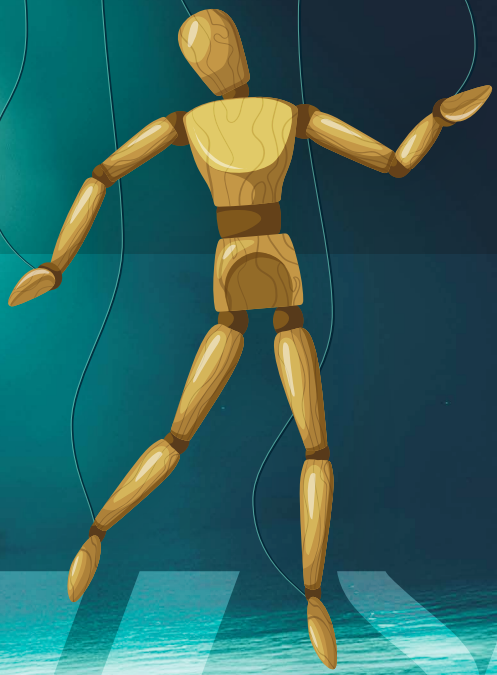
Australian Government

Australian Security Intelligence Organisation

COUNTING AND COUNTERING

THE CO$T OF ESPIONAGE



ASIO

WHO IS PULLING THE STRINGS?

In July 2025, ASIO released

The cost of espionage report.

ASIO commissioned the Australian Institute of Criminology (AIC) to calculate the cost of espionage to Australia. The report is believed to be the first public attempt to measure the wider costs of espionage and the benefits of countering espionage. It attempted to capture the cost of incidents, as well as the costs to mitigate and respond to espionage.

Importantly, the report also estimated the costs prevented by government, industry and business through effective security measures. By definition, espionage is highly secretive and therefore difficult to measure, and the report authors believe the research has significantly underestimated the true cost. Figures used in this booklet are from the report.

The report is available on ASIO's website.

asio.gov.au/coe

COUNTING THE CO$T

Espionage is the state-sponsored theft of information or capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country. It is corrosive and weakens our sovereignty, businesses, military and economy.

The threat Australia faces from espionage is unprecedented. In terms of scale, scope and sophistication, espionage activity is higher than at the height of the Cold War.

Australia remains the target of sophisticated and persistent efforts from a range of nations. Great power competition is driving a relentless hunger for strategic advantage and an insatiable appetite for inside information.

It is estimated espionage cost the Australian economy $12.5 billion in 2023–24. Conservative estimates show espionage could cost Australia tens of billions more if we do not take security seriously.

We also know these figures are significantly underestimated, because by definition espionage is difficult to detect and difficult to measure, which means many of the most serious, significant and cascading costs of espionage are not included in the $12.5 billion figure. Some costs of espionage are obvious and immediate, while others are hidden, subjective, dispersed or enduring in nature, taking months or years to be realised.

In recent years, ASIO has detected and disrupted 23 major cases of espionage and foreign interference against Australia and Australians, which is more than the previous 8 years combined.

Major disruptions of espionage and foreign interference



> We need to uplift our awareness, strengthen our defences and build our resilience against espionage.
>
> Director-General of Security, Mike Burgess AM,
> the 26th Annual Hawke Lecture, 31 July 2025

Espionage is a real, present and costly danger and anyone with privileged information can be targeted.

Espionage takes away Australia's sovereign choices and options. It corrodes our decision-making and damages our economy.

The impact of espionage includes loss of:

- revenue
- intellectual property
- reputation
- defence capabilities and war-fighting capacity
- trust in government
- sovereign decision-making
- strategic advantage.

Espionage undermines investment in:

- research and development
- innovation
- new technologies.

Espionage also enables other significant national security threats, including foreign interference and sabotage.

It has a thousand different effects that chip away at the base of our prosperity and sovereignty.

Espionage cost the Australian economy

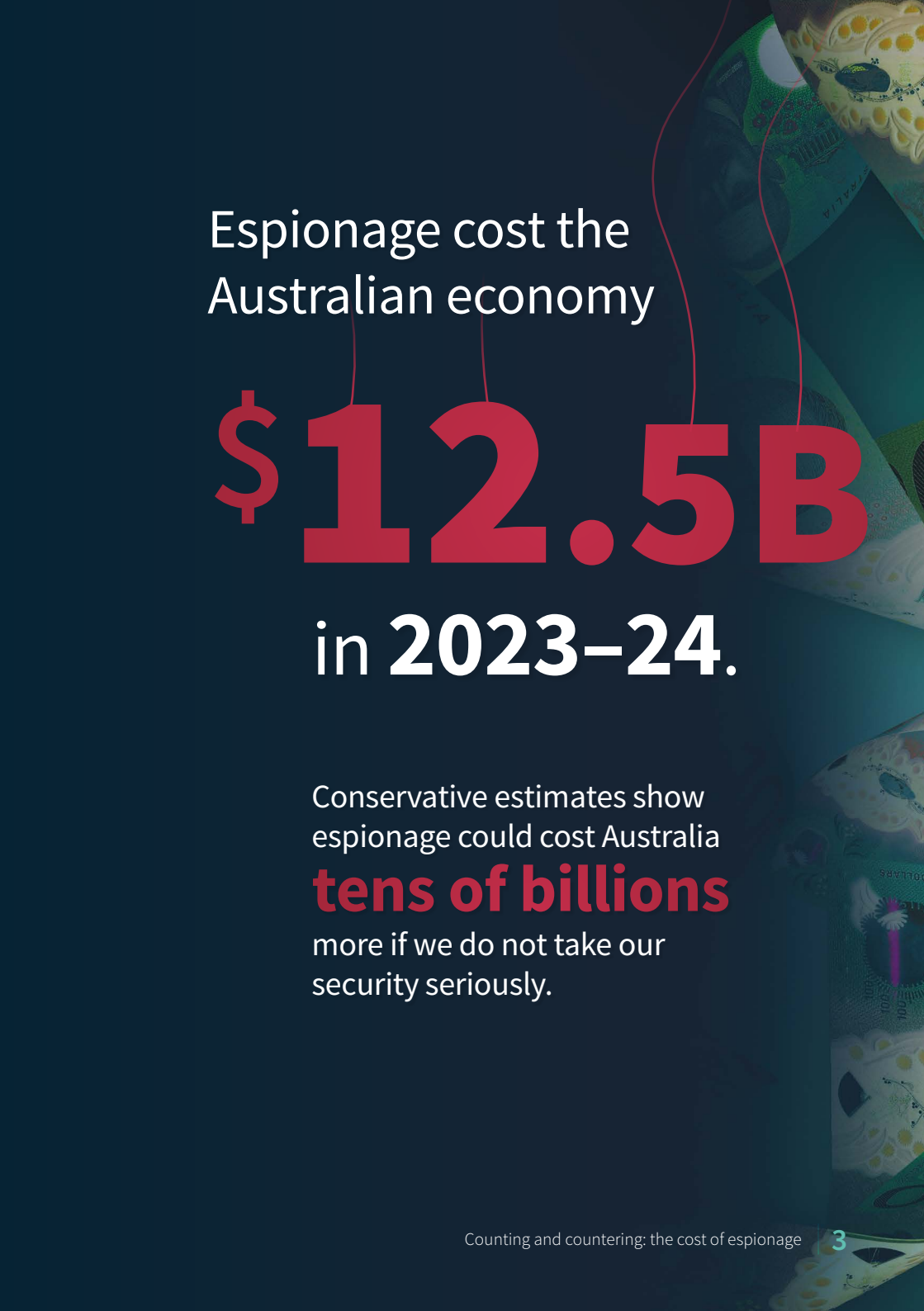
$12.5B

in **2023–24**.

Conservative estimates show espionage could cost Australia

tens of billions

more if we do not take our security seriously.





Direct costs of known or suspected espionage activity in 2023–24 include

AUSTRALIAN MEDIUM AND LARGE BUSINESSES

CYBER SECURITY INCIDENTS **$1.2B**

STATE-SPONSORED INSIDER THREATS **$324.8M**

CYBER-ENABLED THEFT OF INTELLECTUAL PROPERTY AND TRADE SECRETS **$1.9B**

AUSTRALIAN PUBLIC UNIVERSITIES

CYBER SECURITY INCIDENTS **$14.5M**

STATE-SPONSORED INSIDER THREATS **$25M**

GOVERNMENT, NOT-FOR-PROFIT AND HIGHER EDUCATION

INTELLECTUAL PROPERTY THEFT **$628M**

These figures represent a significant underestimate of the true cost of espionage, given the challenges in identifying, quantifying and valuing some of the consequences.

A WAKE-UP CALL

Australians are targets of espionage by both authoritarian regimes and countries we consider friendly. Foreign powers seek to:

- covertly comprehend political decision-making and policy priorities, including our alliances and partnerships – particularly AUKUS
- steal intellectual property and cutting-edge research
- recruit to their own cause elected officials, public servants, members of our military, industry leaders, academics, and leaders in our communities
- obtain personal details of individuals with access to sensitive information so they can be targeted for potential recruitment
- obtain personal information about perceived critics of regimes so they can be monitored, intimidated and silenced
- understand and undermine Australia's military modernisation and identify vulnerabilities in our defence capabilities
- map out Australian critical infrastructure so it can potentially be sabotaged if regional tensions boil over.

Foreign powers or their proxies use cyber, human or technical means, and often a combination of these tactics, to get the information they want.

Foreign intelligence services are proactive, creative and opportunistic in their targeting of Australians. Espionage can be small scale or industrial, with foreign spies masquerading as diplomats, journalists, academics, business people and other professionals to get close to their targets.

> You would be genuinely shocked by the number and names of countries **trying to steal our secrets**.

Director-General of Security, Mike Burgess AM,
the 26th Annual Hawke Lecture, 31 July 2025



CYBER

By employing cyber tactics, such as sending you phishing emails with malicious links or gifting a target a USB device that will execute malware on your computers or networks.



HUMAN

By approaching you directly. They may overtly identify themselves or ask for your help, or they may covertly try to exploit you.



TECHNICAL

By using audio or visual recording devices in areas where you might discuss or conduct sensitive matters.



THE CO$T TO BUSINESS AND INDUSTRY

Business and industry are prime targets of foreign intelligence services seeking a competitive advantage.

The sectors most commonly targeted include: mining, manufacturing, engineering, information and communication technologies, finance, aerospace, and medicine and biotechnology.

Spies can seek to steal information about:

- a product, service or process
- sensitive strategic information, such as pricing
- insider knowledge about upcoming business deals.

The impacts can be far reaching. The AIC estimates a decline in share price resulting in market loss for a large, **publicly listed company of up to $887.2 million per incident**.

ASIO's *Secure your success* and *Secure innovation* protective security advice to help businesses collaborate securely are available at **asio.gov.au/secure-your-success** (right) and **asio.gov.au/secure-innovation** respectively.



In 2023–24

direct costs

of state-sponsored espionage on medium and large Australian businesses



$324.8M

STATE-SPONSORED INSIDER THREATS



$1.9B

CYBER-ENABLED THEFT OF IP AND TRADE SECRETS



$1.2B

CYBER SECURITY INCIDENTS

prevented costs
from espionage on Australian businesses

COSTS THAT CAN BE PREVENTED THROUGH STRONG SECURITY CULTURE



x5

$439M

CYBER ESPIONAGE ATTACK
per incident

A second incident within a year could have a fivefold impact, resulting in more than **$2 billion** in share market losses



$887.2M

TRADE SECRET THEFT
per incident



$5.9B

ECONOMY-WIDE
week-long disruption to digital technology-intensive industries through sabotage

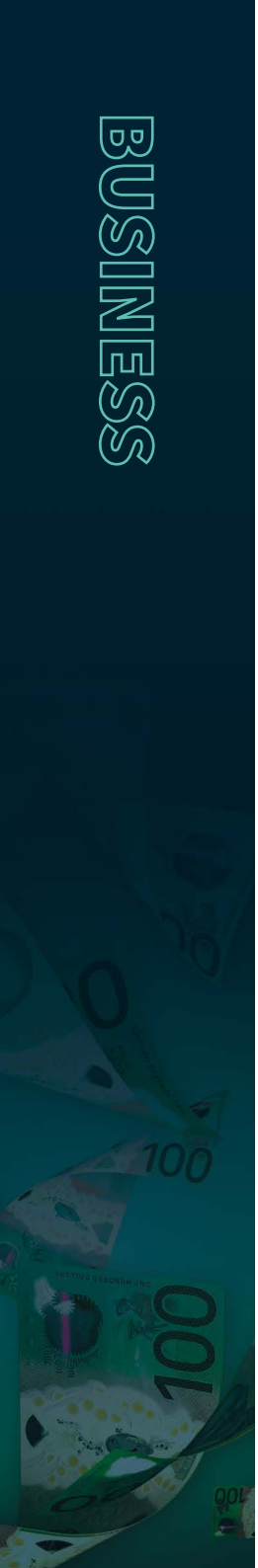
BUSINESS

One Australian company was so comprehensively infiltrated by hackers it was forced to cease trading.

The telecommunications company had its files, data and passwords copied, providing a foreign intelligence service with full access to the company's highly sensitive information. The infiltration ultimately led to the company selling its assets and shutting, but not before it had spent more than $1 million in an attempt to rebuild its network.

This case demonstrates the potential financial consequences of compromise by cyber intrusion and the need for proper information security. It also demonstrates Australian companies are attractive targets to individuals with hostile intent, including foreign intelligence services.

In another incident, a technology company went into voluntary administration after a foreign investor undermined the company's security and commercial prospects. This included the transfer of the company's intellectual property, which had commercial and military applications, to a foreign power.





THE CO$T TO DEFENCE AND DEFENCE INDUSTRY

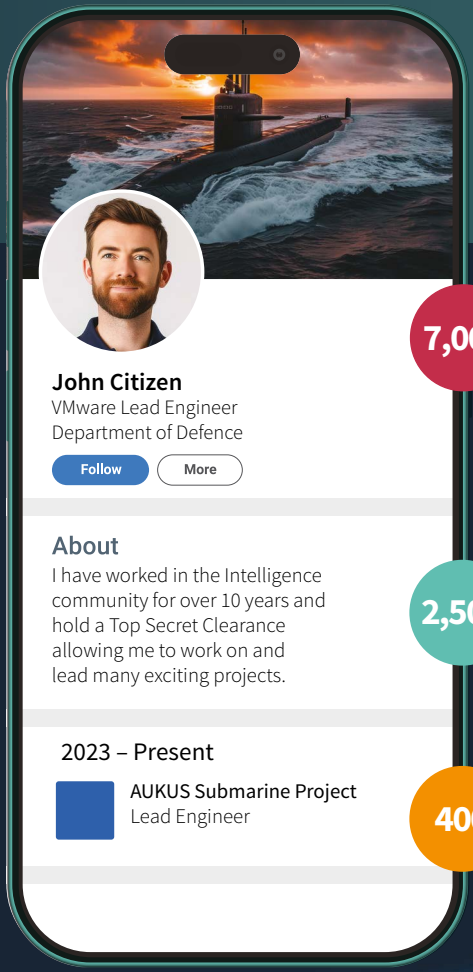
Australia's military capabilities are a top target for foreign intelligence services. They want to blunt our operational edge; gain insights into our operational readiness, tactics and techniques; and better understand our allies' capabilities.

This includes maritime and aviation-related military capabilities, as well as innovations with both commercial and military applications, from fields such as quantum science and communications.

Important Defence projects are put at risk when Australians working on those projects advertise their work, security clearance or other information via social media platforms and job websites. This enables spies from multiple countries to identify, target and cultivate Australians with access to privileged information.



ASIO's protective security advice for the defence sector *Report prying minds* is available at **asio.gov.au/prying-minds** (right).



On just one professional networking site, the profiles of more than **35,000 Australians** indicate they have access to sensitive and potentially classified information.

7,000 **reference their work in Defence**

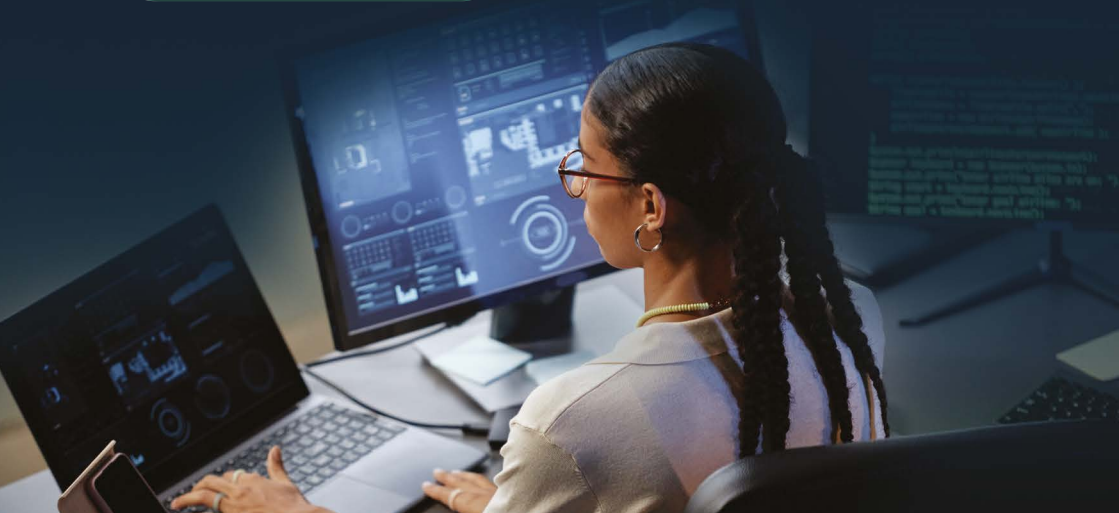
including the specific project they are working on, the team they are working in and the critical technologies they are working with.

2,500 **publicly boast about having a security clearance**

and 1,300 claim to work in the national security community.

400 **explicitly say they work on AUKUS**

and the figure rises above **2,000** if you include broader references to 'submarines' and 'nuclear'.



DEFENCE

Australia's Defence assets are a target for espionage. Adversaries are developing technologies to target the Australian Defence Force (ADF).

In one incident, a foreign intelligence service attempted to compromise a restricted Defence network to gain sensitive data relating to an important project. The same intelligence service also attempted to breach the network of a Defence contractor who was providing a vital service to the project.

In another case, replacement hardware was required for a Defence asset and ordered by procurement officers for delivery straight to the asset location. However, investigations revealed that the parts came from a company with links to a foreign government. The hardware was not installed and harm was avoided.

Australians with security clearances, including members of the ADF, public servants and contractors working at all levels of government, are of particular interest to foreign intelligence services, particularly when travelling overseas for work.



DEFENCE INDUSTRY



Several years ago, an Australian Defence contractor invented, manufactured and marketed a world-leading innovation.

Sales boomed for a while but suddenly collapsed, for no apparent reason. Customers began flooding the company's repair centre with faulty products. While the returns looked genuine, closer examination revealed they were cheap, nasty knock-offs.

An investigation uncovered what happened.

One year earlier, company representatives had attended a defence industry event overseas and were approached by an enthusiastic local. She insisted on sharing some content with them via a USB, which they inserted into a company laptop. The USB infected the system with malware that allowed hackers to steal the blueprints for the product.

Almost certainly, the 'enthusiastic local' was working for a foreign intelligence service, which gave the blueprints to a state-owned enterprise that mass-produced the knock-offs at Australia's expense – the tangible cost of espionage.

Some foreign intelligence services have expanded their activities to employment sites to target Australians.

Fake job ads are created and advertised on popular career sites. The jobs are often well-paid, part-time roles for people with expertise in geopolitics or defence. Be careful what you share about yourself online and on social media.

In one case, an overseas consultancy firm advertised freelance analyst roles that promised to pay US$500 for reports on international politics. An Australian applied for the job and quickly received a return email requesting information on AUKUS and the Indo-Pacific. The firm said it was particularly interested in 'exclusive information' and requested the applicant share his AUKUS-related professional contacts. Fortunately, the applicant became suspicious and reported the engagement via ASIO's Notifiable Incidents, Threats or Reportable Observations (NITRO) portal. ASIO's investigation revealed the consultancy was a cover company for a foreign intelligence service.



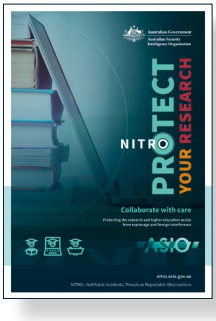
THE CO$T TO UNIVERSITIES, ACADEMIA AND RESEARCH CENTRES

Research expertise and sensitive information are targets for foreign powers seeking to gain advantage by accessing knowledge, expertise and information held by universities and organisations conducting research and development.

Research and development activity is a high-risk target for state-sponsored theft of information, data, methods or concepts. Australian universities, academia and research centres are increasingly the target of cyber espionage campaigns. A primary target for foreign adversaries is research in dual-use technologies that can be used for both civilian and military applications, such as drones or certain chemicals.

Those conducting espionage on universities, academia and research centres are also seeking confidential or personal information about individuals (such as contact details, biometric data, and medical or financial records) in order to facilitate further espionage and foreign interference.

When collaborating with foreign partners, do it with care. Be alert to the risks and put sensible safeguards in place. ASIO's *Protect your research* protective security advice to help researchers and academics collaborate securely is available at **asio.gov.au/protect-your-research** (right).



In **2023–24**

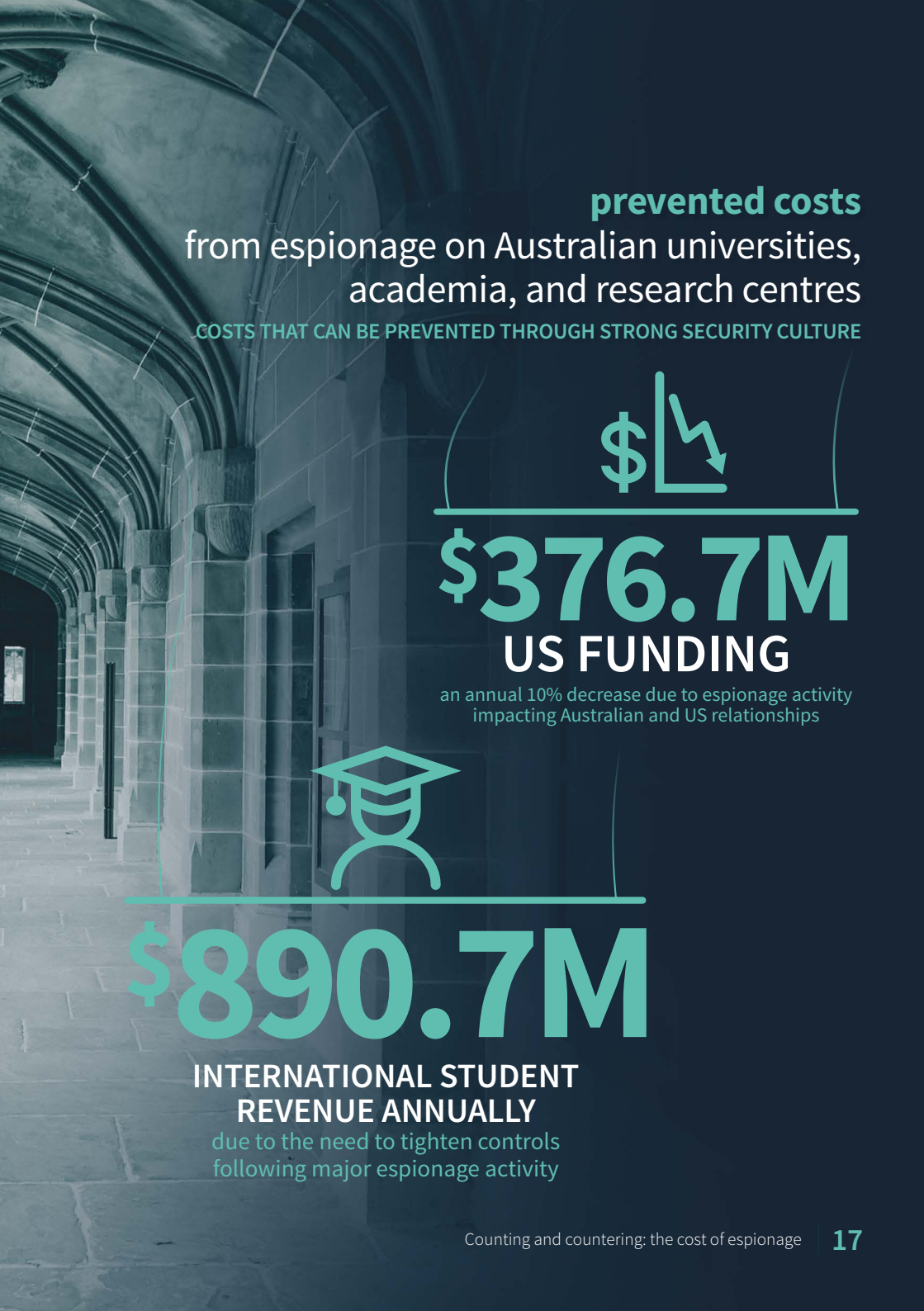
direct costs
of state-sponsored espionage on Australian universities



$14.5M
CYBER SECURITY INCIDENTS



$25M
INSIDER THREATS



prevented costs
from espionage on Australian universities, academia, and research centres

COSTS THAT CAN BE PREVENTED THROUGH STRONG SECURITY CULTURE

$376.7M
US FUNDING
an annual 10% decrease due to espionage activity impacting Australian and US relationships

$890.7M
INTERNATIONAL STUDENT REVENUE ANNUALLY
due to the need to tighten controls following major espionage activity

HIGHER EDUCATION



Universities and research institutes are an attractive target for espionage as their work can give foreign powers an economic, social or military advantage to the detriment of Australia.

In one incident, suspected foreign spies attempted to steal important industrial research from an Australian university's science laboratory.

The university's security was robust but that did not stop a visiting student from trying to access the laboratory. The student attempted to photograph the facility, damaged security locks and tried to tailgate staff as they entered the building.

The university quickly reported the student's actions. ASIO launched an investigation and found the student had made multiple attempts to access secure areas of the facility. If the student had been successful, sensitive research with economic, defence and national security benefits could have been compromised.

Shortly after the incident, the student suddenly departed the country. While we cannot say for certain the student was acting at the direction of a foreign government, the nature of the work being undertaken at the facility and the circumstances of the student's departure makes it highly suspicious to ASIO.

In another case, an Australian academic was groomed by foreign intelligence officers seeking to acquire proprietary research and technology information. The intelligence officers were able to identify the academic's potential and had cultivated a relationship prior to the academic applying for a security clearance from the Australian Government.

The academic had received special treatment from their new-found friends, including travel assistance and preferential treatment when visiting the country in question. The academic was not aware they were being set up to exploit their access to privileged information but was unable to secure a sought-after job in the defence industry.



THE CO$T TO CRITICAL INFRASTRUCTURE

Multiple foreign powers have pursued access that could enable sabotage, disruption or theft from Australia's critical infrastructure networks.

Cyber operators continue to target Australia's critical infrastructure sector seeking to gain information from operators. ASIO believes these foreign spies are laying the groundwork for future operations against Australian infrastructure facilities.

Foreign intelligence services are targeting protected information or technologies related to Australia's critical infrastructure, national assets or systems. They may use this unauthorised access to sabotage or disrupt systems, gain control over essential resources and industries, damage the Australian economy, and create instability and distrust in governments.



ASIO's protective security advice the *Protective security top 10* provides the essential components of a complete security framework and is available at **asio.gov.au/protective-security-top-10** (right).

In **2023–24**

prevented costs
of sabotage of critical infrastructure through state-sponsored espionage

COSTS THAT CAN BE PREVENTED THROUGH STRONG SECURITY CULTURE



$1.2B

PER INCIDENT

CRITICAL INFRASTRUCTURE

Australia's critical infrastructure is subject to consistent and increasingly sophisticated acts of espionage.

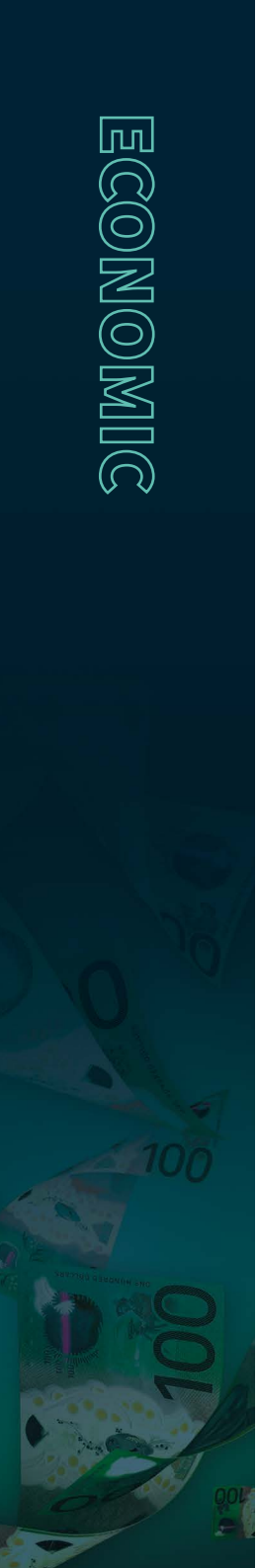
A nation state conducted multiple attempts to scan critical infrastructure in Australia and other countries, targeting water, transport and energy networks.

The reconnaissance was highly sophisticated, using top-notch tradecraft to map networks, test for vulnerabilities, knock on digital doors and check digital locks.

In another incident, a state-operated cyber group attempted to hack more than a dozen Australian telecommunications companies in a bid to steal sensitive communications data about Australians. The persistent attacks on the telecommunications sector risks Australia's national security and breaches Australians' privacy. This incident remains under investigation.



ECONOMIC



Economic espionage can have wide-ranging impacts in individual companies and undermine Australia's national interests, economic prosperity and security. Foreign spies often seek out positions of leadership or influence to deceptively act in the interests of a foreign country.

One person was able to get a board position on an Australian critical infrastructure company, subsequently using their leadership position to block proposals and act as a barrier to strengthen the company's security.

The board member worked through their legitimate position to destabilise the business, force poor commercial decisions to be taken and pressure other executives to consider risk options they would not normally.

ASIO suspects the board member was able to obtain some sensitive information and pass it on to their government.

Foreign spies or their proxies can cause significant economic loss to individual companies and the Australian economy more broadly. They can be difficult to distinguish from legitimate business people and can threaten national security if they gain control of important Australian assets.



THE CO$T TO GOVERNMENTS

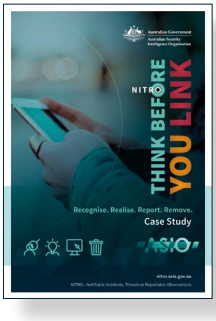
Foreign spies want to better understand Australian and wider Five Eyes government decision-making, and commercial deal-making. One of the greatest potential harms to Australia from espionage is a gradual but pervasive erosion of sovereignty across government.

Foreign powers attempt to use espionage to recruit to their own cause elected officials, public servants, well-placed individuals in business, and leaders in the community. Counter-espionage efforts by governments, businesses and higher education have prevented tens of billions of dollars of additional costs.

Protected information or technologies related to Australia's shared government services, critical infrastructure or other national assets or systems are targeted by foreign intelligence services, who may use this unauthorised access to sabotage or disrupt systems; gain control over essential resources and industries; damage the Australian economy; and create instability and distrust among the public.

Foreign intelligence services have targeted all sides of politics, all levels of government, all states and territories.

ASIO's protective security campaign *Think before you link* provides advice on how to avoid being targeted through professional networks and other online platforms and is available at **asio.gov.au/TBYL** (right).



In 2023–24

direct costs

of state-sponsored theft of intellectual property from government, not for profit, and higher education in Australia



$628M

prevented costs

COSTS THAT CAN BE PREVENTED THROUGH STRONG SECURITY CULTURE



$10.3B

ANNUAL DECREASE IN FOREIGN DIRECT INVESTMENT

diminishing trust in government

GOVERNMENT

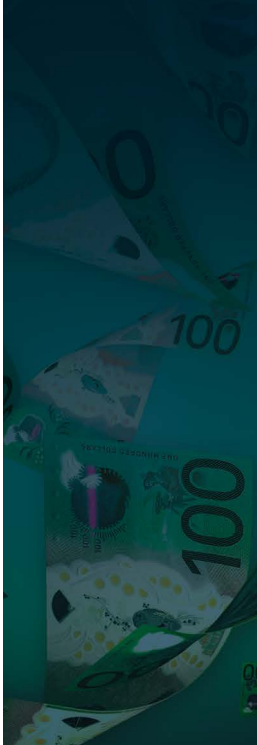
Foreign intelligence services are targeting government officials and Australians with a government security clearance.

In one incident, a travelling group of Australian officials was subject to a range of clandestine activities, including secret listening devices in hotel rooms and bathrooms, photography and surveillance, attempts to access mobile phones, and attempts to sexually exploit the officials with the aim of obtaining compromising images and videos.

In another example, a foreign intelligence service cultivated an individual over an extended period, offering payment in exchange for written reports. At first, the requested topics were general in nature – broad insights into bilateral relations and Australia's strategic policy directions.

But over time, the requests turned into demands, the topics became more specific and the type of information required became more sensitive, such as Australia's intelligence priorities.

ASIO intervened before sensitive material was handed over.



COUNTERING THE CO$T

National security is a shared responsibility. Everyone has a role to play to counter the cost and impact of espionage on Australia and Australians.

ASIO estimates the threat from espionage will grow in intensity and sophistication in the next decade. While the public and private sectors are defending themselves against some espionage, more can be done to counter espionage. The threat is real and anyone with access to sensitive information can be a target. The consequences financially, reputationally and nationally can be severe.

If you have sensitive information, common sense is a good place to start. Don't make yourself a target on social media, use a hard-to-guess password, regularly update your software and follow the rules for handling classified information.

If an offer seems too good to be true, it probably is. If you are pressed for inside information, be discreet. If an approach seems suspicious, report it.

Governments, businesses and organisations can establish robust security measures and maintain a strong security culture.

A strong security culture creates a workplace that is safer, more secure and more resilient to threats. Good security is achievable and it works.

Organisations can build and foster a strong security culture by creating an environment that **ENABLES**, **ENCOURAGES** and **EDUCATES** security-savvy behaviours.

> "Businesses and organisations don't need to be spy catchers – that's ASIO's job – but they can, at the very least, make spying more difficult.
>
> Director-General of Security, Mike Burgess AM, the 26th Annual Hawke Lecture, 31 July 2025

FOSTERING GOOD SECURITY CULTURE

Australian organisations are well versed in protecting themselves against criminal activity, fraud and workplace accidents. Effective defence against potential espionage employs a similar ethos. Simple steps can make a difference in stopping espionage.

Understand the threat – acknowledge the threat is real. Anyone with access to sensitive information can be a target, and the consequences for your bottom line, reputation and the national interest can be severe.

Identify the risk – know what is valuable and what is vulnerable in your organisation, whether it is data, assets or individuals.

Manage the risk – implement a coherent, connected security strategy across your whole enterprise – your people, places, technology and information. Continuous and consistent education and engagement with staff builds a strong culture that is security aware and alert to anomalous behaviour.

ASIO provides a range of resources on our **website** to help organisations understand what a strong security culture looks like.

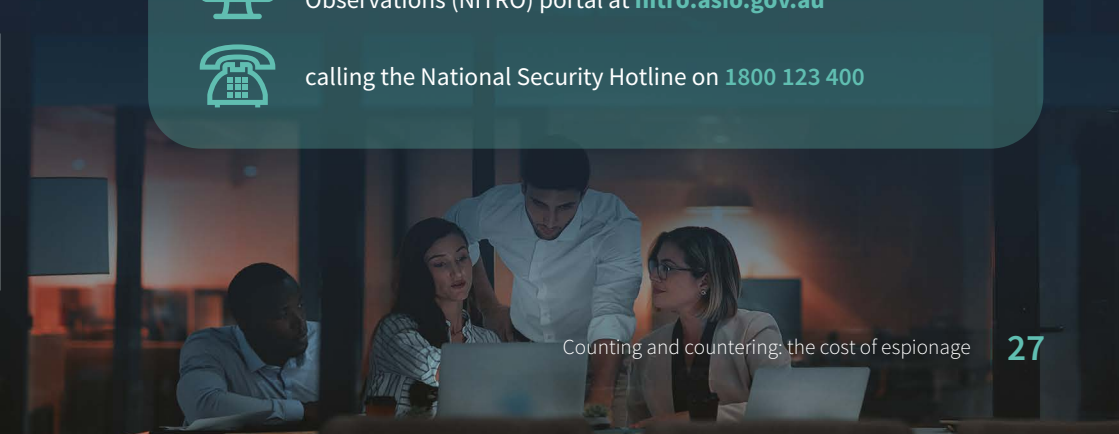
Government workers and security clearance holders have an obligation to report suspicious approaches:

contact your security manager and **fill out a contact report**

Other workers can report suspicious approaches by:

using ASIO's Notifiable Incidents, Threats or Reportable Observations (NITRO) portal at **nitro.asio.gov.au**

calling the National Security Hotline on **1800 123 400**



RESOURCES

ASIO has developed a range of materials, digital and printable, to assist individuals and organisations to protect themselves against espionage. These are publicly available on ASIO's website **asio.gov.au/protective-security-advice**.



Secure innovation provides security guidance to help protect emerging technology companies from a range of threats.



Secure your success provides guidance to individuals and organisations to prevent foreign powers gaining advantage from Australian innovation by stealing intellectual property, harvesting expertise and co-opting academic research.



The Protective Security Top 10 provides the essential components of a complete security framework.



Protect your research explains what you can do to protect yourself and your institution from harm.



Report prying minds provides guidance for the defence industry on the threat of espionage and how to protect against it.



Think before you link explains the threat from malicious social media profiles. It provides guidance on how to avoid being targeted through professional networks and other online platforms.



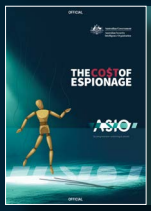
Countering the insider threat provides guidance on hardening your organisation against the insider threat and how to limit damage if compromise occurs.



Clearance holder obligations provides advice on the requirements of maintaining an Australian Government security clearance.



Managing the espionage and foreign interference threat while travelling overseas provides guidance on how you can protect yourself and your assets while travelling internationally.



To read the Australian Institute of Criminology's report, **The cost of espionage**, visit **asio.gov.au/coe.**


ASIO
asio.gov.au