TRANSCRIPT – INTERVIEW #2

ASPI Interview with the Director-General ASIS Paul Symon

28 September 2020

Graeme Dobell (GD): Paul Symon, welcome to ASPI. Paul, what does ASIS do today?

Paul Symon (PS): Three main functions. Firstly it collects intelligence. As we did on the 13 May 1952, we continue to obtain for our government, intelligence from overseas.

The second function is what I broadly describe as intelligence diplomacy. The fact that we have counterpart organisations almost in every country of the world—intelligence agencies talk to intelligence agencies, they share information. They will often have conversations where that line of communication can be on some very sensitive subjects that the diplomats prefer not to have or, indeed, countries on the other side would prefer conversations to be held between intelligence chiefs rather than diplomats. There's that element of intelligence diplomacy. The other element of intelligence diplomacy is in the region, in our near region, there are countries that actually need some support and help, some capability uplift, to let them defend their own national sovereignty better than they currently are. So, again, we help with training programs and deliver some capabilities to countries in our near region. So that's the second.

Firstly—collect intelligence. Secondly—intelligence diplomacy. The third main one under the Act, the Intelligence Services Act, there's a Section 6.1 e provision which indicates that the Minister can direct us to do activities—and that has obviously the ability the government, the ability that if they wish for us to undertake disruptions or activities that are probably going to be enabled by good intelligence. But actually allow us to undertake disruptions, whether it's disrupting a terrorist plot or some type of activity where there is an action that occurs. That's the third broad category. Those activities I can't authorise, they have to be authorised by the Minister and the way the Act is written is that the Minister authorises an activity like that, she also needs to consult other Ministers including the Prime Minister, who may be affected or impacted by those activities that we do.

GD: Where does human intelligence fit in the cyber age / the digital age?

Well, humans are a social animal. There is human along with other forms of intelligence, you mentioned cyber. Well-informed, thoughtful individuals will recognise and appreciate what they say over telecommunications devices and what they say by way of email, that there are agencies that can collect that type of intelligence, and a lot of people know that and therefore avoid that form of communication. So really what most countries need is a combination of cyber, SIGINT and HUMINT. Humans will develop trusting relationships and share secrets—they are willing to build a relationship with a service like ours that cultivates, recruits and validates them. There is a relationship that builds. So when you're trying to understand senior leaders around the region, or further afield, you're trying to understand the way they're thinking, their vision for their country, the risks that they see, and the opportunities they see. Those sorts of conversations are normally held in inner circles, and are between humans, and will always be that way.

GD: Why are people willing to take those risks, why are people willing to betray their country's secrets?

Well, there can be a range of reasons, as a general proposition, I would argue that if you're in a closed society than there is a stronger possibility that you will be concerned about the direction of the country. If people become leaders of everything in their country, if power is concentrated and centralised, then ultimately you become responsible for everything. And you actually become responsible for the way in which your citizens perceive leadership. So there is an interesting medium-to-long term dimension to this, as a general rule closed societies run the risk of a greater number of individuals willing to betray the secrets of their country, because they are not happy, they don't get a voice. We get a voice every three years, we go down to the local school and we vote. But there are a lot of people that don't. That is one motivation.

GD: ASIO says that the threat from espionage from foreign interference to Australian interests is extensive unrelenting and increasingly sophisticated, what does that mean for ASIS?

Well it means that we need to innovate and we need to stay ahead. So there is a really compelling culture in ASIS to understand technology, emerging technology, to look at the environment in relation to start-ups, to new and emerging technologies, and how they can be adapted to allow us to undertake the risky activities we undertake, and reduce the risks of being compromised. So there is a competition at play here, in many ways, if you think of the match analogy, we are playing attack in ASIS, and ASIO [the Australian Secret Intelligence Organisation] by-and-large are playing the defence.

The margins between the two overseas are close. We believe that we still have a marginal advantage to obtaining the secrets that we obtain, but we don't rest on our laurels and we cannot afford to be complacent. That's why science and technology is an important component to how we think about our tradecraft.

GD: Moving from those first four decades of the Cold War, how does ASIS operate in a new environment when you're thinking about grey zone activities, disinformation, multi-polar great-power competition, what does that mean for the sorts of choices you have to make?

Well I think it follows on from that last question—that the operating environment is getting harder and therefore we have to double-up in our determination to use technology, to have the quality of people we require to deal with, as you say, the grey zone environment. The grey zone really is increasingly being used in the lexicon to reflect the fact that we are in this environment of coercion short of conflict. And that is keenly felt inside the intelligence community, whether it is on the defence or the offence. The other comment I would make is that it's often a term that the military is using, and I think our military and the other militaries around the world are thinking very very carefully around coercion short of conflict and the role of the military. We cooperate with and work very closely with the Australian Defence Force, so not only do we have to stay across the best of new technologies or emerging technologies coming through, but our partnership with Defence has to get even deeper and even stronger, and I think that's really driving us at the moment.

GD: What is the legal basis for what you do?

The Intelligence Services Act is the legal basis for what we do. Anyone watching this can get on the internet, and put in Intelligence Services Act 2001 (ISA), and it's there. Section 6, which relates to the roles and functions of ASIS, amended quite recently as you mentioned before, all of those amendments are in there. That's the legal basis on which we are held to account. Held to account politically by my Minister, the Foreign Minister, to whom I am answerable. Answerable in an accountability sense to the Inspector General of Intelligence and Security, who has the powers of a standing royal commission. The IGIS and the staff of the Inspector-General literally drop onto my computer systems, my highly classified systems, they can look at any files, and it is all made

available to them. So at any time if they have concerns about legality or propriety of what we are doing they can actually go in and have a look. Then to Parliament through the Parliamentary Joint Committee of Intelligence and Security who looks more at our administrative aspects of the Service. But it's there in the ISA and observed in the breach every day by the Minister and the Inspector-General.

GD: Everyday as you sit down how do you think about those checks and balances - how does that frame the way you approach each day?

I think it has meant a couple things. The training of our people has to be very well bedded on an understanding of the law, the meaning of propriety and legally, understanding functions and priorities. I cannot, and senior officers cannot, micro-manage our people in the field—they have to make judgements when they are dealing with an agent, that are very fine judgements indeed. The understanding of the law, and the basis upon which they are undertaking activities in the national interest, has to be something that is very well understood.

What it also means is, that inside ASIS, there is this outstanding written record of everything we do. If you looked at our internal correspondence, literally all of our activities are written up in great detail, and when I say great detail, I am not only talking about the nature of the meeting with an agent and the conversation or intelligence or information which is passed, but considerable detail about body language, personal life, all of that is recorded. Because we always want to validate, to check, that all the information we are getting is accurate. That the agent themselves are at a point in their life where they are not getting distracted or not being coerced—there is a lot of things that we are checking on as we build a relationship with our agents. Everything is very well written down inside the Service.

Coming back to your question, it manifests itself in our people having a really good understanding of the law, and the proper purpose and function of the Service, and a very strong written record of everything we do which obliges them to be honest and write down everything they see, observe and hear.

GD: Using that Officer / Agent approach, you've said that ASIS isn't just about providing context and information, it has to make a difference to government. It has to enable outcomes and actions. How do you measure that?

We are actually measured by other agencies, but I will come to that. We are also pretty demanding on ourselves, by demanding I mean, we are awash with information, open source information, very much the mantra inside ASIS is the quality of the insights we are able to help policy makers understand. In other words, as close to the foreign decision makers as we can, to provide those quality insights that our policy makers need. So we are pretty demanding on ourselves, around the quality of the insights. If we get information from an agent, and it doesn't substantially add value to what's available in the public domain, we won't publish it. So we set pretty high standards internally. But we are also evaluated, and this is one of the functions that ONI [Office of National Intelligence] has really stepped up with, so we have 'mission evaluations', a mission may be counter-terrorism. So each year a range of agencies in town, both policy and intelligence agencies, are asked to mark our homework. And they speak very openly and honestly about how we have added value to the counter-terrorist understanding inside Australia, so of course ASIO would be asked, the Federal Police would be asked, policy agencies are asked. Those reports are done on an annual basis, across a while spectrum of areas. We undergo scrutiny from other policy and intelligence agencies, and ONI pull

that together, we've literally just finished a round of evaluations and come under the spotlight from other agencies.

GD: Let's finish this with a discussion of risk. How much harder is it, how much riskier is it, to actually get human intelligence now?

Well there has always been risk involved. We accept risk, we can't be cavalier. There is a very strong thread of education, knowledge and understanding about risk management. We have a whole area separate of the operational line-areas that undertake compliance and risk management, so they oversight operations independently to ensure that risk management techniques are adopted in the way that many organisations think about risk management. International Standard 31000 (ISO31000) which is the international standard to assess risk, the likelihood of those risks being realised, the consequences of those risks. Every activity we do is written in considerable detail, and planned in considerable detail, the vast majority of those activities in the planning stage, contain the risk management plan. Risk has always been part and parcel of what we've done, but I would say it is deeply entrenched in the way we think about our activities and operations, and depending on the overall risk at the end, the overall risk determines who ultimately is the delegate is to approve an activity or operation. Obviously the highest risk ones, I will be the delegate, but there will be lower or moderate risk activities where people at lower levels can approve the activities or operations. I think we've got it about right, in terms of, strong thread of risk, right through the organisation in the way we plan activities—but an agility through the delegation through to overall risk that lets us generate activities quite quickly, certainly at the more low-to-moderate end. Obviously the high-risk activities I take responsibilities for those in case they are compromised.

GD: When those high-risk calls land on your desk, what is the value threshold, the risk threshold, that you use that makes you decide, I am willing to put his person's life at risk because I want these pieces of information—how do you make those judgements?

It's judgement isn't it. It's more art than science with these sorts of things. But at the end of the day you're simply staring at benefits, what the benefits will be for policy makers, what the benefits will be for the national interest, and having to weigh that against the risk that we have to live with in obtaining that information. If we think the benefit is there, it might be that we redo the risks over and over again, in other words, think about every vector to achieve the outcome without necessarily following the first plan that comes forward. Often if the benefit is there, it won't follow that we'll necessarily undertake the activity in the way its first been planned, it may well be that it goes back and we may say, okay what other vectors, what other opportunities, what other INTs could we use, to achieve that effect. And that's where agencies like us and ASD work very closely together to see, if we don't need to take the risk up to a particular threshold, if I can keep the risk down but still obtain the benefit, than that's what I will do. But we are a risk accepting organisation. There are many activities that we do that means you don't sleep as well at night as you might like to, but we've deduced that the benefits are worth it in the national interest.

GD: Finish this by talking to me a little bit about how you weigh that risk and accountability equation, how you think that through, if you have to think that through when you go to bed at night. How does that work for you as the Director-General?

Well it means trust, trust becomes everything. I have to trust my people and know my people in able to trust them in the way they are engaging with the risk. It's also true that my relationship with my Minister and the trust that goes with that relationship is really important, the Foreign Minister carries a heavy burden, she is our chief diplomat, and she is advancing Australia's interests every day. She

has to have faith that we will consciously and diligently undertake activities, we will plan them very carefully, and we will do everything in our power to mitigate the risks. But she, like the other side of politics, has been a beneficiary of ASIS's most extraordinary activities and operations, and very much appreciates everything we do. But trust is everything in this business.

GD: Paul Symon, thank you.