew the information was being, in effect, data dumped, but they are believed to have done some alterations so as to cast doubt on the authenticity of the whole thing.

In terms of civic society and discourse, in advance of the 2020 election the *Washington Post* editorial board did something really interesting. Although it did not come to pass in the way that it did in 2016, they issued a proactive statement to say that if they received very sensitive political information but from a suspect source that was likely to be a foreign intelligence service, they would treat it differently from, say, a leak from within the United States—they might sort of print it differently. There is a discussion about how we handle the outcomes of disinformation, on the assumption that it might happen. That is one idea.

On the other hand, on the duties to protect within Government, for example, we are not always very good at gradations of harm. When I started in the civil service at the end of the last century there was still this approach that any leak of any data was potentially quite serious. These days, there is far too much information to take that approach—things are going to leak all the time. We need to focus on an understanding of harm caused and the duty to protect the most sensitive information.

Q90 Antony Higginbotham (Burnley) (Con): Thank you for your time, Professor. We talked with a previous panel of witnesses about the so-called Confucius institutes, and there was discussion of the fact that the British state may be inadvertently employing agents of foreign powers. Given your work in academia, what are your views on those institutes? Do you think the Bill should seek to restrict or criminalise them?

Professor Ciaran Martin: It is for your detailed scrutiny to work out whether you think that activity that is clearly on behalf of a hostile state is adequately deterrable and punishable by this Bill. It is quite clear, from both my previous job and discussions and concerns in academia, that it is a target sector—of course it is—for hostile foreign powers, particularly China.

I have to say that even before I went to work for a university I thought it was a very, very hard thing to leave to universities to police. I am not a legal expert, so I do not know how this is going to work on the ground, but the question is: does this Bill provide a sufficient legislative framework to deter some of the actions? There is plenty in the Bill that says that damaging foreign intelligence activity in this country is unlawful, and that would obviously include the academic sector. Whether that sufficiently captures activity is an interesting question.

I think it does help, but it is probably quite tricky to specify, if you like, academic institutions as distinct from general malevolent activity in whatever the sector may be. It is a question worth asking, though, because the sector that I work in now is clearly of significant interest to hostile intelligence services in all sorts of different ways, including in respect of people and individual areas of research. That is one of the key threats that legislation like this is designed to counter.

Q91 Antony Higginbotham: Given your role in academia now, do you think the sector would welcome the Bill providing more clarity on the legal position?

Professor Ciaran Martin: I do not mean to be flippant, but obviously there could be as many different opinions as there are academics. I think that Government providing clear frameworks, laws and guidance to universities without infringing on academic freedom is where I would want to be. I do not think that it is fair to rely on universities to police this activity. It is extremely difficult in open and collaborative research environments like universities to be able to identify what is malevolent activity. If they do, it is extremely difficult to know where to go, what the relevant laws are, and so forth. The combination of a clear legal framework and clear guidance to universities is something that I personally would welcome. I imagine quite a few people, particularly in sensitive areas like technological research, would absolutely welcome that.

Q92 Sally-Ann Hart: You said earlier, looking at the increasing concerns about China and cyber-espionage, that the Bill will be useful against the threat from China, but do you think that the Bill will make the UK safer from the cyber-espionage threat from China, or will we require enhanced offensive capabilities?

Professor Ciaran Martin: They are not mutually exclusive. The thing about offensive capabilities is that they are sometimes seen as almost symmetrical—cyber is a sort of enclosed boxing ring, where you have offence versus defence—but offensive cyber can be used for anything. Our own British Government's one declared offensive cyber-operation was against so-called Islamic State, not against the cyber-capabilities of another state.

I need to be reasonably careful about what I say here, but if you think that the US's offensive cyber-capabilities are largely in the Cyber Command and the UK's in the National Cyber Force, the GCHQ-MI6-Ministry of Defence partnership, one would expect that the operational security of those capabilities to be pretty good and therefore make quite hard targets for other actors. Similarly, some of China and Russia's offensive cyber-capabilities against us will have quite good operational security, which will make them hard targets. We cannot rely on offensive cyber-capabilities to stop other people, particularly at the top end of the spectrum, at the elite nation-state level.

There is no magic panacea in the Bill, because no magic panacea is available. Even in the areas we were talking about, such as completely remote activity, one of the things that we saw anecdotally—there is some emerging research to support this—was that when the US in particular had a legal framework, where it can prosecute and indict people in absentia, in China and to some extent Iran, that did have some impact for some time. It did not solve everything, but it did affect the behaviour of some actors—they could not travel to the west, most practically, because they were under indictment by the US and therefore all the US's allies. It meant that the associates of these people, because digital infrastructure is global, could get arrested.

Some people working with Russian groups have been arrested in eastern European countries with which we can co-operate in law enforcement terms. Strengthening that sort of legal framework gives you something. It is probably more incremental than transformative, but it is still something.

The Chair: Damian Hinds, very briefly.

Q93 Damian Hinds: Professor Martin, one of the core aims of this legislation is to bring our counter-espionage capability up to date with the modern world. You spoke a little earlier about data theft in the context of the US Government and police. Will you briefly say something about how technology has changed states' espionage capabilities and how we need to respond?

Professor Ciaran Martin: Why is so-called data sovereignty such an issue? There are all sorts of reasons in economics, but one of them is that the location of the storage of data is really important. Data centres are massive strategic assets and a vulnerability for any sort of country, and you can see that combined effort. Why did we have such a big debate about the role of Chinese technology in UK infrastructure? It is because of the potential—never mind 5G and so on, but rather in things like smart cities—for data to be siphoned off covertly and so forth. It is possible.

There are stats to show, if you had compromised the International Atomic Energy Agency in Vienna and you went in there, how much you could photocopy versus how much you could steal electronically. There is now the possibility and, in some cases, the practice of comprehensive strategic compromise of huge, important datasets and sensitive strategic knowledge across all sorts of sectors by a combination of mostly digital but sometimes human-enhanced means. Until now, as you say, Mr Hinds, we have not really had a legislative framework for it. This Bill does provide a no doubt improvable such foundation.

The Chair: That brings us to the end of this section of questions. On behalf of the Committee, I thank our witness, Professor Ciaran Martin. Thank you very much.

Examination of Witnesses

Dr Nicholas Hoggard, Professor Penney Lewis and Rich Owen gave evidence.

3.21 pm

The Chair: We will now hear from Dr Nicholas Hoggard, Professor Penney Lewis and Mr Rich Owen. We have until 4 o'clock for this session. I would be very grateful if the witnesses introduced themselves for the record.

Dr Nicholas Hoggard: Hello, I am Dr Nick Hoggard. I was the lead lawyer for the Protection of Official Data project at the Law Commission, which was the project referred to us by the Cabinet Office. It informs a number of the offences in part 1 of the National Security Bill.

Professor Penney Lewis: I am Professor Penney Lewis. I am the criminal law commissioner at the Law Commission, so I led that project in its latter stages.

Rich Owen: I am Rich Owen. I am here today in my capacity as the chair of the access to justice committee for the Law Society. I am also director of a pro bono law clinic, the Swansea Law Clinic, which is part of Swansea University, and the chair of a regional advice network for Swansea, Neath and Port Talbot, which was set up by the Welsh Government.

Q94 Scott Mann: Thank you very much for being with us this afternoon. The Law Commission undertook a review, and the result of the review has fed into this Bill. Do you agree that we as a Government have responded to the Law Commission's recommendations on the Official Secrets Act and made the right legislation?

Professor Penney Lewis: That is a great question. This Bill implements the first part of our report, which was concerned with the espionage offences. I think it is worth saying that we did not envisage that any one statute would implement all the recommendations that we made in that report, even were the Government minded to accept them all.

The second and third parts of the report concern unauthorised disclosure and the role of the public interest in relation to unauthorised disclosures. We understand that the Government are still considering those recommendations. But in relation to the espionage recommendations, yes, this Bill implements our recommendations. There are minor differences, which is to be expected as part of the parliamentary drafting process, but we are very pleased that the Government have accepted those recommendations.

We had several concerns about the existing offences; as the previous witness mentioned, they were not fit for the current threat. The focus, for example, on enemies was unhelpful. It did not—does not—fully reflect the nature of the threat against the UK. It also risks causing offence to states with which we are not at war. We had concerns about the territorial ambit of the offences, which are addressed by this Bill—the offences in part 1. We were also concerned that there were not sufficient culpability thresholds, such that individuals might be prosecuted for the existing offences without being sufficiently culpable. We are pleased to see that those thresholds have been raised in the offences in the Bill.

Dr Nicholas Hoggard: As a matter of generality, I think Penney has it absolutely right: the offences reflect well the recommendations that we made. As Penney said, there are some differences that will arise naturally in the course of drafting and negotiating with parliamentary counsel, but our view is that the spirit of our recommendations has very much been carried through. There is probably not much more I need to add at this point.

Q95 Scott Mann: One final question from me: I would welcome your reflections on some of the new powers to address some of these state threats, particularly the investigatory powers and STPIMs.

Professor Penney Lewis: I am afraid that I will be less happy about that question. The Law Commission was asked to look at the Official Secrets Act. The project's terms of reference focused on official Government data, so we have not looked at those matters. There are a number of matters contained in the Bill that were well outside the scope of our project, and I am afraid that we just cannot comment on them.

Q96 Holly Lynch: Thank you for your time today. Can I take you through some different parts of the Bill for your assessment? Perhaps Dr Nicholas Hoggard could answer, as I have had a good look through the chunky read that is the "Protection of Official Data" report and given your work on it. Clause 8 gives the Secretary of State the ability to designate somewhere as being a prohibited place to protect the safety or interests of the UK. Are you comfortable with some of the definitions and powers there?

Dr Nicholas Hoggard: Yes, I think we are. 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.

There are some powers for the Secretary of State that exist under the 1911 Official Secrets Act, but they are quite restricted. What is good to see about the powers under this Bill is they are quite principled powers. The basis on which the Secretary of State can define something as a protected place is much more transparent. There are just three limbs that are easy to understand. That basis for affording the Secretary of the State the power is much more useful. It is more transparent, but it also enables us to capture within the offence places where there is actually a real risk of harm arising from hostile state activity.

On that front, I would say the power is good in so much as it aligns with the spirit of our recommendation. The fact that there will be parliamentary oversight of this process is important. It was a fundamental feature of our recommendations, and the negative resolution procedure is an important part of that process. The Secretary of State's powers are more effective than is permitted under the current law, but also there is sufficient oversight.

Q97 Holly Lynch: So you do not think the ability to do so in the interests of the UK, as well as for its safety, gives some quite sweeping powers, which would be open to challenge?

Dr Nicholas Hoggard: I do not think so. We gave some consideration to the differences throughout the project in many different parts of legislation between, say, national security and safety, and interests of the state. There is a risk that one ends up swimming in a sea of semantic exercises and trying to work out what the differences and permutations might be. The requirement to consider what might be necessary to designate a prohibited place in the context of the safety or interests of the state is an important power. I do not think it affords unlimited sweeping power to designate anything.

I think safety or interests of the state still make up a relatively confined subset of consideration. It does not enable somebody to start thinking about, in very broad terms, what might be necessary. I suppose the concern, which was raised by Government at the time and some of the stakeholders, was that if you frame these considerations in the context of national security alone, that might unnecessarily narrow the inquiry. Our position is that safety or interest of the state is consistent with a lot of the wording that already exists within the Official Secrets Act, it is consistent with the wording in some of the Bill and it avoids what might risk being an unduly narrow focus on national security.

Q98 Holly Lynch: Can I probe other panel members? There are a number of areas where we talk about the UK interest here. Do you think there is any merit in separating UK interest and Government interest in the event that you have information that will embarrass Government but would not be putting UK national security to any detriment? Is there merit in separating those two principles?

Professor Penney Lewis: The espionage offences here really do not fall into that category. The kinds of offences that you are talking about are the ones currently in the Official Secrets Act 1989 that are about unauthorised disclosure, where there is legitimate concern about information that is embarrassing. Indeed, we recommended a mechanism for authorised disclosures to an independent statutory commissioner, which would have appropriate investigatory powers to look into, for example, disclosures that might be embarrassing to the Government.

However, in relation to these offences, they have with them conditions that relate to the purpose of the person committing the offence that take them outside of someone who is leaking information, whether to embarrass the Government or not, and focus them squarely on someone who is acting to help a foreign power. I think we are in a slightly different realm here: the realm of espionage and not the realm of leaks.

Q99 Holly Lynch: Thank you. Can I ask for your thoughts on clause 23, which is on the extension of powers to the security services? The security services feel quite strongly about that and we have heard from them earlier today around encouraging or assisting offences. Did you have any thoughts at the Law Commission about that?

Professor Penney Lewis: Sadly, no. That was not within the scope of our project. It really exceeds the focus of our project on official Government data, so we did not make any recommendations in relation to those kinds of powers and we do not have a view.

Q100 Damian Hinds: I turn to Mr Owen, briefly, to ask about the forthcoming foreign influence registration scheme. From your perspective, what would be your hopes on behalf of the legal profession for that scheme and do you have any concerns?

Rich Owen: We think the solicitors' profession should be subjected to the scheme in just the same way as any other, although we would like an exception on grounds of legal professional privilege. This is an ancient common-law right going back 400 years or more. It is also regarded as a human right and as a corollary of everyone's right to receive legal advice and assistance and we feel it plays a crucial role in the proper administration of justice.

To be clear on what we mean by legal professional privilege, it is communication between a client and lawyer whose dominant purpose is to seek legal advice, or a communication between a client and lawyer in anticipation of pending or actual litigation. We therefore think that if there is a foreign influence registration scheme without legal professional privilege, then solicitors acting for foreign states or foreign state-related actors, such as companies controlled by or influenced by foreign states, would have to disclose documents. We think that profoundly compromises the rule of law and the fairness of trials, and will affect the relationship between client and lawyer.

I think it is easy to forget that legal professional privilege is not a privilege for solicitors or lawyers; it is for the client. Of course, clients want to be open with their lawyers when they are seeking advice, and we think this scheme would inhibit that openness. Of course, very often, the reason why they want to be open with their lawyers is that they want to know how to comply with the law, rather than breach it. That is why an exemption is needed in any such scheme.

Q101 Damian Hinds: What would the loopholes or potential unintended consequences be to such a provision, and how would you guard against them?

Rich Owen: It is important to know the limits to legal professional privilege. It cannot be used to further a crime—because of the so-called "crime-fraud exception" or the "iniquity exception"—so if a solicitor advances an assertion of legal professional privilege in bad faith, then they are not in a privileged situation and could potentially be charged with conspiring to pervert the course of justice.

Legal professional privilege would complement any scheme. The Home Office consultation on a possible scheme said it would respect the human rights framework. That privilege is an ancient common-law right. It is has also been recognised as a human right. The consultation also said that a scheme would not interfere with legitimate activities. It would be a legitimate activity to seek advice from your lawyer and not have that advice disclosed. If anyone was furthering that for espionage purposes, then that would not be a privileged situation; they would be acting outwith legal professional privilege.

Q102 Damian Hinds: So you are not saying that you think that lawyers should be exempted from registering? Your objection is specifically about disclosure of documentation.

Rich Owen: Yes. Well, we are looking for something similar to the Australian scheme. The Australian legislation specifically exempts legal professional privilege, as well as seeking legal advice and assistance. That sort of model, which expressly exempts legal professional privilege, would be a suitable way forward for the scheme.

Q103 Sally-Ann Hart: I just want to look at the provisions relating to arrests without warrant, which is in clause 21 and schedule 3. The provisions relating to that include the ability to delay access to a solicitor and delay notifying a person's family of their detention. Based on similar provisions for terrorism suspects, do you regard that as proportionate and necessary? Can I go to Dr Hoggard first?

Dr Nicholas Hoggard: You can, although I am afraid I will have to be very boring. Speaking with my Law Commission hat on, we are limited in what we can say with respect to those things that did not form part of the scope, regarding the protection of Government data. I am very sorry; I do not mean to be deliberately unhelpful, but we do not really—

Q104 Sally-Ann Hart: Can anyone answer that?

Rich Owen: Well, those provisions are modelled on terrorism legislation, when they concern a serious risk to the public, and there are suitable safeguards attached to them as well, so the position of the Law Society is to regard that provision as proportionate.

Q105 Sally-Ann Hart: Okay, thank you. I would just pick up, Mr Owen, on something that Mr Hinds mentioned about the FIR scheme and legal professional privilege. I was a bit confused; can you clarify if the FIR scheme would help prevent abuse of legal professional privilege, or are you saying that lawyers would be exempt from that?

Rich Owen: I was saying that an exemption on grounds of legal professional privilege, or seeking legal advice and assistance, could not be used for espionage, because you are outwith legal professional privilege. You are seeking to advance a crime, so that does not come within the ambit of legal professional privilege.

Q106 Sally-Ann Hart: I only ask that because I know that with the sanctions against Russian oligarchs there was a bit of confusion over that generally.

Rich Owen: Yes. There has to be access to justice for everyone, including rich people. They can communicate with their lawyer, and if they need advice on the law, that should be privileged. However, if they are seeking, through their communication with lawyers, to advance a criminal offence, then that is outwith legal professional privilege.

Sally-Ann Hart: Thank you for the clarification.

The Chair: We have a little more time if anyone has any further questions?

Q107 Holly Lynch: Perhaps I can return to my previous discussion with Professor Lewis on the issue around UK interests and Government interests? Putting aside the issue around leaks, I want to think about the "Assisting a foreign intelligence service" elements in clause 3. I will use a hypothetical. If there is a Foreign Secretary who has met with a former KGB officer, and you have that information and want to put it in the public domain—an outrageous example that would never happen—would the Government have grounds to say that, in disclosing that, you have acted against UK interests rather than Government interests? That is despite the fact that there was no material advantage to a foreign intelligence service or detriment to UK interests.

Professor Penney Lewis: I am sorry but I am going to be very boring again. The offence in clause 3 is not the implementation of one of our recommendations. It is one of the offences that was outside the scope of our

project. The main espionage offences that are in the existing Official Secrets Act, which implement our recommendations, are in clauses 1 and 4 of the Bill.

Dr Nicholas Hoggard: I will add to that without going outside our own remit, but thinking more broadly about the distinction between UK interests and Government interests. To re-emphasise a point that Penney made earlier, the essence of espionage offences lies in that purpose prejudicial. That is why we see in those offences that have the purpose prejudicial element—where your purpose is prejudicial to the safety or interests of the United Kingdom—that the sentence is so much greater.

The mens rea—the fault element—of those criminal offences lies in that purpose prejudicial. You need not only your purpose but to have known, or ought to have known, that your purpose was prejudicial to the safety or interests of the UK. Also, you must have known, or ought to have known, that you were acting to benefit a foreign power on behalf of a foreign power. Taken together, it is that essence that makes those offences substantively different from the sort of behaviours that might embarrass a Government—or a Government Minister. That sort of thing often falls for consideration within unauthorised disclosure offences, but it is not really the meat of an offence focused on the active interference with the proper safety or interests of a state.

Regularly throughout the project we met with a number of the UK intelligence community in Cobra with the Government security group. The evidence we heard of the nature of hostile state activity does not really have a bearing on the sort of material that sometimes gets disclosed that might embarrass Government Ministers. They are two quite different creatures.

Q108 Damian Hinds: Turning to Law Commission colleagues, you have conducted a very comprehensive review of the four Official Secrets Acts. Let us set aside the Official Secrets Act 1989, which is, as you rightly say, in a different category, because it is about disclosure rather than espionage. Looking at the Acts of 1911, 1920 and 1939, I think it would be useful for the Committee's deliberation to hear a little about how you went about your review and what you learned along the way—perhaps about if you conferred with your equivalent commissions in other countries and what you heard about the changing nature of the threat that we are trying to deal with and so on.

Professor Penney Lewis: Maybe I will start with the high level and then Nick can come in with a bit more detail. I should preface my answer with a slight caveat. This project started in 2015. Nick joined the Law Commission in February 2019 and I joined in January 2020, so while we were heavily involved in the final report, neither of us were involved in drafting the consultation paper or in the consultation period, which happened in 2017. None the less, we have read the consultation responses, and I can also talk slightly more generally about how we go about doing a consultation.

We were asked to take on this project. The way we work is that we undertake a pre-consultation investigative phase where we talk to stakeholders. That involved Government stakeholders, including Government security stakeholders. We talked to a lot of academics who work in this field. We talked to the media, because obviously they were particularly interested in the 1989 Act, and various organisations that are interested in freedom of expression and open government. We then drafted a consultation paper, which contained provisional proposals for reform. We put those out to public consultation. We had a three-month consultation period, and we had a number of consultation events during that. At the same time, we are continuing to talk to Government security colleagues, as Nick mentioned.

We eventually came to an agreement with Government security colleagues about how they would brief us about the details of the threat facing us without us then being in a position where we would have to say in our report, "Well, we have heard all this secret evidence. We can't tell you what it is, but trust us that these are the recommendations we think will safeguard the security and interests of the UK", and without also putting the security and interests of the UK at risk. We agreed a confidential briefing process that involved Nick and me. We then also agreed the disclosure by Government of hypothetical examples that they had drafted to represent the real threats that they told us about confidentially and securely.

Throughout the report, there are hypothetical vignettes that illustrate particular risks. Those are the Government and intelligence services' creatures, but they were the way in which we were able to reflect the reality of the threat. We then considered the consultation responses and the information we had had from the Government security group. We actually changed a number of things we had said in our consultation paper, so in between the provisional proposals and the recommendations there are a number of significant differences, particularly in relation to the 1989 Act. We then published a report in 2020, which contained our final recommendations for reform.

Dr Nicholas Hoggard: I will go into some specifics of what we learned, which is generously open-ended. What Penney says is correct; there were a number of changes that followed the consultation paper, come the final report. One of the major reasons for that was our engagement more substantively with confidential material and representatives from the UK intelligence community—UKIC—and across a number of Departments. It became increasingly clear to us that the scale of the threat was of an order of magnitude that, even in relatively recent integrated reviews, had not really been reflected. That scale really comes from the cyber-threat. I do not want to repeat what far more sophisticated witnesses said earlier in respect of that, but it also became increasingly clear to us that the way in which very capable state actors were wielding that cyber-threat meant that certain of the original provisions we had made needed to be reconsidered.

One example of that would be the extraterritoriality provisions, both in relation to the espionage offences and the unauthorised disclosure offences. The nature of the way in which cyber-information is held—of course, cyber-information now basically means all information—has changed. The existing offences under the 1911 Act and its ancillary Acts are now almost quaint in the way that they perceive espionage as something that happens on our territory. Of course, that is simply not the case anymore. These extraterritoriality provisions, though relatively unusual for criminal offences, are none the less vital if we are to capture the sort of behaviour that we see now. I think the process we went through

in engaging with UKIC was actually vital for the understanding of, and background to, some of the recommendations that we made.

The Chair: If there are no further questions, can I thank our witnesses? We will now move to the next panel.

Examination of Witness

Poppy Wood gave evidence.

3.52 pm

Q109 The Chair: We are now going to hear from Poppy Wood, UK director of Reset.tech. We have until around 4.20 pm for this session. Could you introduce yourself for the record?

Poppy Wood: Good afternoon, everyone. My name is Poppy Wood, and I lead on UK public policy for an organisation called Reset. We are a philanthropic organisation that focuses on digital threats to democracy. We have a particular interest in disinformation. I was a civil servant about 10 years ago, and have worked in tech and, at times, in cyber-security over the past decade. I am pleased to be here today to talk about some of our work as it relates to the Bill, particularly our research on disinformation and state actors.

Q110 Scott Mann: Thank you, Poppy, for being here this afternoon. Do you agree that the Bill strengthens our protections against co-ordinated, state-backed disinformation?

Poppy Wood: That is a good question, and one I hope is being asked every time that we are looking at new versions and new clauses of the Bill. When the consultation came out last year, those of us who had worked in state-backed disinformation for a while were delighted to see some of the questions being asked, at least in the first instance, about the role of state actors and about foreign interference.

When Ken McCallum said last year in his annual threat report that our adversaries are really good at using co-ordinated behaviour to probe UK vulnerabilities, and that we in return really need a holistic response to that—that was about a year ago—a lot of us thought, "But we're not. It's great that they are, but we certainly aren't. No one is really gripping this." That echoed language from the ISC report in 2020—the Russia report, which said that co-ordinated disinformation and state-backed interference is a really hot potato. No one wants to grip it—not GCHQ, not DCMS, not the other security services. It is too difficult, so we were really relieved to see the Bill come forward, and the consultation late last year.

We were even more relieved earlier this week to see that there will be a link between this Bill and the Online Safety Bill. I have not yet seen that amendment brought forward by the Government; I am hoping that is happening now, because we expected to see it yesterday—I hear the Government have been quite busy this week. That is really about saying that the Home Office and DCMS recognise the role of social media in pushing these co-ordinated campaigns, that electoral interference and foreign state interference is a priority, and that we are seeing platforms being weaponised in order to push the sort of disinformation you mentioned in your question.

We have seen that time and again. In the Scottish referendum in 2014, the Free Scotland 2014 campaign turned out to be backed by Russian and Iranian actors. They were massively weaponising social media by putting up inauthentic accounts and Facebook pages, with mocked-up pictures of the royal family, saying they wanted to take all the money from Scotland and buy new houses. It was complete nonsense, the aim of which was to destabilise the Union.

The Free Scotland 2014 campaign was called out by Twitter and Facebook in 2018. So four years later they said, "Hey, we've just found all these accounts that were trying to destabilise the Union four years ago", and we were going, "But what did you do about that four years ago?" I think we are going to see that again in Northern Ireland, we saw it in the US elections in 2016 and 2020, when the US Senate said that Russia was targeting African-American electors as a priority, to drive division in the States, and we will see that in any election we have in the UK.

I am really pleased to see that the Government are trying to link the two Bills. I think there are three words missing from both the Bills, and they are "co-ordinated inauthentic behaviour". This Bill and the Online Safety Bill might be getting towards those words, but one of them has to say them, because we are talking about individuals and organisations in this Bill and social media in the Online Safety Bill, but the examples I have just given are absolutely about co-ordination.

It will be hard to find one person. The extra-territoriality provisions in this Bill are good, but we should not be measuring the success of this Bill as people in prison. This is all about troll armies abroad, so the link is important, but I think it needs to go further on specifically calling out co-ordinated inauthentic behaviour in either or both of these pieces of legislation.

There are some questions about case law linked to the Online Safety Bill and the National Security Bill. In the amendments, we are expecting, hopefully today, for foreign interference to be listed as a priority harm in the Online Safety Bill. The question arises of how social media platforms, which will now effectively be given the power to police these kinds of things, will catch foreign interference when, as the Online Safety Bill says, the

"content amounts to an offence".

How can a social media platform judge how content would amount to a criminal offence?

We need to think about some of the language around how people identify that criminal offence. I think Carnegie UK, or another group, has suggested something along the lines of illegal content meaning content that the provider has "reasonable grounds to believe" amounts to a relevant offence. I do not think that "amounts to" has the precedent, and it is going to be hard, particularly in content law, to catch that.

The other thing about the Online Safety Bill and the National Security Bill is that we may end up seeing the case law being made in the civil courts, because we will see Ofcom taking a case against a platform, that platform appealing and the case being handled in the civil court, even if it involves foreign interference and a criminal offence. That needs to be thought about. I certainly do not have a solution, but I just want to flag it as a risk of linking these two Bills but not thinking about how they are fully linked.

However, going back to my first point, we were delighted to see that the Government are taking this really seriously.

Q111 Scott Mann: You mentioned some of the cyber-threats to elections. Could you expand on the kind of cyber-threats that are posed to national security in the wider sense?

Poppy Wood: Obviously, you have heard from much greater experts than me about hack-and-leak operations et cetera, and I refer you to their remarks about that. In terms of co-ordinated disinformation campaigns, as I said we have seen that in the US election, with really targeted approaches to particular groups that people wanted to divide. When I mentioned that the US Senate said that African-American electors were being targeted, it was clear that the Russians wanted to stir up tensions within that group and between that group and white police. They would really push Ku Klux Klan narratives, false images and all sorts to make sure that those groups were infighting. I would absolutely expect to see that here as well.

Political ads are also a really big issue. I cannot work out whether they are dealt with in the Bill, but they are certainly not dealt with in the Online Safety Bill. The Cabinet Office seems to own the political ads regime, but we are seeing shell companies buying these ads purely to stoke division and tension, and we would expect to see that again. One of the problems with not having a grip of the issue, particularly as we could go into an election period in the UK at any point, is that we need someone to comprehensively pull this all together.

The Russians and the Iranians often leave quite a lot of fingerprints on their work, sometimes intentionally. I know that Ken McCallum, who is director general of MI5, and the FBI discussed the threat from China yesterday. They did not mention disinformation, which I thought was interesting, but the Chinese have historically been much better at not leaving their fingerprints on things, so I cannot really speak to some of their activity. However, we have seen it time and time again.

It is probably best not to talk about the Brexit referendum, but we all know what happened there with the engagement from foreign actors. We should not be surprised to see disinformation. We are vulnerable in the UK because of our role in supporting Ukraine, and we have to pull it all together. If the Online Safety Bill, combined with the National Security Bill, does not do so, I do not know what will.

Q112 Holly Lynch: We have heard in some of the previous contributions that hostile states' use of disinformation does not always cross the thresholds that we are talking about, and that sometimes it is about the amplification of uncomfortable truths. You used the example of pitting different elements of society against each other in the US elections. To what extent do you think we need to improve some of our definitions and understanding, so that we can start looking at how we disrupt disinformation?

Poppy Wood: We have to be careful not to try to define disinformation. There is some language in the Bill about misrepresentation, and the idea of intentionally misrepresenting is important. We will never get a grip on exactly what disinformation is, because it is a shapeshifter.

On the first part of your question, it is about the system of amplifying and the ease with which people with malicious intent can manipulate systems by creating fake accounts, not verifying IDs and exploiting the recommender algorithms so that they hook you with one piece of content. We see this time and time again. One piece of bad content is not the problem, but they hook you on it, which then leads you down a rabbit hole to something much darker and more radical. It does not even have to be radical; it can be the sort of stuff that we were talking about with the Scotland referendum. It can be innocuous, such as stories about what the royal family are doing. It is about sowing seeds and exploiting cognitive dissonance, which bad actors are very good at and which social media is absolutely weaponised to make the most of, because of the pace and amplification of the content.

The Online Safety Bill goes part of the way there; it is imperfect, partly because it is so hard to define disinformation. There is very little in the Online Safety Bill on disinformation. There is an advisory committee that is years down the road. It is ironic that the National Security Bill is about trying to rein in certain types of transparency. Transparency is a really big part of all this, so it is about trying to find out who is behind things and what the data patterns really look like, and building in researchers. I think that was something Ken McCallum said last year. A holistic approach is a cross-Government approach, but it also involves industry, civil society, journalists and researchers. Everyone has to focus on this. Both Bills could go further on systems and, as I say, the co-ordinated inauthentic behaviour language just is not there either.

Q113 Holly Lynch: We will be tabling an amendment that would require the Government to commission an independent review every year on the prevalence of disinformation and the impact that it has on elections. Who would you imagine would be most suited to undertake that report?

Poppy Wood: That is a brilliant idea. It goes back to the point about grip. We are seeing really good work being done by the Home Department and the Department for Digital, Culture, Media and Sport. I think the DCMS counter-disinformation unit is an important tool, but it is very small, as is DCMS, and it is lacking the transparency that such interventions require. It should probably be a body like the Intelligence and Security Committee—some kind of cross-party body, quasi-independent of Government, thinking about the issues, with input from expertise in the relevant services and relevant Departments. I know that the Home Department and DCMS work together closely on this, and I think the Cabinet Office also has a role to play. Instinctively, I feel that something like the ISC would be the best place for it, but I am sure that is to be worked out.

One of the issues with a lot of this stuff is the role of the Executive, and making sure that the body is that far removed from political interference.

Q114 Damian Hinds: Hello. Earlier, you queried why something that happened in 2014 might only have been called out by Facebook in 2018. Isn't it quite obvious that what happened was 2016 in the middle, and all the brouhaha that followed from the American elections and the congressional inquiry, and all the rest of it? It turned out that when Facebook and others went looking, it was amazing what they could find.

Poppy Wood: Absolutely. If you are suggesting that they respond to PR crises, I would agree with you on that one. Of course, this about brands. We have seen with revelations from Frances Haugen that Facebook is not understaffed but just not focusing them in the right direction on this stuff. There are only handfuls of people focusing on co-ordinated disinformation for the whole world within these big technology companies. It should be dozens, especially if they are hiring 10,000 engineers for the metaverse in Europe. They can put some of them on elections and tracking. They say that they go far, but they could go much further. When there is pressure on them, they respond, and so far that pressure has been PR because there has not been regulation.

Q115 Damian Hinds: Would it be fair to say that they have at least got better? If you take the American 2020 election, there does not seem to have been the same volume of attempted disruption as in 2016 election, or at least not in the places where we are now looking, like Facebook?

Poppy Wood: We do not know, because we have not got the transparency. They may seem to have got better, but as a percentage of what, we cannot know. They will say that it has got better and that they have caught this many thousand as opposed to that many thousand last time, and those accounts have been taken down, but we have no idea if it is a percentage of what. That is why people, such as Frances Haugen, who have come forward as whistleblowers to say, "They are telling you this, but the data says that," show that we should not be relying on those people. I am sure we will come on to the whistleblowers, but there have to touchpoints much earlier on, from civil society, from Government, from researchers, to say "Hey, actually, the scale is much larger," or, "You're not even looking at this stuff."

London is one of the most linguistically diverse cities in the world, and when we are talking about counter-terrorism speech, one of Frances's revelations was that 75% of counter-terrorism speech was identified as AI—it is terrorism speech, so it is taken down. We are thinking about the UK as an English monolith, but there is plenty of linguistic diversity that puts us at risk when those platforms are weaponised in elections, focusing on diaspora and so on.

I would hope that the platforms have got better, and I would like to give them the benefit of the doubt, but the truth is that we just do not know.

Q116 Damian Hinds: You mentioned that there is not transparency, but there is at least one type of transparency with Facebook—main Facebook—as in you can see what is on it. I wonder what you think of the role of channels that you cannot see, such as private messaging that includes private parts of Facebook, WhatsApp, and what they call copypasta—copying and pasting SMS messages—and so on. How much do we know about that?

Poppy Wood: I would challenge the first assumption that you can see what you can see on Facebook. They still view that as private information. Researchers cannot get access to that unless they kind of beg, borrow and steal. I understand the question—

Damian Hinds: But you can see public postings on Facebook. That is my point.

Poppy Wood: On your page, you can, but researchers cannot.

Damian Hinds: But that is still more than you can see on WhatsApp, where you cannot see a post at all.

Poppy Wood: That's true. I suppose I would say they could do much more about transparency just about the public posts—that is my first point. Secondly, on encryption, there are concerns about some of the amendments in the Online Safety Bill and what that really means for encryption. I know we are not here to talk about that Bill, but encryption is an important tool. We know that those spaces are misused, but we need to be really clear about some of the benefits that encryption offers to lots of people, particularly the security services, for sharing information safely. We need to be careful.

Q117 Damian Hinds: I was not trying to start an argument or even a discussion or analysis of end-to-end encryption. I was just asking, relatively speaking, how much do we know? There is a hypothesis that the reason why there was apparently less material in recent American elections on Facebook than in 2016 is that large parts of it have moved to other channels where we just cannot see it. We just do not know what is there.

Poppy Wood: Let me give you a good example on Russia Today. We do a lot of work and analysis around Russia and Ukraine. Obviously, Russia Today was taken down from most national broadcast networks. It has been resurrected multiple times on social media. This week, we saw it resurrected with another name, like "Discovery Dig" or something, on YouTube, where lots of the comments, imagery and language were directing people to Telegram channels where they are actively mobilising.

What we see in the active mobilisation on Telegram channels is the outing of national security agents, the putting up of email addresses of politicians and saying, "Target them and say they are on the wrong side of the debate," or, "Write to this national newspaper." In all three of those examples, it is predominantly in the UK. They are telling them it is all fabricated. They are absolutely weaponising those private spaces. As you say, it is quite hard to get into them—but actually, it is not that hard. They are pretty open channels, with thousands and millions of engagements and followers. That is the scarier bit. They are private, but you are getting tens of millions of people and engagements on them. I am not sure that is the true definition of private, but it is certainly in an encrypted space.

Q118 Jess Phillips (Birmingham, Yardley) (Lab): I want to touch on the whistleblower issue you raised. There have been some concerns that the Bill might not sufficiently target those with malicious intent. Is there a risk that it potentially criminalises whistleblowers?

Poppy Wood: The role of whistleblowers in society is really important. I know the Government understand that. There are some good recommendations from the ISC about whistleblowers that I do not think have been adopted in this version of the Bill. That is about at least giving some clarity to where the thresholds lie, and giving a disclosure offence and a public interest defence to whistleblowers so they can say, "These are the reasons why." My understanding is that at the moment it sits with juries and it is on a case-by-case basis. I would certainly commend to you the recommendations from the ISC.

I would also say—this was a recommendation from the Law Commission and also, I think, from the ISC—that lots of people have to blow the whistle because they feel that they do not have anywhere else to go. There could be formal procedures—an independent person or body or office to go to when you are in intelligence agencies, or government in general or anywhere. One of the reasons why Frances Haugen came forward—she has been public about this—is that she did not really know where else to go. There were no placards saying, "Call the Information Commissioner in the UK if you have concerns about data." People do not know where to go.

Getting touchpoints earlier down the chain so that people do not respond in desperation in the way we have seen in the past would be a good recommendation to take forward. Whistleblowers play an important part in our society and in societies all round the world. Those tests on a public interest defence would give some clarity, which would be really welcome. Building a system around them—I know the US intelligence services do that; they have a kind of whistleblower programme within the CIA and the Department of Defence that allows people to go to someone, somewhere, earlier on, to raise concerns—is the sort of thing you might be looking at. I think a whistleblower programme is an ISC recommendation, but it is certainly a Law Commission recommendation.

Q119 Sally-Ann Hart: On malign activity, is there a risk that through clauses 13 and 14 on foreign interference, the Bill could affect free speech, including political speech and journalism? If you think it could, what additional safeguards can be put in place to ensure that only malign activity is captured?

Poppy Wood: I have certainly read and heard concerns about journalism, about the "foreign power" test on civil society and about having Government money being quite a blunt measure for whether or not you might fall foul of these offences. On journalism, I think that is why you should never try to define disinformation: because those kinds of shape-shifting forms are very hard to pin down, particularly with questions like "What is journalism?", "What is a mistruth?", "What is a mis-speak?" and so on. We need to be careful about that.

On your specific question, I refer you to Article 19 and others who have really thought through the impact on journalism and free speech. I am sure it would be an unintended consequence but, again, we are seeing Russia using its co-ordinated armies on Telegram and other channels to target Ukrainian journalists. They are saying, "Complain to the platforms that the journalist is not who they say they are or is saying something false, so they are breaking the terms of service. Bombard the platforms so that that journalist gets taken down and cannot post live from Ukraine for a handful of days."

That is just another example of how these systems are weaponised. This is where you can go much further on systems through the Online Safety Bill and the National Security Bill without worrying too much about speech. But I refer the Committee to other experts, such as Article 19, that have looked really deeply at the journalism issue. I think Index on Censorship may have done some work as well.

Q120 Sally-Ann Hart: You have mentioned disinformation. In this Bill, the Online Safety Bill, and perhaps the review that Ms Lynch mentioned, which you thought was a good idea, what more do you want to see the Government do to address dis, mis or malinformation and malign foreign influence online?

Poppy Wood: I think that where we are now is much better than where we were last year, but my concern is whether this will all be law when we have an election. If not, what are the backstops that the Government have in place to focus on this stuff? It will get tested only when we have an election, really. If that is before March next year or whenever these laws get Royal Assent, there will be a genuine question of crisis management: if this is not law, what are we doing? I would ask that question of the Government and the civil service.

As I said, the disinformation committee in the Online Safety Bill is years down the line. Bring that forward—there is no need not to bring it forward—and please make sure that it is not chaired by someone from a tech platform. I would write that into the Bill, because otherwise there is a risk that that will happen.

Q121 Sally-Ann Hart: Why?

Poppy Wood: Why should the committee on disinformation not be chaired by someone from a tech platform? They have a vested interest in this stuff, so I would get an academic or someone from civil society—someone at arm's length who can take a holistic view. These platforms will want to protect their interests on this stuff, so I would warn against that.

I would like to see the transparency provisions in the Online Safety Bill go much further. This is a bit in the weeds of the Online Safety Bill, if you will forgive me, but there is a very good clause in that Bill, clause 136, which says that Ofcom should ask whether researchers should be given access to data. It is an important clause, but it says, "Ask the question," and it gives Ofcom two years to do it. I do not think it needs two years; I think we know that the answer is "Yes, researchers desperately need access to data."

Almost all the stuff that is caught about malign information operations is caught via Twitter's API. Twitter makes 10% of all the tweets public, and researchers use that to run analysis, so if you ever want to do research on disinformation, you always use the Twitter API. In many cases, that is mapped over to Facebook to identify the same operations on Facebook, but they are always caught in the first instance because of open data. I think that the Online Safety Bill, if this Committee and this Bill want to back it up, could bring that forward and say, "Either do the report in six months or don't even ask the question."

By the way, the European legislation that is equivalent to the Online Safety Bill makes that happen as of Tuesday this week, so researchers should, in theory, be able to access data. I would bring the transparency provisions forward, and I would really want the Bill to call out co-ordinated inauthentic behaviour.

The Chair: That brings us to the end of this panel. On behalf of the Committee, I thank our witness for taking the time to give evidence.

Examination of Witness

Dan Dolan gave evidence.

4.20 pm

The Chair: Last but not least, we will now hear from Dr Nicholas Hoggard, lead lawyer for—I am so sorry; it is that time of day and the lack of coffee. *[Laughter.]*

[The Chair]

I should have confiscated my colleague's coffee and had it for myself! Apologies; we are going to hear from Dan Dolan, the director of policy and advocacy at Reprieve. We have until 4.40 pm for the session. Could you introduce yourself for the record, Mr Dolan?

Dan Dolan: Thank you very much. My name is Dan Dolan, and I am the director of policy and advocacy at Reprieve, a legal action charity that seeks to uphold the rule of law and human rights around the word. Over the past 20 years, Reprieve has provided legal and investigative support to hundreds of prisoners on death row, the families of innocents killed in drone strikes, victims of torture and extraordinary rendition, and scores of prisoners in Guantanamo Bay. Thank you for the opportunity to give evidence.

Q122 Holly Lynch: Thank you for your written evidence. We have heard from the security services that they deem elements of clause 23 necessary to protect some of their staff from possible prosecution. I note that you say in your written evidence that those changes protect Ministers. Can you take us through that in more detail?

Dan Dolan: Absolutely. I should start by saying that we absolutely recognise that the country's intelligence agencies do a difficult and often dangerous job to keep us safe, and we give our evidence in recognition of that. We think clause 23 is much more likely to protect Ministers and senior officials from criminal liability than anyone in the midst of an operation overseas.

The reason why we say that is because there is already a regime, under the Intelligence Services Act 1994, under which acts that could constitute a criminal offence overseas would be authorised by a Minister if they are in the furtherance of the agencies' duties. That is well recognised. The Minister who took that Act through described offences such as bugging, bribery and burglary, which you can imagine an officer of the intelligence agencies may need to do overseas to keep the UK safe. That regime already exists in law, and it allows for authorisation of potentially criminal acts overseas.

Clause 23 disapplies provisions of the separate Serious Crime Act 2007 relating to encouraging or assisting the commission of a crime—specifically, schedule 4, which relates to extra-territoriality, meaning crimes that would be encouraged in the UK but committed overseas. There is already a regime that protects officers of the UK who are involved in operations overseas and do things that may be criminal by giving them insulation from criminal liability.

Clause 23 insulates people from criminal liability for acts undertaken in the UK to encourage or assist offences overseas. Realistically, we are talking about conduct that might take place, for example, behind a desk in Whitehall, but would ultimately result in what would be a criminal offence overseas. There is an existing legal regime to cover offences of those who undertake them outside the country; this is about actions taken within the country, if that makes sense.

Q123 Holly Lynch: The framework of checks-and-balances scrutiny that oversees existing legislation would be weakened by adopting clause 23. Would that be your assessment?

Dan Dolan: Yes, it would be. Effectively, clause 23 looks a lot like an effort to protect Ministers from criminal liability for actions that they encourage or assist in the UK that could constitute a crime overseas. This is not a hypothetical idea. There have been instances that were extensively documented in the Intelligence and Security Committee's detainee report, where UK Ministers and officials authorised intelligence sharing that led to appalling torture and mistreatment of people overseas. The ISC has documented that extensively.

A good example is the case of Abdul Hakim Belhaj and his wife Fatima Boudchar, who in 2004 were rendered to Libya where they faced appalling mistreatment, both in Libya and in the course of their rendition by the US CIA. Subsequently, it emerged that the UK Government had provided the tip-off to enable that extraordinary rendition. The couple ultimately received an apology from Theresa May's Government, recognising that the UK had shared intelligence that had contributed to the couple's absolutely appalling mistreatment.

That is not an isolated case. During the war on terror era, there were many instances where the UK shared intelligence that contributed to torture. That has been recognised. The then Prime Minister recognised that in her response to the ISC's report, and pledged never to do that again. What this clause would do is effectively to insulate Ministers from criminal responsibility for those kinds of offences.

Q124 Holly Lynch: Further to that, we have heard today, and I have heard from the intelligence services before today, this sense that, while hypothetical, the fear of prosecution of individuals acting under orders is having a chilling effect on the work that they need to undertake. On occasion, it has meant that they have had to pause and cease some of the operations that they feel are quite routine or essential as part of defending the UK's national security interest. With that in mind, is there an alternative way through this? Could the provision be amended or alternative safeguards added to arrive at those individuals having the protection that they need, while having some of the safeguards and checks and balances that we are concerned might be missing at this time in clause 23?

Dan Dolan: That touches, importantly, on the point about whether clause 23 would protect officers acting overseas in the UK's national interest, or whether it would protect politicians and officials taking actions in Whitehall, like sharing intelligence. In response to your question, I want to read a quote given by MI6 to the ISC's detainee inquiry—quoted in the report—with respect to section 7 authorisations under the 1994 Act. The Secret Intelligence Service said that, in the cases they were talking about,

"we are … always going to go for a section 7 authorisation. Because, you know, why should my officers carry the risks on behalf of the Government personally? Why should they? So, you know, as we have already discussed, serious risk is…a subjective judgement. So we will go for belt and braces on this."

I think that "belt and braces" is the important phrase to think about, because that is MI6 describing the separate 1994 section 7 authorisations as a belt-and-braces approach to protecting officers from criminal liability. That regime exists already, under the Intelligence Services Act 1994, so why do we need clause 23? It relates to actions taking place here in the UK—not people operating

abroad on operations, but people acting in the UK—so what kind of actions are we talking about? The area that is not covered under existing legislation is the authorisation of acts or the sharing of intelligence that happens here in England or Wales.

We are therefore not of the opinion that the clause would offer additional protection over and above the 1994 Act. The clause covers a different category of offence, and that would be the encouragement or assistance of a crime from within the United Kingdom. We are talking about Ministers and officials approving things here, not people on operations overseas.

My final point—I know this was made on Second Reading—is that the Serious Crime Act 2015, sections of which would be disapplied by clause 23, already includes, in section 50, a reasonableness defence. Even if you imagine a case in which the Government argue that a Minister needs to order something that might be a crime overseas in the national interest—they would have to make a strong case for that—they would have a legal defence under reasonableness to say that their action was reasonable under section 50 of the Serious Crime Act. What we are talking about here is clause 23 disapplying legislation that would hold Ministers to account were they to encourage or assist a crime overseas.

Q125 Jess Phillips: On whistleblowing, which I was speaking to the prior witness about, do you think the Bill does enough to protect people who act against the UK Government, such as whistleblowers?

Dan Dolan: I am sorry to be unhelpful, but Reprieve's evidence largely covers the provisions under clauses 23 and 57 to 61. I can pass it on to somebody.

Q126 Jess Phillips: That is absolutely fine. I can speak to you about part 3 of the Bill and the legal aid regime if you want. What is your view on the legal aid regime—the absence of legal aid—and how it is taken in the Bill? Specifically, I am interested in the offences that now come into that, with regard to accessing legal aid in the future.

Dan Dolan: Part 3 of the Bill—clauses 57 to 61—is in some ways the other side of the coin to clause 23. Clause 23 significantly hampers criminal accountability for ministerial or official involvement in crimes overseas, but there is also a very important civil avenue by which we might get accountability were the UK to get mixed up in torture or unlawful killing.

The Britons who were detained in Guantanamo Bay unlawfully without charge for many years and Abdel Hakim Belhaj, to whom the Government apologised, got accountability for the UK's involvement in their appalling abuse through civil cases. They fought very hard, multi-year legal battles in the civil courts to win recognition from the Government that they had been involved in their mistreatment. Clauses 57 to 60 effectively introduce a range of so-called national security factors that would allow the Government to request a reduction of damages, potentially to nil, if those factors are present.

Say you are Mr Belhaj, who sued the Government and ultimately exposed their involvement in his torture, a national security factor that could have been applied in his case, were it in the form in the Bill, is that the UK, when it undertook the action that enabled his abuse, was acting to avert a real risk of harm. That obviously sounds convincing, but it is difficult to imagine an instance where the intelligence agencies would say they were not acting to avert a risk of harm—that is their core purpose.

The Bill also has national security factors that include the involvement of a third party. Say the UK Government passed on intelligence that led to someone's torture by Colonel Gaddafi's Libya, historically. Colonel Gaddafi's Libya is a third party and its involvement would mean that UK did not need to pay damages on that front. The action happening overseas is another national security factor. If there were any wrongdoing by the UK intelligence agencies that led to torture or abuse overseas, the person would not be able to seek damages because of that factor. Effectively, what we are seeing in clauses 57 to 60 is a really sweeping effort on the part of the Government to get out of paying any damages to anyone who suffers due to Government wrongdoing overseas.

Clause 61 is really interesting, because it effectively relates to all civil cases. It allows for the freezing of damages in all civil cases, not just cases in which the Government are accused of wrongdoing. We just have not seen any basis that there is an issue with global terrorist groups receiving financing from damages in personal injury or medical negligence cases. It seems an incredibly, sweepingly broad curtailment of one's right to receive damages—one that likely duplicates existing provisions for asset freezing and terrorist financing.

Q127 Jess Phillips: It worries me because there are lots of civil remedies in cases of abuse and violence. We made the law protect people who were victims of that so that they were able to access legal aid in a regime where most people cannot access legal aid any more. Victims of domestic abuse, for example, have an exemption. Is your reading of the Bill that you would not be able to get a non-molestation order, for example, which is a civil remedy where you seek legal aid through your exemption?

Dan Dolan: I would say that our evidence to the Committee covers clauses 57 to 60 and does not look in detail at the legal aid provisions, but my understanding of those provisions from the Independent Reviewer of Terrorism Legislation's notes on those is that these are extremely broad provisions, and I would note that—

Jess Phillips: They would not be able to access legal aid.

Dan Dolan: There are a number of people every year—teenagers—who receive non-custodial sentences under terrorism legislation. That might be someone who shares something online at the age of 16, and my understanding is that the Bill would have an incredibly sweeping impact on their ability to receive those kinds of orders, and, equally, on their rights to access the civil courts for the rest of their lives, which is a fairly dramatic constitutional action.

Jess Phillips: It does not stop them accessing the civil courts. To be fair, it stops them accessing legal aid to the civil courts.

Dan Dolan: Which, as you will be aware, may be, at times, the same thing.

Jess Phillips: Just on a point of fact, it stops them from accessing legal aid.

Q128 Sally-Ann Hart: We heard from a Law Society witness earlier that the provisions relating to arrest without warrant—in clause 21 and schedule 3—that include the ability to delay access to a lawyer and delay notifying a person's family of their detention are proportionate and necessary. Do you regard it as proportionate and necessary?

Dan Dolan: I am afraid I might have to give the frustrating answer that our evidence does not cover clause 20. There is clearly a concern there, but I am probably best leaving that to more expert witnesses to answer.

The Chair: Any other questions? Thank you all very much. That brings us to the end of this session. I thank our witness on behalf of the Committee for taking the time to give evidence today.

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

4.37 pm

Adjourned till Tuesday 12 July at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

NSB01 Reprieve

NSB02 Sarah Kendall, PhD Candidate and Sessional Academic, School of Law, University of Queensland