

| | |
|---------------------|--|
| Programme(s) | BBC Radio 4 Today |
| Date & time | Thursday 17 September 2015 08.10 |
| Subject/Interviewee | Interview – Andrew Parker |
| Contact numbers: | Cabinet Office Media Monitoring Unit 020 7276 2084 |

Mishal Husain, presenter: Do the intelligence services have the tools they need to keep us safe in an age where the greatest threats come from terrorism rather than enemy states, and where some of those terrorist threats are home-grown. After the election, the Home Secretary said she would introduce the new Investigatory Powers Bill in the course of this Parliament, a follow-up to the Communications Data Bill that was dubbed the "snoopers charter" by its critics. The new legislation is expected to be a fundamental reset of the powers intelligence agencies have to access our data (emails, voicemails, text messages, what we do on social media, possibly our internet browsing history). The agencies have some of these powers already either through counterterrorism laws or emergency legislation, but the existing framework is widely regarded as piecemeal and in the view of David Anderson QC, the independent reviewer of terrorism legislation, "undemocratic". Well, the Director General of MI5, Andrew Parker, is with me now. It is the first time that a serving head of the organisation has done a live interview in the organisation's 106-year history. *Good morning.*

Andrew Parker, Director General, MI5: Good morning.

MH: *Let's start first with the level of the terrorist threat and where it stands at present.*

AP: Thank you. The terrorism threat is the most serious threat that Britain faces in security terms currently and it takes up most of the work of MI5 and our partner agencies. It's set currently at the level of severe, which means that attacks are highly likely. What that actually means in practice – and over the past year – has been a growing threat that the Prime Minister's referred to in which we've seen six attempts at terrorism in this country just in the last 12 months, that we, and partner agencies with the police, have had to intervene and to stop, and that is the highest number I can recall in my 32-year career, certainly the highest number since 9/11, and I think it represents a threat which is continuing to grow, largely because of the situation in Syria and how that affects our security.

MH: *So the kind of threat that led to the drone strikes in Syria just in recent days. Is that typical of the most serious threats that you're facing?*

AP: The shape of the threat we face today has changed in some ways; changed because, of course, it's driven from conflict zones and the way people react to that, but because of the internet and the way terrorists use social media, including from Syria, and the way we all live our lives using smartphones in our pockets, the terrorists do the same and they're using secure apps and internet communication to try to broadcast their message and to incite and direct terrorism amongst people who live here who are prepared to listen to their message.

MH: *And we'll come to what that means for the capability of your agency in just a moment, but given that you're saying such a high level of threat originates from people who are in Syria, are you concerned about the migrants and refugees who are coming into Europe at the moment, that there may be extremists among them?*

AP: Of course. It's MI5's job with others to monitor where the terrorists may be and how they're operating and how they're moving, and we've done a lot of work to try to discourage and stop with the police people travelling out to Syria to engage in the conflict there, and, of

course, take an interest in those who have been to Syria and are coming back, so as far as the flows of migrants and refugees go, of course, it's something that we're aware of. It isn't actually, as we speak today, the main focus of where the threat is coming from.

MH: *Right, so let's talk then about the tools that you need and particularly the moment that we stand at now where the Government has said that they will put a Bill before Parliament. What is it that you would like to see in that Bill, something that you cannot do now that you want to see possible?*

AP: Can I come to that in a second and just take half a step back on what is it we need to be able to do these days? Because of that threat we face, and the way the terrorists operate and the way we all live our lives today, it's necessary that if we're to find and stop the people who mean us harm, MI5 and others need to be able to navigate the internet to find terrorist communication. We need to be able to use data sets so we can join the dots to be able to find and stop the terrorists who mean us harm before they're able to bring plots to fruition. We've been pretty successful at that in recent years, but it's becoming more difficult to do it as technology changes faster and faster...

MH: *And therefore you would say you need more powers.*

AP: And so the legislation that's coming up is, of course, for the Home Secretary to introduce in due course and for Parliament to decide. It's not for me to say what should or shouldn't be in that Bill, but it's clear that the intent that Government has – already explained by the Home Secretary – is to bring some discussion in Parliament and their legal effect to some of the findings of David Anderson's report, which you mentioned. There was also a review, of course, by the Intelligence and Security Committee, which is our oversight committee in Parliament, which also made some findings and Government will be bringing forward legislation based on those. I think if you... you're asking what I would like out of it and I think the really important thing for MI5 is, as people understand, we operate within a framework of law, set by Parliament, and independently overseen, and as our capabilities move forward, I think it's important that from time to time legislation is updated so that we're operating modern, straightforward law that describes transparently and as fully as it can what sort of thing MI5 does these days.

MH: *Right. But the reason I ask if you want more powers is because when we hear the security agencies talk about the pace of technological change and laws needing to be updated, it rings alarm bells over privacy, and the "snoopers charter", as it was dubbed by its critics, the former bill that was brought forward, that was part of the reason that it became so controversial. So are you saying that you need more powers to access the emails, the browsing history? What is it that you want to be able to do?*

AP: So we need to be able to do in the modern age what we've always done, through our history, in being able to find and stop people who threaten the UK and mean harm to the public, and that means that we need to be able to monitor the communications of terrorists, spies and others. We need to be able to obtain data about their communications. We need to be able to obtain other information about them, but through all this, I think the important thing to say is that we're focused on the people who mean us harm. We're not about browsing through the private lives of the citizens of this country. We do not have population scale monitoring or anything like that. We are focused, on behalf of the public, against those who mean us harm and the powers that Government is considering and are being drafted now, and will be discussed and decided by Parliament and not by me, will be powers that are about doing that in the modern age. For me, perhaps the most important thing is that there is clear and transparent explanation of the sort of thing we do, and in those privacy reports that we've both referred to a minute ago, one of the things that I think is striking when

you read them is that neither the Intelligence Security Committee nor David Anderson made findings against the sort of capabilities we use...

MH: No, but what he did say – and this was the really searing verdict that he had about the state of affairs at present, that essentially it is “undemocratic and – in the long run – intolerable”. What he’s talking about is the legal framework that surrounds your work at the moment. Can you see why he said that – “undemocratic”?

AP: I think he’s made a strong case, which Government is taking very seriously to update the legislation, because if it isn’t transparent, what the sorts of capabilities are that agencies use these days – and bear in mind the laws we operate under now were drafted back in the year 2000, before many of the technologies that are around now were being used. Now, it’s important that it’s explained to people, because, of course, this is a free, liberal democracy and the role that MI5 has is to protect that against those who mean us harm.

MH: And the essential part of that probably is all of us as citizens having the trust that the work that you do is properly overseen and the suggestion that David Anderson made is that ministerial oversight wasn’t enough; that a judge should have to sign off on any request to access communications. Would you accept that?

AP: These are all matters for Parliament to decide. We operate within the framework set by Parliament and we’ll continue to do so.

MH: But would you fight against that? That is quite important, because you’re making an argument for a modern set of laws that give the public confidence that you are working in the right way for everyone’s safety, so would you accept, as part of that, that judicial as well as ministerial oversight is needed?

AP: Look, I don’t have a view about it. It is completely for Ministers to propose and for Parliament to decide, and I’m not trying to avoid your question by saying that. It’s a fundamental point about what MI5 is, that we operate in a framework of law, set by Parliament, and overseen independently. It’s not for me to say what arrangements those should be. It’s for us to follow what’s set by Parliament and that’s what we do.

MH: So you don’t necessarily have a problem with the idea of judicial oversight, even of every attempt to access communications.

AP: It is... as I said, I think it is for Parliament to decide and then it is for us to do the very best we can to protect the country from those who threaten our security and our safety, and that has always been our job for the last century or so and will continue to be.

MH: What is at stake if, for whatever reason, you don’t get the new tools, the powers that you see as adequate for the technological age we live in. Your counterpart in the United States, the Director of the FBI has spoken of the dangers of – in his words – ‘going dark’.

AP: Director Comey has referred a few times publicly to what he calls going dark, by which he means shifts in technology and particularly in internet technology, and the use of encryption and so on, creating a situation where law enforcement agencies and security agencies can no longer obtain under proper legal warrant the content of communications between people they have reason to believe are terrorists. I think that is a very serious issue. It requires that there is a legal framework to authorise, but it also requires the cooperation of the companies who run and provide services over the internet that we all use. And it is in nobody’s interests that terrorists should be able to plot and communicate out of the reach of any authorities with proper legal power.

MH: *And therefore, isn't it the case that even if you do get the new framework in UK law that gives you those tools, you will still have a problem with those tech companies, many of them based in the United States, and therefore beyond the remit of UK law.*

AP: I think it will be a continuing challenge as technology shifts. We have seen the way that technology has moved so far and so fast in recent years. It will keep doing that, and maybe in unpredictable ways. I think it is important into the future that not only is there a framework of clear law in countries like Britain, as there is now, but updated, but also that there is international agreement and arrangements whereby companies have a confident basis on which to cooperate with agencies like mine and with the police in order to protect society and, of course, their customers from people who bring them harm.

MH: *But an international agreement might mean that they have to cooperate with the Russians and the Chinese, and that surely is... you know, you can see why that is the kind of thing that makes people very apprehensive.*

AP: Look, I think you can see that Britain stands for high standards in these things, where we operate only under law. We have independent oversight and we have very, very strict principles of necessity, so we only do what we really need to do, and proportionality. We only do it at the scale that is absolutely necessary. I think it is possible to think of international agreements based on those high standards and principles.

MH: *But, I mean, just to talk about one of those tech companies, Facebook for example, when the Intelligence and Security Committee report into the murder of Lee Rigby was published, it said that there had been a private conversation between one of his killers, Michael Adebolajo, on Facebook with an extremist. Now, that drew a lot of attention to the role of tech companies. But would you really expect it, Facebook in this case, to report conversations like that? It would say that (a) it is not its job to do that and (b) it might not have the tools to report conversations of that kind.*

AP: I don't think the ISC report named any particular company, but your point is well made, and I think it goes to the question of the ethical responsibility of these companies for the communications and the data that they hold and they carry. And this question comes up in the realm of child sexual exploitation, terrorism, other forms of crime, and I think there is a real question about whether companies holding information of that sort should – under what arrangements they should come forward to the authorities and share and report it. In that case, the ISC concluded that had that happened, it might have made a material difference to the outcome.

MH: *But the question of ethical responsibility is an interesting and a tricky one. Essentially, your job is intelligence, not theirs.*

AP: But I think there is a real question here about responsibility for those who carry this information. Some of the social media companies operate arrangements for their own purposes under their codes of practice, which cause them to close accounts, sometimes, because of what is carried. I think there is then a question about, well, why not come forward. If it is something that concerns terrorism or concerns child sex exploitation or some other appalling area of crime, then why would a company not come forward? I think that was the question the ISC was raising. But it is only one of the issues in this realm where, you know, wider cooperation is needed too under legal warrant. Most of the time, the question is if I know and have reason to believe who a terrorist, I know what communications means that they use, we have a warrant signed by the Home Secretary to obtain it, the question then is, can we actually obtain those communications from that company?

MH: *You have talked about plots that have been foiled, as has the Prime Minister but, obviously, there are times when things do go wrong and things are not foiled, and in the case of Michael Adebolajo, again a killer of Lee Rigby, and Mohammed Emwazi, also known as 'Jihadi John', both of those individuals were known to the agency and were not stopped from committing heinous acts. Can you explain how that happens?*

AP: Well, I think the first point to make, as you say, is that there cannot be a guarantee that we can find and stop everything. That simply isn't possible. We would have to operate at such a massive scale, it would be impossible.

MH: *No, but when people are already under surveillance and they are persons of interest, there are conversations, face to face conversations that happen between MI5 agents and people like that and they are not kept under sufficient scrutiny after that.*

AP: the ISC looked into this very thoroughly, and I think it is one of the most details reports into our work today and what it involves and, of course, their conclusion was that it was entirely understandable what had happened. They did not conclude that we should have stopped that attack. And to answer your question, I guess the reason is, because if we do our jobs well, we will know who most of the people are who potentially offer a threat in this country. We can't monitor all of them all the time. We have to – based on the intelligence we have – make choices about where to focus our most intrusive resource on any one day and, of course, we constantly shift that and we do our very best based on what we know to make sure that is always focused where the sharpest threat is. That is how, in the last year, we have been able to find and stop six different plots that would otherwise have resulted in loss of life in this country.

MH: *But do you recognise when, for example, your agency is criticised that, and when people say as Michael Adebolajo's family said that he was pestered by MI5, Emwazi said that he was... complained that one of your agents had been threatening to him. Do you recognise criticism that your approaches can be a cause of alienation and, indeed, perhaps radicalisation.*

AP: No, I think it is – I completely dismiss that. The ISC report dismissed it too. It is the sort of thing that our detractors and, indeed, some people that we need to take an interest in would want to say, but I am afraid it is completely untrue. In the nature of the intelligence work we do these days, of course, we are using intrusive technique against the terrorists, but the success we have comes from the skill and professionalism of the men and women of MI5 and our partner agencies in how they bring together intrusive resource of various sorts against people who are plotting violence against the public. While I am mentioning them, I would want to pay tribute to that work which so often goes unrecognised.

MH: *Right, but we stand at a moment today where we have a greater problem, it would appear, from home-grown terrorism today than we did 10 years ago, despite the budget of your agency going up, despite all the effort of successive governments under the prevent antiterrorism, prevention of terrorism strategy. Are we doing something wrong?*

AP: I don't think we are doing things wrong, we just need to keep doing what we're doing and doing more. The underlying issues are, really, serious and very difficult to get at. If I describe it in these ways, most of the people who try to become involved in terrorism in this country are people who were born and brought up here, have come through our education system, and have nonetheless concluded that the country (their home country) and the country of their birth is their enemy and that they wish to behave accordingly. And that is a difficult thing for people to understand in many ways, but it is the reason why the Prime Minister is determined to push forward with the extremism strategy, to try to develop a whole of Government and a whole society response to that issue, and it is a long-term challenge.

MH: *It is striking that you have chosen to do this interview. You're not only the first MI5 Chief to do a live interview, but I think the first serving Intelligence Chief to do one. What should we conclude from that, greater transparency, perhaps even an era of greater openness?*

AP: I think people would understand, of course, the work that we do most of the time must necessarily be secret, and our operational work needs to remain that way, but I think there is a role in society today for people like me to help increase public understanding about the nature of the work and the sorts of threats that are around, what is necessary for us to do and the way in which we're focused only on the people who mean us harm, as the discussion on privacy rolls on. And I would like people to understand that we welcome the idea that there is clear legislation and oversight that frames what we do, because that is what we believe in, in MI5.

MH: *Some people's understanding of what you do might well be informed whether you like it or not by books and films, James Bond etcetera, when one of your predecessors Eliza Manningham-Buller guest edited this programme a couple of Christmas's ago we brought her together with Judy Dench of the fictional M, she had this to say about the fact versus fiction gap.*

CLIP of Eliza Manningham-Buller, former Director General, MI5: It was a great disappointment to some of my step grandchildren when they discovered what I did because they love James Bond and when they found out what I did they kept saying "Eliza, Eliza does something like that, Eliza does?". and it really rather sort of damaged their delight for James Bond.

MH: *Can you relate to that?*

AP: I certainly can because its, thank you for playing the clip, the men and women who work in MI5 who are of course basically ordinary people who are a part of our society, live in our communities, but are committed to protecting us from those who mean harm, so of course people are perhaps more ordinary than is in fact described in fiction.

MH: *Will you go and see the new James Bond film?*

AP: I do, I love the James Bond films, because they are so distant from reality that we can all enjoy the fiction.

MH: *Andrew Parker, Director General of MI5, thank you very much.*

AP: Thank you.