

THE TERRORISM THREAT, THE INTERNET AND CHALLENGES FACING INTELLIGENCE AGENCIES



Mr David Irvine AO, Director-General of the Australian Security Intelligence Organisation

The United Services Institute of the ACT hosted a presentation by the Director-General of the Australian Security Intelligence Organisation (ASIO), Mr David Irvine AO at the Australian Defence College in Canberra on 9 February 2011. Mr Irvine discussed Australia's current security and intelligence operating environment, covering the following topics. What is the terrorist threat to Australia? Why has the Internet become a double-edged sword? What challenges do intelligence agencies face as they go about their business?

Tonight I should like to convey to you my own observations about the intelligence business, the security environment in which we and other 'western' intelligence services around the world operate, and the challenges to security posed by an increasingly globalised world.

The Intelligence Business

The value of good intelligence towards maintaining national security – often said to be the first responsibility of good government – cannot be underestimated. It is obviously intelligence, and the assessments which are made as a result of it, which help inform governments about how best to manage the risk of threats to security.

This is certainly not an easy task. It is made even more challenging by the need to strike the right balance between the accepted freedoms inherent in a democratic system while preserving the operational capability and integrity of the security intelligence function. I believe that the two are not mutually exclusive.

There is another essential characteristic of the business of intelligence. An intelligence assessment is just that: an assessment. Intelligence agencies are not courts of law, which for the most part render judgements on history, on events that have occurred in the past. The real business of intelligence is all about the future. It is a predictive subjective business providing assessments on the likelihood of events in the future, and in some cases acting to prevent or forestall them. It could be said that intelligence is akin to prophesy, with predictions based on the analysis of known information that in turn requires judgements

about the reliability of such information. Intelligence agencies seek to analyse information about intent and capability, sourced from the public domain through to that which is covertly obtained.

Obviously a modern intelligence agency, such as ASIO, applies rigour and sophistication in the way it advises on threats and risks. I like to think that we also apply reasonableness. In many ways, what we do every day is complex risk management in the national interest – but recognising that complete security can never be a permanent end state. As Eisenhower once said, "we will bankrupt ourselves in the vain search for absolute security".

ASIO's business sees it collecting intelligence through a wide range of means. We rely extensively on assistance from the Australian community to obtain information that enables us to assess and act to prevent threats to national security. This 'human' assistance can take many forms. Most overtly, we have the National Security Hotline, whereby citizens report suspicious behaviour particularly but not exclusively relating to terrorism.

ASIO also has a range of so-called 'special powers' that, when properly authorised by Ministerial warrant, can include telecommunications interception and entering and searching premises. We also conduct both physical and technical surveillance.

Because we are living in a globalised world, threats to Australian security almost invariably have international dimensions. This in turn requires ASIO to cooperate with other intelligence services throughout the world, both operationally and

exchanging intelligence information relevant to possible threats.

ASIO is the only agency in the Australian Intelligence Community authorised in the course of its normal duties to undertake investigations into, and collect intelligence on, the activities of Australian citizens. Given this fact, it is of vital importance that ASIO operations are conducted legally under appropriate legislated authorities and in accordance with a principle of proportionality, whereby our actions must be proportionate to the severity and immediacy of the threat. For this reason, ASIO operates within a particularly stringent oversight and accountability framework. Through committees such as the Parliamentary Joint Committee on Intelligence and Security, Senate Estimates, and the work of the Inspector-General of Intelligence and Security, ASIO is, perhaps, one of the most scrutinised organs of the government.

The Security Environment

We are fortunate to live in a country that has long been one of the most stable and safest in the world, offering its citizens the benefits of democracy, the Rule of Law and a persistent level of prosperity enjoyed by few others. That does not mean, however, that our people, our institutions and our national security are totally free from threat.

Terrorism

Terrorism – or the threat of politically motivated violence – is a persistent and permanent feature of Australia’s security environment. Protecting Australia from a terrorist attack is not only about saving lives; it is also about protecting the freedoms and safety we enjoy in our day-to-day activities.

The main terrorist threat continues to come from extremists who are part of, or take inspiration from, the global violent jihad movement. These extremists follow a distorted and militant interpretation of Islam which calls for violence as the answer to perceived grievances or to establish by force the supremacy of their branch of Islam. Within this architecture, Sunni Islamic terrorism, linked to South East Asia, the Middle East, Yemen, Somalia, and Pakistan/Afghanistan is currently a significant threat to Western interests globally. This is no less the case for Australian interests.

Al-Qa’ida remains the most obvious, but not the only, manifestation of the global violent jihad movement. Its core remains entrenched in the Afghanistan-

Pakistan region and is itself capable of orchestrating attacks. It has links to other extremists operating in various parts of the world. Other groups have remained independent of al-Qa’ida but have ongoing operational, training, propaganda or logistic co-operation with it. These include Jemaah Islamiyah in Indonesia, which was responsible for the deaths of over 90 Australians in terrorist bombings since 2002, and al-Shabab in Somalia.

There is a tendency for Australians to see terrorism as an ‘overseas problem’ – and it is true that the one hundred or so Australian victims of terrorism have been killed in attacks overseas. This view misses a critical element of the contemporary security environment - that plots to attack Australians at home are often inspired by events overseas. Equally, more Australians are being inspired (radicalised), especially through the far reach of the web, and seeking to travel overseas to either to train, support or participate in terrorist activities.

Within the Australian environment, we are seeing a worrying trend of ‘home grown terrorism’. Let me point out the following:

- Of the four terrorist plots disrupted in Australia over recent years, three would have been the work of home-grown groups, with little or no contact with al-Qa’ida or its overseas affiliates.
- Of the 38 people prosecuted for terrorism-related offences in Australia, 37 were Australian citizens, and 34 were either born here or have lived here since childhood.

We do need to ensure, though, a measure of perspective. Those Australians attracted to the violent jihadist ideology are small in number, not representative of broader Australians or any particular community group in Australia. They are a tiny aberrant minority with a dangerously distorted set of beliefs. Unfortunately, it takes only one person to set off a very large explosion in a crowded public place.

ASIO continues to assess that a terrorist attack in Australia is feasible and could well occur. Terrorist tactics appear to be evolving away from major shock attacks such as 9/11, to what has been described as “the strategy of a thousand cuts”. Because of the reasons I have just outlined, I predict we will see more instances of a Mumbai style of attack than those we have witnessed including in our own neighbourhood such as the Bali Bombings. Don’t discount, however, the desire of terrorist groups to inflict as much

damage as possible; no doubt they will make the most of any opportunity afforded them.

As the Government's White Paper on Counter-Terrorism earlier this year made clear, the Government takes the threat of terrorism very seriously indeed. While we can never guarantee that a terrorist attack will not occur and our protection can never be absolute, Governments have, over the years since 9/11, taken progressive steps to strengthen our counter-terrorism defences.

Cyber

One of ASIO's functions, and an issue which is garnering more headlines, is safeguarding against the theft of our secrets – the counter-espionage function. Often the media are focused on the particular challenge of Cyber security, however I do want to make the point that cyber is just one aspect of the larger, and more nefarious threat of espionage. Cyber is but one means to an end, but a focus on it should not diminish the efforts we are placing to counter other aspects of espionage.

The business of espionage has been around for a very long time. And it is still with us. If it were not successful, people would not still be attempting to carry out espionage in its various forms. You just have to look at the impact of recent media coverage on the allegations of industrial espionage at Renault in France to see that targets for attack can be anywhere. So espionage can run the gamut from "cyber warfare" to "economic warfare".

The form of espionage I particularly wish to discuss today is relatively new - cyber espionage has become a very prominent, and equally alarming, aspect of our security environment.

From a national security point of view the Internet presents particular difficulties. Counter-espionage and foreign interference have taken on renewed importance in recent years – in both their traditional forms and in ways that harness technology and the Internet.

We are only just beginning to realise that the extraordinarily democratic institution of the Internet may in fact be a two-edged sword, with implications not simply for commerce and trade, social interaction and privacy, but also for modern national defence efforts.

The explosion of the cyber world has expanded infinitely the opportunities for the covert acquisition

of information by both state-sponsored and non-state actors. Today, we see constant attempts by cyber means to steal the nation's secrets, as well as information vital to the effective operation of critical national industries and infrastructure, not to mention commercial intelligence and criminal fraud.

Cyber espionage has emerged as a serious and widespread concern and one that will continue to gain prominence due to the ongoing digitisation of data and increasing reliance on technology in commercial, governmental and military business. The demand for the convenience of on-line business is not abating. Indeed, the UK's Cyber Security Operations Centre has assessed that dependence on the internet to provide public services will soon "reach a point of no return".

The Internet means we collectively know more about everything than we've ever known before. We have produced more data in the last five years than humanity has produced in the last 100 000 years – of course not all of this data is valuable, or even useful! We expect to access it now. And we expect to be able to access it and share it at a moment's notice.

So what are we doing about Cyber?

The Australian Government is setting up new cyber security frameworks – over the last 12 months we have seen the establishment of the Computer Emergency Response Team Australia (CERT Australia) and the Cyber Security Operations Centre. But, is it solely the domain of Government to protect us?

Cyber is not new. We have all been grappling with IT security – and hackers – for many years, but the issue has gained traction (and headlines) recently. And rightly so. We are tracking behind the curve in a number of areas and it is time to get our collective act together. From my perspective, the threat of cyber espionage to Australian interests is very real, continues to evolve and develop and will present an enduring security challenge we all need to address. To do so, we need to come to grips with the nature of cyber threats and the need for various responses.

In the cyber environment, espionage (and even politically motivated violence and sabotage) can, and does, take place. It is ASIO's role to investigate cyber activity where appropriate and, most importantly, make sense of the cyber threat in the context of the broader security landscape. Cyber activity is just one aspect of a multi-faceted security world – and an

aspect which can be misleading if only seen through 'technical' or 'cyber' eyes.

The Australian Government has devoted considerable effort to redressing the situation, and helping the broader community commence its security stance. Two agencies I mentioned earlier are worth expanding upon as they are close partners of ASIO and demonstrate the direction the Australian Government is taking.

Firstly, CERT Australia, which sits within the Attorney-General's portfolio, is responsible for working with the private sector in identifying computer systems which are important to the national interest and providing these with information and advice to assist in protecting them from cyber threats. It also assists in developing national e-security policy. And CERT Australia is a source of information for the Australian community and, in this sense, works, primarily, in the unclassified space.

The CSOC is located within the Defence Signals Directorate and has two main roles. It provides the Australian Government with an understanding of cyber threats and, secondly, working with relevant agencies, coordinates operational responses to cyber incidents of national importance.

And ASIO is not hiding in the shadows, despite what you may have heard. We engage broadly within government and with our overseas partners, but, we also talk with the private sector – not just to collect information, but to assist the Australian Government's effort to help industry come to grips with security.

We know that despite the efforts to date, there is a way to go. And part of that way involves much greater collaboration between the government and private sectors. The Australian Government is already looking to work closely with the private sector as we try to counter the cyber threat.

In this regard, ASIO has a Business Liaison Unit which is working to provide information to the private sector through its website, briefings and fora. ASIO also engages with companies associated with Australia's critical infrastructure.

Challenges and Opportunities

By way of conclusion, I'd like to underscore some of the key points I've made during the last 40 minutes. I hope the picture I've painted has demonstrated the growing convergence in the threat landscape of intent underpinned by technology, regardless of the threat being terrorist in nature or espionage.

On Terrorism, one of the most significant greatest challenges facing not just Australian intelligence agencies but also our international partners is the rise and rise of 'home-grown terrorists' or what can be titled Micro - Terrorism. It is characterised by smaller scale activities, lower cost, and lower risk. These are local operations using local materials, but inspired by global philosophies. And they are much harder to identify and disrupt.

A good deal of intelligence work deals with secrets and is conducted in secret – using secret means to obtain secrets. We need ongoing secrecy not simply to avoid alerting the subjects of our security investigations, but also to protect both our specific sources and our operational methods. To be effective our officers should remain as anonymous as possible. Most important is our ability to protect the identities of our sources or the provenance of our intelligence information (some of which may come from foreign partners).

I've covered just a small number of issues that ASIO deals with on any given day here, it's a sample of the myriad of challenges and opportunities that our staff negotiate in order to fulfil our vision, "the intelligence edge for a secure Australia".

Biography: Mr David Irvine AO is a career diplomat who joined the Australian Foreign Service in 1970; postings included Rome, Jakarta (twice), Beijing and Port Moresby; High Commissioner to Papua New Guinea (1996-1999); Australian Ambassador to the People's Republic of China, Mongolia and the Democratic People's Republic of Korea (2000-2003) and Director-General of the Australian Secret Intelligence Service (2003-2009). 3. During the five years prior to his appointment in Papua New Guinea, Mr Irvine held several senior management and policy positions in the Australian Department of Foreign Affairs and Trade, Canberra, including management of Australia's relations with the major markets of South, North and East Asia, as well as Indochina. In March 2009, Mr Irvine was appointed Director-General of Security, in charge of the ASIO.