Transcript

Book Launch: *How Spies Think: 10 Lessons in Intelligence*

Professor Sir David Omand

The Strand Group, King's College London

28th October 2020

**Jon Davis**: Good evening everyone. Greetings from Peckham Rye for the forty-second Strand Group. My name's Jon Davis, and I'm Director of the Strand Group. It's my absolute great pleasure to once again introduce to the Strand Group Sir David Omand.

David's been a great friend to the Strand Group but also to its precursor, the Mile End Group, and – if you take them both – we are at 151 events this evening, and David's headlined – spoken at more, but headlined seven; which, with my maths, puts that at about five per cent. So he's got a "season ticket", and we're absolutely delighted that he has.

David, as we all know, is one of the great British experts on security and intelligence, having worked for a very long time at the Ministry of Defence, and then as boss of GCHQ; at the Home Office; and then finishing his career in Whitehall as Security and Intelligence Coordinator.

Tonight we are launching his new book – wonderful stuff – *How Spies Think*. I've had the great pleasure of reading it over the past days; it's a rip-roaring read, and it's really something that will stay with me. And without further ado, I'd like to hand over to Sir David, who's going to speak for about thirty minutes, and then we will hand it over to questions from the audience, so do send them in via chat, and we will select and get through as many as we can. David: you're welcome – so welcome – as always.

**Sir David Omand**: Jon, thanks for the introduction. I'm delighted to be back, talking to the Strand Group; I just look forward to the day when we can actually all meet live at King's College.

[Sir David's talk, to around 31:18]

**Jon Davis**: Thank you so much; so much in there. And I can see that there's a few questions coming in… I'd like to ask just a couple myself – just one up front, and one at the end:

*You finish the book on an optimistic note, after pointing out so many problems – page after page of modern problems. I think that people would like to hear: what are your reasons to be cheerful?*

**Sir David Omand**: In part it is because I am an incorrigible optimist, and therefore that is arguing against myself, because that optimism tends to infect my analysis and I have to be careful about that. But I can see some straws in the wind. The internet companies themselves, who for years have stoutly maintained that they simply controlled pipes, and what passed down the pipes was nothing to do with them – they've now begun to realise that what is passing down their pipes is extremely toxic in some cases, and they actually have not just a moral duty, but a legal duty, to start looking at what is going through their pipes and dealing with it. And Twitter, for example, is now labelling some of President Trump's tweets; Facebook has taken tens of thousands, if not hundreds of thousands, of pieces of Covid disinformation off their platform. So that’s one straw in the wind.

But I think, more fundamentally, what gives me optimism is the effect of "sunlight" – that we are now beginning to understand how the magic of the internet… what is behind it. The online auctions that fill the web page you click on with advertising which is directed at you personally, because the machines know all about you, because they've been collecting this personal data and collating it, and slotting you into a category, along with others, that all share, say, a hundred characteristics. This revelation, really, came to most people after the Cambridge Analytica scandal, but now you can see this is how it works – and it's a good thing, because it means that when you click, information that you're looking for is more likely to surface, because the machines already know – from your past behaviour – what it is you're likely to be looking for.

When I search "1984", it will probably come up with references to George Orwell's book. If someone else were to search the same term, they would come up with a whole lot of historic things that happened in 1984, simply because other people would have different browsing histories.

So we can see that the internet has that magical capability, which – used properly – is actually a benefit. And Covid has demonstrated, of course, that our social interactions are now mediated through the internet. And what a good thing: how would we have kept in touch with our closest others were it not for the power of the internet?

So the fact that we're beginning to understand the bad things – where they come from; how they can be managed. And at the end of the book I suggest that we start in the schools, and we start teaching critical thinking to children at a young age, and take them through their own internet journey so that they become much more critical, and aware of what it is that people are doing to them. And once you've begun to realise that, a lot of this stuff loses its power. It may have had a big impact for example in the Brexit referendum; if you held another referendum, would it have the same power? Probably not, because I think we can now see the machinations that took place.

**Jon Davis**: Thank you. So let me move over to some of the attendee questions. The first one is from Martin Plaut, who asks:

*How badly has the trust between the UK and USA been damaged by President Trump?*

**Sir David Omand**: You have to be careful about using the word "trust": it's quite a slippery word; I prefer the term "trustworthiness". So if you were to look at the intelligence community, or the defence community, and say, "Is there still a high level of trustworthiness in the behaviour of each towards the other?" I would say it's undiminished, and if anything it's been enhanced in the last few years. So the level of cooperation is higher than it's ever been. And trustworthiness comes from integrity – perceived integrity – actually seeing that promises are kept; that behaviours follow the pattern of what you say. So you can actually say, at the professional level, that we are still an extremely trustworthy partner. At the political level – and this is not unique to President Trump; we've been there before, if you remember Edward Heath's conflict with Kissinger over European policy – you can have ups and downs. Or indeed the 1956 Suez crisis; you can have very serious disagreements about policy and approaches, but if you still maintain trustworthiness…

Now, President Trump can be erratic in the views he expresses in tweets, and that makes him harder to read – no doubt this is deliberate, but it makes him harder to read. Therefore it's harder to ascribe trustworthiness to policy utterances that appear on Twitter. But that hasn't affected the underlying relationship between professionals.

**Jon Davis**: Thank you. From Captain John Aitken of the Royal Navy:

*Do we still need spies? Can secrets be kept in a digital, interconnected world?*

**Sir David** **Omand**: Well, there are two parts to that question, aren't there: do we need them; and even if we have them, can they be effective? So let's separate it out into those two components. Do we need them? Yes; and the reason we need them, I think, is very simple: because there are a large number of people out there who do deliberately mean us harm; and they will go to almost any lengths – including extremely violent lengths – to keep their intentions, and their actions, secret from us. So the only way you are going to get a glimpse into what they're up to – and it doesn't matter if you're talking about people-smugglers, or criminal gangs, or terrorist groups, or indeed autocrats – is secret intelligence.

The second part of the question – is it getting harder? In some instances, yes, because in a digital world it is much, much harder to deploy some of the traditional methods of human intelligence. It's not impossible, but it's more expensive; it takes longer; you have to be more careful, and it will take more time. But the digital world also provides information about people as individuals: where they've travelled to and from; how they've communicated; where their money is stored. So being clever about the digital world can give intelligence which previously, in the more traditional world – the analogue world – would simply not have been possible to obtain.

So it's swings and roundabouts. I think we do need to have spies, if you call them that – intelligence agencies – providing that missing dimension, for policy-making and military command; and there are ways, still, of providing it. But it will be different, again, in the future.

**Jon Davis**: Thank you. We've got a question here from Andy Howard:

*How do you feel about the prospect of analysts dealing with "big data" and automation? Is the amount of data too big for human cognition?*

**Sir David Omand**: The answer must be yes, because the amount of data that is potentially available is beyond any human comprehension. You've got three billion people on the planet with digital mobile devices, busy sending stuff to each other, and communicating, and logging on to websites and so on; so you do need clever filtering; and then you need to have the machine-learning systems, the AI systems, which allow sensible questions to be posed to the data, particularly searching for particular kinds of patterns – supplemented by human intelligence – so somebody is seen in an internet café in North Africa, who is suspicious; can you actually find out the IP address of the machine from which he was sending the message, and the time… Can you cleverly search the likely global streams of data to pick out that kind of communication? And as we know, from the work that was made public for the 2016 Investigatory Powers Act, a lot of this *is* possible. And increasingly, of course, we will have visual recognition systems; digitised hi-res cameras at borders… So there will be information which can be sifted and looked at.

One of the most interesting areas which I know the United States is investing in is [to do with the fact that] we have imagery of most of the planet in quite high resolution, both commercially available and from drones and satellites. There is more imagery available than any conceivable number of analysts could look at; you would need millions of people to look at it. But you could have programs running over this data which could say, for instance, that at a particular farmhouse that was associated with a criminal group in the past, a 4x4 has been seen to turn up unexpectedly. That may be the start of an investigation which could have very important consequences. So digitisation has to go hand in hand, in the intelligence world, with the clever development of AI. And it's all got to be done in a legal framework that gives the public reassurance that this is not going to interfere with our privacy rights as citizens. So it will be done in accordance with the Human Rights Act, as it is done today.

Now, that's going to be quite tricky to fix, in relation to – for example – police use of facial recognition systems, as we already see. But it will be done; I'm quite confident about that.

**Jon Davis**: OK. Now I presume that this question is from *Professor* John Gearson – one of your colleagues in War Studies:

*Thank you for a fantastic talk. Your "S" = strategic notice, but how do we achieve strategic confidence between decision-makers and their spies?*

**Sir David Omand**: Well, the first thing, again – it comes back, doesn't it, to trustworthiness. So are the senior spies, if you'd like to call them that – the chiefs of the intelligence agencies – that is, the senior officials there – are they acting in ways that, over time, demonstrate trustworthiness? The information that they provide… The integrity shines through; it's not distorted; it's not aimed to please; it's not aimed to make a point. I sometimes talk about one or two ministers that I've come across in the past, who – for them, the policy-making… *"I'll give you the policy; you go and find me the evidence to support it."* So "evidence-based policy". We all know that that is *not* evidence-based policy, and you need to look at the negatives as well as the positives, which is the point I was making about inductive error. But the intelligence agencies are in a very privileged and special position, and they have to demonstrate that trustworthiness.

At the same time, the politicians and senior officials have to demonstrate, to the intelligence community, trustworthiness going the other way; that they're not going to let individuals swing in the wind, when occasionally you get an error, or occasionally the media stumble across some[thing] and put it on the front page. So it's mutual confidence, and mutual support, based on a fairly open relationship. I think the UK is extremely fortunate in having that kind of relationship; and if you look across Europe, you will find some countries where that relationship of trust simply has not existed, and there is mutual suspicion. And that's a very bad situation to be in. We're not there; we're not in that position.

**Jon Davis**: Another one of your old colleagues – Tim Dowse – asks:

*On the issue of strategic notice, given that political leaders are rarely focused on threats beyond the next election, who should have the responsibility of scanning the horizon for the unknown unknowns? Might think-tanks and academics be better placed to do this than Whitehall officials and bodies like the Joint Intelligence Committee?*

**Sir David Omand**: One of the points I was making in my remarks is that most of the information you need to get a handle on some of these long-term, over-the-horizon risks is available from open sources. You've got the whole world of science and technology; you've got things like climate change; you've got the evident growing tension between the United States and China. You don't need secret intelligence to produce an analysis of some of that. I think the important thing is that those on the inside are prepared to reach out and have dialogue with those on the outside – in particular the academic community, as a sort of outreach. And this happens much more today than it did when I first started to get involved in these sort of activities, because it is quite likely to be the think-tanks, or the academics, that have begun to realise that some development, far off in the future, could become a problem.

But you still need somebody – and I think perhaps it *is* the Joint Intelligence Committee – to take the time to think about what would be the implications were this event, or development, or whatever, to come to fruition. They can focus on national security; others could focus on other parts of national life, and chief scientists are very good at doing that. But if you think about Covid-19… Covid-19 has killed more of our fellow citizens, done more damage to our economy, than any conceivable terrorist incident, or hacking incident, could have done. The national security implications – for example, maintaining the deterrent; keeping our armed forces operational, despite the fact that the supply chains have all been disrupted as people have to shield, and all of that; the huge disruption all of that has caused – these are direct national security interests. So a paper, or a briefing, by those on the inside, drawing on the knowledge of those on the outside, is what I would, I think, recommend.

We sort of already have mechanisms to do that, but I personally think we ought to be thinking about drawing closer together – in adjoining rooms, if you like – those who are looking at the natural hazards that might affect our security, and those whose professional job is to look at national security intelligence – and put those two in adjoining rooms, and you might begin to get a better handle on some of the other things that might come and hit us.

**Jon Davis**: Thank you. An old friend of the Strand Group, Sean Finnan, from the commercial computer world, asks:

*If the internet companies now have to police what is in their pipes, why should we be confident that their truth is any more correct?*

**Sir David Omand**: I don't think we can be confident of that, so you have to keep testing it; it's *"trust but verify"*, as President Reagan used to say. So we will judge by their actions. There are going to be hard cases, and there already have been, where freedom of speech bumps up against protection of the public. We have different laws over what can be said in public, or indeed passed through social media, than the United States does, and they tend to be a bit tougher on the freedom-of-expression side of it. If you go to Germany, you get a much tougher view, for example on antisemitic speech. So each society decides what it is that it really wishes to protect the public from. There is, I think, universal agreement that child abuse is a bad thing, and the internet companies have been driven to look very carefully with AI algorithms at whether images of child abuse are coming down their pipes.

The reason, of course, that they've done that is not just because, as they would say, they are being socially responsible; it's also because advertisers have come up to them and said, *"We are not prepared to place advertisements on your platform if there's a risk that our advertisement is going to appear next to some abusive image, because that will trash our reputation."* And a number of big companies have really applied leverage. So the Facebooks of this world are now employing thousands of people to check out a lot of that material.

But you can't stop there being hard cases at the margin, and sometimes the companies will decide to suppress something that, basically, probably doesn't need suppressing, and vice versa. But as long as most of it gets suppressed, then we're in a better position than simply saying, *"No, there's nobody policing this particular domain."*

**Jon Davis**: Next question, from Julian Huppert:

*Thank you for the talk; I look forward to reading the book. What's your assessment of the importance of encryption – for privacy, cybersecurity, and intelligence?*

**Sir David Omand**: This is one of those questions where the answer has changed in the course of my working lifetime, from *"Encryption is necessary, obviously, for national secrets, but you don't want it to get out of that domain into general use, because it makes law enforcement, and military activity and so on, harder."*

That has changed; encryption is now fundamental to the working of the internet, because of the financial transactions that are carried by the internet internationally, and domestically our use of the internet for purchasing. And if there is doubt about the security of those communications, we are in deep trouble, because we've sold our soul to the internet; our future economic and social life is completely dependent on the internet working and being trusted. So encryption has to be strong, and that poses this awful problem for intelligence and law enforcement: what happens when you seize the suspect's iPhone, and you believe that on it is terrorist-related material, but you can't get in it, because it's securely encrypted.

No fully satisfactory solution to that has been found: sometimes it can be opened; sometimes there are loopholes that have been left by other apps on the phone; sometimes you can get at it through the cloud, with the cooperation of the company, even if you can't hack into the phone. A long-term solution will have to be worked out. Personally I rather favour split-key solutions – I know some of my old colleagues don't think this is workable –but a split key – where you have half of the key in the chip itself, so it can't be meddled with – hard-baked in the chip – and the other half is held by a trusted party; and with the production of a court order, from a court that is accepted as a court of record, then you would get the two halves of the key and you could put them together, *if* you had the device. But that would only open one device; it wouldn't open everybody else's device.

So that's the kind of thinking that needs to go on – well, *is* going on, I know – but actually turning an idea like that into a practical reality that doesn't cost too much money would be a major, major task. So this is still work in progress, and if anyone listening – some of the King's postgrads and so on – if they've come up with a really clever idea, then I think the Home Office would be delighted to hear from them.

**Jon Davis**: Well, one such postgraduate – Harry Bloodworth – asks:

*With regard to the growing potential for a no-deal Brexit, what impact do you see this having on the European security community, and how worrying is it for Britain specifically?*

**Sir David Omand**: A very good question; a timely question. Personally I would divide the security community into two parts. If we have in mind operational cooperation between the British intelligence agencies and their European counterparts – mostly bilateral but sometimes trilateral – then it will make no difference. And that would include most of the counterterrorism work which is conducted through the Berne group [*Club de Berne*], outside the European Union, and these bilateral relationships are valuable to both parties, either side of the channel, and will continue; I have no doubt whatever about that. And they're not governed by the EU, because Article 4 (2) of the European Treaty explicitly says national security is a matter for national governments: it's not an EU competence.

The other half of national security is law enforcement, and law enforcement *is* a European competence, which is why you have the Schengen information systems; you have Europol; you have the Prüm Convention, where granular data about suspects – including DNA, vehicle licences, criminal records – all of that is available at the tap of a key to Schengen members, and, at the moment, to the United Kingdom, because we've signed the necessary agreements, overseen by the jurisdiction of the European Court of Justice [ECJ].

The UK government's view – that you can't possibly have the European Court of Justice overseeing anything in the future – means that, at the moment, there seems to be an impasse, where we can't get access to that kind of information after the end of the year; we would need some new legal instrument. I just hope and pray that the negotiators, somewhere, are busy working out the EU-UK security treaty, or some legal vehicle, which would allow that sharing to continue.

The same is true of things like counter-narcotics information, where there are specialist counter-narcotics bureaux – again, part of the EU competence. We contribute a lot to those, and they help us, particularly in relation to new synthetic drugs. If we are cut off – as, in theory, we would be, certainly by a no-deal, but also if we haven't got another, parallel agreement to put in place – then we will suffer, and so will our European partners. So on the law enforcement side, I am very concerned; so far there's been radio silence from the government about what is going on, if anything, on that front, and we'll have to wait until the end of the year and see if they then magically produce some agreement which allows us to continue to contribute.

When you talk to professionals across Europe, in the law enforcement and intelligence community, they all say, "We must continue to have this granular level of cooperation with the UK": the UK needs it; they need it. At a political level, it's difficult to see quite how you fix that if we are insistent on our conditions – that is, not allowing these arrangements to be subject to the jurisdiction of the ECJ.

So, a mixed answer.

**Jon Davis**: Thank you. We are running out of time, but I just want to ask a few more questions if…

**Sir David Omand**: I'll give quicker answers. *[Laughter]*

**Jon Davis**: No, don't you worry, they're fine. First one from Strand Group member Dr Michelle Clement, who asks:

*What one change would improve decision-making in government today?*

**Sir David Omand**: All right: let me have a punt at that. Safe spaces. If we could be assured that there were safe spaces where the senior politicians – not their special advisers, but the senior politicians themselves, and their senior professional advisers: senior civil servants; scientists; intelligence community; whatever – could meet, and they were talking truths to each other, and because there were no witnesses, people didn't have to pretend – they didn't have to posture on either side – particularly if views changed; and you could actually drill down to *"Well if that's really what you want to do, Minister, this is what it will take to do it; this is how long it will take to do it; and if we've confidence that you understand that, we'll do it."* Too often, I think, we've slipped – partly busy-ness, and all the rest of it – into really not having a deep enough exchange; and it can be painful on both sides – because the official side will have to realise that some of the advice they've given perhaps wasn't quite as good as they thought it was, or the management of the subsequent actions wasn't as efficient; and the ministers will have to recognise that sometimes they've been guilty of magical thinking, and announcing things without really being sure how on earth they were ever going to be implemented.

**Jon Davis**: There seem to have been quite a few students online, and it's possible that you are inspiring them. And so there's a question which I think, in different ways, several people have asked, which is:

*What training would you advise to pursue a career in intelligence and security?*

**Sir David Omand**: It doesn't really matter what initial formation you have; if you've got the right kind of mind, and the right kind of personal characteristics – to be able to work in teams; to be able to lead teams – then the technical knowledge you need you will pick up very quickly. A heretical view perhaps; but given what we've been talking about, Jon – about the importance, in the digital age, of really understanding how all this stuff works – one of the bits of preparation I advise, when I get the chance, is just make sure you *do* understand all of this stuff – it takes a bit of hard work; there are some quite difficult books you've probably got to read, in order to understand – because then you become an intelligent customer.

I'm not suggesting anyone go off and write abstruse code and so on, but you have to be an intelligent customer. One of the reasons GCHQ is so successful is that even if you enter with a first in History – or Mods and Greats, or whatever it might be – within six months, you are expected to master the digital domain. And intelligent people can do that. The tragedy is that in civil government, to express that rather broadly, the level of competence – of being an intelligent customer – is not as high as it needs to be.

**Jon Davis**: Lovely. Thank you. And a last point is that there seems to be quite a bit of discussion online about the painting behind you, and I think that the most specific suggestion is that it's Robert Walpole, or a contemporary – 1720 -1740?

**Sir David Omand**: Bit earlier – about twenty years earlier. Admiral Sir George Rooke: the man who captured Gibraltar. It's not really a Godfrey Kneller, but it says on the bottom, *"Studio of Kneller"*, so it's that period. But he captured Gibraltar, leading an Anglo-Dutch fleet, which is quite an interesting thought. About 1702.

**Jon Davis**: There we are. That brings us to an end; I think it's been great. Thank you David.

**Sir David Omand**: Thank you, Jon.