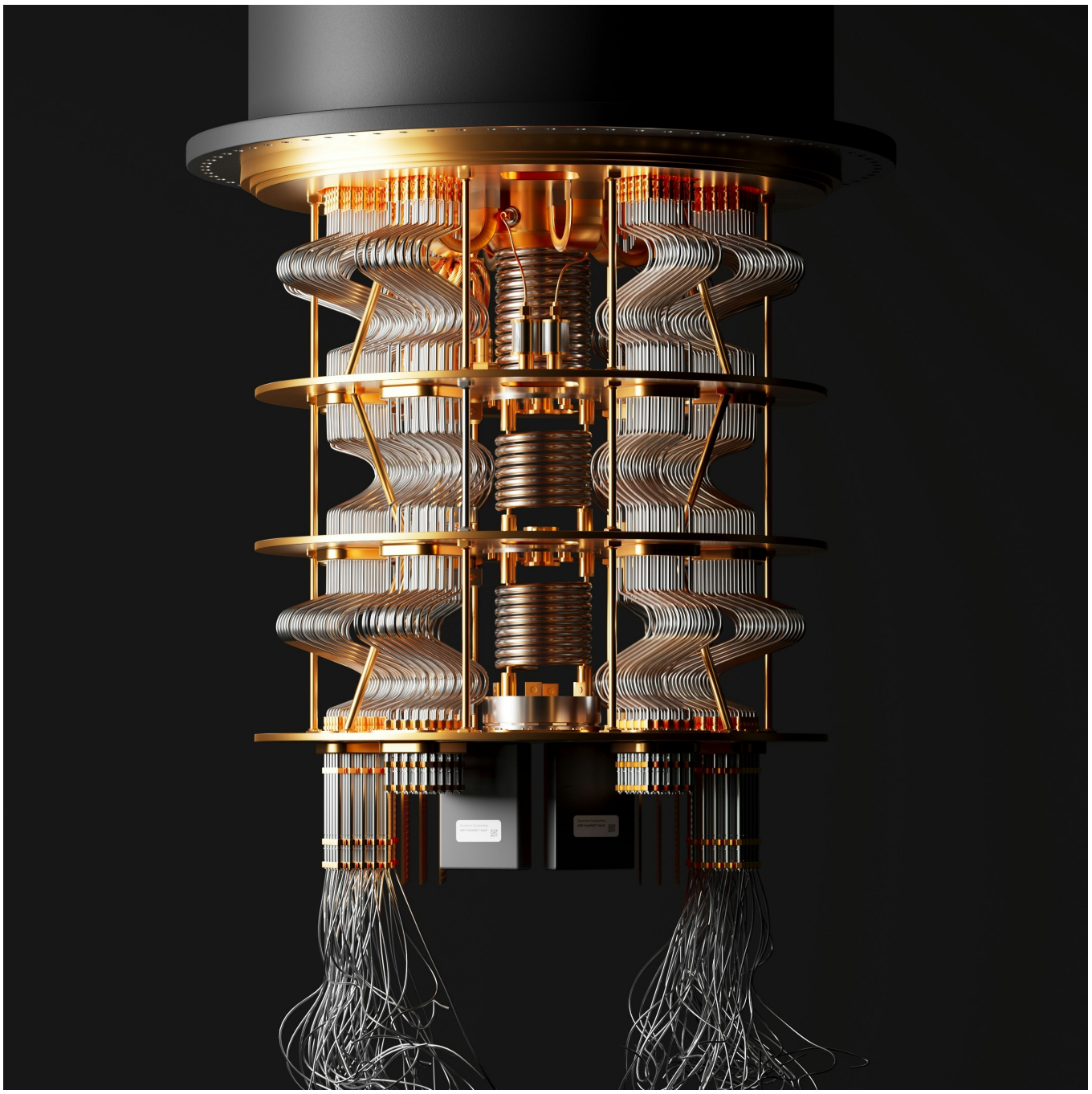

Harvest Now, Decrypt Later: Securing Sea Lines of Communication in the Era of Quantum-Enabled Espionage

By Divij Bhaw

February 2026

UWA DEFENCE & SECURITY | THE UNIVERSITY OF WESTERN AUSTRALIA

Table of Contents

List of Acronyms....3
Executive Summary....4
Introduction....5
Australia's Growing Dependence on Submarine Cable Infrastructure....5
The Impact of Disruptions on Concentrated Data Flows....7
Compromised Cable Landing Stations: Routing and Zero-Day Exploits....8
Harvest-Now, Decrypt-Later: Quantum Decryption Threat....10
Caught Flat-Footed, Accelerated Q-Day Timeline....12
Closing Regulatory Gaps to Mitigate HNDL Exposure....13
Policy Recommendations....14
Conclusion....15
About the Author....15

List of Acronyms

Acronym	Full Term
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
AWS	Amazon Web Services
BGP	Border Gateway Protocol
CIRMP	Critical Infrastructure Risk Management Program
CLS	Cable Landing Station
CRQC	Cryptographically Relevant Quantum Computer
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CVE	Common Vulnerabilities and Exposures
DISP	Defence Industry Security Program
DWDM	Dense Wavelength Division Multiplexing
FIPS	U.S. Federal Information Processing Standards
GDP	Gross Domestic Product
GVA	Gross Value Added
HNDL	Harvest-Now, Decrypt-Later
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
ISM	Information Security Manual
ISO	International Organization for Standardization
MITM	Machine-in-the-Middle
ML-DSA	Module-Lattice Digital Signature Algorithm
ML-KEM	Module-Lattice Key Encapsulation Mechanism
MSS	Ministry of State Security (PRC)
NIST	National Institute of Standards and Technology
OTN	Optical Transport Network
PQC	Post-Quantum Cryptography
PRC	People’s Republic of China
PSPF	Protective Security Policy Framework
Q-Day	Point at which quantum computers can break public-key cryptography
RNMS	Remote Network Management System
ROADM	Reconfigurable Optical Add-Drop Multiplexer
RSA	Rivest–Shamir–Adleman
RITS	Reserve Bank Information and Transfer System
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SLTE	Submarine Line Terminal Equipment
SOCI	Security of Critical Infrastructure (Act)

Executive Summary

Australia’s economic resilience and national security depend on the continuous operation of undersea cable infrastructure. Given that 90% of the nation’s undersea cable landing sites are concentrated in just two metropolitan areas, these systemic chokepoints have created vulnerabilities that could be exploited well before the onset of an open conflict. These risks are no longer theoretical. The Australian Security Intelligence Organisation has warned that the country is facing unprecedented levels of espionage and is nearing the threshold of high-impact sabotage. Disruption to these critical infrastructure would trigger cascading, economy-wide consequences and undermine Defence's operational capability. People’s Republic of China-backed Advanced Persistent Threats (APTs) are actively seeking to pre-position cybersecurity vulnerabilities within the nation’s backhaul networks ahead of an anticipated crisis. Advancements in cryptographically relevant quantum computers (CRQCs) exacerbate this threat by undermining the encryption mechanisms that secure data transmitted over submarine cable networks. Harvest-now, decrypt-later” attacks mean that encrypted data intercepted today may be exposed as early as 2028. Zero-day exploits and rerouting-based cyberattacks enable adversaries to scale their espionage operations, with APTs already amassing large volumes of sensitive data in anticipation of emerging decryption capabilities. Delaying the transition to Post-Quantum Cryptography (PQC) directly undermines Australia’s national security posture by exposing critical assets and classified information to heightened quantum-enabled threats. Without stronger regulatory mandates and accelerated PQC migration timelines, Australia risks being caught flat-footed.

Introduction

Australia's reliance on submarine cable infrastructure underpins its economic prosperity but also represents a growing strategic vulnerability. Carrying approximately 99% of the nation's internet traffic,[1] these cable systems have grown in strategic importance as emerging quantum-enabled decryption capabilities have increased the value of data transiting undersea networks. Amid intensifying strategic competition and rapid technological change, Australia's reliance on digital connectivity has made its maritime data arteries central to national security. Since 2021, intensified grey-zone activity targeting seabed infrastructure in the Indo-Pacific has raised regional concern.[2] However, Australia has yet to fully address the security challenges involved in protecting these vital networks.[3] State-sponsored cyber-espionage campaigns targeting its backhaul networks have heightened the risk of disruption, leaving governments, Australian businesses, and Defence particularly vulnerable. This analysis examines the strategic risks created by state-sponsored cyber actors targeting Australia's undersea cable infrastructure, while highlighting the nation's unpreparedness to respond to emerging quantum-related cyber threats. The paper will identify regulatory gaps within current cybersecurity frameworks that underpin critical services and Defence's supply chains, as well as proposed solutions to safeguard critical assets from quantum-enabled espionage.

Australia's Growing Dependence on Submarine Cable Infrastructure

Australian society is structurally dependent on digital connectivity, with subsea cable systems forming the backbone of operational continuity across all critical sectors.[4] Australian utility services (96.7%), transport and logistics (93.8%), communications (99.3%), healthcare (99%), and financial sectors (97.9%), all exhibit high levels of digital connectivity and are reliant on functioning telecommunication networks to operate.[5] These networks are vital to Australia's rapidly expanding digital economy, which reached $158.9 billion in 2024, accounting for 6.3% of total gross value added (GVA).[6] Australia's financial sectors rely on these cable networks to support essential electronic payment systems. The Reserve Bank Information and Transfer System (RITS) moves on average $300 billion each business day, equivalent to 11% of GDP.[7] Given the deep interdependence on digital connectivity, any disruptions to these sea lines of communication would pose substantial risks to Australia's economic stability and national security. Disruptions can rapidly cascade across sectors, amplifying economic, social, and national security impacts through the loss of essential services.[8]

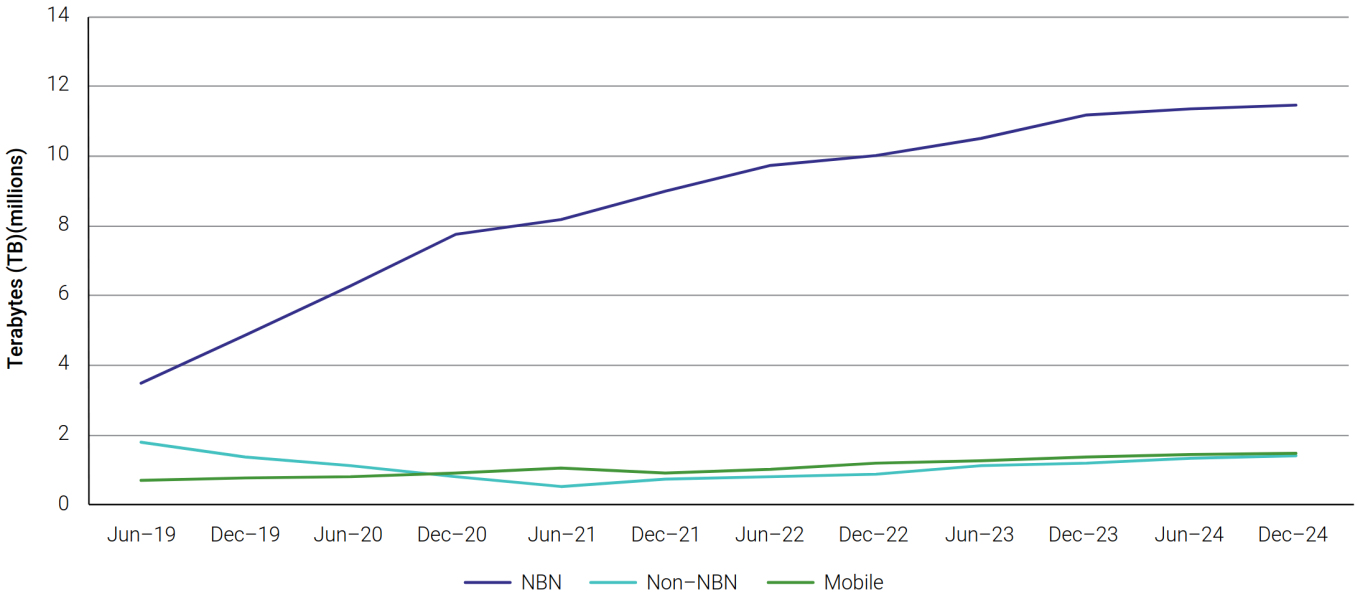

Figure 1: Total Volume of Data Downloaded (2019–2024) Source: [ACCC. Internet Activity Report: For the Period Ending 31 December 2024]

Sustained growth in national internet usage underscores Australia's reliance on undersea cable infrastructure. Over the past five years, bandwidth consumption has risen by 109 %, increasing from 6.9 million terabytes in early 2019 [9] to 14.4 million terabytes by late 2024.[10] The surge in bandwidth consumption has been largely driven by Australian organisations embracing Cloud Infrastructure as a Service (IaaS) offered by hyperscalers (Google, Meta, Microsoft, Amazon, Cloudflare).[11] These firms account for the vast majority of global bandwidth consumption, with content delivery and cloud networks alone generating roughly three-quarters of international demand.[12] Driven by low cost on-demand infrastructure provisioning, cloud adoption among Australian businesses has increased from 19.4% in 2014 to 55.4% by 2020.[13] As of 2022, approximately 59% of Australian businesses now utilise cloud technology.[14] This trend is likely to continue as rapid advancements in artificial intelligence and its integration into various sectors of the economy have intensified demand for high-capacity connectivity.[15] Although hyperscalers have delivered economical and accessible digital infrastructure, they have enabled the offshoring of sensitive data, heightening the risk of foreign jurisdiction access.[16]

The Impact of Disruptions on Concentrated Data Flows

Australia's reliance on cloud centric infrastructure has created structural dependencies on concentrated data channels, heightening the nation's exposure to foreign interference. Australia's external connectivity relies on 18 international submarine cables, with approximately 90% of cable landing sites concentrated in two metropolitan regions.[17] Sydney, which hosts roughly 11 cables (60% of national capacity), serves as the nation's primary connectivity hub, while Perth, with five cables (30%), functions as the gateway to the Indian Ocean and Asian regions.[18] The concentration of undersea cable infrastructure has created systemic vulnerabilities that adversaries are likely to exploit during periods of heightened tension.[19] Driven by intensifying great-power competition, the Australian Security Intelligence Organisation (ASIO) warns that the nation is experiencing "unprecedented levels of espionage" and is approaching "the threshold for high-impact sabotage".[20] State-sponsored Advanced Persistent Threats (APTs) are actively seeking to pre-position vulnerabilities within critical infrastructure networks to enable persistent, covert access and facilitate future disruption of core functions.[21]

ASIO's impact modelling indicates that espionage enabled sabotage of critical infrastructure could impose economy-wide losses of up to $1.16 billion per incident.[22] State-backed disruption operations would severely undermine essential services, impacting government, industry, universities, and the wider community. ASIO's assessment concludes that a week-long disruption to digital, technology intensive industries could incur economic losses of up to $5.93 billion.[23] Cumulative disruptions of digital and logistics systems would likely degrade the Australian Defence Force's operational capability by constraining access to critical inputs (e.g., fuel, transport, data feeds, and materiel), creating supply-chain vulnerabilities that an adversary could exploit long before a conventional conflict fully unfolds.[24]

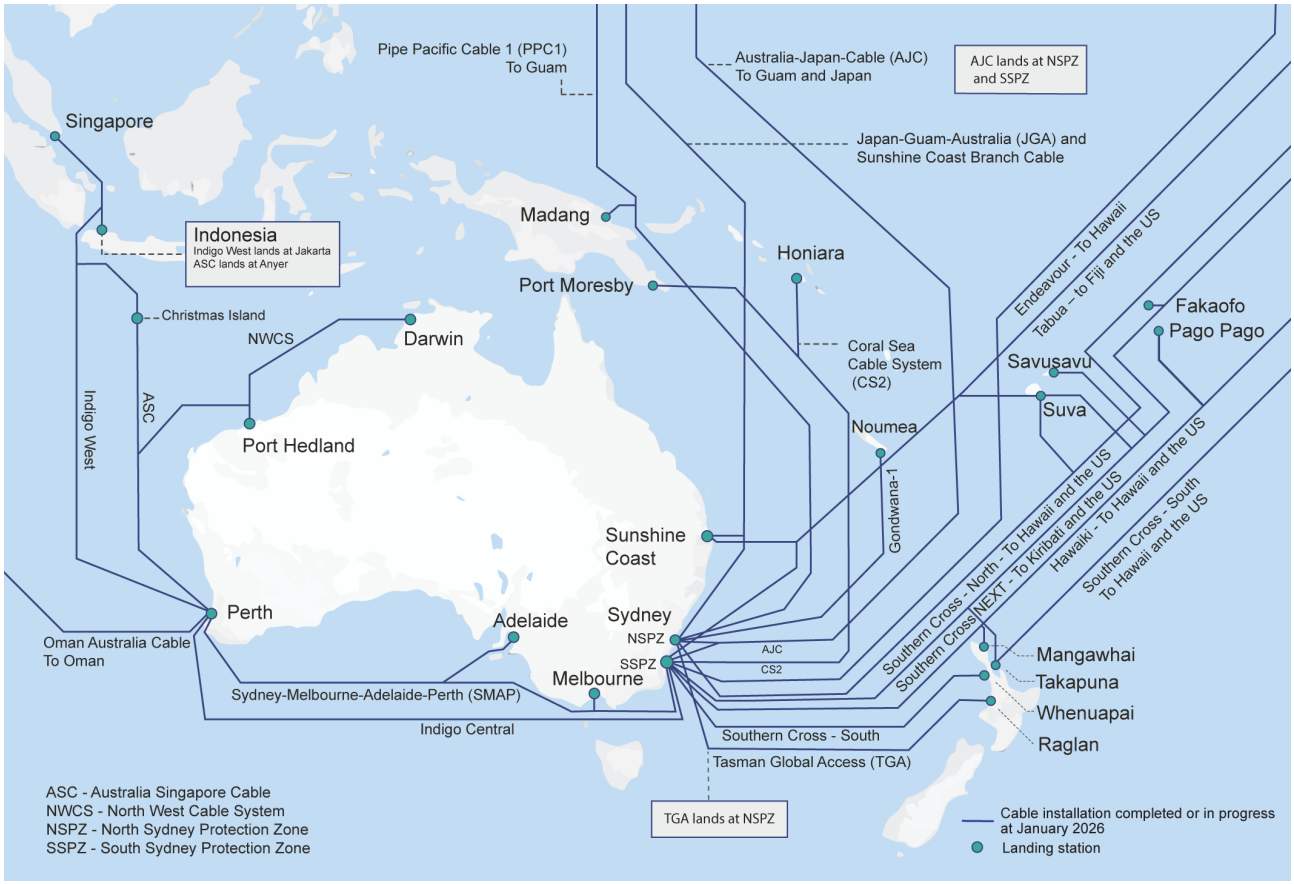

Figure 2: Map of submarine cables landing in Australia Source: [International submarine cables landing in Australia]

Compromised Cable Landing Stations: Routing and Zero-Day Exploits

While intercepting data within the maritime domain remains difficult, cable landing stations (CLS) present a high-reward, low-cost target for APTs.[25] Submarine Line Terminal Equipment (SLTE) and Remote Network Management Systems (RNMS) notably face heightened disruption risks. Given that SLTEs aggregate massive data flows at a single, fragile junction, they are an attractive target for adversaries.[26] The limited number of SLTE/RNMS vendors, coupled with RNMS's reliance on common operating systems (e.g., Linux, Windows NT), makes them particularly vulnerable to cyber intrusion.[27] People's Republic of China (PRC)-linked APTs, such as Salt Typhoon and Volt Typhoon, have targeted major telecommunication providers and backbone infrastructure to facilitate large-scale data exfiltration.[28] The United States (U.S.) government's assessments indicate that Volt Typhoon's activities are not consistent with traditional cyber espionage operations and assess with high confidence that the APT group is pre-positioning initial access points ahead of an anticipated conflict.[29] These groups have experience utilising sophisticated techniques to bypass protective network segmentation boundaries and establish cross-segment persistence.[30]

PRC-aligned APTs may attempt to compromise optical transport network devices (DWDM/OTN/ROADM control-planes), which converts undersea cable signals to terrestrial signals.[31] These systems provide the critical intermediate layer that links SLTEs to data centres and internet service providers.[32] Mercury ISS's security audits of optical transport devices (Ciena Optical Multiservice Edge 6500) operating on the Southern Cross Cable Network identified outdated and vulnerable firmware components in use, including flaws that enable remote code execution (Log4Shell CVE-2021-44228).[33] Their assessment indicates that major telecom providers are still utilising unpatched 2017-era software.[34] Machine in the middle (MITM) or passive eavesdropping attack vectors targeting the optical transport layer would allow adversaries to block specific wavelengths or intercept data packages traversing through backhaul networks.[35]

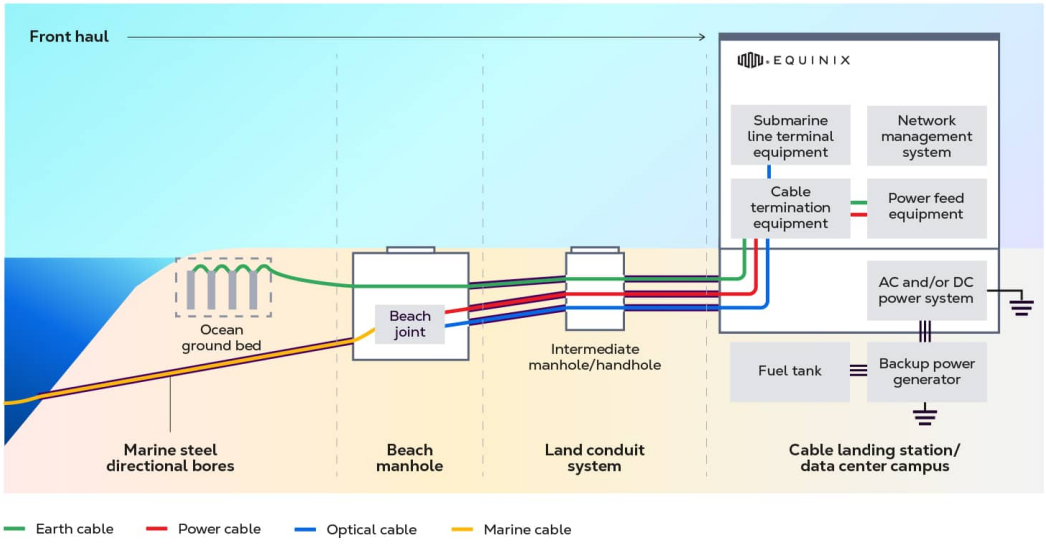

Figure 3: Front Haul Diagram of CLS architecture source : [What Is a Cable Landing Station?]

By degrading CLS availability or exploiting upstream network vulnerabilities in the Border Gateway Protocol (BGP), the PRC has the capability to reroute undersea cable traffic towards its surveillance infrastructure. BGP determines how data packets are routed between CLS, selecting the most efficient path to their destination.[36] By manipulating BGP route announcements, particularly during periods of network instability, the PRC could covertly reroute Australian and regional transit internet traffic.[37] Rerouting attacks would enable adversaries to scale MITM interception and data exfiltration operations. This threat is well established. In 2016, malicious BGP announcements silently rerouted traffic from Canada to South Korean government websites through China for nearly six months, enabling sustained surveillance.[38] Similarly, in 2010, China Telecom briefly hijacked about 15% of global internet routes for roughly 18 minutes, likely exposing U.S. government and military-related traffic.[39] Mitigating or detecting stealthy BGP attacks at scale remains difficult, as the protocol is effectively trust-based and lacks universal, verifiable cryptographic validation.[40]

The true scope of the risks involved remains unclear as the PRC is known to stockpile undisclosed “zero-day” vulnerabilities to strengthen its cyber capabilities.[41] China’s vulnerability-disclosure architecture systematically diverts newly discovered flaws away from public reporting.[42] The PRC mandates that new vulnerabilities must be reported to the Ministry of State Security (MSS) within 48 hours of being discovered, allowing Beijing to assess whether those exploits can be used against foreign targets.[43] Their offensive cyber capabilities operate under a “military–civil fusion” framework, where private and civilian industry cyber resources are integrated with intelligence and military agencies.[44] That arrangement allows APTs to embed supply chain vulnerabilities that can be strategically activated.[45]

The Australian Government should invest in federally funded bug bounty programs to identify supply-chain weaknesses in critical infrastructure networks. This would bring Australia into alignment with the United States and the United Kingdom, which have adopted such programs to systematically identify and report vulnerabilities.[46] At a time of unprecedented espionage activity, any unaddressed weaknesses that allow critical systems to be compromised risk eroding allied confidence in the nation’s information security posture.[47]

Harvest-Now, Decrypt-Later: Quantum Decryption Threat

Concentrated data channels have enabled “harvest-now, decrypt-later” (HNDL) attacks, in which adversaries collect encrypted traffic today with the expectation that future cryptographically relevant quantum computers (CRQCs) will enable its decryption.[48] As CRQCs and quantum optimisation algorithms mature, sensitive data harvested through state-sponsored espionage campaigns may become accessible, particularly data transiting undersea cable networks or stored within large cloud service providers.[49] APT groups are already amassing large volumes of encrypted data in anticipation of these capabilities.[50]

Modern systems rely on symmetric and asymmetric cryptographic schemes, most commonly the Advanced Encryption Standard (AES) for symmetric encryption and Rivest–Shamir–Adleman (RSA) for asymmetric encryption.[51] AES encryption is used for fast encryption of data at rest (such as files and disks), while RSA-2048 bit encryption is utilised for online communications, encrypted email, key exchange and financial transactions.[52] The security of these schemes depends on the assumed computational infeasibility of certain mathematical problems.[53] RSA is secure under the belief that integer factorization is computationally infeasible by traditional systems.[54] Classical computers would require on the order of hundreds of trillions of years to break RSA-2048.[55] However, sufficiently powerful quantum computers undermine these computational hardness assumptions that secure modern systems.

CRQCs leverage quantum mechanics and quantum bits (qubits) to process information. Unlike conventional systems that utilise classical bits (0 or 1), Qubits exist in a probabilistic state that is simultaneously both 0 and 1.[56] This enables parallel computation, which allows CRQCs to solve complex mathematical problems exponentially faster than traditional computers.[57] Shor's algorithm enables a sufficiently powerful quantum computer to solve these hardness assumption problems efficiently, rendering RSA-2048 and asymmetric based protocols vulnerable.[58] Symmetric encryption is not immune. Grover's algorithm accelerates exhaustive key searches, reducing the cost of brute-force attacks and effectively halving the security of AES.[59] This is particularly alarming, as RSA-2048 underpins core authentication mechanisms and highly sensitive correspondence, while AES is trusted to safeguard classified data.[60]

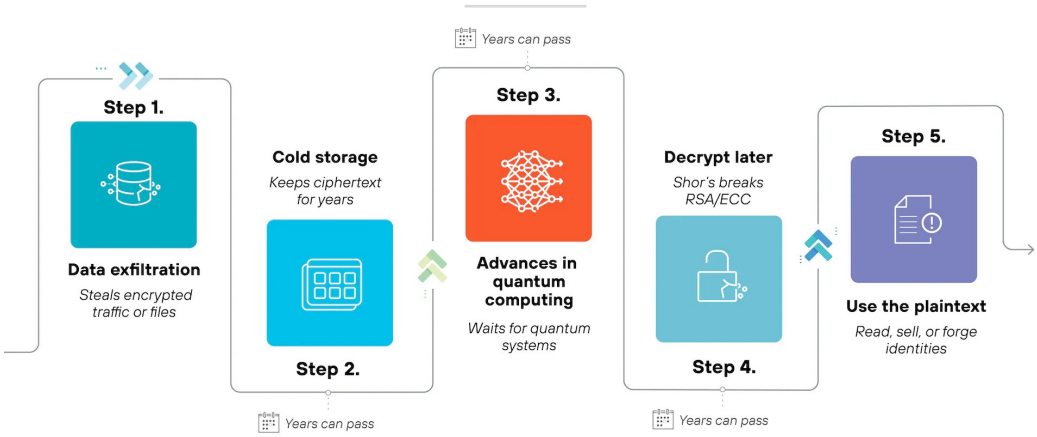

Figure 4: How does a harvest now, decrypt later attack work? source : paloaltonetworks

In response, the U.S National Institute of Standards and Technology (NIST) has released Federal Information Processing Standards (FIPS) engineered to withstand attacks from quantum computers.[61] These post-quantum cryptography (PQC) standards are designed to secure a wide range of electronic information and enable organisations to begin transitioning away from quantum-vulnerable public-key cryptography.[62] The three finalised standards expected to see widespread adoption include FIPS 203 (ML-KEM) for general encryption, FIPS 204 (ML-DSA) for primary digital signatures, and FIPS 205 (SLH-DSA) as a hash-based backup digital signature scheme.[63] Major cloud providers including, AWS, Google Cloud, Microsoft Azure, and Cloudflare have already begun integrating PQC schemes ahead of NIST's finalised standards.[64]

To mitigate exposure to HNDL attacks, the Australian Government must work closely with hyperscalers to accelerate PQC adoption timelines, particularly across cloud services that underpin critical infrastructure. Hyperscalers and the Government should support PQC as the default configuration, strengthen organisational awareness of HNDL attacks, and accelerate migration pathways across the public and private sectors.

Caught Flat-Footed, Accelerated Q-Day Timeline.

Advances in the maturity of quantum algorithms are accelerating the approach of "Q-Day," the point at which quantum computers can break today's public-key cryptography.[65] Publicly known improvements in quantum decryption optimisation have significantly reduced the resources required to break RSA-2048, indicating a growing and imminent threat. In 2012, estimates suggested such an attack would require around one billion physical qubits, placing it well beyond realistic feasibility.[66] By 2019, work by Gidney and Ekerå reduced the estimated RSA-2048 decryption requirement to roughly 20 million physical qubits (6,200 logical qubits) with an execution time of roughly eight hours, shifting the attack from infeasible to theoretically practical.[67] As of 2025, estimates from Google researcher Gidney indicate the same attack could be completed in under a week using fewer than one million physical qubits (1,400 logical qubits), a 95% reduction from his 2019 estimate.[68]

Commercial CRQC roadmaps reinforce this trajectory. IonQ's aggressive projections indicate that it aims to build systems capable of approximately 1,600 logical qubits by 2028,[69] while more conservative estimates by IBM place systems of around 2,000 logical qubits in the early 2030s.[70] This implies that "Q-Day" could become commercially feasible as early as 2028. The Australian Signals Directorate (ASD) recommends that organisations begin transitioning to PQC by 2028, prioritising critical systems and sensitive data.[71] By the end of 2030, organisations should have completed their PQC transition.[72] However, given the accelerating pace of CRQC development and the fact that HNDL activity is already occurring, these timelines are increasingly tight and may leave organisations exposed during the transition window. Accelerated PQC migration timelines are needed to mitigate immediate threats and avert irreversible long-term risks.

Despite the imminent threat, only 5% of organisations consider it a near-term priority or have a defined PQC transition plan.[73] The CSIRO 2025 Quantum Readiness Survey shows Australia is profoundly unprepared for the post-quantum transition, with half of organisations unaware of ASD's 2030 PQC deadline.[74] The study spanned critical sectors (telecoms, finance, energy/water, transport, health, and public administration/safety) that all report a lack of PQC awareness, leaving them exposed to HNDL attacks.[75] Over 70% of organisations are unaware of or unsure about the cryptographic shift itself, and 65.4% remain unsure or uncommitted to migration.[76] Fewer than 29% have taken any action, and just 3.8% have an allocated budget, leaving 77% with no funding, no plans, or no visibility at all.[77]

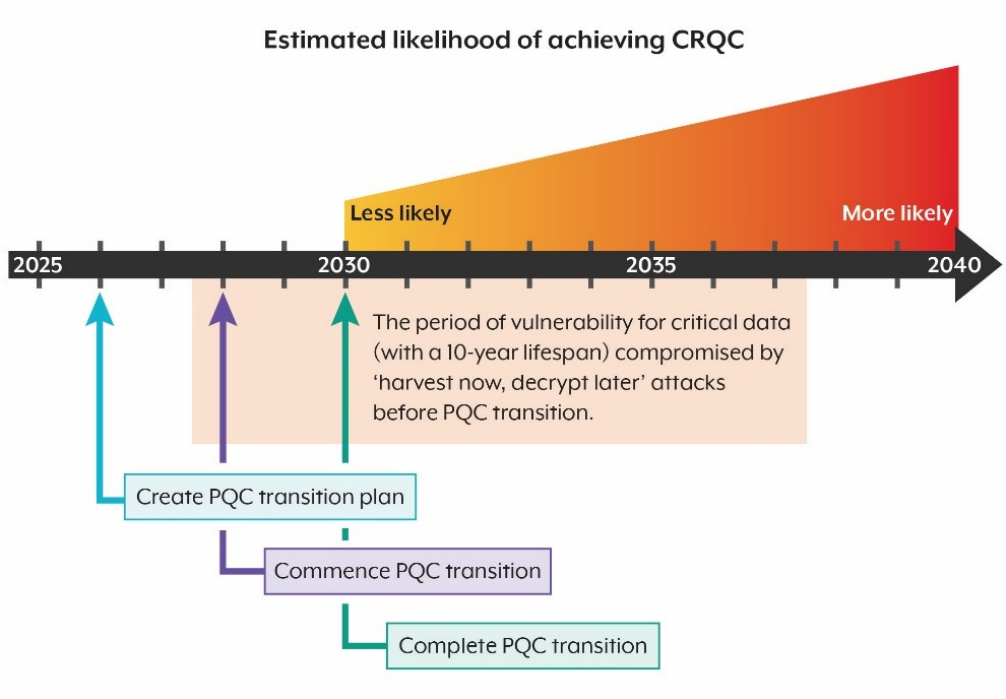

Figure 5: ASD's 2025 recommended PQC transition timeline source : [ASD's Transition timeline]

Closing Regulatory Gaps to Mitigate HNDL Exposure

The Australian Government must urgently address gaps within the Security of Critical Infrastructure (SOCI) Act 2018 and Defence Industry Security Program (DISP) to minimise exposure to HNDL risks. Under DISP, contractors must meet or exceed ASD Essential Eight Maturity Level 2 for all corporate ICT systems used for Defence correspondence.[78] However, the Essential Eight framework does not explicitly address HNDL risks or provide any guidance on PQC, which leaves a critical gap in protection against emerging cryptographic threats.[79] DISP allows entities that comply with other international security standards, such as ISO 27001:2022, to demonstrate compliance.[80] However, ISO/IEC 27001 Control 8.24 requires cryptography to be applied where risk warrants it, without prescribing specific algorithms or methods.[81] This means the current use of RSA remains acceptable, and there is no explicit regulatory pressure to transition to PQC.

Organisations that store, process or transmit SECRET or TOP SECRET classified information must comply with the ASD Information Security Manual (ISM), as required by the Australian Government's Protective Security Policy Framework (PSPF).[82] PQC is endorsed but not currently mandatory under the ISM and organisations are strongly encouraged to prepare for a 2030 PQC transition.[83] RSA remains an ASD-approved cryptographic algorithm under the ISM and may be used in accordance with approved key sizes.[84] Under PSPF Release 2025, the use of ASD-approved PQC algorithms is only mandatory for newly procured cryptographic equipment and software (PSPF Requirement 0212).[85]

The PSPF and ISM do not mandate immediate PQC uplift for existing systems, provided those systems remain authorised and compliant with current ISM controls. In practice, organisations may achieve DISP and PSPF compliance while still relying on vulnerable cryptographic algorithms, introducing systemic risk across Defence's supply chain. This exposes classified information, Defence research and development, and intelligence to heightened HNDL exposure. Defence must close this gap by embedding HNDL risk management and mandatory PQC transition planning into DISP to proactively mitigate CRQC threats across its supply chains.

Under Part 2A of the SOCI Act, and pursuant to section 30AH, the Critical Infrastructure Risk Management Program (CIRMP) Rules require responsible entities to comply with subsection 8(4), including adoption of an approved cyber security framework such as ISO/IEC 27001:2015 or the ASD Essential Eight.[86] PQC was not a practical consideration in 2015 when ISO 27001:2015 was formalised, reflecting the threat landscape of that period rather than emerging quantum risks. Proposed enhancements to the CIRMP Rules, include the adoption of ISO/IEC 27001:2023.[87] However, neither the ASD Essential Eight nor ISO/IEC 27001:2023 mandates PQC or have HNDL mitigation strategies. As a result, entities are largely left to self-select controls, with minimal regulatory pressure to plan for quantum-era threats. The Australian Government must amend the CIRMP Rules to require ASD's ISM as the baseline cybersecurity framework to ensure PQC resilience across its critical infrastructure and minimise the impact of PRC-enabled HNDL espionage campaigns.

Policy Recommendations

- Mandate post-quantum cryptography for all classified ICT systems under the Protective Security Policy Framework, explicitly including legacy systems to mitigate "harvest now, decrypt later" threats and protect critical assets.
- Mandate compliance with the ASD Information Security Manual across the SOCI Critical Infrastructure Risk Management Program and the Defence Industry Security Program to safeguard classified information from quantum-enabled threats.
- Strengthen partnerships with hyperscalers to accelerate post-quantum cryptography adoption among Australian businesses, bridging the transition gap ahead of 2028.
- Take proactive measures by investing in federally backed vulnerability research and bug-bounty programs to systematically identify and remediate supply-chain weaknesses affecting critical infrastructure.

Conclusion

As great-power competition intensifies, rapid advances in quantum decryption leave Australian businesses and Defence's supply chains increasingly vulnerable to Chinese-backed espionage campaigns. Current cybersecurity regulations entrench existing harvest-now, decrypt-later risks by allowing organisations to defer PQC transitions until 2030, leaving classified and sensitive information exposed. Organisations compliant with current cybersecurity frameworks remain vulnerable, as compressed Q-Day timelines could render intercepted encrypted data accessible as early as 2028. Immediate action is required to close existing cybersecurity gaps and apply regulatory pressure to drive PQC adoption, particularly among organisations subject to Protective Security Policy Framework, Defence Industry Security Program, and Security of Critical Infrastructure (Act) obligations. Given that 77% of Australian organisations lack awareness of the imminent quantum decryption threats, the Australian government must work with hyperscalers and cloud service providers to accelerate PQC adoption. The Australian government should invest in federally funded bug bounty programs to systematically identify and remediate cybersecurity supply-chain vulnerabilities. Without proactive cybersecurity measures, Australia risks eroding allied confidence in its information security posture and Defence's operational readiness.

About the Author

Divij Bhaw is a GIAC Certified Forensic Analyst who specialises in investigating complex cybersecurity threats. He has recently completed a Bachelor of Arts at the University of Western Australia, majoring in Politics and International Relations, and participated in the 2024–25 UWADSI U.S.–Australia Alliance Emerging Leaders Program. His academic background complements his technical expertise, reinforcing his commitment to advancing national security initiatives.

Endnotes

[1] Andrew Horton, “The Achilles’ Heel of a Digital Nation: Australia’s Dependence on Subsea Cables,” *The Strategist* (Australian Strategic Policy Institute), 6 June 2024, accessed 24 November 2025, https://www.aspistrategist.org.au/the-achilles-heel-of-a-digital-nation-australias-dependence-on-subsea-cables/

[2] Bashfield, Samuel. 2025. “Defending Seabed Lines of Communication.” Australian Journal of Maritime & Ocean Affairs 17 (4): 557–69. doi:10.1080/18366503.2024.2363607

[3] Bashfield, “Defending Seabed Lines of Communication.”

[4] Australian Government. Department of Home Affairs. Critical Infrastructure Security Centre. Critical Infrastructure Annual Risk Review 2025. 3rd ed. November 2025. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2025.pdf Accessed December 22, 2025.

[5] Australian Bureau of Statistics. *Characteristics of Australian Business, 2021-22: Table 1 – Use of information technology and the internet by businesses, 2021-22 (Catalogue no. 8167.0, DO 005).* Excel file, 2023. Accessed November 23, 2025. https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2021-22/81670DO005_202122.xlsx

[6] Australian Bureau of Statistics 2025. Digital activity in the Australian economy: Table 1 – Share in total digitalactivity value added (%), 2019-20 to 2023-24 (Excel file). Released 24 October 2025. Retrieved from https://www.abs.gov.au/statistics/economy/national-accounts/australian-national-accounts-supply-use-tables/latest-release#digital-activity-in-the-australian-economy

[7] Reserve Bank of Australia. 2025. “Non-cash Payments.” Payments System | Reserve Bank of Australia. https://www.rba.gov.au/payments-and-infrastructure/payments-system.html#non_cash_payments

[8] Department of Home Affairs, *Critical Infrastructure Annual Risk Review 2025*

[9] Australian Competition and Consumer Commission. *Internet Activity Report – December 2019*. April 2020. https://www.accc.gov.au/system/files/Internet%20Activity%20Report%20%28December%202019%29_2.pdf

[10] Australian Competition and Consumer Commission. Internet Activity Report: For the Period Ending 31 December 2024. Canberra: ACCC, October 2025. https://www.accc.gov.au/system/files/internet-activity-report-december2024_0.pdf

[11] McMillan, Henry, Tim Murray, Catherine de Fontenay, and Ralph G. Lattimore. *Head in the Cloud: Firm Performance and Cloud Service: Conference Paper*. Productivity Commission, 2022.

[12] Mauldin, Alan. “International Bandwidth Demand Surpasses 6.4 Pbps.” *TeleGeography Blog*, May 12, 2025. Accessed November 24, 2025. https://blog.telegeography.com/used-international-bandwidth-reaches-new-heights

[13] McMillan et al., *Head in the Cloud*, 7.

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

[15] Horton, "Achilles' Heel of a Digital Nation."

[16] Australian Cybersecurity Magazine. 2024. "Data Beyond Bord17ers — Australian Data Stored in Non-Australian Cloud Environments." Australian Cybersecurity Magazine, October 28, 2024. https://australiancybersecuritymagazine.com.au/data-beyond-borders-australian-data-stored-in-non-australian-cloud-environments/

[17] TeleGeography, Australia: Submarine Cable Map, Submarine Cable Map, accessed November 25, 2025, https://www.submarinecablemap.com/country/australia

[18] TeleGeography, "Australia: Submarine Cable Map."

[19] KANG, JOCELINN, and DR JESSIE JACOB. "Connecting the Indo-Pacific: The future of subsea cables." (2024).

[20] Caisley, Olivia. 2025. "Spy Chief Warns of China Espionage Threat to Business, Critical Infrastructure." ABC News, November 11. https://www.abc.net.au/news/2025-11-12/spy-chief-warns-of-china-espionage-threat-to-business/105999522

[21] Department of Home Affairs. *Critical Infrastructure Annual Risk Review: Second Edition*. Canberra: Australian Government, 2024. Accessed 7 December 2025. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2024.pdf

[22] Morgan, Anthony, and Amelia Voce. The Cost of Espionage. Special Reports. Canberra: Australian Security Intelligence Organisation, 2025. https://www.aic.gov.au/publications/special/special-21

[23] Morgan and Voce, *Cost of Espionage*.

[24] Turnbull, Benjamin. "Cyber-Resilient Supply Chains: Mission Assurance in the Future Operating Environment." Australian Army Journal 14, no. 2 (2018): 41–56. https://search.informit.org/doi/10.3316/informit.344417545553155

[25] Petit, Zelie. 2024. "Beneath NATO's Radars: Unaddressed Threats to Subsea Cables." Center for Strategic and International Studies (blog), December 2, 2024. https://www.csis.org/blogs/strategic-technologies-blog/beneath-natos-radars-unaddressed-threats-subsea-cables

[26] Petit, "Beneath NATO's Radars."

[27] Sherman, Justin. "Cyber defense across the ocean floor." *The Geopolitics of Submarine Cable Security.(Washington, DC: Atlantic Council* (2021).

[28] Australian Cyber Security Centre. 2025. *"Countering Chinese State-Sponsored Actors: Compromise of Networks Worldwide to Feed Global Espionage System."* August 28, 2025. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system

[29] U.S. Cybersecurity and Infrastructure Security Agency; National Security Agency; Federal Bureau of Investigation; and partners. 2024. *"PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure."* February 7, 2024. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/prc-state-sponsored-actors-compromise-and-maintain-persistent-access-us-critical-infrastructure

[30] Infosecurity Magazine. "Chinese Espionage Targets VMware." July 25, 2025. https://www.infosecurity-magazine.com/news/chinese-espionage-targets-vmware/

[31] Submarine Networks. "Stations." *SubmarineNetworks.com*. Accessed December 5, 2025. https://www.submarinenetworks.com/en/stations

[32] *Submarine Networks, "Stations"*

[33] Mercury Information Security Services. *Critical Links: Technical and Strategic Risk Assessment of Submarine Cable Infrastructure in the Pacific*. Version 2.0. 4 September 2025. Accessed 3 December 2025. https://mercuryiss.com.au/Submarine-Cable-Report

[34] Mercury Information Security Services, Critical Links.

[35] *Petit, "Beneath NATO's Radars."*

[36] Cloudflare. "What Is BGP? | BGP Routing Explained." Cloudflare Learning Center. Accessed December 8, 2025. https://www.cloudflare.com/learning/security/glossary/what-is-bgp/

[37] Demchak, Chris C., and Yuval Shavitt. "*China's maxim–leave no access point unexploited: The hidden story of china telecom's bgp hijacking*." *Military Cyber Affairs* 3, no. 1 (2018): 7.

[38] Demchak and Shavitt, "China's Maxim—Leave No Access Point Unexploited."

[39] Demchak and Shavitt, "China's Maxim—Leave No Access Point Unexploited."

[40] Birge-Lee, Henry, Maria Apostolaki, and Jennifer Rexford. *Global BGP Attacks that Evade Route Monitoring*. arXiv, August 19, 2024. https://arxiv.org/abs/2408.09622

[41] Latimore, Jasmine. 2022. "How China Is Using Network Vulnerabilities to Boost Its Cyber Capabilities." *The Strategist* (ASPI), December 15, 2022. https://www.aspistrategist.org.au/how-china-is-using-network-vulnerabilities-to-boost-its-cyber-capabilities/

[42] Dakota Cary and Kristin Del Rosso, *Sleight of Hand: How China Weaponizes Software Vulnerabilities* (Washington, DC: Atlantic Council, September 6, 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/

[43] Cary and Del Rosso, *Sleight of Hand*.

[44] Dohr, Peter. 2025. "China's Weaponization of Global Cyber Supply Chains." *Strategic Technologies Blog*, Center for Strategic and International Studies (CSIS), December 1, 2025. https://www.csis.org/blogs/strategic-technologies-blog/chinas-weaponization-global-cyber-supply-chains.

[45] Dohr, “China’s Weaponization of Global Cyber Supply Chains.”

[46] Dobell, Adam, and Ilona Cohen. “Australia’s Cyber Strategy Needs a Vulnerability Disclosure Upgrade.” The Strategist, Australian Strategic Policy Institute, April 9, 2025. https://www.aspistrategist.org.au/australias-cyber-strategy-needs-a-vulnerability-disclosure-upgrade/

[47] Dobell and Cohen, “Australia’s Cyber Strategy Needs a Vulnerability Disclosure Upgrade.”

[48] Palo Alto Networks, “*Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat*,” *Cyberpedia*, accessed December 11, 2025, https://www.paloaltonetworks.com.au/cyberpedia/harvest-now-decrypt-later-hndl

[49] Palo Alto Networks, “Harvest Now, Decrypt Later (HNDL).”

[50] Federici, Joseph. "Vying for Quantum Supremacy: US-China Competition in Quantum Technologies." (2025).

[51] GeeksforGeeks. “Difference Between AES and RSA Encryption.” Last updated July 23, 2025. https://www.geeksforgeeks.org/computer-networks/difference-between-aes-and-rsa-encryption/

[52] GeeksforGeeks, “Difference Between AES and RSA Encryption.”

[53] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography: Principles and Protocols* (Boca Raton, FL: Chapman & Hall/CRC, 2007), chap. 8, 285–286.

[54] Katz and Lindell, *Introduction to Modern Cryptography*, chap. 8, 285–286.

[55] QuintessenceLabs. “Breaking RSA Encryption - an Update on the State-of-the-Art.” June 13, 2019. https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art

[56] Federici, “*Vying for Quantum Supremacy*.”

[57] Federici, “*Vying for Quantum Supremacy*.”

[58] Bagourd, Paul, Julian Jang-Jaccard, Vincent Lenders, Alain Mermoud, Torsten Hoefler, and Cornelius Hempel. "Practical Challenges in Executing Shor's Algorithm on Existing Quantum Platforms." *arXiv preprint arXiv:2512.15330* (2025).

[59] Fortinet. “Understanding Shor’s and Grover’s Algorithms and Their Impact on Cybersecurity.” Fortinet, accessed December 21, 2025. https://www.fortinet.com/resources/cyberglossary/shors-grovers-algorithms

[60] Australian Signals Directorate, “Guidelines for Cryptography,” Cyber.gov.au, last updated December 4, 2025, accessed December 21, 2025, https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography

[61] National Institute of Standards and Technology. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. NIST, 13 Aug. 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[62] NIST, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards.”

[63] NIST, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards.”

[64] Lawton, George. “The Cloud’s Role in PQC Migration.” Search Cloud Computing, TechTarget, July 7, 2025. https://www.techtarget.com/searchcloudcomputing/tip/The-clouds-role-in-PQC-migration

[65] Palo Alto Networks. “What Is Q-Day, and How Far Away Is It—Really?” Palo Alto Networks . Accessed December 21, 2025. https://www.paloaltonetworks.com.au/cyberpedia/what-is-q-day

[66] Fowler, Austin G., Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. “Surface codes: Towards practical large-scale quantum computation.” arXiv (2012). https://arxiv.org/abs/1208.0928

[67] Gidney, Craig, and Martin Ekerå. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits." *Quantum* 5 (2021): 433.

[68] Craig Gidney, *How to factor 2048 bit RSA integers with less than a million noisy qubits*, arXiv preprint, May 21, 2025, arXiv:2505.15917, https://arxiv.org/abs/2505.15917

[69] IonQ. “IonQ’s Accelerated Roadmap: Turning Quantum Ambition into Reality.” IonQ Blog, June 13, 2025. https://www.ionq.com/blog/ionqs-accelerated-roadmap-turning-quantum-ambition-into-reality

[70] IBM Quantum. IBM Quantum Roadmap: Development and Innovation Roadmap Explainer. IBM Corporation, 2025. https://www.ibm.com/downloads/documents/us-en/1443d5cda24021e4

[71] Australian Signals Directorate. “Planning for Post-Quantum Cryptography.” Cyber.gov.au. First published July 6, 2022; last updated September 22, 2025. Accessed December 24, 2025. https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography

[72] ASD, “Planning for Post-Quantum Cryptography.”

[73] ISACA. “Despite Rising Concerns, 95% of Organizations Lack a Quantum Computing Roadmap, ISACA Finds.” Press release, April 28, 2025. https://www.isaca.org/about-us/newsroom/press-releases/2025/organizations-lack-a-quantum-computing-roadmap-isaca-finds

[74] Chhetri, Mohan Baruwal, Rebecca Coates, Yue Huang, David M. Douglas, Chehara Pathmabandu, Gabi Skoff, and Lauren S. Ferro. "Quantum shift: How are Australian organisations navigating the quantum frontier." (2025).

[75] Chhetri et al., Quantum Shift.

[76] Chhetri et al., Quantum Shift.

[77] Chhetri et al., Quantum Shift.

[78] Australia, Department of Defence. “Eligibility and Suitability.” Defence Industry Security Program, Department of Defence. https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/eligibility-suitability/

[79] Australia, Australian Cyber Security Centre. “Essential Eight Maturity Model.” Cyber.gov.au, Australian Government. https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model/

[80] Department of Defence, “Eligibility and Suitability.”

[81] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 3rd ed. Geneva: ISO/IEC, 2022.

[82] Department of Home Affairs. *Australian Government Protective Security Policy Framework: Release 2025*. Canberra: Australian Government, July 2025. https://www.protectivesecurity.gov.au/system/files/2025-07/pspf-release-2025.pdf

[83] Australian Signals Directorate. 2025. *Information Security Manual*. Canberra: Australian Government. Last updated December 2025.https://www.cyber.gov.au/sites/default/files/2025-12/Information%20security%20manual%20%28December%202025%29.pdf

[84] Australian Cyber Security Centre. Guidelines for Cryptography. Information Security Manual. December 2025. https://www.cyber.gov.au/sites/default/files/2025-12/22.%20ISM%20-%20Guidelines%20for%20cryptography%20%28December%202025%29.pdf

[85] Department of Home Affairs, Protective Security Policy Framework: Release 2025.

[86] Cyber and Infrastructure Security Centre (CISC). Guidance for the Critical Infrastructure Risk Management Program. Australian Government Department of Home Affairs, March 2025. https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf

[87] Australian Government, Department of Home Affairs. Consultation Paper: Proposed amendments to enhance the CIRMP Rules, published 9 December 2025. https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-enhancements-to-cirmp-rules/consultation-paper-proposed-amendments-enhance-cirmp.pdf