Transcript

CHATHAM HOUSE
The Royal Institute of International Affairs

# The Snowden Revelations


## Julian Borger

Diplomatic Editor, *The Guardian*

## Jane Harman

Director, President and CEO, Wilson Center

## David Omand

Visiting Professor, Department of War Studies, King's College, London

## Chair: Robin Niblett

Director, Chatham House


12 June 2014




10 St James's Square, London SW1Y 4LE T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
www.chathamhouse.org

Patron: Her Majesty The Queen Chairman: Stuart Popham QC Director: Dr Robin Niblett Charity Registration Number: 208223

## Robin Niblett

Ladies and gentlemen welcome to Chatham House, I'm Robin Niblett, director of the Institute. First of all I want to say a big thank you to everyone for coming out slightly out of sync from our usual members' meetings in the afternoon but we have a particularly busy day today at Chatham House, with all sorts of other events, but we did not want to miss (a) the opportunity to mark this I suppose important anniversary of the... We've titled them 'The Snowden Revelations'.

Obviously the Snowden Revelations are part of a much, much bigger and more complex debate and we didn't want to take (a) the opportunity of missing that anniversary or secondly missing the opportunity of having Jane Harman, who's going to be in London this week and seemed like the perfect opportunity to be able to have this discussion which we're going to have today.

We're going to be having a bit of a Working Group meeting after it and hope to continue some work involving both Chatham House and the Woodrow Wilson Center as we look to the future on this issue of intelligence, surveillance, privacy and all of the incredibly important and vexed questions that have been raised in this past year. So with that in mind I just want to say very quickly that we have, I think, a super panel to discuss this topic and reflecting multiple views and perspectives. The first person to kick off, and I'll introduce them as who they are first, and then let them say some remarks as we go forward from here...we may have to pull a few extra chairs into the room here but we'll see how it's going...

The first will be Julian Borger, who's diplomatic editor at the *Guardian*. He therefore is part of the *Guardian* team that won the Pulitzer earlier on this year for their coverage of the whole issue around the Snowden Revelations and all that's flowed from it. He has the benefit of being the diplomatic editor, from our perspective and in terms of this conversation, and I think it's also especially useful that he served as the Washington Bureau Chief from 1998 to 2007, so somebody who really brings a good knowledge as well of the US, as well as the many other stories and parts of the world that he's covered over his career.

We're then going to turn to Jane Harman. Jane, I think known to many of you here, she is now director and CEO of the Woodrow Wilson Center in Washington. She has done much of her career as a Democratic Representative of Congress, California's 36$^{th}$ Congressional District, two terms, 1993 to 1999; 2001 to 2011, and I think importantly in the context of this conversation she served on all of the major security committees; Armed Services, Intelligence and also Homeland Security.

Since she left, she has, as often is the case in the US, kept herself part of the mix from that advisory dimension as one does in the United States. She's a member of the Defence Policy Board, the State Department's Foreign Policy Board, the DNI; the Director of National Intelligence's Senior Advisory Group, and also she served on the CIA external advisory board from 2011 to 2013.

We then will be turning to Sir David Omand. David Omand is now visiting professor at King's College Department of War Studies here in London. He was the first UK security intelligence coordinator, having spent some seven years on the JIC, on the Joint Intelligence Committee. He oversaw both intelligence issues and also national counter-terrorism strategy, at a particularly important time in the context of the UK. He's also served as director of GCHQ and as permanent secretary of the Home Office.

I just say all of this by way of saying that I think we've got – and I've taken up a few minutes of our limited amount of time - but I do want to just put this group into context, in terms of the perspectives that they bring in.

I thought rather than trying to marshal this conversation in some way, it would be a good idea just to let each of our speakers to share five, seven minutes, just some opening thoughts on this anniversary, what this last year has meant to them, perhaps what's different, what's changed, and I'll see what you say but hopefully we'll see where we're going from here which obviously I think is as important as how we got to where we are today and Julian, without more ado, over to you.

## Julian Borger

Knowing that... Okay so a year ago more or less today, as far as I can remember, I was in a small over-heated room, and this is how I spend most of my summer, going through hundreds and hundreds of documents, of top secret documents belonging to the NSA and the GCHQ, and journalists of other nationalities were doing the same thing on three continents. It was a huge amount of material; it covered operations in Iran, the rest of the Middle East, Afghanistan, much of the world.

But in the *Guardian* at least, we were skimming over that material. We were told - and there was a list of rules pinned to the wall - to focus on one core issue: the question of bulk collection in the US and UK because that's what the source of these documents, Edward Snowden, had said he'd leaked them for, because of. And that was our prima facie public interest case for investigating the material in the first place.

I'm going to talk a bit about the impact and the consequences of what we published, which drew on a very tiny percentage, probably less than one per cent of the total material, but it was material that fitted our public interest criteria. But I also want to talk a bit about the bigger issue; the 99 per cent, which we didn't publish, only briefly glanced at. And the big question for me is, why did this, the crown jewels of British Intelligence when it comes to GCHQ document, end up in the hands of a disillusioned young contract worker in Hawaii? For me it's a debacle up there with Saddam Hussein's WMD. And the question really is why are we having these catastrophic failures, the consequences of which are going to play out for years, and not in a good way?

So let's talk first about what we did publish. There were two broad categories; one spying on allies and the other one, bulk data collection from the web and telephone systems. Spying on allies. So it turns out we were spying on friendly countries including NATO allies, largely for economic reasons. A lot about the global financial infrastructure. In a lot of cases it really looked as though it was basically to give Gordon Brown an edge when he

went to talk about the shape of the global financial infrastructure. The question is, was this a good use of our intelligence resources? Well we argued, probably not. Is it going to stop? Maybe but I really doubt it.

Let's go on to bulk data collection and bulk decryption of that data. So the basic story is that with fibre option cables, your capacity to suck up information far outpaces democratic oversight of that capacity. The same laws, basically, that applied to the era of the crocodile clips and copper wire applied to the fibre optics although those fibre optics carried millions of communications at the same time.

Our argument was that this was a fact that citizens had a right to know. The counter-argument is that this was all passive collection. You had these rivers of information that were being driven into a reservoir. Now for GCHQ and NSA to go fishing in that reservoir they needed a permit, and the counter-argument is that strict rules applied to the getting of those permits. So no harm, no foul.

Now, to what extent is this really okay? To a certain extent it depends on how much you trust a government. In the US, where distrust of government's role in the lives of the citizen is kind of in the national DNA, as expressed in the constitution, it's not okay with a lot of people. Europeans of course, with their experience of totalitarian regimes, feel even stronger about it. Here in Britain we trust the authorities a lot more.

For example we're completely okay with blanket CCTV in a way that's not the case in the US and Europe. Here I think CCTV is a good analogy, because it's passive collection. On the whole, someone's only going to bother to look at it if something bad happens and so we're happy with that. So it's similar in that way to bulk data collection, about which William Hague has assured us that if you're a law-abiding citizen you have nothing to fear.

But let's try a thought experiment on that and extend our analogy. CCTV is in public places. What if the network was extended into our workplaces, places we go to socialize and into every room in our house? So imagine there's this bald guy in overalls who comes into your bedroom and is putting up a camera and a mike and saying, 'No don't worry, if you've done nothing wrong then you have nothing to fear.' I think in that case you wouldn't be feeling quite as at ease as you were, and you're wondering when exactly as a society did we talk about this and of course we didn't. And neither the Cabinet nor the NSC nor ISC had a discussion about the reach of Tempora.

And if you think about it, we think about Britain as well, we're never going to have a government that's going to pervert the intelligence, we don't have those same fears that they have on the Continent. But really you only have to look back to 2002, 2003 for evidence that in this haven of rectitude you can end up with a government that was prepared to bend the intelligence, to a certain extent with the compliance of the intelligence agencies.

Then you look at the GCHQ guidance that it gave to the NSA when the NSA kind of hosted a legal thing for the NSA analysts who were going to come to Britain and do their training here. It's basically an advertisement and here's a quote from the PowerPoint

presentation: ‘We have a light oversight regime compared with the US and we’re less constrained by NSA’s concerns about compliance.’ It points out that Britain does have an investigatory powers tribunal, which assesses complaints about the intelligence agencies but so far, quote: ‘It’s always found in our favour.’

Now just a little bit about the question of damage and here I'm just talking about the material we put out. Before we published any of our stories, there was an extensive dialogue with the government in both the UK and the US about the potential and you know here we had the D-Notice Committee and there was also to and fro with the DA-Notice Head of committee. He made a point to us, he said that when a publication of information represents a direct threat to life in any way, he abandons the normal rules, he abandons neutrality in which he's a kind of broker between media and the agencies, and abandons the confidentiality of the discussions and so an injunction could be applied. He made it clear that never happened in our case, with his discussions with us.

Now on the claim that monitored terrorists and criminal networks going dark as a result of the disclosures, well looking through the documents, that was always a threat throughout. It was a threat through encryption, where there would be lots of memos saying, ‘it's going dark’ and then the biggest threat of all was geo-political.

The telecoms companies are moving more and more of the fibre optic networks to the Far East and so our distinctive advantage of having viewed where all the transatlantic fibre optics came up was whittling away and there was lots of concern about that. So it's always in danger of going dark and it's always a fight to stay ahead.

But - how much time do I have?

### Robin Niblett

You’ve talked for about 10 –

### Julian Borger

10?!

### Robin Niblett

Yes.

### Julian Borger

Okay I can leave the rest of the discussion and cut to the end

### Robin Niblett

Cut to the end then we’ll come back.

## Julian Borger

Okay, yeah. I wanted to talk about how did this material end up with Snowden?

## Robin Niblett

It was your opening question exactly.

## Julian Borger

I'll run through it quickly. The figure we were given, 850,000 Americans have access to data, we didn't pluck that figure out of the air; it was given to the Cabinet Office by Washington when they asked for the extent of the damage. That's the number of NSA contractors who had top secret clearance. Now not all of them had the same access as Snowden but there was a good number of them who had it or could get it.

My big question is, this was a big surrender of sovereignty going on, a big surrender of control and you could see it happening in the documents and how did it come about? Really the answer was kind of gleefully in the big corporate drive in GCHQ was to get as close as lips and teeth with NSA, and to do that you break down all barriers and in the end you put all the common data in a common cloud and that's how it happened.

Has the society, politics, the intelligence agencies begun to address that? No, not really. What there is, is there's still a criminal investigation of us at Scotland Yard. There's a unit looking into us, which is kind of the British way, which is to give the press a really good kicking and hope that the problem goes away.

## Robin Niblett

Well, as I think we can see from everyone here in the audience today, I think the problem or certainly the debate is not going away. You put a number of ideas on the table there Julian, I think there were many more you wanted to put forward and I'm sure you'll have a chance to come back to them.

I found it very interesting that you kicked off - and I'm just saying this so everyone can reflect on the key points, rather than for you to come back and I'll see whether Jane or David want to come up on these within their opening remarks - but you kicked off about this being about spying against allies and for economic reasons. That's an interesting point because certainly from the approach that's been laid out, at least publicly, certainly by the US administration is that spying of this sort is done for national security reasons if it is, not for economic reasons.

So what you said there is a very important point and you gave the example of giving Gordon Brown an edge in G20 negotiations as one example of maybe what the Brits wanted but that's the important point.

The second then I think is all about the bulk data collection, which you spent most of your remarks on and this really was the issue of oversight. I didn't hear you challenge as much whether bulk collection, good or bad, but certainly and maybe you do have views on that

– hold them – but the big issue becomes about oversight and I know Jane this is a place where you have particular experience, having had to play an oversight role in the US and I look forward to your remarks on that.

The third point I hope we will come back to is the issue of vulnerability. The point you're making is the *Guardian* and Edward Snowden in other words have actually done a public service by demonstrating perhaps, the extent to which these issues are out there and therefore hackable by many other people. Jane, I'll let you make the remarks you want, on the points you want, if you can keep it to seven or eight minutes that would be great.

## Jane Harman

I will. Thank you Robin, thank you first of all for your leadership here but also for your partnership with the Wilson Center. Many in this audience I think know about the Wilson Center, we have a network of 4,500 alumni scholars, many of them in England and in fact Mike Van Dusen, our former long term executive vice-president is here because his daughter is a Don at Cambridge but he's also putting this network together so those of you who know and love us please step forward.

The other person I want to acknowledge is Meg King, who is my chief of staff and who put together the first of this series, which was a panel in Washington, Sir David was beamed in – technology is marvellous – and we had a number of Americans on three different panels, the last of which was young people. I see some young people here, talking about their perceptions of these issues, which differ considerably from old people - that would be me - and whether they're better or worse, young people will be the decision-makers in the future so their views are going to be, I think, what controls.

At any rate I'm delighted to be part of this, I've been here twice in the last year, speaking in smaller groups in the pit room to some of the membership here about these issues and I still care intensely about them. I'm still to some extent in the game and I also have to recognize Sir John Scarlett, who I think has done enormous service in this country, who actually showed up for some of my prior gigs and I'm very grateful to him for showing up again and for participating in some other activities today.

So, I don't start this debate with 5 June 2013, the day that the Snowden leaks began. I start it with 9/11 2001. All of you were alive, I personally was headed to the dome of the US Capitol, I was then a member of Congress on the intelligence committee and that is where the intelligence rooms formerly were housed, in the dome of the Capitol and most people think that that dome was the intended target of the fourth hijacked plane, which went down in Pennsylvania.

So it was a pretty riveting experience. Cell phone rings, office calling, something horrible has happened, the Capitol was just closed. I head back to my office, second phone call, the office buildings are now closed, everyone is milling around and we had absolutely no evacuation plan or any kind of plan, survival plan. I mean looking back some might think that...never mind I won't go there. That was intended to be humorous, not as dark humour as it came out.

## Robin Niblett

Yes, I was going to pick up on it.

## Jane Harman

Don't put that on your list Robin. So, unprepared. We talk about intelligence failures, massive intelligence failure, no question about it, even though numbers of people including me, had written reports predicting a major attack on US soil, there was not enough attention paid to the possibility that this could happen and obvious mistakes were made in finding the clues and connecting the dots so that possibly this could've been prevented. But at any rate, riveting moment, really changed America and many of our friends.

I - and lots of others in positions of power at the time - was determined to prevent another such attack on US soil and that framed a lot of the actions that I participated in and I think that was the right call. We anticipated another major attack, fortunately it hasn't come. There have been attempted attacks and small attacks but nothing major and I do think some of that can be credited to the fact that post-9/11, practices were put in place that have so far helped thwart another major attack. Not just in the US but in Europe too. Some of the really ghoulish ideas that have been out there have been foiled in collaboration with our friends at GCHQ and other places and the West remains a target.

So, just going quickly through this, there were laws on the books, the laws permitting the intercept of phone calls were not new laws. Those began basically in the 1980s when Ronald Reagan was president, through an executive order. An executive order does not have the force of law, it can be superseded by law but it was in effect and that's the legal basis on which, to the extent this happened, cell phones are tapped. We can talk about this more, but that's not a post-9/11 law.

The collection of metadata and some of the other things we discussed happened after 9/11. First the practices happened in secret; the Bush White House determined that using the president's emergency powers system should be put in place to enable information about a foreign terrorist - that was always the predicate: a foreign terrorist – to be traced through 'chaining', a system that now most of you understand, to other phone numbers.

That was the origin of that programme. Congress was not consulted. When it became clear three or four years later, after the programme leaked, that it did not comply with our law, which is the Foreign Intelligence Surveillance Act, I won't go through all the details, but we can't... Congress had a public debate about this programme and amended the law and since then the programme has been in compliance with law. It's been overseen by the Congress and it has been reviewed by our Foreign Intelligence Surveillance Court, which is a federal court. That's sort of the short summary.

So segue to a year ago and Edward Snowden's leaks, what have we learnt? I'm hopeful that Edward Snowden's personal 15 minutes are about to be up. The guy whose 15 minutes I'd like to extend, is Banksy. I was very impressed that he confessed to doing a mural near the GCHQ headquarters recently but it is not that we should not be paying

attention, but we should be paying attention it seems to me, in a format that does not put a – as you called him, Robin, – a young,... one of you did, you did. I don't want to put words in your mouth but they were basically 'a 29 year old kid in the driver's seat here.'

We should be having this public debate. Let me be clear: we should be mending the laws in the United States and we should be working with allies on a set of international norms that we can agree to, and we should make sure that an anxious public feels respected. But we also should, I clearly believe we should, have a system of laws and practices that help us find the plans and intentions of foreign terrorists who are intending to attack us. Let's just focus our attention on the events of the last couple of days.

This group, far more extreme than Al-Qaeda, called ISIS, is in process of taking over Iraq and destabilising the entire neighbourhood around Iraq, and I would like to know, if some of those terrorists, who may be from the West; Americans are suspected of being in Syria training with this group, at least seventy of them. Numbers of Brits are also possibly part of this group and other Westerners, the figure I heard was two thousand plus Westerners being trained.

I would like to know if those people have plans and connections and are coming back using passports that will get them back and then possibly coming back through Europe to the United States to attack us, and possibly mount a very serious and devastating attack. And that is the reason why we need these laws and practices.

Final thing to answer your three questions Robin, spying on allies for economic reasons. The United States does not do that, Britain does not do that, another Western country may do that, and certainly China and Russia do that. But we don't do that. The telephone programme, my view, tapping Merkel's cell phone, my view, if it occurred - I don't think it's ever been really acknowledged – was a bad idea. As President Obama said, 'Just because we can, doesn't mean we should.' And we should not have done that.

Your second one was oversight. I think our system of oversight could work better but I think it works and the third vulnerability, I think I have just addressed that and I would finally conclude by saying that politicians – I am a recovering politician – and laws, are analogue.

These problems are digital, and it will always be a struggle to come up with a frame that will give people comfort and protect us, that can cope with the evolving technology. I don't really know how to do that but I'm counting on the younger generation to figure that out since your minds work that way, in a way that the rest of us, the digital adapters like me, I don't have that mind digital natives do.

## Robin Niblett

Thank you Jane. I now think of ourselves as a kind of analogue panel as you said, trying to deal with a digital problem. If you don't mind being included in that group David, as an analogue part of the response. You've got a range of points to pick up on; two different ways of looking into this anniversary, I think one could say, perhaps not that much

different actually on how they come out of it but certainly different ways of going into it. How do you see it?

## David Omand

Well, let me say something about what I think the public has learnt over the last year since these revelations. The first is, we've learnt a great deal about the nature of intelligence activity in the digital age and the nature of cyber activity in a digital age and what we've learnt is not just applicable to the United States or United Kingdom as a close ally but to what China and Russia and Israel and France and a whole list of other countries that the Vodafone report that was released last week reveals, are all rather interested in digital intelligence. So we've learnt something that perhaps we should've known before, or realized before as the public.

Secondly the public has learnt too much for its own safety, for our safety, about the details of intelligence activity in the digital age because the public also includes the foreign dictators, the terrorists, the serious criminals, the proliferators, the paedophile networks, the people smugglers and all the other people who mean us harm and they have learnt a great deal and we're now beginning to get a feel for the level of damage that has been done to our intelligence and law enforcement intelligence gathering. The figure of 25 per cent reduction in coverage of serious criminals is one that I saw very recently. So that's a second point.

I don't in that respect look at the *Guardian* newspaper and say, 'you've been irresponsible.' I fully accept that the *Guardian* took steps to make sure there was no direct threat to life, but the nature of the publicity around the whole story, the details of what was released and even if it wasn't the *Guardian*, the *Guardian* for example withheld one particularly damaging report but it popped out anyway because the journalist thought that it was wrong for the *Guardian* to suppress it. And there are lots of news media around the globe who've been pushing this stuff out or putting it on websites so that has done damage.

We have much more damage to come to our law enforcement, through the difficulty of serving proper legal warrants on criminal activity, serving those on the ISPs because internet companies have all made it very clear that they don't want to be seen to cooperate with government; they'll only respond to a legal warrant and they're busy moving themselves offshore. There's a whole policy agenda about trying to construct a better way of international warranting to get round that problem that Snowden has accelerated.

In the United Kingdom, speaking now about the UK, we have learnt or, we should have learnt, from the work that's been done by the Interception Commissioner - a very senior retired judge, tough judge, Sir Anthony May - that a) everything GCHQ has been doing is lawful, b) what they have been doing and the processes they have been following are compliant with the European Convention on Human Rights and the Human Rights Act, in particular in relation to Article 8.

The judge has put in his report that there is a very strict system of warranting both by the home secretary, for domestic communications, and the foreign secretary, for overseas

communications and these distinguish between the bulk access, which is authorized to the internet by the computers to obtain warranted information, and which bits of information on people or targets it is authorized to look at and bring out.

So I very much regret that one of the things that the public may have learnt is completely the wrong point, which is to confuse bulk access to data by computers, in order to find the communications of the terrorists and criminals, and mass surveillance. And every time I open the *Guardian* there's some headline or piece talking about mass surveillance. And as the senior judge, Sir Anthony May said, there is no mass surveillance being conducted in the United Kingdom or against the United Kingdom by GCHQ or indeed against any other country.

I think we've learnt, perhaps quite usefully, the power of communications data for law enforcement and when the judge looked at the warrants and so on, the huge majority of those were police, they were law enforcement, most of them were reverse look-ups; simply finding missing children, eliminating suspects from enquiries and some of them then actually led to evidence being produced in court from the communications data.

But we've also learnt from the judge that the British definition of communications data in the Act is narrow. If you like it's an analogue definition and quite right too, because the British definition is 'who called who, where and when', as you would with an old-fashioned telephone. The fancy metadata stuff about which there's been a lot of Snowden revelations, including our complete browsing history, the address book sucked out of our mobile device - that's content in UK law, and you need a warrant for that. And that was not, I think, understood by most of the journalists.

Personally I wouldn't touch that in the legislation. I don't want to see that turned into a digital bit of legislation, which then actually lowers the bar. I think I feel much more comfortable knowing that a Secretary of State has to sign a warrant and lawyers look at it and all the rest of it before they can actually get at your browsing history.

We've learnt quite a lot about oversight. Some reassuring, some less reassuring. I'm very reassured by the Interception Commissioner's report; he's kind of broken ranks with his predecessor, he's published a detailed report explaining how it all works. Why on earth that couldn't have been done years ago and therefore the revelations wouldn't have been so revelatory, I don't know, I actually do criticize government over the last few years, for now having been much more open. Not about the details of intelligence activity, but about how the system works, how oversight works, how the warrant system works.

There's a bigger question mark over the Parliamentary oversight and I think Malcolm Rifkind, current Chairman of the Committee, and a former foreign secretary, former Defence Secretary; very experienced statesman, is beginning to recognize that to be credible, a Parliamentary oversight committee has to be technically competent, has to be able to listen to and absorb arguments which are contrary to the Establishment's arguments. In the United States a sort of Civil Liberties panel has been set up to advise, and maybe that's the kind of thing we need to think about.

I shocked the home secretary yesterday at RUSI where she was giving a speech, by asking a question saying, 'Why don't you actually publish some specimen warrants, anonymised? Change the details so you couldn't relate it, but actually so that the public can see that this isn't somebody walking in and saying, 'Can we buy X?' It's a detailed case, lawyered with justification, and every one of those warrants again we've learnt, has to pass the necessary test; it has to pass the proportionality test and that is in the law.'

Two quick points because I'm almost out of time. We've learnt, as the public, something that is pretty shameful we didn't realize before, which is the business model of the internet. How is it that these internet companies make tens of billions of dollars a year, and charge us nothing for the services they provide? And the answer is because they monetize all our personal data so if you really want a debate at Chatham House, I think it's much more relevant to talk about the private sector's use of data. Frankly I trust the public sector's use of data in a way more than I do necessarily the private sector's.

I think probably I should stop there. Oh I'll just say that the 85 of 850,000 people at top secret clearances in America, for a country of how many? 100 million, 400 million? 300 million? Well it's a daft argument because just because you have a top secret clearance does not mean you get to see code word signals intelligence material], and certainly not British material and the British materials on the GCHQ intranet, which was mirrored over so that the Brits in the National Security Agency and a certain small number of key Americans working there, would have access to it.

What Mr Snowden of course managed to do, not just with that but with American, is actually get into all of that. That was a serious security breach, it showed a great deal of laxness, the NSA has confessed this to Congress and steps are in hand, I'm sure, to make sure it couldn't happen again. But just remember after 9/11, which newspapers were talking about 'end the need to know. Go for the dare to share.' All the politicians in Congress and elsewhere saying this must never happen again, we must join up the dots.

## Robin Niblett

David, thank you. I've just realized as we went through this, of course we've had three different types of perspectives from three key parts of democratic governance: the media, the legislature and the executive in a way, as well as getting three different perspectives in terms of outlook. There are so many issues one can pick up on, I'm not going to try to. I'd like to get people in as quickly as possible and I think rather than going one at a time, given how much limited time we have, I'd sort of like to get a range of viewpoints up and let you react to them.

I think Julian you may want to come back as well, on some of the points you heard from Jane and David, which were kind of addressed to your opening remarks and you could maybe come back on them on the economic issue or whatever. One issue I would hope we'd come back to as well, if it doesn't come up in one of the questions here, is the issue – and I've heard you Jane talk about this before and I think we did it in Munich as well – the lack of a public debate about how allies deal with the new security threat.

We went through CND, whether nuclear deterrent is good or bad, painful protest debates but they were done sort of in the open and we got somewhere. People may not have agreed with the final system of deterrence that was used in the Cold War but at least it was debated, whereas it seems that in that post-9/11 moment, a lot of this was pulled together almost secretly, it was never debated publicly and therefore there's a huge catch-up effort now, to try to get people on board. People in the government say, 'well you should've known, of course we had to do this for your security, didn't you know?'

Well, it wasn't debated and there are different perspective and obviously we're playing catch-up now. I've seen some hands go up, so I'll grab them. Please say who you are, it can be a comment, doesn't have to be a question but try and keep them short so we get as many viewpoints in as possible. If people are comfortable I might run five or so minutes over because we are recording some of this, we don't have to finish bang on 4:30, some of you may have to leave, but I'd like to get some viewpoints in.

## David Omand

I have to finish up, I've got to go and teach.

## Robin Niblett

You'll have to go 4:30 on the dot because you have to go and teach but I may just go two or three minutes over if I have to. So you had your hand up very insistently, I'll let you come first, introduce yourself. I'm looking around here.