ACTIVE
COUNTER MEASURES

ASIO ESPIONAGE RESEARCH

TECHNICAL SURVEILLANCE

SECURITY

Scan the QR Code to
Contact Us using
Confidential Methods

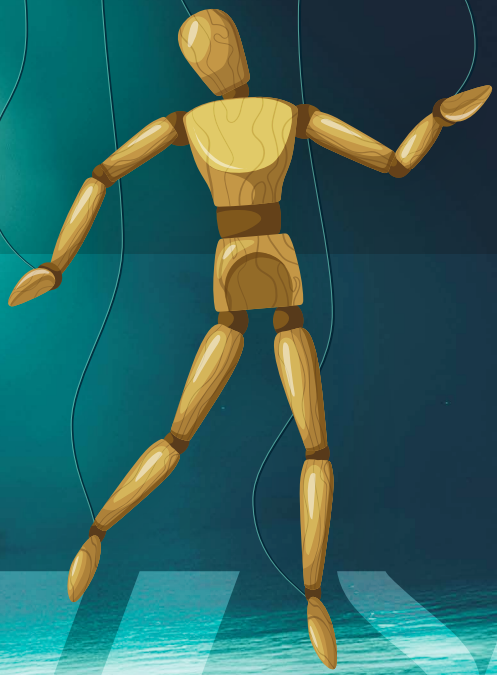
PRIVACY

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

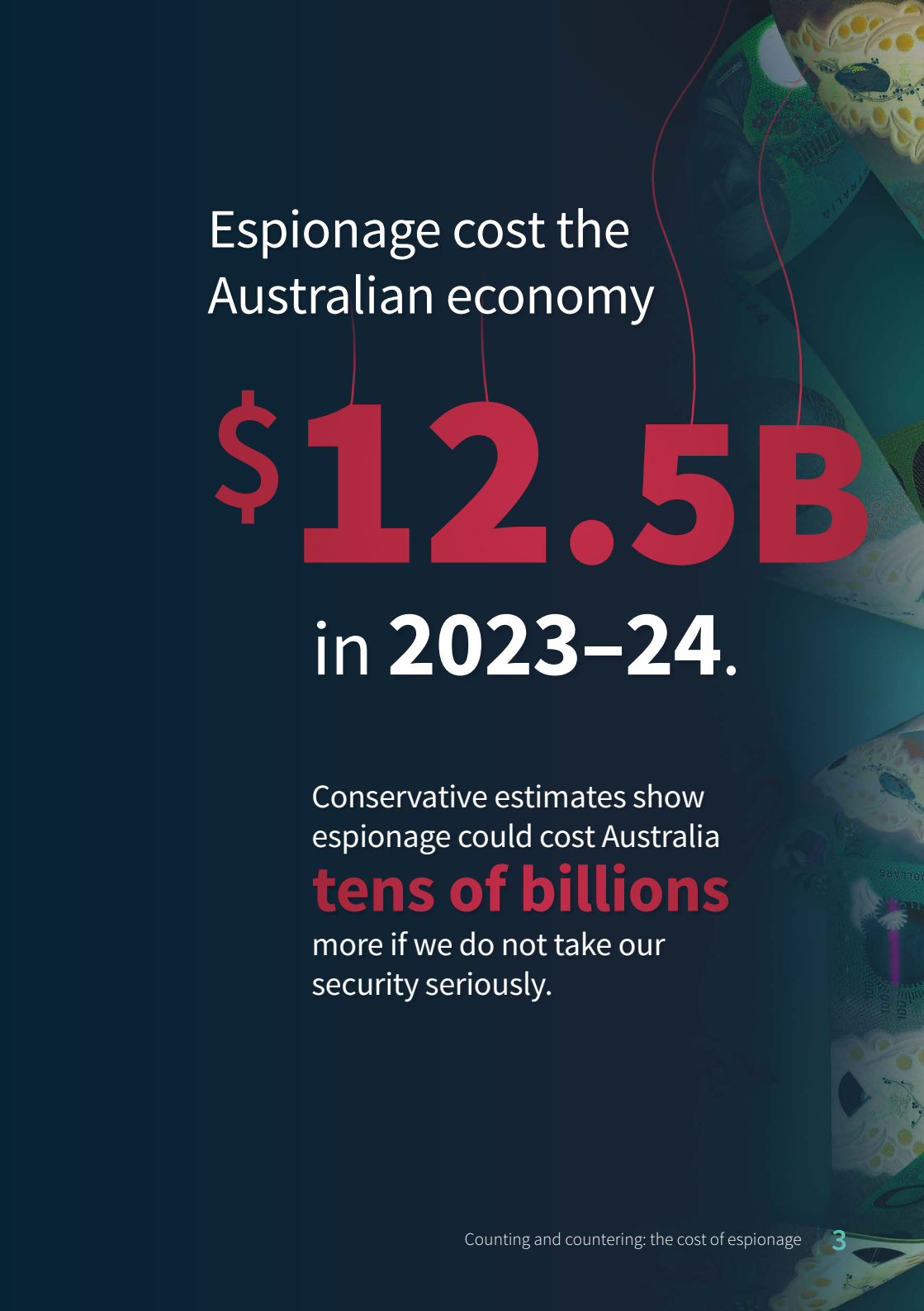
$12.5B

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

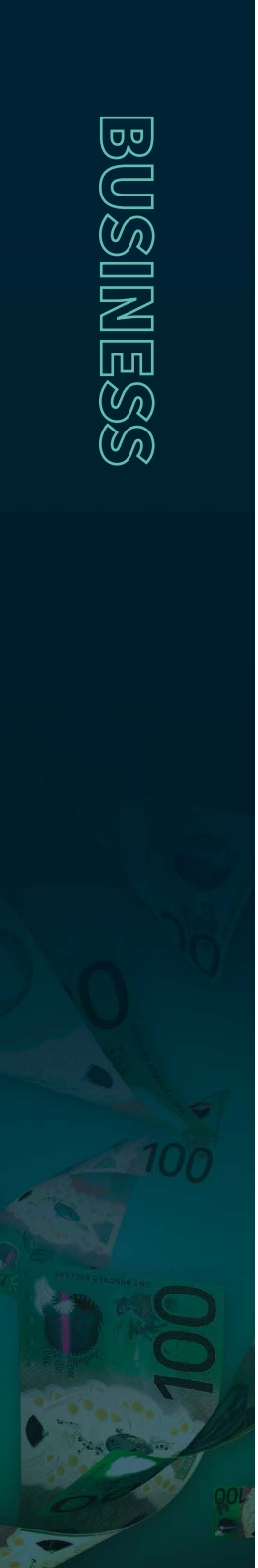
BUSINESS

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.



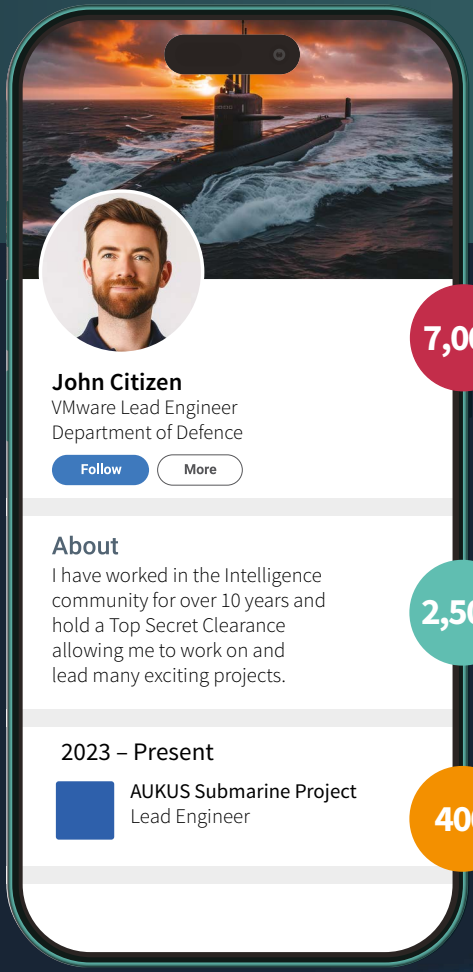
THE CO$T TO DEFENCE AND DEFENCE INDUSTRY

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**

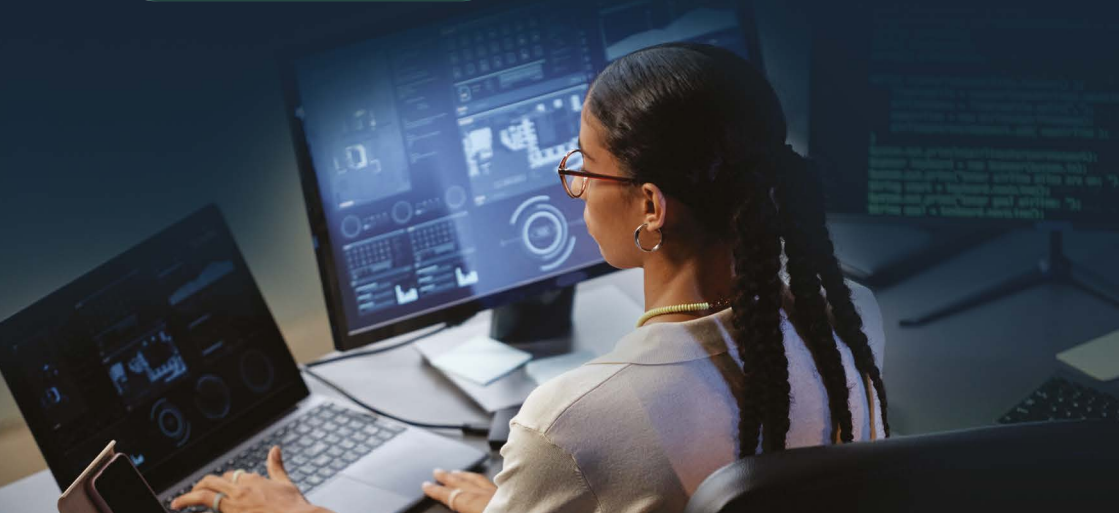
including the specific project they are working on, the team they are working in and the critical technologies they are working with.

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.

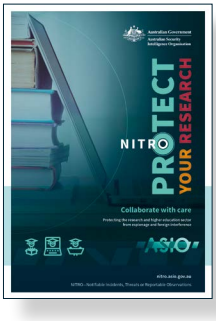
THE CO$T TO UNIVERSITIES, ACADEMIA AND RESEARCH CENTRES

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).

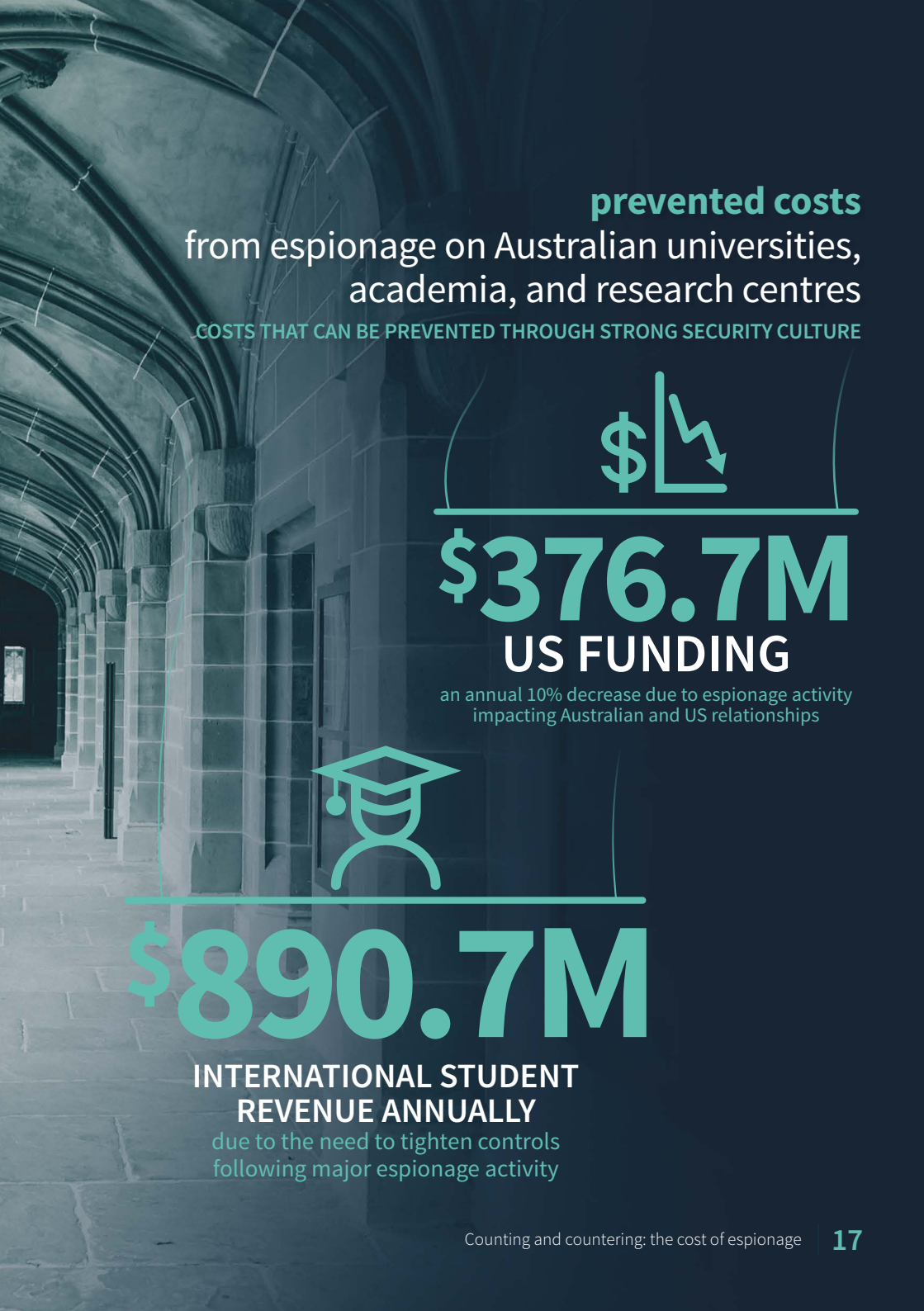


In **2023–24**

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

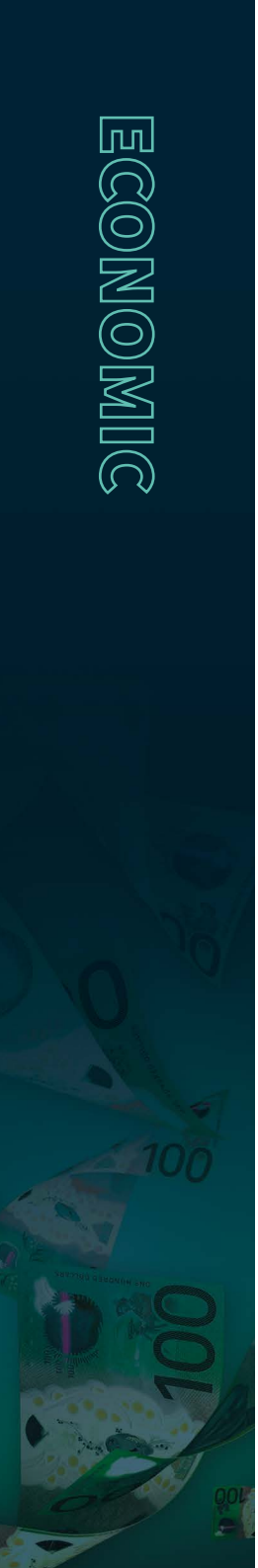
Australia's critical infrastructure is subject to consistent and increasingly sophisticated acts of espionage.

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

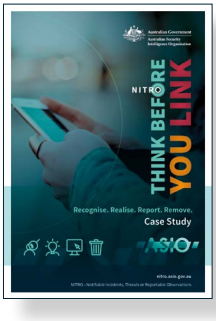
Foreign spies want to better understand Australian and wider Five Eyes government decision-making, and commercial deal-making. One of the greatest potential harms to Australia from espionage is a gradual but pervasive erosion of sovereignty across government.

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

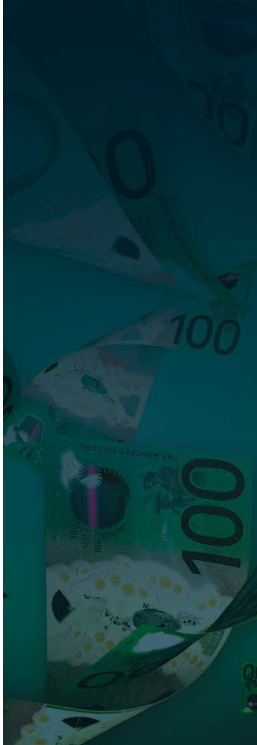
Foreign intelligence services are targeting government officials and Australians with a government security clearance.

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.

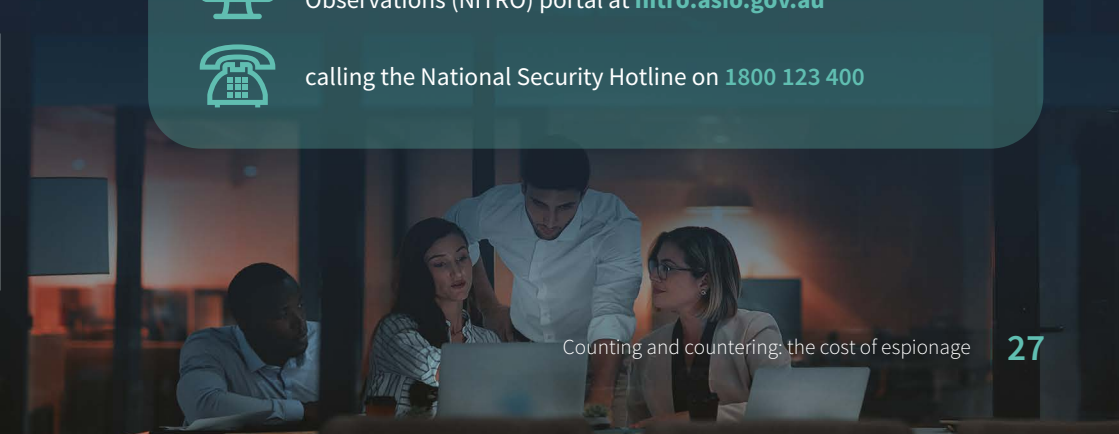
Government workers and security clearance holders have an obligation to report suspicious approaches:

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.

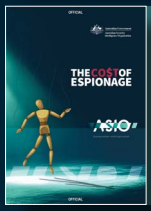
Report prying minds provides guidance for the defence industry on the threat of espionage and how to protect against it.

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.

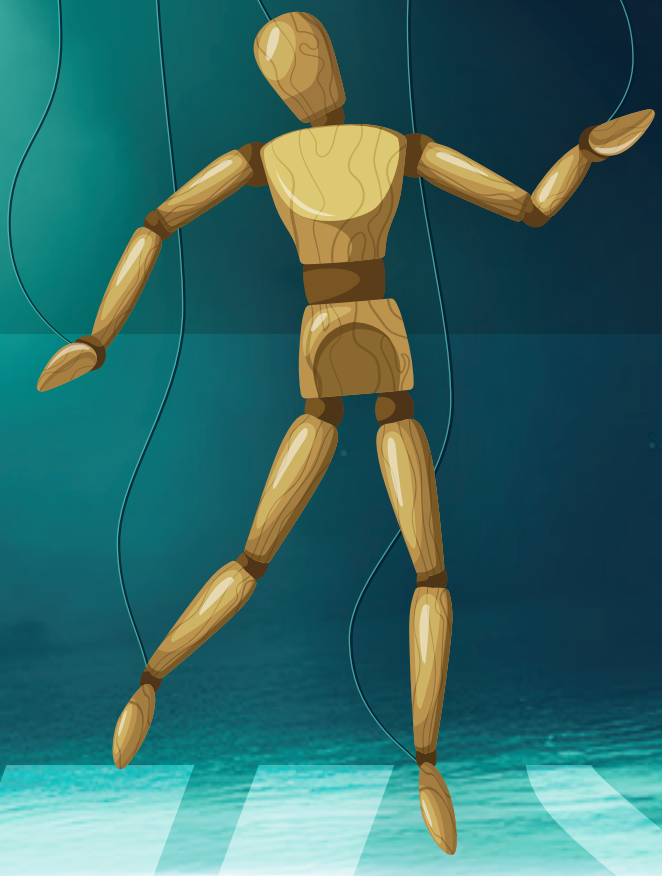


To read the Australian Institute of Criminology's report, **The cost of espionage**, visit **asio.gov.au/coe.**


ASIO
asio.gov.au

Australian Government
Australian Security Intelligence Organisation

THE CO$T OF ESPIONAGE



ASIO

Securing Australia—protecting its people

Director-General of Security's foreword

I am pleased to present the Australian Institute of Criminology's (AIC) *The cost of espionage* report. It is quite possibly the first public analysis of its kind in the world. Certainly, it is the most comprehensive.

Espionage is one of Australia's principal security concerns.

Multiple countries – even ones we consider friendly – are targeting anyone and anything that could give them a strategic or tactical advantage, including sensitive but unclassified information.

Espionage can result in the loss of revenue, trade secrets, reputation, sovereignty and, in the case of defence capabilities, war-fighting advantage.

The AIC calculates espionage cost the Australian economy $12.5 billion in 2023–24. This includes the direct impact of espionage – for example, intellectual property theft – as well as mitigation and response costs.

The modelling was informed by classified Australian Security Intelligence Organisation (ASIO) assessments and case studies, and the researchers gathered further insights from the Australian Signals Directorate, government departments including Defence, industry groups, universities, think tanks and other key stakeholders.

While $12.5 billion is a significant figure, the AIC acknowledges it is an underestimate. Many of the most serious, significant and cascading costs of espionage are not quantifiable, and are not included. The potential loss of strategic advantage, sovereign decision-making and war-fighting capacity hold immense value, but not a concrete dollar value.

The cost of espionage report is a sobering and timely wake-up call; evidence espionage inflicts significant harm on our democracy, economy and society. Security is a shared responsibility and we – all of us – need to take security seriously.

This is critical because ASIO is not all seeing and all knowing, and does not want to be. We cannot catch every spy.

I thank the Australian Institute of Criminology for its report, and the ASIO subject matter experts who contributed to this ground-breaking modelling.

I hope it will provide a baseline for further research into how we can count and counter the cost of espionage.

Mike Burgess AM
Director-General of Security

Australian Government
Australian Institute of Criminology

The cost of espionage

Prepared by the Australian Institute of Criminology for the Australian Security Intelligence Organisation

Anthony Morgan and
Alexandra Voce

July 2025

Contents

Figures

Tables

Acronyms and abbreviations

ABS	Australian Bureau of Statistics
ASIO	Australian Security Intelligence Organisation
ASX	Australian Stock Exchange
FDI	foreign direct investment
GDP	gross domestic product
ICT	information and communications technology
IP	intellectual property
PwC	PricewaterhouseCoopers

Acknowledgements

This work was funded by the Australian Security Intelligence Organisation (ASIO). The Australian Institute of Criminology acknowledges ASIO's generous support and the assistance of subject matter experts from ASIO who contributed to this research.

We also acknowledge the experts from other government agencies, think tanks, the higher education sector, and other contributors who shared important insights that helped to inform our work.

Abstract

Espionage has become one of the most significant national security threats to Australia, impacting government, businesses and the university sector. The highly secretive nature of espionage makes it extremely difficult to measure. In this study we estimated, for the first time, the actual and prevented costs of espionage. Building on the Australian Institute of Criminology's method for measuring the costs of serious and organised crime, we estimated the mitigation and response costs and the direct costs of espionage impacting Australia. We also estimated the preventable costs associated with a number of possible scenarios. The numbers are conservative and an underestimate of the true cost, given the challenges in identifying and measuring espionage activity and its consequences.

In 2023–24, espionage cost Australia at least $12.5 billion. This includes the direct costs of the consequences of known or probable espionage activity – primarily losses due to state or state-sponsored cyber attacks, insider threats and intellectual property theft – as well as the public and private sector response, remediation and mitigation costs. There are also tens of billions in additional costs that Australia may have prevented by countering potential espionage. For example, in just one week, a single incident of espionage-enabled sabotage from a large-scale cyber attack could cost the Australian economy nearly $6 billion. These prevented costs are significant, and highlight the importance and benefit of investing in efforts to reduce the threat of espionage and minimise the harm in high-risk settings.

Executive summary

The threat of espionage – the state or state-sponsored theft of Australian information or capabilities – is now at extreme levels, posing an enormous risk to Australia's national security. This threat is expected to worsen in future. Understanding the real and potential harm from espionage to the government, private and university sectors, and to the wider community is an important step in ensuring that appropriate action is taken to build our resilience to the threat posed by state and state-sponsored actors.

We relied on a review of known cases, published and unpublished research, and data on espionage and espionage-related harms, along with input from subject matter experts, to estimate the mitigation and response costs, direct costs of espionage, and the prevented costs of espionage. We limited our analysis of direct, mitigation and response costs to the 2023–24 financial year. Some calculations of espionage-related expenditure were based on sensitive and classified data, and therefore these costings are not itemised in this report.

It is important to note at the outset that these numbers, while significant, underestimate the true cost of espionage in Australia. Espionage, by definition, is difficult to detect, and many of its most serious impacts cannot be assigned a dollar value. We have chosen to be conservative in our calculations.

This is an important first attempt to measure the range of costs from known and suspected incidents of espionage, using a methodology that has been applied to other areas of national security. While this report highlights the importance of taking action to prevent espionage to protect Australia's national interests, it also draws attention to the need for further work to help us better understand the impact that espionage has on government, businesses, universities and the wider community.

Actual costs from espionage

Our estimate of the actual costs from espionage includes both the direct costs of known or suspected espionage activity, and the mitigation and response costs to government, businesses and universities.

Direct costs of known or suspected espionage activity

We estimated the actual cost of state or state-sponsored cyber espionage, insider threats and intellectual property (IP) theft through a range of methods including:

- Cyber security incidents impacting Australian medium and large businesses were estimated to cost up to $1,193.8 million.
- Cyber security incidents impacting Australian public universities were estimated to cost up to $14.5 million.
- Insider threats involving state or state-sponsored actors impacting Australian businesses were estimated to cost up to $324.8 million.
- Cyber security incidents involving state or state-sponsored actors impacting federal government agencies (not itemised here).
- Insider threats involving state or state-sponsored actors impacting Australian public universities were estimated to cost up to $25.0 million.
- Cyber-enabled theft of IP and trade secrets from businesses was estimated to cost up to $1,901.0 million.
- IP theft from government, the not-for-profit sector and universities was estimated to cost up to $628.0 million in 2023–24.

These costs were incurred in a single financial year (2023–24). These represent a significant underestimate of the true cost of espionage, given the challenges in identifying, quantifying and valuing some of the consequences.

Mitigation and response costs

Significant resources are invested in the public and private sectors to mitigate and respond to espionage. These include the cost to federal government agencies entities related to the identification, investigation, disruption and prosecution of espionage incidents in Australia, as well as the development and enactment of policy and legislation regarding espionage in Australia. Other costs of mitigation include those associated with implementing and maintaining security measures, community outreach, and education and awareness raising. Many of these mitigation measures (particularly legislation) have been introduced in response to previous incidents of espionage or foreign interference, and thus can be considered long-term costs of espionage in Australia. We used a combination of top-down and bottom-up approaches to estimate these costs, relying on data on the operating expenditure of each agency and expert input from senior representatives from these agencies and other stakeholders.

We also estimated the cost of cyber security to state, territory and local government agencies, businesses and universities. We determined the operating expenditure of each sector and relied on industry estimates of the proportion of total expenditure that is spent on information and communications technology (ICT) and, of that, the proportion spent on cyber security. We then estimated the proportion of these cyber security costs associated with espionage.

There are also costs to businesses associated with personnel security and vetting, as well as the costs associated with applying for commercial foreign investments to the Foreign Investment Review Board (which assesses, among other things, risks to national security). Critical infrastructure is a major target for foreign actors seeking to undermine Australia's national security and, in addition to the costs to the Australian Government, there have been costs to industry associated with several major reforms to the regulation of critical infrastructure to reduce the risk of espionage. Universities also incur costs associated with due diligence activity, including vetting of international students and assessing the risks associated with partnerships with foreign institutions. We used a range of methods and data sources to estimate these costs.

These mitigation and response costs have not been itemised, and the full detail regarding our costing methodology has not been provided because it relies on sensitive and classified data. The mitigation and response costs are included in the total cost estimate.

Several additional costs are incurred as a consequence of the action taken by government, businesses and the university sector to mitigate the risk of espionage. Among these are:

- the costs of having to use more expensive technology, or technology that is less than optimal, rather than technology that may be available from a foreign adversary
- the costs incurred by government suppliers in certain high-risk sectors in order to meet security requirements
- declines in potential foreign investment due to our current national security posture
- missed opportunities for international research collaborations with leading academics and organisations.

Although these costs are likely to be significant, they have not been estimated in the current research due to a lack of sufficient data.

Prevented costs from espionage

We estimate the counter-espionage efforts of governments, businesses and universities may have prevented tens of billions of dollars of additional costs to the Australian economy. While there have been many examples of espionage impacting Australia and our international partners, other harms have been avoided.

We modelled a range of scenarios to estimate the potential costs that may have – to the best of our knowledge – been prevented, but which would be incurred in the future if efforts to prevent espionage were not successful.

- Sabotage of critical infrastructure enabled by espionage could cost up to $1,161.2 million per incident.
- An economy-wide, week-long disruption to digital technology-intensive industries, enabled by sabotage, could cost the Australian economy $5,930.4 million.

- Theft of trade secrets from a large, publicly listed Australian company could result in share market losses of up to $887.2 million per incident.
- Cyber espionage attacks targeting a large, publicly listed Australian company could result in share market losses of up to $439.6 million per incident.
- Diminishing trust in government security due to espionage activity could result in an annual decrease in foreign direct investment inflows of up to $10,291.2 million.
- The potential annual losses from a decline in international student revenue because of a need to tighten controls following major espionage activity could be up to $890.7 million.
- A 10% decrease in annual US funding for research following espionage activity impacting Australian and US relationships could lead to potential same-year economic losses of up to $376.7 million.

Many of these costs relate to, or would result from, single incidents of espionage. The cost from multiple repeated attacks targeting government, businesses and university sectors would be significantly higher. As such, the total prevented costs depend on the nature and scale of future espionage activity impacting Australia but are estimated to be tens of billions of dollars.

Total actual and prevented costs from espionage

When we combine the mitigation and response costs and the direct costs of espionage that could be measured, the total known cost to government, businesses, universities and the broader community in 2023–24 is estimated to be at least $12.5 billion. We estimate that tens of billions further in espionage costs may have been prevented through effective mitigation and counter-espionage activity. These costs are preventable – but only if appropriate action is taken to address the threat from those who seek to harm Australia's national interests.

Total actual costs: $12.5B

Direct costs of known or suspected espionage

Public and private sector mitigation and response costs

Prevented costs:

Tens of billions of dollars

Introduction

Espionage is the state-sponsored 'theft of Australian information or capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country' (ASIO 2024: 143). According to the most recent threat assessment by ASIO's Director-General, the threat posed by espionage is at extreme levels (Burgess 2025), with more Australians being targeted than ever before (Burgess 2024). And it is expected to worsen, driven by advances in technology and growing competition for power in the region.

> Espionage and foreign interference are already at extreme levels and we anticipate they will only intensify.
>
> In a more complicated, competitive world, nation states will want greater insights into their enemies – and some of their friends – to better understand strategic intent and capability.
>
> Espionage and foreign interference will be enabled by advances in technology, particularly artificial intelligence.
>
> Director-General of Security, Mike Burgess AM, Annual Threat Assessment (2025)

While it is difficult to measure the true scale of the problem, according to ASIO's *Annual report 2023–24*, there were 12 major disruptions of espionage and foreign interference in 2022, and a further 11 major disruptions in 2023. There were more disruptions in these 2 years than in the previous 8 years combined. The Counter Foreign Interference Taskforce has conducted more than 120 operations since it was established in mid-2020, while successful disruptions have increased nearly threefold (ASIO 2024). The threat from espionage is expected to intensify in the near future, driven by technological advancements and increasing geopolitical competition and tension.

Espionage is also an enabler of other significant national security threats, including foreign interference and sabotage. Foreign interference refers to activities carried out by, on behalf of, or in collaboration with a foreign power, directed or subsidised by that foreign power, that are clandestine or deceptive and that involve a threat to a person or detriment to Australia's interests (Department of Home Affairs 2024a). It is distinct from foreign influence, which is more transparent and respectful of democratic processes. ASIO considers sabotage as any activity that damages, impairs or introduces a vulnerability to public infrastructure, including electronic systems, prejudicing Australia's national security or to advantage a foreign power.

The serious consequences of espionage are widely acknowledged. Theft of IP and trade secrets, including the outcomes of significant investment in research and development, can undermine innovation, reduce competition and cause large financial losses for private industry (Curti et al. 2023; European Commission & PricewaterhouseCoopers (PwC) 2018). Cyber espionage can lead to the loss of important and sensitive data, compromise entire networks and enable sabotage of critical infrastructure, disrupting essential services (Department of Home Affairs 2022). Espionage also results in increased distrust and strained diplomatic relations between countries, which can undermine cooperation between governments (Department of Home Affairs 2024a).

One of ASIO's main responsibilities is to educate and support government, industry and academia to be more resilient to espionage. Critical to this is the need to communicate the seriousness of espionage and to raise community awareness of, and resilience to, the harms it can cause. This includes the significant costs to the Australian economy.

There is no current, reliable estimate of the total cost of espionage impacting Australia. Espionage is extremely difficult to detect because it is a highly secretive and covert activity that takes many forms. Espionage that has been disrupted represents a small fraction of the activity threatening Australia's national security. Any attempt to estimate the cost of espionage is likely to be a significant underestimate.

Many of the most harmful consequences are impossible to quantify. In this report, we describe an attempt to measure the mitigation and response costs, direct costs and prevented costs from espionage using a method that is innovative, conservative and well supported by the best available evidence and expert assessments.

Previous attempts to measure the cost of espionage

Several studies by government and industry bodies have attempted to quantify the costs of stolen information in different countries and regions. Most analyses have focused specifically on the compromise of IP and other 'trade secrets' in commercial contexts, and included all types of threat actors, including state-sponsored adversaries, domestic and international competitor companies, disgruntled employees, organised crime groups, 'hacktivists' and others.

A survey approach was used by the United States International Trade Commission (2011) to calculate the cost of IP infringement incurred by US companies operating in China. Over 5,000 US companies were surveyed about the IP infringement of their products in China and the associated costs to the company (including lost revenue, response costs, changes in sales, research and development expenditure, and lost employees). Statistical sampling techniques were used to extrapolate the findings to the US economy to determine that infringement cost the US economy US$48.2 billion in 2009. The scope of this report included all forms of infringement, including counterfeit consumer goods and digital piracy (e.g. pirated music and movies). These activities do not constitute espionage in a national security context (which must provide a strategic advantage to a foreign power).

In 2014, PwC attempted to estimate the cost of trade secret theft to the US economy. It collated reports on the proportion of gross domestic product (GDP) lost to other types of financial crimes or cybercrimes – such as tax evasion, corruption, copyright infringement, drug trafficking and money laundering – and reasoned that these crimes would have a comparable impact to trade secret theft. On this basis, PwC estimated that trade secret theft could cost between 1% and 3% of GDP for industrialised economies such as the US. The US Commission on the Theft of American Intellectual Property (2017) applied PwC's (2014) lower estimate to the US economy, to estimate that IP theft by foreign actors cost the US economy US$180 billion in 2015. While this crude estimate (i.e. percentage of GDP lost) is a useful heuristic, it does not disaggregate the many distinct short- and long-term consequences for different sectors of society (government, businesses, universities or other sectors), or the costs of preventing and responding to espionage.

A study by Detica (2011), in partnership with the UK Cabinet Office, estimated the costs of different types of cybercrime to the UK Government, industry and the broader community, using publicly available data and expert opinion from the public and private sectors. To calculate the cost of IP theft, the authors estimated the economic value of IP, the likelihood of cyber theft, the exploitability of IP and the potential revenue impact for sectors of the UK economy. To calculate costs associated with industrial espionage – specifically, the theft of confidential information that gives a rival company a competitive or strategic advantage – the authors estimated the annual value of large-scale business dealings (e.g. mergers and acquisitions); the likelihood that business dealings could be subject to cyber espionage; the exploitability of the stolen information; and the potential revenue impact for sectors of the UK economy. It was estimated that the UK economy lost £9.2 billion due to IP theft and £7.6 billion due to industrial espionage during 2009. The focus of this report was cyber espionage specifically, so these estimates do not include other vectors of illicit transfer, such as theft by compromised insiders.

Most recently, a survey of 1,003 German businesses (Bitkom Research 2024) found that 81% had been affected by at least one verified incident of data theft, industrial espionage or sabotage in the last 12 months, and one-fifth (20%) of these incidents were attributed to foreign intelligence services. The researchers extrapolated these data to the wider economy to estimate that German businesses lost a total of €266.6 billion in 2024 due to data theft, industrial espionage and sabotage.

Verizon's *Data breach investigations report* is an annual cyber security report that analyses data breaches and security incidents worldwide. Although not reporting the economic costs associated with data breaches, this report provides valuable insight into the scale of cyber attacks in specific sectors that are attributable to different threat actors. Between November 2023 and October 2024, there were 12,195 data breaches in which data were confirmed to have been disclosed to an unauthorised actor (Verizon 2025). State-sponsored espionage was estimated to have been responsible for 17% of all breaches globally and 34% of breaches in the Asia-Pacific region (including Australia). State-sponsored espionage varied by sector, with over half of breaches (55%) in mining and utilities, and over one-third (36%) of breaches in the information industry (i.e. media, broadcasting and internet services) attributed to espionage. Although state-sponsored data breaches were primarily motivated by espionage (74%), state-sponsored actors also engaged in these activities for financial gain (28%) or secondary reasons (26%), such as assuming control of infrastructure for later use.

McAfee Intel and the Centre for Strategic and International Studies (Lewis, Malekos Smith & Lostri 2020) produced a series of reports that compiled various sources to estimate the cost of cybercrime (including cyber espionage) to the US and global economy. These estimates are based on published data, governmental and private sector reports, and survey and interview data. The authors referred to the annual value of IP in the US (US$12 trillion) and assumed that losses were comparable to those of other types of cybercrime to determine the annual costs of IP theft to the US economy (US$10–12 billion) and global economy (US$50–60 billion). Although this study provides a useful reference point for understanding the costs associated with cyber espionage globally, it does not capture other vectors of illicit transfer and the estimates are not specific to the Australian context.

While these studies serve as a valuable starting point to inform the current project, they do not capture all incidents relevant to estimating the cost of espionage in Australia. Most analyses have focused specifically on the compromise of IP and other 'trade secrets' in commercial contexts, and do not capture impacts in other sectors, such as universities, government or defence. These estimates also do not apply to other types of classified or sensitive data or technologies that are targeted by foreign adversaries, such as information about critical infrastructure or military capabilities. With the exception of Bitkom Research (2024) and the recent report by Verizon (2025), these reports have not differentiated the impacts associated with specific threat actors, making it difficult to estimate the costs attributable to state-sponsored adversaries.

A study by researchers from Texas A&M University (Bell et al. 2010) attempted to provide the US Government with an estimate of how damaging economic espionage is to the US economy. As the researchers relied on a very small number of publicly available case studies of economic espionage (n=12), it was not possible to estimate the cost per incident in monetary terms (actual dollars lost). Instead, the researchers developed a model where users could input details of an incident of economic espionage and the model gives a qualitative 'severity score' (low, medium or high) to indicate the likely impact of that incident on the US economy. The model was developed based on qualitative analysis of the available case studies, and was further refined using statistical techniques and survey information from 12 experts in academia, government and industry. Although the model is potentially useful for understanding the economic loss associated with specific incidents of espionage, it does not estimate the cost of espionage incidents across the whole US economy.

As this shows, there is a significant gap in our understanding of the harm associated with espionage. It is not surprising this specific topic has not received more research attention, given some of the challenges associated with accessing and using classified information for research purposes. Our goal was to address this gap and provide, to the extent possible, a clearer picture of the cost of espionage in Australia.

Our approach

This project was modelled on the approach the Australian Institute of Criminology used to estimate the costs of serious and organised crime in Australia (see Smith 2024 for the most recent version, and Australian Crime Commission 2015 for a technical report describing the original methodology). This is based on the Australian Institute of Criminology's work measuring the cost of crime that has spanned more than 20 years. The most recent report represents the most robust and reliable estimate of the costs of serious and organised crime since this research commenced (Smith 2024).

In short, our approach to estimating the cost of espionage involved 4 main stages.

1. **Define** the scope of the analysis, including the definition of espionage used, time frame for analysis, and type of costs included.
2. **Identify** the range of possible consequences associated with espionage, including the relevance and significance of these to the Australian context, and who is responsible for preventing and responding to the problem.
3. **Quantify** the size of these consequences and the extent to which they can be attributed to espionage, and quantify the proportion of total resources used by different agencies to prevent and respond to the problem.
4. Estimate the **value** of the consequences and agency resources once they have been quantified.

The current study relied on 3 main sources. The first was the input of stakeholders with relevant subject matter expertise. We conducted a series of workshops with ASIO subject matter experts to identify the types of espionage impacting Australia, some of the consequences that have been observed, and the extent to which these consequences can be attributed to acts of espionage. We also interviewed representatives from other agencies to establish what proportion of their agency resources were involved in preventing and disrupting espionage. These interviews also provided further insights into the consequences of espionage in Australia and overseas.

The second source was our review of espionage cases known by ASIO to have occurred or which were disrupted, both in Australia and overseas. This helped to identify real-world examples of the consequences associated with different espionage acts. Where possible, we have referred to some of these (de-identified) case studies in our report.

The third source of information was our review of published and unpublished research and data, including Australian and international literature, on espionage and espionage-related harms. Relevant government publications such as annual reports, portfolio budget statements, and intelligence and threat assessments were included as part of this review. This was used to identify, quantify and value the impact of espionage, and to estimate the value of agency resources involved in mitigating and responding to espionage.

The monetary values in this report are expressed in Australian dollars, rounded to billions or millions where appropriate. Totals in tables may differ from more precise estimates due to rounding.

Scope

There were 3 important considerations regarding the scope of our research: the definition of espionage, the time frame for our analysis and the range of costs included.

We used ASIO's definition of espionage as per the introduction of our report. This has 2 defining characteristics: the theft of information or capabilities that would not have been willingly shared; and the involvement of, or benefit to, a state or state-sponsored actor. Regarding the latter, many incidents will have been directed or undertaken by a state actor; however, in other cases the state actor may have given citizens clear incentives (e.g. financial rewards or threats to safety) to undertake activity that would constitute espionage on their behalf.

We included commercial espionage, whereby the target of state-sponsored theft of commercially valuable assets can be government, the private sector or research institutions. Industrial espionage, which occurs between private entities, was excluded from our analysis because it does not involve a state or state-sponsored actor and is therefore not the focus of our report.

Consistent with research into the costs of serious and organised crime, we have included an estimate of the mitigation and response costs associated with espionage, as well as the direct costs associated with espionage activity impacting Australia. These costs may be incurred by the government, businesses or university sectors or the wider community. In an important departure from our previous research, we have also estimated the prevented espionage costs – the costs that may have been avoided through effective mitigation and counter-espionage activity.

Finally, we agreed the time frame of our analysis would be the 2023–24 financial year. This is also consistent with the approach we took to estimate the costs of serious and organised crime. We note that some of the costs of espionage we have included may not have been incurred within this time frame; however, we have only included these costs where they were the consequence of espionage activity that occurred within this financial year and which can be reasonably attributed to espionage.

Challenges

We have already highlighted some of the challenges associated with disrupting espionage activity. These also have implications for measuring espionage and its associated costs.

Measuring the prevalence and characteristics of espionage

The scope of activities that can constitute espionage is extensive and diverse. Threat actors continually adapt the vectors used, and the individuals and entities targeted, based on emerging vulnerabilities, technologies and geopolitical events (Department of Home Affairs 2024a).

Espionage is clandestine in nature, with threat actors exerting considerable effort to hide their activities, meaning that many incidents are likely never detected, or detected months or years after the incident. Victim entities may not report to authorities out of fear of damaging their reputation if the incident is made public (European Commission & PwC 2018). Targets may not realise that they are being exploited if they misconstrue espionage for legitimate forms of information transfer, such as international research collaborations (ASIO 2023; Horton 2024).

Determining whether incidents involve a state or state-sponsored actor or are intended to benefit a foreign power

It is difficult to verify that domestic insiders have been recruited or coerced by a foreign government without evidence of this interaction and, among foreign individuals or groups, it can be difficult to verify how closely aligned these actors are to their government. Even when a link is established, it is difficult to prove that the actor intended to transfer information to benefit a foreign power (Lifhits 2024). Compromised insiders steal information from their workplaces for various reasons beyond state-sponsored espionage, including:

- to advance their career, by using the information to start their own business;
- for financial gain, by selling information to commercial competitors or organised crime groups; or
- to cause harm to the entity for personal or ideological reasons (Commonwealth Fraud Prevention Centre 2023).

Most detected cyber attacks are attributed to non-state actors (Verizon 2025), who are typically motivated by financial gain (e.g. organised criminal groups), ideological reasons (e.g. 'hacktivists'), or personal vendettas (e.g. disgruntled customers or employees seeking to harm the entity).

Cyber threat actors attack networks from outside Australia, making it difficult to attribute the incident to a specific jurisdiction or actor. These actors use various techniques to obscure their identities, such as using multiple hacked user accounts or by using internet protocol addresses that are dynamic (i.e. temporary and changing), cloaked or falsified (Lee-Makiyama 2018).

When a threat actor acts on behalf of a foreign adversary, that government often denies any involvement in the espionage activity and can refuse to cooperate in the investigation or prosecution of the threat actors in their country (Levite et al. 2022).

Assigning mitigation and response costs to espionage versus other national security threats

Most national security strategies and frameworks aim to mitigate a range of interrelated threats, including espionage, foreign interference, terrorism, sabotage and supply chain disruption (Department of Home Affairs 2024b). This means it is difficult to apportion out the cost of implementing these strategies in order to isolate the specific costs of espionage. Even in the absence of other national security threats, most of these same protections would still need to be implemented to adequately mitigate and respond to espionage.

Attributing observed consequences to espionage

It can be very difficult to attribute a consequence directly to an espionage incident, particularly when the consequence occurs months or years after the espionage incident or when a consequence impacts a wide segment of society (i.e. a whole industry) rather than a specific individual or entity. In these cases, there are typically many other potential geopolitical, social and economic factors that could also explain the outcome.

Measuring consequences of espionage when most known cases have been disrupted

It is difficult to assess the prevented consequences of espionage incidents as most known incidents of espionage are thwarted or mitigated before the threat actor fully succeeds in their aims. As a result, the consequences of more severe scenarios involving espionage remain hypothetical rather than based on real-world observable impacts.

Assumptions

Because of these challenges, we have made a number of assumptions about the scale and characteristics of espionage impacting Australia. These assumptions, informed by consultation with subject matter experts, underpin our approach to estimating costs.

- The range of known cases in recent years reflects the pattern of regular espionage activity targeting Australia.
- Espionage-related activity impacting politically, socially or economically comparable countries is likely to be similar to that of Australia, and we can draw on data from these countries where no such data exist for Australia.
- Certain sectors and industries are more likely to be the target of espionage activity because of their vulnerabilities and potential value to state actors, and the prevalence and cost of consequences will reflect this.
- Espionage enables foreign interference, sabotage and further espionage, and the response to these other national security risks (and, therefore, associated mitigation and response costs) will also reduce the risk of espionage activity.
- Cyber-enabled espionage is the most tangible threat, and a growing proportion of espionage activity will involve a cyber component.
- Some of the most harmful consequences of espionage have, to the best of our knowledge, not been observed in the Australian context – but are plausible if there are insufficient controls in place.

There are additional assumptions that relate to specific cost items, and these are explained in the relevant section of this report.

Limitations

We have already noted several important limitations associated with this research. The first, and most obvious, is that we know that we have underestimated the true cost of espionage. Espionage is extremely difficult to detect. It is, by its very nature, a highly secretive and covert activity that takes many forms. Espionage activities that have been detected – and, even more so, the cases that have been prosecuted – represent only a small fraction of the actions threatening Australia's national security.

We have made the intentional choice to be conservative in our approach and to try not to include unsubstantiated costs. Our estimate draws on existing data and subject matter expert assessments – but we recognise that this approach does not allow us to quantify all costs. We have almost certainly underestimated both prevention and response costs and the direct cost of espionage, but we are satisfied that there is sufficient evidence to support our findings.

We decided to limit the scope of this work to one financial year. Many of the consequences arising from espionage activity in 2023–24 will not be observable (or even realised) until future years. Indeed, there is evidence that it can take, on average, more than 6 months for espionage activity to even be detected (European Commission & PwC 2018). Limiting our estimate to a single financial year was necessary for practical reasons, but it is not without its problems.

Finally, it is important to recognise that the work on which this has been based – the Australian Institute of Criminology's estimate of the costs of serious and organised crime – has now been reproduced several times. This has provided an opportunity to build on the original methodology and refine these estimates.

The previous cost of crime report also draws on a body of applied research into serious and organised crime. This is the first ever attempt to measure the range of known and suspected costs from espionage. While our methodology has been applied to other areas of national security, there are undoubtedly improvements that can (and should) be made in the future.

Espionage impacting Australia

A key step in trying to estimate the cost of espionage was understanding espionage in the Australian context and identifying the range of possible consequences. This section provides a high-level overview of our findings and the framework that guides the rest of our report. It draws on published research, intelligence assessments and interviews with subject matter experts.

State-sponsored actors target information or capabilities that align with the foreign government's strategic, political, military, social or economic goals (Lifhits 2024). All sectors of Australian society can be targeted by foreign adversaries based on how their classified, sensitive or proprietary information, data or technology can be exploited. Primary targets include the military, scientific, academic, legal, political, diplomatic, economic, corporate, industrial and technological sectors (ASIO 2025).

Targets

Foreign adversaries target protected and classified information from Australia's state and federal governments and defence industry, especially those related to military capabilities (ASIO 2022). This information allows foreign adversaries to obstruct Australia's military strategies, capabilities and intention, and to undermine Australian governments and gain political power and influence. Protected information or technologies related to Australia's shared government services, critical infrastructure, or other national assets or systems are also targeted by foreign adversaries, who may use this unauthorised access to sabotage or disrupt these systems, gain control over essential resources and industries, damage the Australian economy,and create instability and distrust among the public.

Foreign adversaries often target confidential or personally identifiable information about individuals (such as contact details, biometric data, medical or financial records) to facilitate foreign interference. Foreign interference is a state-sponsored activity that often occurs in tandem with espionage, in which a foreign power attempts to improperly and covertly interfere in Australian society to advance their goals (Department of Home Affairs 2024a).

To do this, foreign adversaries will obtain personal information about potential targets to identify, influence or coerce those in government, defence, journalism or academia, international students, diaspora communities, or other politically or culturally relevant positions (Taylor 2024).

The theft of proprietary or commercial information from a private business or company that is undertaken by a foreign government or state-sponsored actor is referred to as commercial espionage (Priyandita, Hogeveen & Stevens 2022). Adversaries may attempt to gain a competitive advantage by targeting IP about a product, service or process (e.g. product formulation), sensitive strategic information about marketing (e.g. product pricing), or insider knowledge about an upcoming business dealing (e.g. a company's bid price) (Intellectual Property Australia 2024; World Intellectual Property Organization 2025). International evidence indicates that the most common targets for IP theft are manufacturing, mining, engineering, information and communication technologies, finance, aerospace, medicine and biotechnology (Detica 2011; European Commission 2013; Verizon 2025).

Research and development activity is also a high-risk target for state-sponsored theft of information, data, methods or concepts (ASIO 2023). Cyber espionage campaigns have increasingly targeted universities, academia and research centres in Australia (Horton 2024), Europe (European Commission & PwC 2018) and the United States (Strider Global Intelligence Team 2019). A primary target for foreign adversaries is research and development in dual-use technologies, which have both civilian and military applications, such as drones or certain chemicals (Department of Defence 2025).

Vectors

The illicit transfer of Australian information or capabilities occurs through several means (vectors), including cyber attacks, insiders, partnerships or investments, technical collection, physical compromise, or a combination of these vectors (Burgess 2025, 2024).

With significant advancements in the sophistication and range of technologies available in recent years, foreign adversaries are increasingly using cyber attacks to remotely access protected digital networks, referred to as cyber espionage (Segal et al. 2018). Cyber attacks can involve highly sophisticated techniques (e.g. hacking) or simpler cybercrime techniques, such as phishing scams or ransomware attacks. ASIO recognises cyber espionage as an 'effective, highly deniable, low-cost and sometimes enduring vector' that is used to access very extensive collections of data, obtain strategic information, or to disrupt or damage systems. Foreign adversaries often employ groups of 'advanced persistent threat' actors, who are sophisticated and well-resourced malicious actors who conduct very deliberate and tailored attacks through a combination of cyber techniques, often after spending extensive periods of time gathering intelligence about a network to identify vulnerabilities (Australian Signals Directorate 2020).

An insider is a current or former employee or contractor who has legitimate or indirect access to a workplace's people, information, techniques, activities, technology, assets or facilities (Commonwealth Fraud Prevention Centre 2023). Espionage can occur when insiders use this access to transfer Australian information or capabilities to a foreign country. This transfer may be inadvertent or unknowing (an unintentional insider) or deliberate (intentional insider). Insider threats can come from affiliates, partners or supplementary staff (i.e. maintenance workers) of a targeted workplace (ASIO 2023). Insiders also include foreign professionals, students or scientists who are sent from an adversarial country to prominent positions in Australia (e.g. research laboratories) to gain training and knowledge that is then transferred to the adversarial country when the citizen returns (Strider Global Intelligence Team 2019).

The illicit transfer of information or capabilities can also occur through partnerships, collaborations or investments involving foreign individuals, groups or entities (Department of Home Affairs 2024a).

Such arrangements can include domestic companies entering into partnerships with foreign investors; foreign investors purchasing land, buildings or assets near sensitive sites (e.g. near a military site, airport, seaport or mining site); or domestic academics collaborating with foreign researchers (e.g. setting up a joint laboratory) (Strider Global Intelligence Team 2019). Foreign investment in facilities could allow adversaries to gain access to sensitive areas, information or systems.

Finally, espionage has often involved forms of technical collection, in which threat actors use audio, visual or cyber surveillance to gather imagery, electronics and signals intelligence (such as using audio recording devices to monitor private communications). Forms of physical compromise are also used, where threat actors physically trespass into secure buildings or areas, or steal physical items, such as documents, substances, hardware or devices (ASIO 2023; Kendell 2019). These vectors are often used in combination with other methods – for instance, a government employee's laptop is stolen by an adversary (physical compromise), who uses the laptop to gain access to a protected computer network and exfiltrate classified data (cyber attack).

Impacts

An incident of espionage against Australia can have numerous consequences for victim entities, which could include government, businesses or universities, as well as for the broader Australian economy and community.

Immediate and short-term impacts

Immediate and short-term impacts include the cost of investigation and response, dealing with damaged assets, reduced profitability, loss of expertise, and reputational damage.

Investigation and response costs

This includes investigation and prosecution by law enforcement and governmental authorities. Internal investigations are conducted by the victim entity to detect, contain and eradicate the threat. Time and resources are spent addressing the aftermath, such as preparing incident reviews, engaging with media, and debriefing with staff and stakeholders.

Lost/damaged assets

This includes cleaning, repairing or (in severe cases) entirely rebuilding infrastructure or digital systems that have been compromised and building temporary infrastructure. System downtime can interrupt government services or reduce revenue for businesses (e.g. loss of online sales). Physical assets may be lost, stolen or damaged (i.e. infected devices following a cyber attack).

Reduced profitability

This includes reduced actual or potential revenue from a product or service, particularly if theft nullifies a first-to-market advantage. Investment in research and development can be squandered and a competitive advantage lost, as a competitor can produce the same product for a lower price without spending time or funds on research and development.

Loss of expertise

Espionage by a compromised insider can result in a loss of expertise when the insider leaves Australia. Entities lose that insider's knowledge and skills, which could otherwise have been transferred within Australia (Strider Global Intelligence Team 2019).

Reputational damage

When incidents become public, there is reduced trust in an institution's ability to protect customer data or systems. Universities lose prospective students, staff or collaborations, and private companies lose customers or contracts, resulting in a devaluation of their stock value. Entities face regulatory or legal consequences as a result of security failures, such as financial penalties and class action lawsuits (Office of the Australian Information Commissioner 2024). Compromise of sensitive or classified government information damages Australia's reputation with international intelligence partners, who may restrict Australia's access to intelligence-sharing networks. Loss of trust among the public in the security and integrity of the government may also result (Commonwealth Fraud Prevention Centre 2023).

Long-term impacts

Potential long-term impacts are more persistent and severe.

Economic downturn

Innovation and investment in the overall market is inhibited when the perceived risk of research misappropriation is too high. Some researchers will forgo commercialisation opportunities due to these risks. Lower investment reduces productivity 'spillovers' that occur in the local economy (e.g. infrastructure built to support an investment). Adversaries can potentially control a strategically significant market by gaining large market share, meaning victim companies struggle to compete. When this happens, lower sales and reduced profitability can result in market distortion (due to lack of competition), job losses, bankruptcies and downturn in the wider Australian economy (Commonwealth Fraud Prevention Centre 2023).

Reduced international partnerships

International investors may avoid conducting business in Australia due to perceived lack of security (Commonwealth Fraud Prevention Centre 2023). Necessary restrictions on some high-risk foreign partnerships or investments can reduce investment and adaptability within an industry. Similarly, necessary restrictions on international students, collaborators or funding sources from adversarial countries limits potential revenue for universities. Reduced international students and partnerships can damage diplomatic and trade relationships with other countries and reduce productivity 'spillovers' in the local economy (e.g. demand for student housing).

Erosion of sovereignty

Stolen information is used to identify, influence or coerce those in government, defence, journalism, academia, diaspora communities or other politically or culturally relevant positions (Taylor 2024). This erodes decision-making and independence across these sectors of Australian society. Stolen information is also used to identify targets for follow-on espionage, cyber attacks, exploitation or financial crime (e.g. fraud or blackmail).

Increased risk of sabotage

Stolen information can also be used to monitor, disrupt or sabotage critical infrastructure. This interference could have extremely severe impacts on many essential services in Australian society, including disruptions to telecommunications networks, transport and traffic management systems, and crucial supplies of food, pharmaceuticals and fuel (Critical Infrastructure Centre 2020).

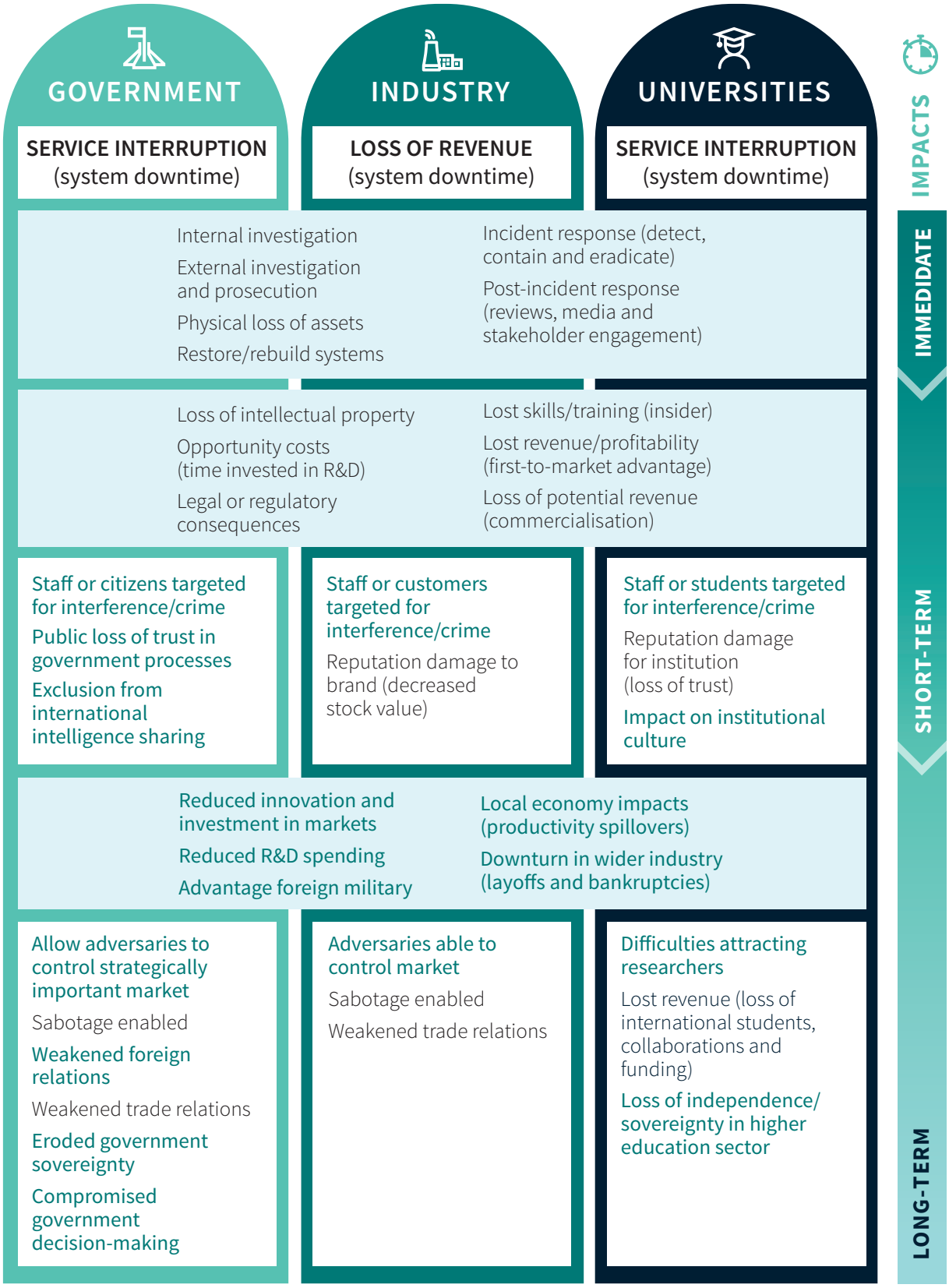
Stronger foreign military capabilities

The theft of information about Australia's defence or intelligence operations, tactics or capabilities, or the theft of military or dual-use technologies, would advantage an adversary's military (ASIO 2022). This would endanger Australia's citizens, allies and defence personnel.

Mapping the consequences of espionage

Figure 1 displays these immediate, short-term and long-term consequences of espionage, organised according to whether the target is the government, industry or university sector. As we have noted, state-sponsored espionage has many potential consequences that cannot be easily measured or quantified in monetary terms because they are hidden, subjective, dispersed or enduring in nature, taking months or years to be realised. Although they cannot be easily observed, these intangible costs often represent the greatest harm to Australia, such as a gradual but pervasive erosion of sovereignty across government. Moreover, even when a consequence is observable or measurable, it can be extremely difficult to attribute the outcome (e.g. economic downturn) directly to an espionage incident, as opposed to the many other potential political, social and economic factors that could contribute to that outcome. The consequences that have not been possible to cost in the current paper are presented in green text (Figure 1).

Figure 1: Potential impacts of espionage in Australia on the government, industry and university sectors



Green text indicates consequences that cannot be costed in current study

Mitigation and response costs

Significant resources are invested by government, the private sector and universities to mitigate and respond to espionage. Most of the data used to calculate these costs are sensitive or classified, and these costs have therefore not been itemised in this report.

Public sector expenditure

Public sector costs included the money spent by the federal government agencies to mitigate and respond to espionage incidents in Australia. The costs incurred by Commonwealth entities when responding to cases of espionage include those related to:

- identification, investigation and disruption by the Counter Foreign Interference Taskforce, law enforcement (Australian Federal Police) or other government authorities (ASIO)
- reconfiguring security systems, networks and controls after a compromise
- prosecution of espionage cases by authorities, such as the Australian Federal Police and the Commonwealth Director of Public Prosecutions
- legal advice around suspected cases of espionage (e.g. from Commonwealth Director of Public Prosecutions).

Costs related to developing and enacting policy and legislation regarding foreign interference and espionage are also included. These costs relate to:

- coordination between government agencies to counter espionage, primarily within the Counter Foreign Interference Coordination Centre (Department of Home Affairs)
- the Foreign Investment Review Board screening, reviewing or monitoring applications for foreign investment or foreign partnerships under the Foreign Arrangements Scheme, and compliance monitoring of these applications by adjacent agencies (e.g. the Australian Taxation Office)
- frameworks or task forces aimed at identifying and managing threats in research (Australian Research Council's Countering Foreign Interference Framework) or universities (e.g. University Foreign Interference Taskforce)
- additional screening of visa applicants in high-risk sectors such as critical technology (e.g. the Protecting Australia's Critical Technology Visa Screening Framework)
- other frameworks or task forces aimed at identifying and managing threats in high-risk sectors, including critical Infrastructure (e.g. under the *Security of Critical Infrastructure Act 2018* (Cth)) or the technology industry (e.g. the Technology Foreign Interference Taskforce).

Calculations included the costs of implementing and maintaining security measures, such as:

- cyber security software and measures to protect digital assets (measured in detail in the next section)
- other information and physical security measures to protect Australian Government staff, information, buildings, equipment and other physical assets located overseas (e.g. at Australian embassies or military bases)
- personnel vetting and ongoing security clearance monitoring conducted internally by Commonwealth agencies or the Australian Government Security Vetting Agency
- internal training programs for staff aimed at maintaining personnel, physical and information security (e.g. cyber security training).

Commonwealth entity resources related to community outreach were costed, including:

- education and awareness-raising programs for universities, industry, businesses, government, and vulnerable community populations (e.g. ASIO Outreach team)
- management of reporting mechanisms for espionage and related national security incidents (such as ASIO's Notifiable Incidents, Threats or Reportable Observations (NITRO) portal or the Australian Cyber Security Hotline)
- advice and assistance provided to Australian entities to prevent, identify and respond to cyber espionage (e.g. the Australian Cyber Security Centre).

It is important to note that many of the risk mitigation measures currently implemented across government – particularly legislation – were introduced in response to previous incidents of espionage or foreign interference. In this way, many of these mitigation and response costs can also be considered long-term consequences of espionage in Australia.

Federal government agencies were included if they have a policy responsibility to counter espionage or foreign interference or if they were identified as relevant by ASIO or stakeholders. Most of the included entities are involved in multiple risk mitigation and response functions that are undertaken across different divisions. Other agencies are involved in countering espionage through more narrow, specific functions performed by specialist teams. For instance, the Australian Federal Police and the Commonwealth Director of Public Prosecutions are primarily involved in the investigation and prosecution of espionage cases.

To estimate each entity's expenditure on mitigating or responding to espionage, we relied on expert input from senior representatives from these agencies, ASIO and other stakeholders. Publicly available and classified documents from these agencies were also reviewed. The operating expenditure of each entity was sourced from 2023–24 annual reports, with the exception of the Australian Secret Intelligence Service and the Office of National Intelligence, where portfolio budget statements for 2023–24 were used.

In most cases, stakeholder meetings provided detailed information about the annual resources (i.e. full-time effective staff or annual budget) allocated to programs or divisions dedicated to countering espionage. A 'bottom-up approach' was then used to calculate the proportion of the relevant budget relative to the total expenditure of that entity (expressed as a percentage). For other entities, particularly where activities related to espionage were dispersed across multiple teams, a 'top-down approach' was used. In these cases, we took the entity's total operating expenditure and applied an estimated proportion of the total expenditure that related to countering espionage.

These calculations do not include annual recurrent expenditure on cyber security by government departments, or the specific costs of cyber attacks (such as the costs of repairing compromised infrastructure or digital systems), as these costs have been included elsewhere in this report. These calculations also do not include the cost of offensive foreign intelligence operations.

Cyber security expenditure by government, businesses and universities

Given the high volume of cyber attacks targeting all sectors – including but not limited to state-sponsored attacks – Commonwealth, state, territory and local governments, businesses and universities all spend a proportion of their operating expenditure on cyber security. We estimated these separately, since cyber security does not fall under the espionage-specific prevention and response costs measured above.

We relied on several sources to estimate the cost of cyber security measures across government, businesses and universities. First, we determined the operating expenditure of each sector based on data reported by the Australian Bureau of Statistics (ABS) for government (ABS 2024b) and businesses (ABS 2024a) and data reported by the Department of Education on university expenditure (Department of Education 2024). We then relied on industry estimates of the proportion of total expenditure that is spent on ICT (Avasant 2024) and, of that, the proportion spent on cyber security (IANS Research 2022). We were unable to produce industry-specific estimates for business; however, we know that some industries likely spend more than others on ICT and cyber security.

The use of cyber security measures varies according to the size of an organisation. We therefore made further adjustments to account for the fact that, according to the ABS (2023) survey of the 'Characteristics of Australian Business', the likelihood of having cyber security measures in place varied between small (70.4%), medium (90.9%) and large (98.8%) organisations. We also assumed that the proportion of ICT budgets spent on cyber security varied by sector and business size, with Australian Government agencies and large businesses spending a higher proportion of their ICT budgets on cyber security measures.

Having estimated the total operating expenditure spent on cyber security by each sector, we then relied on input from subject matter experts to determine what proportion of these costs were associated with espionage. This varied by sector, with the assumption that higher costs would be incurred by sectors more frequently targeted by state or state-sponsored actors.

Mitigation costs to businesses, critical infrastructure and universities

There are other costs to businesses, some of which we have been able to include as part of our estimate. These include the costs associated with personnel security and vetting. We estimated the costs associated with assessments conducted by the Australian Government Security Vetting Agency for private industry, especially for personnel working in areas related to national security, but were unable to account for the (likely substantial) costs incurred by businesses that use commercial vetting companies, national police checking services or other suitability assessment tools to screen applicants for security risks.

There are also costs associated with applications for commercial foreign investments to the Foreign Investment Review Board (Treasury 2025). National security concerns are only one of several factors considered when assessing investments under the national interest test. We estimated that a portion of the fees paid when submitting a foreign investment proposal were therefore associated with espionage.

Critical infrastructure is a major target for foreign actors seeking to undermine Australia's national security. In addition to the costs to the Australian Government, there have been costs to industry associated with several major reforms to the regulation of critical infrastructure to reduce the risk of espionage (Department of Home Affairs 2022, 2020). We included an estimate of the annual cost to industry to implement the *Security of Critical Infrastructure Act 2018* (Cth) reforms, including the cost associated with adhering to mandatory incident reporting obligations and maintaining compliance with risk management program obligations.

Universities also incur costs associated with due diligence activity. This includes vetting of students who apply to conduct postgraduate research projects as part of high-risk or high-value research programs (especially in areas related to national security). We estimated the losses from denying admission to international students assessed as being high risk, which included the lost revenue to universities, the lost economic contribution of international students and their visitors, and the losses associated with the forgone research expenditure and associated benefits of productivity spillovers and economic growth. Related to this, under the voluntary University Foreign Interference Taskforce (2021) guidelines, universities have set up screening processes for collaboration in sensitive areas to assess the risks associated with partnerships with foreign institutions. We estimated the cost of providing advice and compliance checking, and the costs of setting up any joint programs between Australian universities and international partners – a portion of which would be related to national security.

Additional costs

There are several additional costs incurred as a consequence of the action taken by government, businesses and the university sector to prevent espionage. These mainly take the form of premiums paid because the alternative presents too great a risk to Australia's national security.

- Subject matter experts identified several examples where the most suitable, optimal or cost-efficient technology from an overseas supplier could not be used because of the unacceptable risk that the technology would pose to national security. In these instances, an alternative product must be sourced and procured, often resulting in increased cost or, in some instances, suboptimal performance.
- Government suppliers, especially those working in areas related to national security, must meet certain minimum security standards, partly to reduce the risk of espionage. The supplier costs associated with meeting these security requirements would be passed on to government.

- A major package of foreign investment reforms was introduced in 2021 to address the risks to Australia's national interest. Australia has in place mechanisms to review applications for foreign investment to consider, among other things, the risk posed to national security. This may impact foreign investment in 2 ways. First, it may deter potential investors. Second, some investment opportunities may be rejected because of the risk to national security.
- It is possible that the risk of espionage also means that government agencies, businesses and universities, having undertaken appropriate due diligence, choose not to enter into formal research agreements with foreign partners, whether they be individuals or organisations. This may limit opportunities for Australian researchers and institutions to partner with international researchers and benefit from their expertise and standing. This could have funding implications, as well as a detrimental impact on the potential returns from investment in research and development.

There was strong support from subject matter experts for these costs being included in our estimate, and some available data indicate that these represent very significant costs incurred by Australia. Nonetheless, we were unable to find sufficient data to fully and accurately estimate these costs.

Direct costs of known or suspected espionage

Our estimate of the direct costs of espionage is focused on state or state-sponsored activities, including cyber security incidents (cyber espionage), insider threats, and IP and trade secret theft. These impacts were measured across businesses, universities and government.

Cyber security incidents (excluding intellectual property theft)

A range of direct costs are incurred as a result of cyber espionage that extend beyond the value of any IP that is stolen or compromised. These costs are measured here, and include the cost of investigating incidents, replacing or rebuilding systems, legal and regulatory consequences, damage or disruption to information systems or operational processes, loss of revenue during system downtime, reputational damage with customers and suppliers, and other costs. The estimated value of IP that has been stolen or compromised (through any vector of espionage) is estimated separately.

Results are presented for the impact on businesses and universities. Estimates of the cost to government from cyber security incidents have been omitted from this report due to the use of sensitive and classified data.

Impact on businesses

To estimate the cost of cyber espionage incidents (excluding IP theft) impacting businesses, we relied on data from the ABS (2023) 'Characteristics of Australian Business' survey. It represents the most recent, robust and representative survey of cyber security incidents impacting businesses of all sizes. It provides an estimate of the prevalence of 8 types of cyber security incidents among all Australian businesses in the 12 months prior to June 2022. Overall, 22.1% of businesses reported having experienced at least one incident. However, the most common incident type was scams or fraud (16% of all businesses). While it is possible that some of these incidents were state-sponsored, we excluded these from the estimate. Unfortunately, some of these businesses will have also experienced the other types of cyber security incidents; however, in order to avoid overcounting, we decided to rely on as our principal measure the proportion of businesses that experienced a cyber security incident but that were not a victim of scams or fraud (5.7% of all businesses).

These businesses may have experienced:

- unauthorised access to, or use of computers, networks or servers by people internal or external to the business
- improper use of computers, networks or servers
- computers infected with malicious software
- denial-of-service or distributed denial-of-service attacks
- disruption or defacement of online presence
- impersonation of the business or its employees online or by email
- other cyber security incidents.

In addition to data for all businesses, the ABS reported the prevalence of cyber security incidents by industry type. We relied on these industry-specific estimates as the basis of our calculations. The survey also showed that large businesses (200 or more employees) were much more likely to report a cyber security incident, followed by medium businesses (20–199 employees), when compared to small (5–19 employees) and micro (0–4 employees) businesses. We therefore used the overall prevalence by business size to produce adjusted estimates of the prevalence of cyber security incidents by industry (Table 1).

Table 1: Prevalence of cyber security incidents among Australian businesses, by industry and business size, 2021–22 (%)

	Small	Medium	Large
Agriculture, forestry and fishing	2.8	4.6	6.1
Mining	9.8	16.1	21.5
Manufacturing	7.8	12.9	17.2
Electricity, gas, water and waste services	5.8	9.6	12.8
Construction	5.3	8.6	11.5
Wholesale trade	11.7	19.2	25.7
Retail trade	7.8	12.9	17.2
Accommodation and food services	2.5	4.1	5.4
Transport, postal and warehousing	1.7	2.8	3.7
Information media and telecommunications	10.5	17.3	23.1
Financial and insurance services	4.6	7.5	10.0
Rental, hiring and real estate services	6.9	11.4	15.2
Professional, scientific and technical services	7.5	12.4	16.5
Administrative and support services	2.9	4.7	6.3
Public administration and safety	6.0	9.9	13.2
Education and training	6.0	9.9	13.2
Health care and social assistance	5.9	9.8	13.1
Arts and recreation services	5.7	9.4	12.6
Other services	4.5	7.3	9.8
Currently unknown	4.5	7.3	9.8

Note: Proportion of businesses that experienced a cybersecurity incident, but which were not a victim of scams or fraud. Source: ABS (2023)

Of course, not all of these incidents would have been state-sponsored. We therefore had to develop a method for determining what proportion of incidents were related to espionage. Verizon (2025) and Bitkom Research (2024) have produced very similar overall estimates of the prevalence of state-sponsored cyber security incidents – 17% and 20%, respectively – but Verizon also provided industry-specific figures. We mapped these estimates to the ABS industry categories as best as we could and estimated the number of businesses in each industry that we believe were impacted by an incident of cyber espionage (Table 2). We verified these allocations with subject matter experts. We limited our estimate to medium and large businesses because this aligned with the case studies that we were able to review and avoided overcounting (especially for industries with a disproportionate number of small businesses, which were, based on the case studies, less likely to be targeted by state or state-sponsored actors).

We made a further adjustment to account for the fact that not all victims of cyber security incidents will experience harm or incur costs. The ABS (2023) 'Characteristics of Australian Business' survey included estimates of the proportion of businesses that had experienced a cyber security incident and experienced at least one impact. We used the proportion of businesses that experienced any impacts, by industry, to determine the number of businesses that had experienced a cyber security incident in the previous 12 months, related to espionage, and which were impacted as a result.

Finally, we estimated the costs associated with these incidents. There are various estimates of the costs of cyber security incidents. While the Australian Signals Directorate (2024) reports the average cost per incident for small, medium and large businesses, these are self-reported estimates with little information about what is included. They also relate to all incident types, especially fraud and scams, which we have excluded from our estimate. We have therefore relied on 2 industry estimates of the cost per data breach incident. For medium businesses, we elected to use the estimate by Bitkom Research (2024), based on their survey of German businesses. For large businesses, we relied on the estimate produced by IBM Corporation (2024) on data breaches. Both included direct and indirect costs. Importantly, they not only published an overall estimate of the cost per incident but also provided sufficient information to determine the various cost components. Some of the cost to business will come from the loss of IP and trade secrets. While this cost was captured as part of the estimates, we have captured these losses elsewhere and excluded the associated costs from this estimate. The estimated average cost per incident for medium businesses was $969,875, while for large businesses it was $4.6 million.

The results are presented in Table 3. These show that the cost of cyber security incidents impacting Australian businesses ranged from $761.6 million to $1,193.8 million, with considerable variation between industries.

The estimated cost of state-sponsored cyber security incidents impacting Australian medium and large businesses in 2023–24 was up to **$1,193.8 million**.

Table 2: Involvement of state or state-sponsored actors in cyber security incidents, by industry (%)			
	Small	Medium	Large
Agriculture, forestry and fishing	29.7	33.0	44.6
Mining	49.5	55.0	74.3
Manufacturing	18.0	20.0	27.0
Electricity, gas, water and waste services	49.5	55.0	74.3
Construction	20.7	23.0	31.1
Wholesale trade	0.0	0.0	6.3
Retail trade	8.1	9.0	12.2
Accommodation and food services	15.3	17.0	23.0
Transport, postal and warehousing	14.4	16.0	21.6
Information media and telecommunications	32.4	36.0	48.6
Financial and insurance services	10.8	12.0	16.2
Rental, hiring and real estate services	0.0	0.0	6.3
Professional, scientific and technical services	15.3	17.0	23.0
Administrative and support services	15.3	17.0	23.0
Public administration and safety	26.1	29.0	39.2
Education and training	16.2	18.0	24.3
Health care and social assistance	14.4	16.0	21.6
Arts and recreation services	16.2	18.0	24.3
Other services	27.9	31.0	41.9
Currently unknown	27.9	31.0	41.9

Note: The medium estimate of the proportion of incidents that were state-sponsored is based on the industry estimates produced by Verizon (2025). Those estimates are of the proportion of incidents motivated by espionage. The high estimate accounts for the fact that around one-quarter of state-sponsored incidents were motivated by financial gain.

Table 3: Estimated cost of cyber security incidents (excluding IP theft) related to espionage impacting Australian small, medium and large businesses ($m)

	Small	Medium	Large
Agriculture, forestry and fishing	$16.1	$17.9	$24.1
Mining	$61.3	$68.1	$92.0
Manufacturing	$129.7	$144.1	$194.5
Electricity, gas, water and waste services	$20.9	$23.3	$31.4
Construction	$81.0	$90.0	$121.5
Wholesale trade	$0.0	$0.0	$42.6
Retail trade	$40.3	$44.7	$60.4
Accommodation and food services	$52.0	$57.7	$77.9
Transport, postal and warehousing	$7.6	$8.5	$11.4
Information media and telecommunications	$40.6	$45.2	$61.0
Financial and insurance services	$12.8	$14.2	$19.2
Rental, hiring and real estate services	$0.0	$0.0	$8.8
Professional, scientific and technical services	$100.4	$111.5	$150.6
Administrative and support services	$41.7	$46.4	$62.6
Public administration and safety	$12.3	$13.7	$18.5
Education and training	$34.2	$38.0	$51.3
Health care and social assistance	$70.2	$78.0	$105.3
Arts and recreation services	$15.8	$17.6	$23.7
Other services	$24.2	$26.9	$36.3
Currently unknown	$0.4	$0.5	$0.7
Total	**$761.6**	**$846.2**	**$1,193.8**

CASE STUDY 1

Cyber attack on Australian university to steal personal data

A sophisticated nation-state actor gained unauthorised access to the IT network at a large Australian university. The hackers initially gained access using a sophisticated 'spear-phishing email' that was targeted at specific individuals, and the actors were present in the system for approximately six weeks. A forensic investigation of the incident determined that student and staff data were stolen, including personally identifying information, sensitive financial records and other confidential data. The intruders had access to intellectual property and research information; however, investigators did not find evidence that this information was stolen. It remains unclear how the stolen information has been used, however, the risk of follow-on espionage or foreign interference is notable given that the university is closely tied to the Australian Government and intelligence community, and conducts research with many defence, strategic and commercial applications (Segal et al. 2018).

Note: Information about this incident has been sourced from publicly available reports.

Impact on universities

We separately estimated the cost of cyber security incidents to public universities, excluding the value of stolen or compromised IP. We relied on data from the UK's 'Cyber Security Breaches Survey 2024' (UK Home Office 2024). According to that survey, 97% of higher education institutions in the UK identified a breach or an attack in the 12 months prior to the survey. One-third of institutions said that their accounts or systems had been compromised and used for illicit purposes.

Based on this, we estimated that 13 Australian public universities in 2023–24 experienced a data breach or attack resulting in their accounts or systems being compromised (we assume none of these universities were a victim of more than one incident). We used the industry-specific estimate of espionage-motivated data breaches from the Verizon (2025) study for the education sector (18%), with the same adjustment as before to account for state-sponsored breaches motivated by financial gain. This resulted in an estimate that 16.2% (low), 18.0% (medium) to 24.3% (high) of cyber security incidents impacting universities are related to espionage. We assume the same cost per incident as for large businesses ($4.6 million).

This resulted in a final estimated cost of between $9.6 million and $14.5 million for state-sponsored cyber security incidents impacting Australian public universities.

The estimated cost of state-sponsored cyber security incidents impacting Australian public universities in 2023–24 was up to **$14.5 million**.

Insider threats

We estimated the costs related to insider threats, including but not limited to physical loss of assets; cost of investigation, detection and remediation; reputational damage and loss of confidence among stakeholders; legal or regulatory consequences; and the cost of system downtime on revenue and productivity. Again, the value of lost or stolen IP was costed separately.

Impact on businesses

There is very little Australian data on the prevalence of insider threats. Industry data suggests that between 83% and 89% of all businesses have had at least one insider threat (Allied Universal 2023; IBM Corporation 2024). However, not all of these will be motivated to harm the business – it includes employee or contractor negligence. According to the Ponemon Institute (2022), 26% of organisations that reported experiencing an insider threat said the insider had a criminal or malicious intent.

We used this estimate (equivalent to 21.6% of businesses) to calculate the number of medium and large Australian businesses that had a malicious insider. This included individuals who used their access to data or networks for harmful, unethical or illegal activities (Ponemon Institute 2022). Only a fraction of these insider threats will have involved a state or state-sponsored actor.

Based on input from subject matter experts, we estimated that only 2% of these cases were related to espionage (this also assumes only one incident per business). We used this as our high estimate, because it included reported and unreported cases. Our lower estimate was based on the number of insider threats reported to intelligence agencies in 2023–24.

We used the Ponemon Institute's (2022) estimate of the cost per incident for malicious insiders, adjusted to Australian dollars. This included the costs of surveillance to detect an incident, investigation of the source and magnitude of the incident, escalation to company management, incident response to contain and manage the severity of the incident (such as shutting down vulnerabilities), post-incident strategies to minimise similar future incidents, and remediation to repairing systems and business processes. We excluded indirect costs related to IP and trade secret theft (see Case study 2), which are counted elsewhere. This also does not include the costs associated with external investigation and, where applicable, prosecutions.

Drawing on our low and high estimates of the number of malicious insider threats related to espionage impacting Australian businesses, we assessed the cost in 2023–24 to be between $266.6 million and $324.8 million.

The estimated cost of insider threats involving state or state-sponsored actors impacting Australian businesses in 2023–24 was up to **$324.8 million**.

CASE STUDY 2

Insider theft of intellectual property from an American company

In 2021 a foreign national in the US was convicted of conspiracy to steal trade secrets (United States Department of Justice 2021). The offender stole trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans, which she had access to while employed as a development manager at a beverage company in the US. Developing the proprietary technology was a very expensive and time-consuming process and reportedly cost nearly US$120 million (Lifhits 2024). The offender intended to use this technology to start a rival company in her homeland, and had received millions of dollars in grants from her native government to support this venture. Her intention to benefit the foreign government was demonstrated in her grant application, which was shown at trial. The court concluded that because the market was a monopoly, the offender would have absorbed all purchases of BPA-free coatings in her home country, with a potential revenue of $17.4 million per year (Lifhits 2024).

Impact on universities

We adopted a similar approach to estimate the cost associated with malicious insider threats involving state or state-sponsored actors impacting Australian public universities. On this occasion, we relied on data on suspected insider threats reported to intelligence agencies, since no equivalent published data were available. We used the Ponemon Institute's (2022) average cost of malicious insider threats in the education sector, which was lower than that of other sectors.

Taken together, we estimated the cost of espionage-related insider threats impacting Australian public universities to be up to $25.0 million. This excludes all of the indirect costs that can result from insider threats, including the loss of IP (counted elsewhere) and the loss of revenue and commercial advantage (see Case study 3).

The estimated cost of insider threats involving state or state-sponsored actors impacting Australian public universities in 2023–24 was up to **$25.0 million**.

CASE STUDY 3

Student misappropriates intellectual property from an American university

One of the world's leading experts on metamaterials from a large American university accused his former PhD student of stealing his research into quantum invisibility metamaterials (Miller 2019). The professor had received millions of dollars in funding from the US Department of Defense to develop a prototype for a 'quantum invisibility cloak' that makes objects undetectable by microwave signals. The Pentagon was interested in this technology's significant military applications for advancing stealth aircraft and vehicles, which would give the US an immense strategic advantage over other militaries.

While the PhD student was working in the university laboratory, he allegedly withheld information from the professor about his intentions to replicate the research. The student allegedly convinced the professor to allow him to bring foreign colleagues into the laboratory, who covertly gathered data on the quantum invisibility equipment (McFadden, Nadi & McGee 2018).

The student returned to his home country after completing his PhD, where he quickly developed and commercialised his own prototype of the quantum invisibility cloak, which is allegedly identical to the technology developed at the American university. In a private email exchange found after the student had returned to his home country, the student apparently confirmed that he had been sent to the laboratory by his government to steal the 'invisibility cloak' technology for its military applications (McFadden, Nadi & McGee 2018; Weichert 2021). The former student is now the founder of a $6 billion technology company that features the quantum invisibility cloak technology. This laboratory has begun mass-producing quantum invisibility metamaterials for use in the foreign military's fleet of warplanes, with annual production capacity of more than 10,000 square metres of metamaterial plates (Weichert 2021). In 2010 the Federal Bureau of Investigation opened a case into this potential theft of US IP; however, the case was closed after several years due to a shortage of evidence.

Intellectual property theft

Impact on businesses

To measure the costs associated with the theft of IP and trade secrets from business, we used the ABS (2023) 'Characteristics of Australian Business' survey. Businesses that had experienced a cyber security incident were asked whether they had been affected by corruption, theft, compromise or the loss of hardware, software, data, IP, personal or financial information (8% of all businesses that had experienced an incident, equivalent to 1.8% of all businesses). We used this to measure the prevalence of cyber-enabled IP theft by industry.

Because this figure captures impacts other than IP theft, we made a further adjustment using data from the Australian Institute of Criminology's 'Australian Cybercrime Survey' (Voce & Morgan 2023), which includes a specific question about the loss of IP among small to medium businesses (2.5% of businesses that were a victim of at least one incident). We used this adjusted estimate to calculate the proportion of businesses, and therefore the number, that were impacted by cyber-enabled IP and trade secret theft involving any type of actor (Table 4).

The estimated cost of cyber-enabled theft of IP and trade secrets from businesses involving state or state-sponsored actors in 2023–24 was **$1,901.0 million**.

Table 4: Prevalence of cyber-enabled intellectual property and trade secret theft, by industry and business size (%)

	Small	Medium	Large
Agriculture, forestry and fishing	0.87	1.43	1.91
Mining	0.66	1.09	1.46
Manufacturing	0.79	1.29	1.72
Electricity, gas, water and waste services	0.23	0.38	0.51
Construction	0.69	1.13	1.51
Wholesale trade	0.62	1.01	1.35
Retail trade	0.01	0.01	0.02
Accommodation and food services	0.56	0.92	1.23
Transport, postal and warehousing	0.14	0.23	0.31
Information media and telecommunications	0.86	1.42	1.90
Financial and insurance services	0.40	0.65	0.87
Rental, hiring and real estate services	0.57	0.94	1.25
Professional, scientific and technical services	0.90	1.48	1.97
Administrative and support services	0.23	0.38	0.50
Public administration and safety (private)	0.50	0.81	1.09
Education and training (private)	0.50	0.81	1.09
Health care and social assistance (private)	0.46	0.76	1.01
Arts and recreation services	0.50	0.83	1.11
Other services	0.21	0.35	0.47

CASE STUDY 4

Cyber-enabled economic espionage affecting a mining company

In 2008 a mining company operating in Australia was targeted by a cyber espionage operation, in which state or state-sponsored actors allegedly stole IP and commercially sensitive information relating to price negotiations with buyers. The company lost an estimated $1.43 billion in revenue (over $2 billion in 2024 dollars) from both IP loss and commercial disadvantage in negotiations as buyers were able to compel the company to sell their product at a reduced price (Segal et al. 2018).

Table 5: Estimated loss in profits due to cyber-enabled intellectual property and trade secret theft by a state or state-sponsored actor, by industry ($m)

	Low	Medium	High
Agriculture, forestry and fishing	$38.24	$42.49	$57.36
Mining	$924.23	$1,026.93	$1,386.35
Manufacturing	$59.16	$65.73	$88.74
Electricity, gas, water and waste services	$18.24	$20.27	$27.36
Construction	$55.02	$61.13	$82.53
Wholesale trade	$0.0	$0.0	$15.82
Retail trade	$0.21	$0.24	$0.32
Accommodation and food services	$10.17	$11.30	$15.26
Transport, postal and warehousing	$3.27	$3.63	$4.91
Information media and telecommunications	$12.95	$14.39	$19.43
Financial and Insurance Services	–	–	–
Rental, hiring and real estate services	$0.0	$0.0	$13.55
Professional, scientific and technical services	$91.87	$102.08	$137.80
Administrative and support services	$3.30	$3.67	$4.96
Public administration and safety (private)	$1.65	$1.83	$2.48
Education and training (private)	$4.16	$4.62	$6.24
Health care and social assistance (private)	$17.04	$18.94	$25.57
Arts and recreation services	$3.36	$3.73	$5.04
Other services	$4.89	$5.43	$7.33
Total	**$1,247.8**	**$1,386.4**	**$1,901.0**

Note: Data were not available on operating profit for financial and insurance services.

To estimate the cost of IP and trade secret theft from businesses, we focused on the impact of the theft on profitability. Research conducted on behalf of IP Australia measured the relationship between IP rights and profitability (Zhang 2020). While not strictly a measure of the value of IP and trade secrets, it provides a useful metric of the value of exclusive IP rights to profitability, finding that businesses with IP rights were 1.6 times more profitable than those without. We converted this estimate, assuming that the loss of exclusive rights due to IP theft would have the inverse effect on business profitability. Using ABS (2024b) data on the operating profit (before tax) of Australian businesses, by industry and business size, we were then able to estimate the loss in profitability due to IP and trade secret theft.

We applied the same industry-specific estimates of state or state-sponsored actor involvement in cyber security incidents (Table 2) to determine the proportion of these total losses that were due to espionage. This approach yielded an estimated cost of cyber-enabled theft of IP and trade secrets from businesses in 2023–24 of between $1,247.8 million and $1,901.0 million (Table 5). Most of this is attributable to losses in the mining sector (>70%), which reflects the sector's vulnerability to commercial espionage by foreign actors (see Case study 4).

Impact on government, not-for-profit sector and universities

We adopted a different approach to estimate the cost to government and universities of IP theft by state or state-sponsored actors. In this case, we estimated the financial gains that would have resulted from the technological innovation generated from research and development expenditure, had the IP not been stolen.

We started with data from the ABS on research and development expenditure by federal government agencies and state and territory governments, the private non-profit sector and the higher education sector (ABS 2024c, 2024d). This includes all 'creative and systematic work undertaken in order to increase the stock of knowledge and to devise new applications of available data' (ABS 2024c). Taken together, these sectors spent nearly $20 billion on research and development in 2023–24.

There is, to the best of our knowledge, no credible estimate of the prevalence of IP theft specifically targeting research. To overcome this gap, we relied on research into the extent of plagiarism among journal submissions. Obviously not all research supported by this expenditure will result in published articles; however, it represents a useful metric for measuring research output, even for critical technologies and other topics that are at risk of being targeted by foreign actors (Leung, Robin & Cave 2024). A recent global survey of nearly 400 journal editors found that, while respondents estimated that up to 15% of submissions contained plagiarised or duplicated content, they had encountered plagiarised content in between 2% and 5% of submissions (Smart & Gaston 2019). Rates of reported plagiarism were highest among Asian editors. Most of the duplication related to relatively minor issues. Other studies focused on 'problematic' journals have reported much higher rates of plagiarism (e.g. Abalkina 2024).

We used an estimate from the lower end of this range (2.5%) as the basis for calculating the cost of IP theft. While, on the one hand, this may overestimate the extent of fraudulent plagiarism and IP theft, it helps to account for the fact that much of what we expect to occur in cases of espionage will not result in published research outputs. We used this to determine the proportion of research expenditure lost to IP theft and which, therefore, was unlikely to produce a return on investment in Australia.

We used research by Wynn, Liu and Cohen (2021) to measure the return on investment in research and development. That study applied a method that had been used elsewhere to measure the relationship between domestic gross expenditure on research and development (the same metric we used) and GDP growth per capita. Importantly, it measures economic growth resulting from technological innovation but accounts for both successful and unsuccessful investments, and the cost and delay involved in converting research and development into new capital inputs. This metric is better than others, such as productivity spillovers (used elsewhere in this report), since these other metrics include benefits that would still be gained from research even if it were subsequently stolen.

According to this study, every dollar invested in research and development in Australia produces an average of $3.50 in economy-wide benefits. This return is not immediate, but for our purposes represents the current value of research and development expenditure. We used this to estimate the total return on investment from research and development expenditure, according to the socio-economic objective of the research. We then estimated the total value – including the return on investment – that was lost because of research being stolen, by applying our estimate of the prevalence of plagiarised research (2.5%).

We used the same industry-specific estimates of state or state-actor involvement from Verizon (2025) – adapted to suit the different categories used for research and development expenditure – to determine the proportion of these total losses that were due to espionage. This resulted in estimated losses of between $413.0 million and $628.0 million from espionage-related IP theft (Table 6). Health accounted for the largest proportion of these losses (21.5%), followed by expanding knowledge (a broad category of research that was not categorised elsewhere; 17.3%) and defence (10.9%).

The estimated cost of IP theft from government, the not-for-profit sector and universities involving state or state-sponsored actors was up to **$628.0 million** in 2023–24.

Table 6: Estimated cost to government, the not-for-profit sector and universities of intellectual property theft by a state or state-sponsored actor, by socio-economic objective ($m)

	Low	Medium	High
Animal production	$13.4	$14.9	$20.1
Commercial services and tourism	$1.6	$1.7	$2.3
Construction	$3.6	$4.0	$5.5
Culture and society	$0.0	$0.0	$5.1
Defence	$45.8	$50.9	$68.8
Economic framework	$9.2	$10.3	$13.8
Education and training	$6.7	$7.5	$10.1
Energy	$28.6	$31.8	$42.9
Environmental management	$38.1	$42.4	$57.2
Environmental policy, climate change and natural hazards	$20.1	$22.3	$30.2
Health	$90.0	$100.0	$134.9
Indigenous	$0.0	$0.0	$3.4
Information and communication	$16.9	$18.8	$25.4
Law, politics and community	$14.5	$16.1	$21.8
Manufacturing	$15.5	$17.3	$23.3
Mineral resources (excl. energy)	$13.6	$15.1	$20.4
Plant production	$19.7	$21.9	$29.6
Transport	$2.9	$3.2	$4.3
Expanding knowledge	$72.6	$80.7	$108.9
Total	**$413.0**	**$458.9**	**$628.0**

Prevented costs from espionage

The final category of cost estimates included in this research is the cost of espionage that may have been prevented through effective mitigation efforts and counter-espionage activity. The costs that are summarised in this section are those which have not yet been documented but which are plausible in the event of significant espionage activity impacting Australia.

It is worth noting that the direct costs of espionage reported in the previous section are also preventable. They would almost certainly have been higher without mitigation efforts and counter-espionage activity. An increase in espionage activity targeting Australia could also see these costs rise if cyber security incidents, insider threats and IP theft were to worsen. This should be considered alongside the prevented costs in this section.

Disruption to critical infrastructure

Disruption to critical infrastructure – especially where it is prolonged and widespread – can have a range of serious consequences. Various incidents in Australia and overseas, while not caused by espionage, have illustrated these consequences.

These incidents were used as case studies in a regulatory impact analysis completed by the Department of Home Affairs (2022, 2020) to inform changes to the regulation of critical infrastructure. These reforms were focused on increasing the resilience of critical infrastructure and supply chains to all hazards, which includes natural and physical hazards, cyber incidents, trusted insiders, unlawful interference and espionage.

These case studies (Table 7) were used to determine the estimated potential benefits of the proposed reforms – the costs that could be avoided if the reforms were introduced and the risks effectively managed. Modelling was applied to a hypothetical supply shock for each type of infrastructure and the direct and indirect costs that were expected to result. For each type of infrastructure, severe, moderate and low-cost scenarios were modelled, with multiple case studies presented or a relative cost used (for example, where the low-cost scenario was 50% of the cost of the moderate scenario, without relying on an actual example). Our main assumption in relying on these scenarios is that, while the cause of the disruption may not have been espionage, the consequences are likely to be similar.

We used these case studies and estimated costs (inflated to current Australian dollars) to illustrate the potential cost of sabotage enabled by espionage (Table 8). Consistent with the regulatory impact statement, we present the moderate scenarios as the most likely outcome. Sabotage resulting from espionage could, based on these scenarios, cost anywhere in the range of $4.4 million to $1,162.2 million per incident.

Sabotage of critical infrastructure enabled by espionage could cost up to **$1,161.2 million** per incident.

Table 7: Case studies used to estimate direct and indirect costs of disruptions to critical infrastructure

	Low	Moderate	Severe
Critical gas assets	25% of severe scenario	50% of severe scenario	Varanus Island disruption (2008)
Critical liquid fuel asset	Colonial Pipeline ransomware attack (2021)	50% of severe scenario	Varanus Island disruption (2008)
Critical electricity asset	50% of moderate scenario	South Australian blackout (2016)	150% of moderate scenario
Critical energy market operator assets	50% of moderate scenario	South Australian blackout (2016)	150% of moderate scenario
Critical freight infrastructure and critical freight services assets	ForwardAir ransomware attack (2020)	50% of severe scenario	TNT Express NotPetya attack (2017)
Critical telecommunications asset	50% of moderate scenario	Incident impacting a major telecommunications carrier	200% of moderate scenario
Critical water asset	UK water supplier scam (2017)	Sydney water crisis (1998)	Queensland floods (2010–11)
Critical hospital asset	10% of severe scenario	50% of severe scenario	NHS 2017 cyber attack
Critical data storage or processing asset	Former employee targets Cisco Systems (2018)	Kaseya ransomware attack (2021)	200% of moderate scenario
Critical food and grocery assets	JBS attack (2021)	Coop Supermarket attack (2021)	150% of moderate scenario
Critical payment system assets	50% of moderate scenario	NAB service outage (2018)	200% of moderate scenario
Critical broadcasting assets and critical domain name systems	50% of moderate scenario	ABC's South Coast transmitter bushfire incident (2020)	200% of moderate scenario costs

Source: Department of Home Affairs (2022, 2020)

Table 8: Cost per incident causing disruption to critical infrastructure, by severity of incident and type of asset ($m)

	Low	Moderate	Severe
Critical gas assets	$595.1	$1,161.2	$2,219.1
Critical liquid fuel asset	$16.8	$1,161.2	$2,219.1
Critical electricity asset	$568.4	$986.0	$1,484.8
Critical energy market operator assets	$568.4	$986.0	$1,484.8
Critical freight infrastructure and critical freight services assets	$21.0	$419.9	$840.0
Critical telecommunications asset	$105.0	$210.0	$420.0
Critical water asset	$1.4	$147.1	$4,754.8
Critical hospital asset	$26.7	$133.3	$266.6
Critical data storage or processing asset	$5.3	$113.7	$227.4
Critical food and grocery assets	$28.2	$55.7	$83.5
Critical payment system assets	$7.9	$15.7	$31.4
Critical broadcasting assets and critical domain name systems	$2.2	$4.4	$8.9

Sophisticated cyber attacks against multiple sectors

The final scenario represents the worst-case scenario – a sophisticated cyber attack that cuts across a range of economic sectors. AustCyber (2020) modelled the effect of an economy-wide digital disruption impacting digital technology intensive industries. Taking into account the direct economic impact of these industries, including market-related expenditure and flow-on effects, and the indirect economic impact, such as household expenditure by employees in those industries, AustCyber estimated the effects of a one-week and a 4-week digital disruption on the Australian economy due to a sophisticated cyber attack. That disruption could involve repeated attacks designed to harm Australia's economy. Similar to the scenarios above, these attacks could be enabled by espionage.

They concluded that a one-week digital disruption would have a total economic impact of $5,930.4 million (in current Australian dollars), while a 4-week digital disruption would cost the Australian economy $35,580.1 million.

Decline in share prices following public reporting of espionage

The *Economic Espionage Act of 1996* was introduced in the US to address commercial espionage by foreign actors targeting US companies. While it also criminalised industrial espionage between private entities, it was a response to a perceived increase in trade secret theft by foreign actors.

Several studies have now measured whether the publicity associated with being a victim of trade secret theft has an impact on the stock price of the company (Carr & Gorman 2001; Michaelides et al. 2024). The assumption behind these studies is that stock prices reflect the value of a company, based on publicly available information. Trade secrets represent an important intangible asset that contributes to company value and economic growth. When a company is the target of trade secret theft, and a criminal prosecution is publicly announced, the market is expected to react strongly and negatively because of an anticipated loss in future revenue for that company.

A week-long economy-wide disruption to digital technology intensive industries, enabled by sabotage, could cost the Australian economy **$5,930.4 million**.

Michaelides et al. (2024) analysed cases where the announcement of judicial proceedings was the first time there was public mention that a company had been victim to trade secret theft. They found abnormal negative returns of between 1.26% and 1.74% in the short term and 2.20% after 30 days following disclosures of trade secret theft carried out on behalf of a foreign government. This represented a loss of between US$1.6 billion and US$2.6 billion per incident. Importantly, the companies that were victims of trade secret theft were larger than average publicly listed companies and were in IP intensive industries associated with dual-use technologies. These were also conservative estimates, because they did not account for the loss of competitive advantage or impact on future business partnerships.

We used this analysis to estimate the potential impact of falling victim to espionage on the share price of Australian companies. This is a proxy for the impact of trade secret theft on the profitability of a company. Obviously, this assumes that the theft becomes public knowledge; however, we assume the loss of profitability would be similar in cases that are not made public (an assumption we were able to test by comparing our result to a historical case impacting a mining company). We used the mean market capitalisation for all companies listed on the Australian Stock Exchange (ASX) in relevant sectors – materials, pharmaceuticals, biotechnology and life sciences, telecommunication services, energy, utilities, transportation, technology hardware and equipment, and semiconductors and semiconductor equipment.

We then applied the estimated abnormal negative returns produced by Michaelides et al. (2024) to the mean market capitalisation to determine the impact of trade secret theft on share prices for publicly listed Australian companies (Table 9). We did the same for the top 50 and top 20 ASX listed companies in these sectors. Given Michaelides et al. (2024) showed companies that experienced trade secret theft were larger than average, we estimate that the impact of trade secret theft per incident would be in the range of $429.7 million to $887.2 million.

Decline in share prices following public reporting of cyber attacks

We used a similar approach to estimate the decline in a company's share price due to public reporting of a cyber attack resulting in the loss of personal or financial information. The benefit of this approach is that it allows us to better capture the indirect costs associated with cyber attacks, which are substantially larger than the direct costs (of remediation etc.; Kamiya et al. 2021). While early studies using this approach tended to find only small effects (if any), more recent studies have consistently found large, negative effects on share prices following breach announcements (Vergara Cobos & Cakir 2024). Much like with trade secret theft, the impact on share price is believed to reflect the loss of trust or confidence in a company among consumers and investors.

Trade secret theft from a large, publicly listed Australian company could result in share market losses of up to **$887.2 million** per incident.

Table 9: Estimated abnormal negative returns following disclosures of trade secret theft carried out on behalf of a foreign government ($m)

	All ASX listed companies	Top 50 ASX listed companies	Top 20 ASX listed companies
Mean market capitalisation	$1,103.0	$19,530.2	$40,326.3
Low range, short-term impact (-1.26%)	$13.9	$246.1	$508.1
High range, short-term impact (-1.74%)	$19.2	$339.8	$701.7
Loss after 30 days (-2.20%)	$24.3	$429.7	$887.2

A cyber espionage attack targeting a large, publicly listed Australian company could result in share market losses of up to **$439.6 million** per incident.

Table 10: Estimated abnormal negative returns following announcement of a cyber attack against a company ($m)

	All ASX listed companies	Top 50 ASX listed companies	Top 20 ASX listed companies
Mean market capitalisation	$1,103.0	$19,530.2	$40,326.3
Any data breach (−0.84%)	$9.3	$164.1	$338.7
Cyber attack with personal information loss (−1.09%)	$12.0	$212.9	$439.6
Second incident within 1 year (−5.14%)	$56.7	$1,003.8	$2,072.8

Kamiya et al. (2021) found that external cyber attacks lead to significant shareholder wealth loss. The declines in share prices were larger when there was a loss of personal information, with abnormal negative returns of around −1.09%. The effect increased fivefold for companies that were victim a second time within 12 months. Importantly, they showed (but did not quantify) that the market reaction was worse when it took more time to uncover the breach and in industries with more opportunities for growth. They also revealed that negative effects were contagious to industry peers – other companies in the same industry were also impacted following a cyber attack.

That the size of the effect is similar to that of trade secret theft, reported above, suggests that the implied loss of commercially valuable information is as damaging as the actual loss of trade secrets. It also helps validate applying this method to cyber attacks, given that this research was not limited to state or state-sponsored attacks. Nevertheless, we assume that the results would be similar for cyber attacks involving either state or non-state actors.

As with trade secret theft, we used the mean market capitalisation for all ASX listed companies in relevant sectors and applied the estimated abnormal negative returns produced by Kamiya et al. (2021; Table 10).

We did the same for the top 50 and top 20 ASX listed companies in these sectors. We focus on incidents that resulted in the loss of personal information and estimate that a cyber attack involving the loss of personal information would cost up to $439.6 million per incident. Given that many cases of cyber espionage take a long time to discover and involve persistent access (European Commission & PwC 2018), and the effects on industry peers, we expect the true cost per incident to be higher than our estimate.

Decline in foreign investment

A large body of evidence shows that corruption, terrorism and the failure to properly respond to money laundering risks can impact trust in government such that it reduces foreign investment. Gök (2023) conducted a meta-regression of corruption studies, finding an overall net negative effect. Most of these studies relied on evidence of widespread government corruption (as measured in cross-national metrics) and therefore reflect the effect of long-term corruption rather than specific corruption incidents. However, research has shown that the discovery of the so-called ‘Pandora papers’ was associated with declines in foreign investment in the countries implicated (Zander 2021). Similar effects have been observed for acts of terrorism due to the risks associated with political instability, damage to infrastructure and the overall cost of doing business (Bandyopadhyay, Sandler & Younas 2014; Enders, Sachsida & Sandler 2006).

More recently, research by Kida and Paetzold (2021) found that a developing country being grey-listed (being subject to increased monitoring from the Financial Action Task Force to address deficiencies in its anti-money laundering / counter-terrorism financing regime) has a large, negative effect on foreign direct investment inflows (as a proportion of GDP). The outcomes of this study were used in a recent impact analysis in support of the Australian Government's proposed money laundering reforms (Attorney-General's Department 2024).

Consistent with that impact assessment, we used a more conservative estimate of the effect size, noting that developing economies may not be as resilient as Australia. We used data on foreign direct investment inflows into Australia reported by the ABS (2025), using the average for the last 10 years to account for annual fluctuations. Because research from the US showed that terrorism had a greater impact on foreign investment from the Organisation for Economic Co-operation and Development) (OECD) countries (Enders, Sachsida & Sandler 2006), and because of Australia's close intelligence ties with fellow Five Eyes countries, we used data on foreign investment from all countries, OECD countries and Five Eyes countries.

We used different estimates of the potential effect of espionage on foreign direct investment (FDI) as a percent of GDP to produce low (0.1 percentage point decrease in FDI/GDP), medium (0.25 percentage point decrease) and high estimates (0.5 percentage point decrease; Table 11). In line with advice from subject matter experts, we assumed that the decline in investment from OECD countries is the most likely scenario. Based on this scenario, we estimated that diminishing trust in government security due to espionage activity could result in an annual decrease in FDI of up to $10.3 billion.

Decline in international student revenue

We previously presented evidence of the costs associated with denying admission to international students assessed as being high risk. In the event of major espionage activity impacting an Australian university that involves an international postgraduate student working on behalf of a foreign state, it is plausible that universities would need to tighten controls and lower the risk threshold for accepting students from certain countries.

We modelled the effect of a 5% decrease in international student commencements from 2 high-risk countries. Given the number of students from these countries who study at Australian universities, the long-term growth in numbers and annual fluctuation, this is a plausible change.

Diminishing trust in government security due to espionage activity could result in an annual decrease in foreign direct investment inflows of up to **$10,291.2 million**.

Table 11: Estimated decline in foreign direct investment (FDI) net flows following disclosure of a major incident diminishing trust in government security, by potential change in FDI/GDP

	Five Eyes countries	OECD countries	All countries
Foreign direct investment, 2015–2024			
Average FDI ($m)	$27,438	$45,869	$59,246
Average FDI/GDP (%)	1.32	2.26	2.94
Projected losses ($m)			
Low (0.10pp decrease in FDI/GDP)	$1,203.3	$2,058.2	$2,672.7
Medium (0.25pp decrease in FDI/GDP)	$3,008.3	$5,145.6	$6,681.6
High (0.50pp decrease in FDI/GDP)	$6,016.6	$10,291.2	$13,363.3

We calculated the average annual tuition fee for an international student by dividing the total income from overseas students by the total number of enrolments, and used this to estimate the lost revenue from international student fees that would no longer be available to fund research ($75.6 million). We relied on a report by Deloitte Access Economics (2020) that estimated the economic contribution of international students and their visitors to determine the lost economic contribution per student (in 2024 Australian dollars) over and above tuition fees. We estimated this to be $323.1 million.

Noting that income generated by international students is also used to support university research, we assumed a portion of this income would have been converted to research expenditure. There are various studies on the benefits of research expenditure by universities, including a report by London Economics (2018). That research, which focused on Australia's Group of Eight universities (which account for around 75% of all university research), estimated that for every dollar invested in research there were same-year productivity spillovers of $9.76. We took this as our high estimate. A study by Deloitte Access Economics (2020) was more conservative, suggesting that GDP increased by $5 for every dollar invested in research and development. We took this as our low estimate. The return on investment was estimated to range from $252.0 million, based on the impact on GDP (low estimate), up to $492.0 million, which was based on the impact in terms of productivity spillovers (high estimate).

The lost revenue from a decline in international students – including the loss of student fees ($75.6 million), the lost economic contribution of international students and their visitors ($323.1 million), and the loss of productivity spillovers ($492.0 million) – could be up to $890.7 million annually.

Decrease in US Government funding for Australian research

Recent reports have highlighted the significant investment by the US Government in Australian university research. According to the Australian Academy of Science (Jagadish 2025), in 2024 US Government research funding involving Australian research organisations totalled $386 million. This does not include in-kind contributions or provision of critical research infrastructure.

It is plausible that espionage activity targeting Australian university research funded by the US Government could negatively impact perceptions of the security of research at Australian universities. This could lead to a reduction in US Government funding for Australian universities, particularly as it relates to sensitive topics.

We used the same methodology as before to estimate the financial losses that would be associated with a decline in US Government funding for universities. Assuming there was a 10% decrease in funding, we estimate that the total could be between $193.0 million and $376.7 million.

The potential losses from a decline in international student revenue because of a need to tighten controls following major espionage activity could be up to **$890.7 million** annually.

A 10% decrease in annual US funding for Australian university research following espionage activity could lead to potential same-year economic losses of up to **$376.7 million**.

References

URLs correct as at May 2025

Abalkina A 2024. Prevalence of plagiarism in hijacked journals: A text similarity analysis. *Journal of Accounting Research* 17: 1–19. https://doi.org/10.1080/08989621.2024.2387210

ACIL Allen Consulting 2025. *Economic impact case studies: Establishing the broad economic value of the defence science technology program.* Melbourne: ACIL Allen Consulting. https://www.dst.defence.gov.au/economic-impact-2015

Allied Universal 2023. *World Security Report 2023.* London: Allied Universal. https://www.worldsecurityreport.com/

ASIO—see Australian Security Intelligence Organisation

Attorney-General's Department 2024. *Anti-money laundering and counter-terrorism financing regime (AML-CTF) reforms.* Canberra: Attorney-General's Department. https://oia.pmc.gov.au/published-impact-analyses-and-reports/anti-money-laundering-and-counter-terrorism-financing-regime

AustCyber 2020. *Australia's digital trust report 2020.* Canberra: Department of Industry, Science, Energy and Resources. https://www.austcyber.com/resource/digitaltrustreport2020

Australian Bureau of Statistics (ABS) 2025. *International investment position, Australia: Supplementary Statistics, 2024.* Canberra: ABS. https://www.abs.gov.au/statistics/economy/international-trade/international-investment-position-australia-supplementary-statistics/latest-release

Australian Bureau of Statistics 2024a. *Australian Industry, 2022–23.* Canberra: ABS. https://www.abs.gov.au/statistics/industry/industry-overview/australian-industry/latest-release

Australian Bureau of Statistics 2024b. *Government finance statistics, Australia, June 2024.* ABS. Canberra: ABS. https://www.abs.gov.au/statistics/economy/government/government-finance-statistics-australia/jun-2024

Australian Bureau of Statistics 2024c. *Research and experimental development, government and private non-profit organisations, Australia.* ABS. Canberra: ABS. https://www.abs.gov.au/statistics/industry/technology-and-innovation/research-and-experimental-development-government-and-private-non-profit-organisations-australia/latest-release

Australian Bureau of Statistics 2024d. *Research and experimental development, higher education organisations, Australia.* ABS. Canberra: ABS. https://www.abs.gov.au/statistics/industry/technology-and-innovation/research-and-experimental-development-higher-education-organisations-australia/latest-release

Australian Bureau of Statistics 2023. *Characteristics of Australian Business, 2021–22.* Canberra: ABS. https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2021-22

Australian Crime Commission (ACC) 2015. *The costs of serious and organised crime in Australia 2013–14: Methodological approach.* Canberra: ACC. https://www.acic.gov.au/publications/unclassified-intelligence-reports/costs-serious-and-organised-crime-australia

Australian Government Security Vetting Agency 2024. *Australian Government Security Vetting Agency Annual update 2023–24.* Canberra: Department of Defence. https://www.agsva.gov.au/about/key-performance-indicators

Australian Security Intelligence Organisation (ASIO) 2022. *Annual report 2021–22.* Canberra: ASIO. https://www.asio.gov.au/resources/asio-annual-report-2021-22.

Australian Security Intelligence Organisation (ASIO) 2023. *Secure your success.* Canberra: ASIO. https://www.asio.gov.au/system/files/2023-10/Secure%20Your%20Success.pdf

Australian Security Intelligence Organisation (ASIO) 2024. *Annual report 2023–24.* Canberra: ASIO. https://www.asio.gov.au/resources/asio-annual-report-2023-24

Australian Security Intelligence Organisation (ASIO) 2025. *What is espionage and foreign interference?* https://www.asio.gov.au/about/what-we-do/counter-espionage

Australian Signals Directorate (ASD) 2024. *Annual cyber threat report 2023–2024.* Canberra: ASD. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023–2024

Australian Signals Directorate 2020. *Advanced persistent threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services.* Canberra: ASD. https://www.cyber.gov.au/about-us/alerts/advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services

Avasant 2024. *IT spending and staffing benchmarks 2024/2025.* California: Avasant. https://avasant.com/report/it-spending-and-staffing-benchmarks-2024-2025-chapter-1-executive-summary/

Bandyopadhyay S, Sandler T & Younas J 2014. Foreign direct investment, aid, and terrorism. *Oxford Economic Papers* 66(1): 25–50. http://hdl.handle.net/10.1093/oep/gpt026

Bell R, Bennett E, Boles J, Goodoien D, Irving J, Kuhlman P & White A 2010. *Estimating the economic costs of espionage.* Texas: Texas A&M University. https://oaktrust.library.tamu.edu/items/2b73fa8b-ca99-4f53-bf54-3e5b90b36edf

Bitkom Research 2024. *Corporate Security 2024.* Berlin: Bitkom Research. https://www.bitkom.org/EN/List-and-detailpages/Publications/Economic-Security-2022

Burgess M 2025. *Director-General's annual threat assessment 2025.* Canberra: ASIO. https://www.asio.gov.au/director-generals-annual-threat-assessment-2025

Burgess M 2024. *Director-General's annual threat assessment 2024.* Canberra: ASIO. https://www.asio.gov.au/director-generals-annual-threat-assessment-2024

Carr C & Gorman L 2001. The revictimization of companies by the stock market who report trade secret theft under the Economic Espionage Act. *The Business Lawyer* 57(1): 25–53. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=299436

Commission on the Theft of American Intellectual Property 2017. Update to the IP commission report. Washington, DC: National Bureau of Asian Research. https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/

Commonwealth Fraud Prevention Centre 2023. *Countering the insider threat: A guide for Australian Government.* Canberra: Attorney-General's Department. https://www.ag.gov.au/integrity/publications/countering-insider-threat-guide-australian-government

Critical Infrastructure Centre 2020. *Protecting critical infrastructure and systems of national significance: Consultation paper.* Canberra: Department of Home Affairs. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Curti F, Macchiavelli M, Mihov A, & Pisciotta K. 2023. *Corporate espionage and innovation: Evidence from the theft of trade secrets.* https://doi.org/10.2139/ssrn.4613975

Deloitte Access Economics 2020. *The importance of universities to Australia's prosperity.* https://universitiesaustralia.edu.au/publication/the-importance-of-universities-to-australias-prosperity/

Department of Defence 2025. *Defence and strategic goods list.* Canberra: Department of Defence. https://www.defence.gov.au/business-industry/exporting/export-controls-framework/defence-strategic-goods-list

Department of Education 2024. *Higher education providers finance tables, 2023.* Canberra: Department of Education. https://www.education.gov.au/higher-education-publications/resources/finance-2023-financial-reports-higher-education-providers

Department of Home Affairs 2024a. *Countering foreign interference in Australia.* Canberra: Department of Home Affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

Department of Home Affairs 2024b. *Protective Security Policy Framework Release 2024.* Canberra: Department of Home Affairs. https://www.protectivesecurity.gov.au/pspf-annual-release

Department of Home Affairs 2022. *Regulation impact statement: A risk management program framework for critical infrastructure assets.* Office of Impact Analysis ID: OBPR22–02914. Canberra: Department of Home Affairs. https://oia.pmc.gov.au/sites/default/files/posts/2025/03/2022%20RIS%20-%20RMP%20for%20Critical%20Infrastructure%20Assets.pdf

Department of Home Affairs 2020. *Regulation impact statement: Critical infrastructure systems of national significance.* Office of Best Practice Regulation ID: 25902. Canberra: Department of Home Affairs. https://oia.pmc.gov.au/sites/default/files/posts/2020/12/ci_sons_regulation_impact_statement_-_final_second_pass.pdf

Detica 2011. *The cost of cyber crime.* Surrey, UK: Detica Limited. https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report

Enders W, Sachsida A & Sandler T 2006. *The impact of transnational terrorism on U.S. foreign direct investment.* Political Research Quarterly 59(4): 517–531. https://www.jstor.org/stable/4148055

European Commission 2013. *Study on trade secrets and confidential business information in the internal market.* Brussels: European Commission. https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf

European Commission & PricewaterhouseCoopers 2018. *The scale and impact of industrial espionage and theft of trade secrets through cyber.* Brussels: European Commission. https://data.europa.eu/doi/10.2873/48055

Gök A 2023. Whether corruption sands or greases the wheels of foreign direct investment: A meta-regression analysis. *International Review of Economics* 70(4): 477–501. https://ideas.repec.org/a/spr/inrvec/v70y2023i4d10.1007_s12232-023-00428-5.html

Horton A 2024. *Safeguarding Australia's sensitive academic research.* Canberra: Australian Strategic Policy Institute. https://www.aspistrategist.org.au/safeguarding-australias-sensitive-academic-research/

IANS Research 2022. *2022 Security budget benchmark summary report.* Boston: IANS Research. https://cdn.iansresearch.com/Files/Marketing/IANSResearch-2022SecurityBudgetBenchmarkSummaryReport.pdf

IBM Corporation 2024. *Cost of a data breach report 2024.* New York: IBM Corporation. https://www.ibm.com/reports/data-breach

Intellectual Property (IP) Australia 2024. *Australian intellectual property report 2024.* Canberra: IP Australia. https://www.ipaustralia.gov.au/tools-and-research/professional-resources/data-research-and-reports/publications-and-reports/Australian-Intellectual-Property-Report-2024

Jagadish C 2025. *Statement on US Government intervention in Australia–US research collaboration.* Canberra: Australian Academy of Science. https://www.science.org.au/news-and-events/news-and-media-releases/statement-on-us-government-intervention-in-australia-us-research-collaboration

Kamiya S, Kang J, Kim J, Milidonis A & Stulz R 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139: 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kendell S 2019. Australia's new espionage laws: Another case of hyper-legislation and over-criminalisation. *University of Queensland Law Journal* 38(1): 125–161

Kida M & Paetzold S 2021. *The impact of gray-listing on capital flows: An analysis using machine learning.* International Monetary Fund working paper No. 2021/153. Washington, DC: International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2021/05/27/The-Impact-of-Gray-Listing-on-Capital-Flows-An-Analysis-Using-Machine-Learning-50289

Lee-Makiyama H 2018. *Stealing thunder: Cloud, IoT and 5G will change the strategic paradigm for protecting European commercial interests.* European Centre for International Political Economy Occasional paper No. 2/18. https://ecipe.org/publications/stealing-thunder/

Levite A, Chuanying L, Perkovich G & Yang F 2022. *Managing U.S.-China tensions over public cyber attribution.* Washington, DC: Shanghai Institutes for International Studies. https://carnegieendowment.org/research/2022/03/managing-us-china-tensions-over-public-cyber-attribution

Lifhits J 2024. Sentencing economic espionage in an era of great power competition. *Georgetown Journal of Law and Public Policy* 1. https://www.law.georgetown.edu/public-policy-journal/in-print-2/volume-22-1-winter-2024/sentencing-economic-espionage-in-an-era-of-great-power-competition/

London Economics 2018. *The economic impact of Group of Eight universities.* London: London Economics. https://go8.edu.au/research/economic-impact-group-of-eight-universities

McFadden C, Nadi A & McGee C 2018. *Education or espionage? A Chinese student takes his homework home to China.* NBC News. https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881

Michaelides A, Milidonis A, Ryabinin V & Wiwattanakantang Y 2024. *The value of trade secrets: Evidence from economic espionage.* https://ssrn.com/abstract=4866808

Miller J 2019. *The China problem.* United States Naval Institute proceedings 145/10/1,400. Maryland: United States Naval Institute. https://www.usni.org/magazines/proceedings/2019/october/china-problem

Office of the Australian Information Commissioner 2024. *OAIC takes civil penalty action against Medibank.* Canberra: Office of the Australian Information Commissioner. https://www.oaic.gov.au/news/media-centre/oaic-takes-civil-penalty-action-against-medibank

Ponemon Institute 2022. *2022 Cost of insider threats global report.* Michigan: Ponemon Institute. https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf

PricewaterhouseCoopers (PwC) 2014. *Economic impact of trade secret theft: A framework for companies to safeguard trade secrets and mitigate potential threats.* Delaware: PwC. https://www.innovation-asset.com/hubfs/blog-files/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf

Priyandita G, Hogeveen B & Stevens B 2022. *State-sponsored economic cyber-espionage for commercial purposes: Tackling an invisible but persistent risk to prosperity.* Policy Brief Report No. 67/2022. Canberra: Australian Strategic Policy Institute. https://www.aspi.org.au/report/state-sponsored-economic-cyberespionage/

Segal A, Hoffman S, Hanson F & Uren T 2018. *Hacking for ca$h: Is China still stealing Western IP?* Canberra: Australian Strategic Policy Institute. https://www.aspi.org.au/report/hacking-cash/

Smart P & Gaston T 2019. How prevalent are plagiarized submissions? Global survey of editors. *Learned Publishing* 32(1): 47–56. https://doi.org/10.1002/leap.1218

Smith RG 2024. *Estimating the costs of serious and organised crime in Australia,* 2022–23. Statistical Report no. 50. Canberra: AIC. https://doi.org/10.52922/sr77796

Lewis J, Malekos Smith Z & Lostri E 2020. *The hidden costs of cybercrime.* Washington, DC: Center for Strategic and International Studies. California: McAfee Intel. https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf

Strider Global Intelligence Team 2019. *Quantum dragon: How China is exploiting Western government funding and research institutes to leapfrog in dual-use quantum technologies.* Salt Lake City: Strider Global Intelligence Team. https://www.striderintel.com/resources/quantum-dragon-report/

Taylor C 2024. *Foreign interference is a threat to Australia—including diaspora communities.* Canberra: Australian Strategic Policy Institute. https://www.aspistrategist.org.au/foreign-interference-is-a-threat-to-australia-including-diaspora-communities/

Treasury 2025. *Quarterly report on foreign investment – 1 July 2024 to 30 September 2024.* Canberra: The Treasury. https://foreigninvestment.gov.au/news-and-reports/reports-and-publications/quarterly-report-jul-sep-2024

United Kingdom (UK) Home Office 2024. *Cyber security breaches survey 2024.* London: UK Home Office. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

United States Department of Justice 2021. *Ph.D. Chemist convicted of conspiracy to steal trade secrets, economic espionage, theft of trade secrets and wire fraud.* Washington, DC: United States Department of Justice. https://www.justice.gov/archives/opa/pr/phd-chemist-convicted-conspiracy-steal-trade-secrets-economic-espionage-theft-trade-secrets

United States International Trade Commission (USITC) 2011. *China: Effects of intellectual property infringement and indigenous innovation policies on the U.S. economy.* USITC publication 4226. Washington, DC: USITC. https://www.usitc.gov/publications/332/pub4226.pdf

University Foreign Interference Taskforce 2021. *Guidelines to counter foreign interference in the Australian university sector.* Canberra: Department of Education. https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector

Vergara Cobos E & Cakir S 2024. *A review of the economic costs of cyber incidents.* Washington, DC: World Bank. https://documents.worldbank.org/curated/en/099092324164536687

Verizon 2025. *2025 Data breach investigations report.* https://www.verizon.com/business/en-au/resources/reports/dbir/

Voce I & Morgan A 2023. *Cybercrime in Australia 2023.* Statistical Report no. 43. Canberra: AIC. https://doi.org/10.52922/sr77031

Weichert B 2021. *The curious case of China's quest for 'invisibility cloak'.* Asia Times. https://asiatimes.com/2021/07/the-curious-case-of-chinas-quest-for-invisibility-cloak/

World Intellectual Property Organization 2025. *What is intellectual property?* https://www.wipo.int/en/web/about-ip

Wynn K, Liu M & Cohen J 2021. *Quantifying Australia's returns to innovation.* Canberra: CSIRO. https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/innovation-business-growth/quantifying-australias-returns-to-innovation

Zander T 2021. Does corruption matter for FDI flows in the OECD? A gravity analysis. *International Economics and Economic Policy* 18(2): 347–377. https://ideas.repec.org/a/kap/iecepo/v18y2021i2d10.1007_s10368-021-00496-4.html

Zhang H 2020. *Intellectual property rights, business profitability and competition in the Australian economy.* IP Australia economic research paper 10. Canberra: IP Australia. https://www.ipaustralia.gov.au/tools-and-research/professional-resources/data-research-and-reports/publications-and-reports/business-profitability-and-competition


ASIO
asio.gov.au