ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INSLM review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences

Chris Taylor (Head, Statecraft and Intelligence Policy Centre)

June 2025

20 June 2025

Mr Jake Blight

Independent National Security Legislation Monitor

3-5 National Circuit

BARTON ACT 2600

via INSLM@inslm.gov.au

Dear Mr Blight,

INSLM review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences

Please consider my submission to the Independent National Security Legislation Monitor (INSLM) review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences (hereafter 'the review' and 'the 2018 offences', respectively), as follows.

I thank you for the opportunity to make this submission and for conducting the review, including the production of the detailed Issues Paper.

In line with ASPI's Charter, this submission does not reflect a singular ASPI perspective and is the opinion of the author alone. Nor does this submission represent the views of the Australian government or any government agency.[1]

ASPI is Australia's preeminent national security and strategic policy thinktank. ASPI's Statecraft & Intelligence Policy Centre is unique, as the only research institution in Australia focused on intelligence issues, including the conduct of espionage and counter-espionage.[2]

Given ASPI's expertise in strategic policy and national security, this submission focuses on the broader context in which the 2018 espionage-related offences were introduced. Specifically, it addresses the evolving threat environment, the adaptation of foreign intelligence services, shifts in the conception of national security, and the strategic rationale underpinning the introduction of the offences. It is not intended to provide legal analysis in the professional or academic sense, but rather a security policy perspective grounded in operational reality.

It is my belief that the Australian Parliament enacted the 2018 offences to address long-standing gaps in the previous legislative framework, gaps that had become increasingly untenable given the scale and complexity of hostile foreign activity being directed at Australia. These reforms were not only timely but necessary, enacted against a backdrop of deteriorating global stability and a marked increase in espionage and foreign interference activities targeting Australian interests.

In my considered view, the introduction of these offences marked a significant and positive step forward in both protecting Australia's national security and reinforcing the resilience of our democratic institutions. While some critics warned that the laws could have unintended consequences for civil liberties, those concerns have not materialised. To date, the application of these laws has been proportionate, targeted, and aligned with the intent of Parliament.

Accordingly, I submit that the 2018 offences continue to play a vital role in defending Australia and Australians from the covert, coercive, and deceptive actions of foreign powers. They should be retained in their current form, with minimal revision.

---

[1] Noting I am employed by ASPI while on long-term leave from the Australian Government, see https://www.aspi.org.au/bio/chris-taylor/

[2] For information on the Statecraft & Intelligence Centre please see https://www.aspi.org.au/programs/statecraft-and-intelligence-program/

The Threat Environment

Since the late 2010s, governments of both persuasions have recognised the magnitude of the extraordinary national security challenge facing Australia as a result of a decline in relative national power, Chinese ascendancy and an ongoing breakdown in the international rules-based order. In 2020, then Prime Minister Scott Morrison said Australia was facing 'one of the most challenging times we have known since the 1930s and the early 1940s'.[3] His successor, Prime Minister Anthony Albanese, reinforced this by describing 'a time of profound geopolitical uncertainty'.[4] According to a media statement from current Defence Minister Richard Marles, 'Australia faces the most complex and challenging strategic environment since the Second World War.'[5] Foreign Minister Penny Wong has said it's 'nothing less than a contest over the way our region and our world work'.[6]

This contest challenges the very heart of our liberal democracy and its future. As ASPI's Executive Director Justin Bassi noted in his introduction to the recently published volume *Agenda for Change: Preparedness and Resilience in an Uncertain World*,

> 'When we talk about the challenges of sharpening strategic competition, we need to be asking ourselves: 'For what are we competing?' The answer is that we're competing to shape the international system that, whether we like it or not, determines our national security, and ensure that it reflects our values and principles such as openness, sovereignty, respect for human rights, and economic competition on a level playing field based on agreed rules that are enforced.'[7]

As the strategic environment continues to deteriorate, and the prospect of major power war in our region becomes ever more possible, the threat posed to Australian interests by hostile foreign statecraft tools such as espionage and sabotage becomes more acute. What was already intolerable in more benign circumstances, such as in the 1990s, is now existential.

It is fortunate then, and prescient, that the Australian Parliament passed the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018, establishing the offences that are now the subject of this review. Not least given the inadequacy of the preceding laws in relation to espionage and sabotage, and the absence of criminal laws in relation to foreign interference and theft of trade secrets.

Since 2018 the level of foreign intelligence activity directed at Australia has increased in intensity and volume, as attested to by the Director-General of Security in his Annual Threat Assessments –most notably in February this year.[8] This has included espionage (noting an ongoing prosecution in this regard, of Kira and Igor Korolev) and foreign interference (including the prosecution of Alexander Csergo and the conviction of Di Sanh Duong). With regard to foreign interference, the experience in Australia - attested to publicly by both the current Minister for Home Affairs and their predecessor - has been similarly reflected in recent Canadian experiences.

Of particular note has been the resurgence of sabotage internationally, within a broader push by competing states to employ hybrid threats (harmful tactics calibrated below the level of war) against each other. In fact, as I wrote last year,

> 'Sabotage—destroying, damaging or obstructing for military and/or political advantage—is back. [In a matter of weeks in 2024] we saw Hezbollah's pagers and radios surreptitiously changed into anti-personnel explosive devices and detonated across Lebanon and Syria. Russia-linked fires plague

---

[3] Hon Scott Morrison, 'Address – Launch of the 2020 Defence Strategic Update', 1 July 2020, as at https://pmtranscripts.pmc.gov.au/release/transcript-42881

[4] Hon Anthony Albanese MP, 'Address to the National Press Club', 22 February 2023, as at https://www.pm.gov.au/media/address-national-press-club

[5] Hon Richard Marles MP, '2024 National Defence Strategy', 17 April 2024, as at https://www.minister.defence.gov.au/media-releases/2024-04-17/2024-national-defence-strategy

[6] Senator the Hon Penny Wong, 'National Press Club Address: Australian interests in a regional balance of power', 17 April 2023, as at https://www.foreignminister.gov.au/minister/penny-wong/speech/national-press-club-address-australian-interests-regional-balance-power

[7] Raelene Lockhorst & Chris Taylor (eds.), *Agenda for Change: Preparedness and Resilience in an Uncertain World*, ASPI, 2025, p.4, as at https://www.aspi.org.au/report/agenda-for-change-2025-preparedness-and-resilience-in-an-uncertain-world/

[8] Michael Burgess, 'Director-General's Annual Threat Assessment 2025', ASIO, 19 February 2025, as at https://www.asio.gov.au/director-generals-annual-threat-assessment-2025

> European and American factories supporting Ukraine's defence. Ukrainian nationals implicated in the Nord Stream 2 pipeline bombing. Concerns raised about Chinese components in systems internationally, at moments of future crisis. Alarm on the Olympics' opening day, as arsonists [struck] France's high-speed railway network.'[9]

There is nothing particularly unique about Australia that will spare us from this wave. Nor from the enabling phenomenon of state actors contracting criminal proxies to undertake quasi-intelligence activities, including the carrying out of sabotage as a service (an extension of 'crime as a service – a theme in Europol's recent report *The changing DNA of serious and organised crime*).[10] And the subject of an ongoing case in the British courts where six men are on trial for allegedly carrying out the arson of a warehouse in London housing aid to Ukraine at the behest of the Russian intelligence-linked Wagner Group mercenary company.[11]

As the same Europol report observed, the hybrid threats in question (including as enabled by criminal proxies) have an accumulating effect on democratic national interests:

> 'Much like a woodpecker weakens a tree over time through repeated strikes, hybrid threat actors engage in ongoing, seemingly minor actions that collectively erode stability, security, and trust in institutions.'[12]

The Evolution and Adaptation of Foreign Intelligence Methodologies

A hallmark of the offences and their legislative form – most notably the breadth of definition of 'foreign principal' (to include variously by offence: 'foreign principal', 'foreign government principal' and 'foreign intelligence agency') - is the ability to effectively address a wide range of vectors and methodologies of hostile foreign intelligence activity. This is important given the continual evolution evident in foreign intelligence methodologies.

Of particular note for Australia is the adaptation and evolution of Chinese foreign intelligence practices over the past fifteen years. This has included moving to recruit non-ethnically Chinese agents (a significant departure from past practice), as well as targeting serving and former national security officials (notably in the US). This means that China is now operating more akin to a 'foreign directed' intelligence model, marking a significant shift away from an historic Chinese intelligence model that prevailed until approximately 2011.[13] Australia's counter-espionage laws need to be equally adaptable and comprehensive in response.

Elsewhere a particularly good pen portrait of contemporary Russian espionage practices, and the use of non-official cover 'illegals' (and the importance of Brazil as an enabling environment), was recently published by the *New York Times*. Of note is the use of non-descript business cover (e.g. modelling, jewellers, 3D printing companies) for intelligence operations, disassociated from the Russian government.[14] A similar attempt to separate intelligence operations from the Russian government, in this instance by using Bulgarian nationals as proxies, was uncovered by British security authorities and successfully prosecuted last month.[15]

---

[9] See Chris Taylor, "You'll shut me down with a push of your button': 21st century sabotage', *The Strategist*, 24 September 2024, as at https://www.aspistrategist.org.au/youll-shut-me-down-with-a-push-of-your-button-21st-century-sabotage/

[10] *The changing DNA of serious and organised crime: European Union Serious and Organised Crime Threat Assessment*, European Union Agency for Law Enforcement (Europol), 2025, as at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf. See also Lisa O'Carroll, 'Russia using criminal networks to drive increase in sabotage acts, says Europol', *The Guardian*, 19 March 2025, as at https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol

[11] Michael Holden, 'Six go on trial over London arson attack blamed on Russian Wagner group', Reuters, 5 June 2025, as at https://www.reuters.com/business/media-telecom/six-go-trial-over-london-arson-attack-blamed-russias-wagner-group-2025-06-04/

[12] *The changing DNA of serious and organised crime: European Union Serious and Organised Crime Threat Assessment*, European Union Agency for Law Enforcement (Europol), 2025, p.15, as at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[13] See Jimmy Zhang, 'From China with love?: Analyzing the PRC's shift to a 'foreign-directed' intelligence collection model' in *American Intelligence Journal* 37(1), 2020, pp.11-24. Also, Nicholas Eftimiades, *China's Espionage Recruitment Motivations: Getting rid of MICE*, European Intelligence Academy Research Paper Series #5, December 2023

[14] Michael Schwirtz & Jane Bradley, 'The Spy Factory', *New York Times*, 21 May 2025, as at https://www.nytimes.com/2025/05/21/world/americas/russia-brazil-spies-deep-cover.html

[15] Ruth Comerford & Chris Bell, 'Six Bulgarians jailed for spying for Russia', BBC, 13 May 2025, as at https://www.bbc.com/news/articles/cq69l0e2vjno

Foreign intelligence services are also seeking to recruit new types of agents, including minors and other hitherto unlikely sources, often in response to counter-intelligence measures adopted in the West (including expulsions of suspected intelligence officers working under diplomatic cover[16]). For example, last year a Canadian minor was arrested in Poland after having been recruited by Russian intelligence to undertake operational activities in Europe on their behalf. The minor was drawn into this covert service after volunteering to serve with pro-Russian forces in the Ukraine War. Also importantly, the minor had no direct access to national security classified material of their own.[17]

These developments are particularly important in appreciating the capacity of foreign intelligence services to adapt to counter-intelligence measures – and to identified gaps in legal frameworks. These accounts also underscore the reality and pervasiveness of espionage internationally now.

Developments are not limited to the foreign intelligence services themselves. Self-motivated wannabe espionage agents, seeking out foreign services (rather than vice versa), remain a worrying phenomenon. This was after all a characteristic of the seminal Australian cases of Jean-Philippe Wispealaare and Simon Lappas. Indeed, just a month ago a US intelligence agency employee (ironically an insider threat analyst at the Defense Intelligence Agency) was arrested after trying to offer their services, and classified material, to German intelligence.[18]

Likewise, the phenomenon of espionage by recklessness remains a real security problem. For example, in the cases of Benjamin Bishop[19] and Kevin Mallory[20] in the US, where the individuals' espionage advantaging China began after they recklessly shared classified material with persons they did not know were agents of Chinese intelligence (believing them to be a student/girlfriend and a thinktank respectively).

Spectrum of Defence against Espionage, Foreign Interference, Sabotage and Theft of Trade Secrets

It is important to contextualise the offences within the broad spectrum of Australian defence against foreign intelligence activities. As the Issues Paper acknowledges, 'prosecutions are not the only responses to the threat'. This deserves further emphasis in the review's considerations, for there is a tendency to equate a 'lack' of prosecutions for espionage and foreign interference offences (and indeed no prosecutions as yet for sabotage or theft of trade secrets) as somehow indicative of redundancy. In this view the limited application of the offences to date somehow suggests the offences are unnecessary. Nothing could be further from the truth.

Rather the approach undertaken to date would seem to align Australia's broader response with the principle of the 'least restrictive means to protect the interest' per the United Nations Special Rapporteur.[21]

This spectrum of responses – including counter-intelligence disruption, public attribution, expulsions of diplomatic personnel, demarches, administrative security reviews – is anchored by the offences. The spectrum serves not only to ensure the administration of justice in the most egregious of cases, but to deter foreign principals from operating in and/or against Australia and Australians from collaborating in such activities.[22] It is illustrative, for example that the offences (and their maximum penalties) feature prominently in the public

---

[16] See for example, Thomas Escritt & Sarah Marsh, 'Russia buying spies to make up for expelled diplomats, German agency says', Reuters, 19 June 2024, as at https://www.reuters.com/world/europe/russia-buying-spies-make-up-expelled-diplomats-german-agency-says-2024-06-18/

[17] Mari Saito et al, 'Russia recruited a teenage spy. His arrest led to a crypto money trail.', Reuters, 12 June 2025, as at https://www.reuters.com/investigates/special-report/europe-espionage-teen-spy/

[18] US government employee arrested for attempting to provide classified information to foreign government', US Department of Justice, 29 May 2025, as at https://www.justice.gov/opa/pr/us-government-employee-arrested-attempting-provide-classified-information-foreign-government; see also John Schindler, 'Did a DIA spy sell out America because he hates Trump?', *Washington Examiner*, 6 June 2025, as at https://www.washingtonexaminer.com/restoring-america/patriotism-unity/3433005/nathan-laatsch-germany-dia-trump/

[19] 'Benjamin Pierce Bishop case-study: unauthorized retention and communication of classified material', Center for Development of Security Excellence, as at https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-bishop.pdf

[20] 'Kevin Patrick Mallory case-study: espionage', Center for Development of Security Excellence, as at https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-mallory.pdf

[21] Issues paper, p.20

[22] Similar to the deterrence effect of other national security laws, such as the Counter Terrorism Legislation Amendment (Declared Areas) Act 2024. Note the advice to this effect of the Attorney General's Department to the Parliamentary Joint Committee on Intelligence & Security inquiry into that declared areas legislation.

messaging of the Australian Government to deter, and inform and reassure Australians - as in the *Countering Foreign Interference in Australia* public document released in January 2025.[23]

The offences also serve as a contingency for future circumstances, where for example there is a significant increase in activities directed against Australia or the occasion of a rare but consequential action undertaken against Australia. In this way the spectrum – and the offences – anticipate potential future circumstances appropriately. The resurgence in global instances of sabotage described above is illustrative. If this had not been effectively anticipated in the reform of sabotage offences in 2018 the Australian Parliament would now be scrambling to respond. Worse still if it was having to respond in the wake of an incident in Australia. It is not unfair to observe that where national security law making has been hyper-reactive over the past quarter century it has ultimately been less effective than where responses have been proactive and anticipatory.

As to a more general observation on some of the criticisms of the offences at the time and subsequently (including in works and submissions cited in the Issues Paper), I would simply note that there is no apparent evidence that 'the laws have had unintended consequences including on academic collaboration and press freedom'. In this regard, as a current security clearance holder, former senior national security official, and prolific public commentator on intelligence and national security I would be happy to provide some personal reflections privately to the review.

What is 'National Security'?

Chapter three of the Issues Paper raises the question: 'is the definition of 'national security' sufficiently clear as an element of serious criminal offences? If not, why and what refinements should be made?' Amidst the arguments surfaced in that chapter it is important to consider what 'national security' means for Australia in 2025.

It would be difficult to argue that 'national security' in that context is intended to, or should, have a reductive and/or limited definition. The concept of national security is almost universally used to mean more than a limited application to the threat of military action or coercion or the workings of the intelligence community alone – as has sometimes been insinuated.

Nor is this a recent phenomenon. The last official national security strategy produced by the Australian Government, almost fifteen years ago, defined 'national security' as:

> '[A] broad and evolving concept. It is concerned with how we shape the environment, and how we prevent and prepare for threats to our sovereignty, people, assets, infrastructure and institutions. National security is also concerned with how we respond to such threats, and recover from any event which may occur. In fulfilling its national security responsibilities, Australia draws primarily on its defence, intelligence, diplomatic, development, law enforcement and border security capabilities. [...]
>
> Importantly, national security is not just about countering threats; it is also about making the most of opportunities. In particular, Australia seeks to shape the international environment, both to prevent the emergence of security threats, and to achieve broader benefits for Australia (such as trade and economic benefits).'[24]

Furthermore, Australia's 'national security objectives' were described as:

- 'To ensure a safe and resilient population: the safety of the population as a whole.
- To protect and strengthen our sovereignty: the independence of our decision-making, and authority over our territory and resources.
- To secure our assets, infrastructure and institutions: including physical facilities, supply chains, intellectual property, information technologies, communication networks and Australia's natural wealth.

[23] *Countering Foreign Interference in Australia: Working towards a more secure Australia*, Department of Home Affairs, 2024
[24] *Strong and Secure: a Strategy for Australia's National Security*, Department of the Prime Minister & Cabinet, 2013, p.5

- To promote a favourable international environment: to influence and shape our regional and global environment to be conducive to advancing Australia's interests and values.'[25]

The reference in the 2013 National Security Strategy to 'trade and economic benefits' is particularly apt as the economic dimension to national security has been an apparent target of some concerned commentary, as noted in the INSLM Issues Paper.[26]

ASPI has published a significant range of analysis supporting the criticality of economic security to the conception of Australian national security in the current strategic environment.[27] This view has also been supported by recent independent reviews. For example, the 2024 Independent Intelligence review conducted by Dr Heather Smith PSM and Mr Richard Maude assessed that:

> 'Of all the changes [since 2017], three stand out as the most profound for intelligence and statecraft. One is a much more contested global order defined by tense competition between nation-states, and especially between the United States and China. A second is technological shifts. The third is a new era of global economic fragmentation, economic nationalism, coercion and protectionism, derisking, and industrial strategy.' [my emphasis]

In fact, the Independent Intelligence Review was particularly strong in its argument that economic security is an increasingly important requirement for Australian intelligence, complementing 'national security'. The Review noted that:

> 'Economic security can be defined in various ways. We are concerned… with a broad area of policy making that considers how, in an era of geopolitical rivalry, Australia can best balance the opportunities and risks that arise from economic interdependency.'[28]

This included specific recommendations (#13-15) by the review that:

- Treasury lead a 'broad review of the structure and effectiveness of economic security functions' across the Australian government;
- A 'distinct economic security function be established in the Treasury' including secondees from the National Intelligence Community; and,
- The 'capacity of the Office of National Intelligence to support economic security decision making be strengthened'.[29]

This is not an argument for so diffuse an 'all hazards' approach to 'national security that the concept loses meaning or clarity. But it is clear that now is not the time to re-read into the legislative framework defending Australia's national security a misplaced and unrealistic limitation upon that national security that does not accord with either the intentions of the Australian Government, the Australian Parliament nor the actualities of our national circumstances now and into the foreseeable future.

Theft of Trade Secrets

---

[25] *Strong and Secure: a Strategy for Australia's National Security*, Department of the Prime Minister & Cabinet, 2013, p.4

[26] For example at pp.30-31.

[27] A brief selection includes: Marc Ablong, 'The gathering storm: urgent geoeconomic threats and Australia's national security crisis', *The Strategist*, 31 May 2025, as at https://www.aspistrategist.org.au/the-gathering-storm-urgent-geoeconomic-threats-and-australias-national-security-crisis/; James Corera, 'Economic security and geostrategic competition: fostering resilience and innovation', *The Strategist*, 26 March 2025, as at https://www.aspistrategist.org.au/economic-security-and-geostrategic-competition-fostering-resilience-and-innovation/; David Uren, *The trade routes vital to Australia's economic security*, ASPI Special Report, March 2024, as at https://www.aspi.org.au/report/trade-routes-vital-australias-economic-security/; Ulas Yildirim, 'National security and economic prosperity are two sides of the same coin', *The Strategist*, 11 November 2022, as at https://www.aspistrategist.org.au/national-security-and-economic-prosperity-are-two-sides-of-the-same-coin/.

[28] *2024 Independent Intelligence Review*, Department of the Prime Minister & Cabinet, Australian Government, p.61

[29] *2024 Independent Intelligence Review*, Department of the Prime Minister & Cabinet, Australian Government, p.11

In addition to addressing the question raised in the Issues Paper about the definition of 'national security' the above also illustrates why trade secrets are the targets of foreign intelligence services seeking to advantage their own countries and disadvantage others (including Australia).

For example, ASPI's world-renowned Cyber, Technology & Security program has published a significant body of analysis identifying that the threat of state-sponsored economic cyberespionage is now more significant than ever, with countries industrialising their cyberespionage efforts to target commercial firms and universities at a grander scale.[30] At a less macro-scale this is also apparent in the Linwei Ding case in the US, where Ding remains under indictment for seven counts of economic espionage and seven counts of theft of trade secrets after planning to steal sensitive commercial information on artificial intelligence from his employer Google, on behalf of China.[31]

This is not simply an Australian concern, nor one shared only by Australia's more traditional defence partners. Regional partners like the Republic of Korea, who are the target of concerted espionage efforts by China (amongst others), have also sought to protect sensitive commercial information that is not national security-classified but is of vital national interest.

Case Study: South Korea's Legislative Response to Theft of Trade Secrets in the Tech Sector

South Korea has experienced a notable increase in the theft of trade secrets in recent years, especially with respect to technologies relevant to its national interests and/or by foreign principals. Despite the passage of legislative amendments to respond to this growing threat to technological competitiveness and national security, the effectiveness of legislation such as the *Unfair Competition Prevention and Trade Secrets Protect Act* and the *Act on Prevention of Divulgence and Protection of Industrial Technology* respectively have been called into question.

Between 2019 and 2024, South Korea recorded 97 attempted leaks of business secrets to foreign entities. Of those, 40 cases occurred within the country's semiconductor industry, [32] an industry that constituted 17.17% of the share of the global semiconductor market in 2022.[33] Aside from the importance of safeguarding semiconductor technologies for South Korea's economic prosperity, the theft of semiconductor-related technologies has national security implications. Since semiconductors are used as an input in civilian and dual-use technologies including 6G communications, artificial intelligence and drones, countries who steal trade secrets in this area able to consolidate the develop of their own respective capabilities for both domestic and export purposes. Furthermore, by increasing their share of the global market for technologies such as semiconductors, countries like China have been able to increasingly block and restrict access to global supply chains as a tool of statecraft within the context of growing strategic competition with the US in the Indo-Pacific region.

One notable example of trade theft in South Korea occurred in June 2023 with the indictment of a former Samsung Electronics executive. The executive was found guilty of leaking confidential semiconductor data with the intent of establishing a copycat chip factory in China through this intellectual property. In September 2024, the same individual faced new allegations concerning the theft of Samsung's proprietary information related to 20-nanometre DRAM chip processing technology.[34]

---

[30] See Gatra Priyandita & Bart Hogeveen, *State sponsored economic cyber-espionage for commercial purposes: Governmental practices in protecting IP-intensive industries*, ASPI Policy Brief, February 2025, as at https://www.aspi.org.au/report/state-sponsored-economic-cyber-espionage-commercial-purposes-governmental-practices/; and Gatra Priyandita & Bart Hogeveen, *State sponsored cyber-espionage for commercial purposes: tackling an invisible but persistent threat to prosperity*, ASPI Policy Brief, December 2022, as at https://www.aspi.org.au/report/state-sponsored-economic-cyberespionage/

[31] 'Superseding indictment charges Chinese national in relation to alleged plan to steal proprietary AI technology', US Department of Justice, 4 February 2025, as at https://www.justice.gov/opa/pr/superseding-indictment-charges-chinese-national-relation-alleged-plan-steal-proprietary-ai; see also Ryan Lucas, 'Chinese national arrested and charged with stealing AI trade secrets from Google', NPR, 6 March 2024, as at https://www.npr.org/2024/03/06/1236380984/china-google-fbi-ai

[32] Semiconductor factsheet, Invest Korea, as at https://www.investkorea.org/ik-en/cntnts/i-312/web.do

[33] 'South Korea vows to prevent technology leaks with heavier penalties', Reuters, 17 October 2024, as at https://www.reuters.com/markets/asia/south-korea-vows-prevent-technology-leaks-with-heavier-penalties-2024-10-17/

[34] Ju-min Park, 'South Korean chip executive detained again over alleged technology leak to China', Reuters, 6 September 2024, as at https://www.reuters.com/technology/south-korean-chip-executive-detained-again-over-alleged-technology-leak-china-2024-09-06/

The South Korean government has responded to the theft of trade secrets, especially in response to the growing frequency of economic espionage incidents from China, through a range of legislative amendments. The *Unfair Competition Prevention and Trade Secret Protection Act* was first enacted in 1961 and has undergone a series of amendments, most recently in 2023, to address evolving business practices and to enhance the protection of intellectual property rights.[35] However, this piece of legislation is broadly focused on safeguarding business interests and fair market practices in South Korea, rather than specifically focusing on the national security imperative for preventing the theft of trade secrets.

In contrast, South Korea's *Act on the Prevention of Divulgence and Protection of Industrial Technology* is a more analogous example that can be compared with the trade secrets provisions under Division 92A of Australia's *Criminal Code Act*. South Korea's legislation specifically targets the leakage of industrial technology and has undergone multiple amendments including in January 2023 and December 2024. The latter revision in December 2024 strengthened punitive measures in response to the growing number of Korean citizens engaging in economic espionage on behalf of Chinese and other foreign firms. The amendments involved increasing penalties for leaking industrial technology overseas, with a higher penalty of 6.5 billion won (approximately 7.3 million AUD) applicable for cases involving technologies critical to South Korea's national interests. [36] In addition, the December 2024 revision notably relaxed evidentiary thresholds in establishing the misappropriation of technologies.

Despite recent legislative amendments to safeguard trade secrets in South Korean industry, these measures continue to face criticism. One key concern is that enforcement efforts fail to address the role of foreign governments that orchestrate theft operations by disproportionately targeting the individuals directly involved in espionage activities. Therefore, the theft of trade secrets needs to be framed as a geopolitical rather than exclusively criminal issue. Going forward, South Korea can better respond to theft of trade secrets by foreign countries, especially in the technological sector, by increasing scrutiny over international talent recruitment programs, as well as joint ventures between companies, universities and research institutions that facilitate technology transfers. [37]

Also reinforcing the threat posed to national interests by foreign intelligence efforts directed at commercial information is the recent analysis published by security firm DTEX on the sophisticated campaign by North Korean authorities to use covert operatives masquerading as remote IT workers to infiltrate foreign businesses (including in Australia) for both immediate commercial and long-term strategic ends. An effort sometimes supported by both witting and unwitting persons in the target countries.[38]

This is the reality of the security environment in 2025 with which the offences must grapple.

Opportunities for improvement

Laws are the work of women and men. It would be unreasonable to expect that those laws are perfect and unimprovable. The case made above is not intended to preclude the benefits which might derive from prudent revisions that otherwise preserve the intention of the Parliament seven years ago to strengthen and broaden the protection of Australia from the activities of foreign intelligence services.

For example, the Issues Paper itself identifies a number of such opportunities for prudent, limited revision, such as:

- Inclusion of local government in the protection of 'political or governmental process of the Commonwealth, state or territory' from foreign interference; and,

[35] South Korea's *Unfair Competition Prevention and Trade Secret Protection Act* can be found online at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62546&lang=ENG

[36] Ko Dong-hwan, 'Korea to toughen penalties for technology theft', *The Korea Times*, 6 February 2024, as at https://www.koreatimes.co.kr/business/tech-science/20240206/korea-to-toughen-penalties-for-technology-theft

[37] Ben Forney, 'Changing South Korea's espionage law is good for business', *The Peninsula*, 24 September 2024, as at https://keia.org/the-peninsula/changing-south-koreas-espionage-law-is-good-for-business/

[38] See Michael Barnhardt, *Exposing DPRK's Cyber Syndicate and Hidden IT Workforce*, DTEX, 2025, as at https://www.dtexsystems.com/exposing-dprk/

- Consideration of including foreign political processes in those same protections where foreign interference is directed at persons inside Australia.

Conclusion

The passage of the 2018 offences by the Australian Parliament was an important and positive development in preparing Australia for the stormy strategic waters in which we now find ourselves. The laws also recognised the particular threat posed to core national interests from the efforts of foreign intelligence services targeting Australia and Australians.

As the Minister for Home Affairs noted in January this year:

> 'Foreign interference and espionage threaten our most valuable national assets – our social cohesion, our trusted democracy, our security and prosperity and our freedom of thought and expression.'[39]

Now is not the time to water down the laws that underpin our defences against espionage, sabotage, interference and theft of Australia's trade secrets.

I would be happy to discuss this submission with you, including at a forthcoming hearing.

Chris Taylor, Statecraft & Intelligence Policy Centre head

[39] Hon Tony Burke MP, 'First ever analysis of Foreign Interference and Espionage Threats', media release, 14 January 2025