Director-General's Annual Threat Assessment

Director-General of Security
Monday, February 24, 2020

Ladies and Gentlemen, thank you for coming.

And welcome to the Ben Chifley Building.

I'd like to pay tribute to three former Directors-General who are here – David Irvine, Dennis Richardson, and David Sadleir, along with his wife, Judith.

I'm honoured by the attendance of so many friends, colleagues and partners across government, the intelligence community, the public service and policing – including members of the Parliamentary Joint Committee on Intelligence and Security, Directors-General, Secretaries, Commissioners and the Inspector General of Intelligence & Security.

Our foreign friends and partners are also represented, including by the Canadian High Commissioner. Welcome.

And it would be remiss of me not to acknowledge and welcome members of the media.

The main purpose of my talk tonight is to deliver my first Annual Threat Assessment.

Some of you may think of this as ASIO stepping out of the shadows.

The glib response to that might be that we have always been out of the shadows it's just that our people are so good at what they do you have just never noticed them!

A more considered response is I'm taking this opportunity to talk about the security environment we are facing, explain what the threats are and why they are a problem.

I want to move beyond the bureaucratic language of annual reports and help everyone understand the significant threats we see directed at Australia and Australians. And I want to give you some insights into what ASIO does every day.

I want to be clear that the ASIO I have the privilege to lead is not a secret organisation operating as a law unto itself, conducting shadowy business around the margins of our democracy and our law.

Nothing could be further from the truth and nothing could be further from the vision I have for ASIO and its place in the life of Australia.

We are an organisation that operates in full accordance with Australian law.

ASIO has significant powers under law, but our application of these powers is proportionate to the security threat or matter at hand.

We are not seeking to be a secret organisation with secret powers. That would not be an agency that I or my staff would want to have any part of. And I'd also be confident neither would any of you.

Yes, we need to keep secret the precise nature of many of our operational capabilities and the details of our operational activity.

These are the tools of our trade that give my team its edge to prevail against some of the most difficult challenges imaginable and so must be protected.

I will never knowingly put any of my team at additional risk by carelessly talking about their operations.

I see ASIO very much as your security service, working to protect Australia and all Australians from those who would seek to do us harm.

As Director-General of Security I am committed to ensuring that ASIO always operates legally and ethically.

As your security service we don't just do what is allowed; we do what is right.

As part of that I intend to bring my own personal belief in the power of sunlight and transparency to bear as a fundamental principle of my tenure as Director-General.

I will therefore be as open and frank with you as I can about what we do and why we do it.

I will continue to welcome public debate on the extent of ASIO's powers. Such conversations are a vital part of our democracy.

And, I will continue to welcome our regular and frank engagement with parliamentary committees and with the Inspector General for Intelligence and Security, who, I remind you, has powers that are very similar to a Royal Commission's.

I'm very pleased to see Margaret Stone is here this evening. I can assure you that the Inspector General is rigorous in her oversight of us, and that is entirely appropriate.

ASIO is enabled by the law and we are overseen by our Minister, the Attorney-General, the Government, our Parliament and the Inspector General. The law and our oversight are fundamental to our success.

At times I will seek to talk about ASIO publicly. At other times it will be through open and respectful conversations with community and business groups, the media and with our elected members of Parliament.

I hope you will value this engagement and I trust you will also understand and respect when I say that I cannot talk about certain subjects in the detail you might want.

If I cannot discuss something it will be because it will risk a significant national security capability or it will risk the safety of my officers or the Australians they seek to protect.

Through the parliament, the Australian people have entrusted ASIO with significant powers of investigation. These are used to protect Australia from only the most serious threats.

Unlike many other agencies in the National Intelligence Community, we use our powers to investigate fellow Australians.

Of course some of ASIO's enquiries establish no threat to security and no further action is required. In these cases it is imperative that our enquiries remain confidential.

This is one reason why you will often hear me say I cannot comment on specific individuals or cases. A security service in a liberal democracy like ours must investigate in secret to protect the reputation of the innocent.

So, let me start by talking a little about ASIO as an organisation.

When I commenced my role as Director-General of Security I made a commitment to my team that I would spend my first 90 days listening and learning about the organisation and about my new role.

And as it turned out, my 90th day was a Friday, Friday the 13th … I didn't plan that … but I did enjoy that fact… just a little bit.

And for those who know me will know how difficult it was for me to listen for that long!

But it was vital that I did so because ASIO and the role of Director-General are like no other organisation or role I could imagine.

It perhaps goes without saying that I have been impressed by the work ASIO does.

I have also valued the fact that my organisation is part of the Home Affairs Portfolio and part of a highly capable and dedicated National Intelligence Community.

ASIO in fact operates as part of a wider national security team that includes state and federal agencies, departments and enforcement agencies, as well as our overseas partners.

Protecting Australians and Australia's interests' demands partnerships.

And of course, one of our key partnerships is with the Australian community.

So, on that note, please let me take a few moments to highlight the single most important element of ASIO's business: our people.

The people who work alongside me every day are ordinary Australians just like you. They may be doing extraordinary things to protect you but when they are not at work they are ordinary members of our community.

They have family and caring responsibilities. Many of them have mortgages and worry about the same sorts of things that we all do.

They may be your neighbours or your friends and you may stand beside some of them in a supermarket queue or on the sidelines of a sporting event.

Members of our team have also been on the front-lines battling bush fires and at times of crisis many of them put on their ADF Reserve uniforms to continue their service to their community in other ways.

The point is we are you. It is just that the people on my team spend their days working anonymously but tirelessly to identify and stop those people who would seek to do our community harm.

My team put themselves on the line and wrestle with significant complexity and risk every day.

Their efforts ensure that Australians can live their lives in safety, and that our economy and institutions remain secure and free from covert, pernicious foreign interference.

If they do not tell you where they work, or they sometimes have to use assumed identities, it is not because they wish to be deceptive. Rather it is a very necessary part of enabling them to do what they do effectively and safely.

In the national security business the term, *human intelligence*, refers to the classical business of recruiting and managing human sources for intelligence purposes.

Such operations are a rich part of our heritage and remain a critical part of our armoury, even in this fifth generation world of hyper-connectivity, massive data and artificial intelligence.

If I can riff off that heritage and offer a shameless recruitment plug for ASIO, our success is built on the imagination and intelligence of our humans.

We need people who can out-think and out-imagine our adversaries, and who can harness the power of technology and data alongside good old fashioned relationship building to achieve our mission of protecting Australia.

We also need to ensure that our workforce continues to mirror the diversity of the society we serve.

So if you are interested, I'm just saying… www.asio.gov.au

I promised at the start I would provide you with the first of my annual threat assessments, but before I do that I must address one other aspect of our operating environment.

Some of you might be wondering how technology impacts and enables ASIO's business. Surely, the time of human-focussed intelligence has come and gone?

As the first Director-General of Security to have also led ASD, I am perhaps uniquely placed to answer this.

ASIO's range of capabilities and special powers are more relevant than ever in this transformative technological age.

But it is also fair to say we are also challenged by technology, the Internet, encryption and the dark web.

In responding to this challenge let me first recognise the enormous upside to technology and connectivity.

The internet has massively democratised access to knowledge and it has enabled incredible new businesses.

Global connectivity and the ready availability of messaging apps which are encrypted for privacy, offers tremendous capabilities to connect with each other, whether across the street or across the world (or even across the lounge room or dinner table – you will know what I mean if you have young people at home).

While these things are a force for good they also have a potential dark side when used by those who would seek to do harm.

Encrypted communications damage intelligence coverage in nine out of 10 priority counter terrorism cases.

That's 90% of priority cases!

And that's just counter-terrorism. In the counter-espionage world we are dealing with even more sophisticated targets.

The government recognises this dilemma as do senior executives in the tech sector. We need to work together to help organisations like ASIO and the police defeat the threats posed by malicious use of the Internet, while protecting the opportunities and freedoms it offers for all Australians.

It is important we continue our open and productive dialog. We must be open about the challenges, open about the need for balance between privacy and security, and open about the importance of the rule of law that supports a free society, while at the same time providing the right response to the security threats we all face.

Technology should not be beyond the rule of law.

Contemporary legislation, such as TOLA (*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*) that came into force just over one year ago offers a clear case in point.

The relentless advance of technology was outstripping our technical capabilities to monitor threats and protect our fellow Australians. Remember, encrypted communications impacts intelligence coverage in nine out of 10 priority Counter-Terrorism cases.

So we needed some changes in legislation to allow us to deal with the effects of that technology while still preserving the essential integrity and privacy of those communications for ordinary Australians.

I can confirm that ASIO has used the Assistance and Access Act to protect Australians from serious harm. We needed to take advantage of the new powers within 10 days of the legislation coming into effect – a clear indication of its significance to our mission. And I'm happy to report that the internet did not break as a result!

The bottom line was this, these new powers helped ASIO prevent a real risk of injury to Australians.

That is not to say we've solved this challenge, we haven't and we continue to face challenges to our lawful access capabilities.

We know this and we are responding with energy and purpose.

We are making judicious investments in technology and our people. And we are continuing to balance the need for new powers alongside privacy and other concerns to ensure that we can continue to deliver on our mission.

Consideration of new powers is not just confined to the impacts of technology, we also review our powers and their suitability in helping ASIO identify and deal with evolving security threats.

Having the right technology applied to the right problems is of course vital, but it is our people that have always been the critical element of our success. And I am confident that by putting the right people with the necessary legal authorities onto the right problems we will succeed.

Now getting to the main purpose of tonight's talk. Let me begin with the terrorist threat.

ASIO's number one mission continues to be protecting Australians from threats to their lives.

The terrorist threat remains at PROBABLE.

That is, we have credible intelligence that individuals and groups have the capability and intent to conduct terrorism onshore.

ASIO has previously assessed and stated publicly that the threat posed by terrorism in Australia has plateaued at an unacceptable level. This is sometimes misunderstood as the fact that the threat has simply plateaued.

So let me be clear: the threat of terrorism at home is PROBABLE and will remain unacceptably high for the foreseeable future.

The unfortunate reality is that, right now, terrorists are still plotting to harm Australians.

Some of that plotting is occurring within small cells of people meeting in secret but equally worrying is the ease with which terrorists continue to use the internet to spread their hateful messages, radicalise people to their cause and provide how-to-advice on committing atrocities against Australians.

I am particularly concerned that we continue to see vulnerable and impressionable young people at risk from being ensnared in the streams of hate being spread across the internet by extremists of every ideology.

As a father, I find it truly disturbing to see cases where extremists are actively trying to recruit children who have only just started high school and are as young as 13 or 14.

Our view is that the threat of terrorism will remain a constant feature of the global security environment in 2020 and the threat to Australia and Australian interests will remain.

The number of terrorism leads we are investigating right now has doubled since this time last year.

The character of terrorism will continue to evolve and we believe that it will take on a more dispersed and diversified face.

Violent Islamic extremism of the type embodied by the Islamic State and al'Qaida and their off-shoots will remain our principal concern.

Tens of thousands of Islamic extremists travelled to the Middle East to join AQ aligned groups and ISIL, including from countries which weren't previously known as sources of Islamic extremists. And as we all know Australians joined that movement.

There are now more Islamic extremists from more countries active in more places than ever before.

But we are also seeing other actors operating in the terrorism arena.

Intolerance based on race, gender and identity, and the extreme political views that intolerance inspires, is on the rise across the western world in particular.

Right-wing extremism has been in ASIO's sights for some time, but obviously this threat came into sharp, terrible focus last year in New Zealand.

In Australia, the extreme right wing threat is real and it is growing. In suburbs around Australia, small cells regularly meet to salute Nazi flags, inspect weapons, train in combat and share their hateful ideology.

These groups are more organised and security conscious than they were in previous years.

We continue to see some Australian extremists seeking to connect with like-minded individuals in other parts of the world, sometimes in person. They are not merely seeking to share ideology and tactics.

Earlier this year, ASIO advice led to an Australian being stopped from leaving the country to fight with an extreme right wing group on a foreign battlefield.

While these are small in number at this time in comparison to what we saw with foreign fighters heading to the Middle East, any development like this is very concerning.

Meanwhile, extreme right wing online forums such as The Base proliferate on the internet, and attract international memberships, including from Australians. These online forums share and promote extremist right wing ideologies, and encourage and justify acts of extreme violence.

We expect such groups will remain an enduring threat, making more use of on-line propaganda to spread their messages of hate.

While we would expect any right wing extremist inspired attack in Australia to be low capability, i.e. a knife, gun or vehicle attack, more sophisticated attacks are possible. And we also need to be mindful of state-sponsored terrorism as states seek to use terrorism to further their goals.

This dispersal of the terrorist threat and the range of actions they might choose to carry out will continue to complicate our efforts to combat the threat they pose.

We will need to continue to monitor a threat spectrum that stretches from self-radicalising lone actors across the range of extremist ideologies through to experienced terrorists associated with long standing extremist groups.

And we will need to protect against attacks that range from individuals using knives or their vehicles as weapons in crowded spaces, to meticulously-planned high-casualty terrorism.

It is also clear that we will need to remain constantly alert to the enduring power and attraction of extremist messaging to those vulnerable to radicalisation.

Despite the best efforts of governments here and abroad to manage terrorists who have been jailed for their offences, extremist ideologies run very deep.

We have all been shocked by the recent experiences of our UK friends, where radicalised individuals, released from prison, took the opportunity of their freedom to attack their fellow citizens in the name of their extremist cause.

I recognise that this is a complex problem to solve but it does reinforce to me, at least, the need to remain vigilant about the reach and the strength of extremist messaging.

We cannot afford to become complacent about the potential threat posed by terrorists after their release from prison.

Let me be clear that, whatever the motivation of terrorists, whatever the method planned, they will continue to be creative in evolving their methods in response to both our investigative efforts and protective security measures.

ASIO must therefore remain vigilant and be ready to take the necessary actions in response to these threats.

Threat to life will always be our top priority but it is not the only serious security threat I am concerned about. So let me now cover espionage and foreign interference.

Espionage is pretty much what it says on the tin: foreign intelligence services seeking to steal and gather national security, economic or other information.

Most nation states conduct espionage. Indeed, countering espionage was the reason ASIO was formed more than 70 years ago and it has remained a central part of our mission ever since.

Foreign interference is a broader, more nuanced concept.

All foreign states seek to influence deliberations of importance to them. When those activities are conducted in an open and transparent manner they are not of concern.

However when it is conducted covertly by, or on behalf, of a foreign actor; when it is clandestine, deceptive corrupting or threatening in nature and when it is contrary to Australia's sovereignty and interests, we classify this as foreign interference.

Foreign interference is about covertly shaping decision-making to the advantage of a foreign power and, left unchecked, it becomes highly corrosive.

Almost every sector of our community is a potential target for foreign interference, particularly:

- our parliamentarians and their staff at all levels of government;
- government officials;
- the media and opinion-makers;
- business leaders; and
- the university community

Regardless of the methods employed by hostile services and nation states, Australia is currently the target of sophisticated and persistent espionage and foreign interference activities from a range of nations.

ASIO has uncovered cases where foreign spies have travelled to Australia with the intention of setting up sophisticated hacking infrastructure targeting computers containing sensitive and classified information.

We've seen visiting scientists and academics ingratiating themselves into university life with the aim of conducting clandestine intelligence collection.

This strikes at the very heart of our notions of free and fair academic exchange.

And perhaps most disturbingly, hostile intelligence services have directly threatened and intimidated Australians in this country. In one particular case, the agents threatened the physical safety of an Australia-based individual as part of a foreign interference plot.

The level of threat we face from foreign espionage and interference activities is currently unprecedented. It is higher now, than it was at the height of the cold war.

Indeed, some of the tactics being used against us are so sophisticated, they sound like they've sprung from the pages of a cold war thriller.

As one example, I can reveal that a foreign intelligence service sent a ‘sleeper’ agent to Australia. The agent lay dormant for many years, quietly building community and business links, all the while secretly maintaining contact with his offshore handlers.

The agent started feeding his spymasters information about Australia-based expatriate dissidents, which directly led to harassment of the dissidents in Australia and their relatives overseas.

In exchange for significant cash payments, the agent also provided on-the-ground logistical support for spies who travelled to Australia to conduct intelligence activities.

These are the sort of insidious activities ASIO works to detect and disrupt every day. And in the case of the sleeper agent, I can confirm ASIO did disrupt the operation. Regardless, the threat is real and the threat is extremely serious.

What we are trying to protect here is nothing less than who we are as a society and who we want to be into the future.

As Director-General and as Mike Burgess, private citizen, I would think that is something worth protecting with all the energy we can muster.

So why do we use the term ‘unprecedented’? Well, it is because of its scale, breadth and ambition.

Espionage and foreign interference are affecting parts of the community that they did not touch during the Cold War.

And the intent is to engineer fundamental shifts in Australia’s position in the world, not just to collect intelligence or use us as a potential ‘back-door’ into our allies and partners.

There are more foreign intelligence officers and their proxies operating in Australia now than at the height of the cold war and many of them have the requisite level of capability; the intent and the persistence to cause significant harm to our national security. But the character and focus of that espionage activity continues to evolve.

Hostile foreign intelligence services are being directed to target us:

- because of our strategic position and alliances;
- because of our leadership in science and technology;
- because of the unique expertise that exists across our economy; and
- because we are comprehensively retooling our defence force and the defence industrial base.

Hostile foreign intelligence agencies have always sought access to personal information because they want to identify and cultivate potential human sources.

We still see hostile services continuing their efforts to recruit human sources in much the same way they always have but, thanks to the efforts of ASIO and others, that is getting more challenging and includes more risk for those services than ever before.

As a result we are also seeing hostile foreign intelligence services recognising the opportunities presented by the internet and the proliferation of social networking applications.

In the past, attempted recruitment was time-intensive, expensive and risky because the foreign spies would need to operate on location and in person.

But now, they can use the internet to work from the safety of their overseas headquarters to launch cyber operations against Australian networks and to send thousands of friend and networking requests to unsuspecting targets with the click of a mouse.

Many of the attributes that make social media so valuable also make it vulnerable. Professional and social networking sites share rich stocks of personal information, and that makes it much easier for hostile foreign intelligence services to gather the information they want.

Critically, those same platforms then offer those hostile services a low-cost and easily disguised method to approach their targets and so we are working to help educate people on these threats.

It can be difficult for me to talk in detail about this aspect of our work because we don't want to make life easier for our adversaries by telling them what we do and don't know about their operations.

But I can tell you this: over the last few years, ASIO has consistently detected and regularly disrupted espionage operations in Australia.

While terrorism is almost always public – it's visible both when we disrupt it and sadly when we don't – espionage and foreign interference has been different.

Due to the very nature of spying, the efforts of my organisation to detect and counter espionage have almost always been hidden from public view.

But this is changing.

While we will continue to deploy our traditional highly classified tools and tradecraft to counter espionage and interference, these tools will not be enough on their own.

There is now a robust public discussion on the threats posed to our safety and prosperity by espionage and foreign interference. This is a conversation which I very much welcome as a vital part of strengthening the resilience of our community and our democracy.

As part of this conversation, the Parliament passed new legislation, relating to espionage and foreign interference. This is already bringing dividends and it is likely to grow in importance for us.

And the government has recently announced the establishment of a Counter Foreign Interference Task Force which is operating out of this building. With all of the critical elements of the national security community engaged by the Task Force it will become a vital element of our strategy to defeat this threat.

I can tell you tonight that the mere passage of this new law caused discomfort and possibly pain for foreign intelligence services. We have seen tradecraft and behaviours change; we've made it more difficult for them to operate here.

We know this won't stop it all, but it does and it has made a difference, driving more cost into their risk calculus.

I'm confident any future announcement of a prosecution will have a further chilling effect – and certainly a successful prosecution will – although it's important to understand that prosecutions are not the only weapons in this space.

Where ever possible, ASIO seeks to 'detect and protect' before damage is done. In this context, for example, I can confirm that ASIO has recommended visa cancellations when we've identified foreign agents trying to travel to Australia, and we've intercepted foreign agents when they've arrived here.

The point is that the unprecedented nature of the threat will require ASIO and our national security partners to deploy an array of effects to identify espionage operations directed against us.

Our thinking and our actions, our capabilities and our law must reflect the threat and provide what is needed to manage the risk and consequences effectively.

As Director-General of Security, I intend to step up our actions to counter espionage and foreign interference.

We will actively support the prosecution of espionage and foreign interference before the courts.

Now, for reasons I have already made clear, I won't talk about any of these matters any further, other than to say that we will need to have a wide range of tools in our tool box to counter this growing threat.

No one of them will succeed on their own but there is real power in being able to draw on all of them in the right combination to defeat individual threats and to develop the necessary cumulative effects to make Australia a harder target for our adversaries.

My message here is simple. If you intend to conduct espionage or foreign interference against Australia, ASIO and our partners will be hunting you. We will shine the light on this behaviour and we will deal with it.

In conclusion let me reiterate that ASIO is a capable organisation and our security and law enforcement partners are equally capable.

Those threats across the terrorism, espionage and foreign interference domains are formidable and continually evolving.

They will require us to deploy a range of imaginative and sophisticated effects to harden our environment to make sure we continue to detect threats and raise the cost of entry for our adversaries.

I know that, as private citizens and members of your security service, the members of our team are incredibly mindful of the very significant powers they have been granted.

They are focussed on only using those powers lawfully and in the most proportionate manner possible. And, always, in support of the mission to protect Australia and Australians from harm.

As an organisation we have a lot of work ahead of us to ensure that we can meet the challenges of technology and data that are impacting our operations.

But I am confident that with the thoughtful and innovative plans we already have in place, we will be able to bring the right technology and the right people together to solve those issues.

To ensure this happens we will be redoubling our efforts to make sure that we can continue to attract the best and brightest Australians to work with us on these challenges.

This will not only ensure that we can bring the ability to out-think and out-imagine our adversaries but it will also ensure that we continue to reflect the diversity of the community we serve.

As I've outlined tonight, the threats are significant, the security landscape is evolving and our adversaries are more determined and sophisticated than ever before.

But so is ASIO.

Nobody at ASIO, me included, is under the illusion that combatting these security challenges will be anything but really hard work.

But I can assure you that the ASIO team relishes the challenge and is up for that work.

We are your security service. And we are determined to make a difference.

Thank you.