HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 1

Strong businesses and citizens

- Support SMEs to strengthen their cyber security
- Help Australians defend themselves from cyber threats
- Disrupt and deter threat actors from attacking Australia
- Work with industry to break the ransomware business model
- Provide clear cyber guidance for businesses including sharing lessons learned from cyber incidents by establishing a Cyber Incident Review Board (CIRB)
- Make it easier for Australian businesses to access advice and support after a cyber incident
- Secure our identities and provide better support to victims of identity theft.

US

(5 pillars) - 2023 to FY26

Pillar 1

Defend critical infrastructure

Strategic Objective 1.4: Update federal incident response plans and processes including ensuring that the cyber security community benefits from lessons learned through the Cyber Safety Review Board (CSRB).

Pillar 2

Disrupt and dismantle threat actors

Strategic Objective 2.4: Prevent abuse of US-based infrastructure

Strategic Objective 2.5: Counter cyber crime, defeat ransomware.

Pillar 4

Invest in a resilient future

Strategic Objective 4.5: Support development of a digital identity ecosystem.

UK

(5 pillars) - 2022 to 2025

Pillar 1

UK cyber ecosystem - strengthening the UK's cyber ecosystem

Objective 1: Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber

Objective 3: Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy.

Pillar 2

Cyber resilience - building a resilient and prosperous digital UK

Objective 1: Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

Objective 2: Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens

Objective 3: Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.2 Building a European cyber shield: Proposal to build a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), which will constitute a real "cyber security shield" for the EU, able to detect signs of a cyber attack early enough and to enable proactive action, before damage occurs

1.6 Greater global internet security

1.7 A reinforced presence on the technology supply chain - dedicated support to small and medium-sized businesses (SMEs), under the Digital Innovation Hubs.

See also **2. Building operational capacity to prevent, deter and respond.**

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 2

Enable a safer cyberspace

- Secure digital infrastructure, devices, and applications that power our digital economy
- Safeguard our cyberspace activities
- Empower our cyber-savvy population for a healthy digital way of life.

Foundational enabler 1

Develop a vibrant cyber security ecosystem

- Develop advanced capabilities for economic growth and national security
- Innovate to build world-class products and services
- Grow cyber security market.

China

(9 strategic tasks) - 2016

Task 4

Strengthening the construction of online culture

Task 6

Perfect network governance systems

Persist in managing and governing the web in a lawful, open and transparent manner, realistically ensure that there are laws to rely on, laws must be relied on, law enforcement must be strict, and violations of the law must be punished.

Task 8

Enhancing cyberspace protection capabilities

Cyberspace is a new territory for national sovereignty. Build cyber security protection forces commensurate with our country's international standing and suited to a strong cyber power, forcefully develop cyber security defence means, timely discover and resist cyber intrusions, and cast a firm backup force to safeguard national cyber security.

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 2

Safe technology

- Ensure Australians can trust their digital products and software
- Protect our most valuable datasets
- Promote the safe use of emerging technology.

US

(5 pillars) - 2023 to FY26

Pillar 3

Shape market forces to drive security and resilience

Strategic Objective 3.1: Hold the stewards of our data accountable

Strategic Objective 3.2: Drive the development of secure IoT devices

Strategic Objective 3.3: Shift liability for insecure software products and services to manufacturers and software publishers

Strategic Objective 3.4: Use federal grants and other incentives to build in security

Strategic Objective 3.5: Leverage federal procurement to improve accountability

Strategic Objective 3.6: Explore a federal cyber insurance backstop.

UK

(5 pillars) - 2022 to 2025

Pillar 3

Technology advantage - taking the lead in the technologies vital to cyber power

Objective 1: Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power

Objective 2: Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace

Objective 2a: Preserve a robust and resilient national Crypt-Key enterprise[8] which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most significant risks including the threat from our most capable of adversaries

Objective 3: Secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply

Objective 4: Shape global technology standards - work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic advantage through science and technology.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.4 Securing the next generation of broadband mobile networks - EU citizens using advanced and innovative applications enabled by 5G and future generation of networks should benefit from the highest security standard. Under the new Cybersecurity Strategy, Member States, with the support of the Commission and ENISA - the European Cybersecurity Agency, are encouraged to complete the implementation of the EU 5G Toolbox, a comprehensive and objective risk-based approach for the security of 5G and future generations of networks

1.5 An internet of secure things - working to ensure transparent security solutions and certification under the Cybersecurity Act and to incentivise safe products and services without compromising on performance. Possible new horizontal rules to improve the cyber security of all connected products and associated services placed on the Internal Market, which may include a new duty of care for connected device manufacturers to address software vulnerabilities.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 2

Enable a safer cyberspace

- Secure digital infrastructure, devices, and applications that power our digital economy.

Foundational enabler 1

Develop a vibrant cyber security ecosystem

- Innovate to build world-class products and services.

China

(9 strategic tasks) - 2016

Task 7

Fostering innovation, web safety and talent

Give high regard to software security, and accelerate the dissemination and application of safe and trustworthy products.

[8] *"Crypt-Key is the term used to describe the UK's use of cryptography to protect the critical information and services on which the UK government, military and national security community rely, including from attack by our most capable adversaries. It underpins our ability to choose how we deploy our national security and defence capabilities. To be a world-leading Crypt-Key nation we need the right skills and technologies both in government and in the private sector."*

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields)
- 2023 to 2030

Shield 3

World-class threat sharing and blocking

- Create a whole-of-economy threat intelligence network
- Scale threat blocking capabilities to stop cyber attacks.

US

(5 pillars) - 2023 to FY26

Pillar 2

Disrupt and dismantle threat actors

Strategic Objective 2.1: Integrate federal disruption activities

Strategic Objective 2.2: Enhance public-private operational collaboration to disrupt adversaries

Strategic Objective 2.3: Increase the speed and scale of intelligence sharing and victim notification

Strategic Objective 2.4: Prevent abuse of US-based infrastructure

Strategic Objective 2.5: Counter cybercrime, defeat ransomware.

UK

(5 pillars) - 2022 to 2025

Pillar 5

Countering threats - detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace

Objective 1: Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens

Objective 2: Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens

Objective 3: Take action in and through cyberspace to support our national security and the prevention and detection of serious crime.

EU

(3 areas of EU action)
- 2020 to 2027

Area 2

Building operational capacity to prevent, deter and respond

2.1 Joint Cyber Unit - the Commission is preparing, through a progressive and inclusive process with the Member States, a new Joint Cyber Unit, to strengthen cooperation between EU bodies and Member State authorities responsible for preventing, deterring and responding to cyber attacks, including civilian, law enforcement, diplomatic and cyber defence communities

2.2 Tackling cyber crime

2.3 EU Cyber Diplomacy Toolbox - the High Representative puts forward proposals to strengthen the EU Cyber Diplomacy Toolbox to prevent, discourage, deter and respond effectively against malicious cyber activities, notably those affecting our critical infrastructure, supply chains, democratic institutions and processes

2.4 Boosting cyber defence capabilities – the EU will also aim to further enhance cyber defence cooperation and develop state-of-the-art cyber defence capabilities, building on the work of the European Defence Agency and encouraging Member States to make full use of the Permanent Structured Cooperation and the European Defence Fund.

China

(9 strategic tasks) - 2016

Task 2

Resolutely safeguard national security

Prevent, curb and lawfully punish any act of using the network to engage in treason, separatism, incite rebellion or subversion, or incite the overthrow of the people's democratic dictatorship regime; prevent, curb and lawfully punish acts of using the network to steal or leak State secrets and other such acts harming national security; prevent, curb and lawfully punish foreign powers using the network to conduct infiltration, destruction, subversion and separatist activities.

Task 5

Attacking cyber terrorism, law-breaking and crime

Strengthen online anti-terrorism, counterespionage and anti-theft capabilities, and strictly attack cyber terrorism and cyber espionage activities.

HOW AUSTRALIA’S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields)
- 2023 to 2030

Shield 4

Protected critical infrastructure

- Clarify the scope of critical infrastructure regulation
- Strengthen cyber security obligations and compliance for critical infrastructure
- Uplift cyber security of the Commonwealth Government
- Pressure-test our critical infrastructure to identify vulnerabilities.

US

(5 pillars) - 2023 to FY26

Pillar 1

Defend critical infrastructure

Strategic Objective 1.1: Establish cyber security requirements to support national security and public safety by creating new regulations, harmonising and streamlining new and existing regulation and enabling regulated entities to afford security

Strategic Objective 1.2: Scale public-private collaboration

Strategic Objective 1.3: Integrate federal cyber security centres

Strategic Objective 1.4: Update federal incident response plans and processes including ensuring that the cyber security community benefits from lessons learned through the Cyber Safety Review Board (CSRB)

Strategic Objective 1.5: Modernise federal defences.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 1

Build resilient infrastructure

- Enable a coordinated approach to national cyber security with Critical Information Infrastructures (CIIs) at its core
- Ensure government systems are secure and resilient
- Safeguard important entities and systems beyond CIIs.

EU

(3 areas of EU action)
- 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.1 Resilient infrastructure and critical services - proposal to reform the rules on the security of network and information systems, under a Directive on measures for high common level of cyber security across the Union (revised NIS Directive or ‘NIS 2’), in order to increase the level of cyber resilience of critical public and private sectors: hospitals, energy grids, railways, but also data centres, public administrations, research labs and manufacturing of critical medical devices and medicines, as well as other critical infrastructure and services, must remain impermeable, in an increasingly fast-moving and complex threat environment.

To respond to the growing threats due to digitalisation and interconnectedness, the proposed Directive on measures for high common level of cyber security across the Union (revised NIS Directive or ‘NIS 2’) will cover medium and large entities from more sectors based on their criticality for the economy and society. NIS 2 strengthens security requirements imposed on the companies, addresses security of supply chains and supplier relationships, streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. The NIS 2 proposal will help increase information sharing and cooperation on cyber crisis management at national and EU level.

1.3 An ultra-secure communication infrastructure - the EU Governmental Satellite Communications, a component of the Space Programme, will provide secure and cost-efficient space-based communication capabilities to ensure the security- and safety- critical missions and operations managed by the EU and its Member States, including national security actors and EU institutions, bodies and agencies.

2. Building operational capacity to prevent, deter and respond

The proposed Critical Entities Resilience (CER) Directive expands both the scope and depth of the 2008 European Critical Infrastructure directive. Ten sectors are now covered: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space. Under the proposed directive, Member States would each adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments. These assessments would also help identify a smaller subset of critical entities that would be subject to obligations intended to enhance their resilience in the face of non-cyber risks, including entity-level risk assessments, taking technical and organisational measures, and incident notification. The Commission, in turn, would provide complementary support to Member States and critical entities, for instance by developing a Union-level overview of cross-border and cross-sectoral risks, best practice, methodologies, cross-border training activities and exercises to test the resilience of critical entities.

China

(9 strategic tasks) - 2016

Task 3

Protect critical information infrastructure

National critical information infrastructure refers to information infrastructure that affects national security, the national economy and the people’s livelihood, where whenever data is leaked, it is destroyed or loses its functionality, national security and the public interest may be gravely harmed, including but not limited to basic information networks providing public telecommunications, radio and television transmission, and other such services, as well as important information systems in areas and State bodies such as energy, finance, transportation, education, scientific research, hydropower, industry and manufacturing, healthcare and medicine, social security, public undertakings, etc., important internet application systems, etc. Adopt all necessary measures to protect critical information infrastructure and its important data from attack and destruction. Persist in laying equal stress on technology and management, simultaneously developing protection and deterrence, focus on identification, prevention, monitoring, early warning, response, handling and other such segments, in establishing and implementing a critical information infrastructure protection system, expand input in areas such as management, technology, talent and finance, synthesise measures and policies according to the law, and realistically strengthen security protection of critical information infrastructure.

Protecting critical information infrastructure is a common responsibility of government, businesses and the entire society, controlling and operational work units and organisations must, according to the requirements of laws, regulations, rules and standards, adopt the necessary measures to ensure the security of critical information infrastructure, and progressively realise that evaluation happens first, and application afterwards. Strengthen risk assessment of critical information infrastructure. Strengthen security protection in Party and government bodies, as websites in focus areas, grass-roots Party and government bodies’ websites must be built, operated and managed according to the intensification model. Establish orderly cyber security information sharing mechanisms for government, sectors and enterprises, and fully give rein to the important role of enterprises in protecting critical information infrastructure.

Persist in opening up to the outside world, and safeguarding cyber security in an open environment. Establish and implement cyber security examination structures, strengthen supply chain security management, launch security inspections for important information technology products and services purchased and used in Party and government bodies, as well as focus sectors, raise the security and controllability of products and services, prevent product and service providers and other organisations from using their superiority in information technology to engage in improper competition or to harm users’ interests.

HOW AUSTRALIA'S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 5

Sovereign capabilities

- Grow and professionalise our national cyber workforce
- Accelerate our local cyber industry, research and innovation.

US

(5 pillars) - 2023 to FY26

Pillar 4

Invest in a resilient future

Strategic Objective 4.1: Secure the technical foundation of the internet

Strategic Objective 4.2: Reinvigorate federal research and development for cyber security

Strategic Objective 4.3: Prepare for our post-quantum future

Strategic Objective 4.4: Secure our clean energy future

Strategic Objective 4.5: Support development of a digital identity ecosystem

Strategic Objective 4.6: Develop a national strategy to strengthen our cyber workforce.

UK

(5 pillars) - 2022 to 2025

Pillar 1

UK cyber ecosystem - strengthening the UK's cyber ecosystem

Objective 2: Enhance and expand the nation's cyber skills at every level, including through a world-class and diverse cyber profession that inspires and equips future talent.

EU

(3 areas of EU action) - 2020 to 2027

Area 1

Resilience, technological sovereignty and leadership

1.8 A cyber-skilled EU workforce - increased efforts to upskill the workforce, attract and retain the best cyber security talent and invest in research and innovation that is open, competitive and based on excellence.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Foundational enabler 2

Grow a robust cyber talent pipeline

- Support youths, women, and mid-career professionals to pursue a cyber security career
- Create an upskilling culture for a globally competitive workforce
- Foster a dynamic sector with strong professional communities.

Foundational enabler 1

Develop a vibrant cyber security ecosystem

- Grow our cyber security market.

China

(9 strategic tasks) - 2016

Task 1

Resolutely defending sovereignty in cyberspace

Manage online activities within the scope of our country's sovereignty according to the Constitution, laws and regulations, protect the security of our country's information infrastructure and information resources, adopt all measures, including economic, administrative, scientific, technological, legal, diplomatic and military measures, to unwaveringly uphold our country's sovereignty in cyberspace. Resolutely oppose all actions to subvert our country's national regime or destroy our country's sovereignty through the network.

Task 7

Fostering innovation, web safety and talent

Implement the cyber security talent project, and strengthen the establishment of cyber security science majors, forge first-rate cyber security academies and innovation parks, and create an ecology and an environment beneficial to the fostering of talent, innovation and start-ups.develop cyber security defence means, timely discover and resist cyber intrusions, and cast a firm backup force to safeguard national cyber security.

Task 4

Strengthening the construction of online culture

HOW AUSTRALIA’S STRATEGY COMPARES WITH OTHER JURISDICTIONS

Australia

(6 cyber shields) - 2023 to 2030

Shield 6

Resilient region and global leadership

- Support a cyber resilient region as the partner of choice
- Shape, uphold and defend international cyber rules, norms and standards.

US

(5 pillars) - 2023 to FY26

Pillar 5

Forge international partnerships to pursue shared goals

Strategic Objective 5.1: Build coalitions to counter threats to our digital ecosystem

Strategic Objective 5.2: Strengthen international partner capacity

Strategic Objective 5.3: Expand US ability to assist allies and partners

Strategic Objective 5.4: Build coalitions to reinforce global norms of responsible state behaviour

Strategic Objective 5.5: Secure global supply chains for information, communications and operational technology products and services.

UK

(5 pillars) - 2022 to 2025

Pillar 4

Global leadership - advancing UK global leadership and influence for a secure and prosperous international order

Objective 1: Strengthen collective action and mutual cyber resilience - strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries

Objective 2: Shape global governance to promote a free, open, peaceful and secure cyberspace

Objective 3: Leverage and export UK cyber capabilities and expertise to boost our strategic advantage and promote our broader foreign policy and prosperity interests.

Singapore

(3 pillars and 2 foundational enablers) - 2021

Strategic pillar 3

Enhance international cyber cooperation

- Advance the development and implementation of voluntary, non-binding norms, which sit alongside international law
- Strengthen the global cyber security posture through capacity-building initiatives and the development of technical and interoperable cyber security standards
- Contribute to international efforts to combat cross-border cyber threats.

EU

(3 areas of EU action) - 2020 to 2027

Area 3

Advancing a global and open cyberspace through increased cooperation

3.1 EU leadership on standards, norms and frameworks in cyberspace - the EU will step up work with international partners to strengthen the rules-based global order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms online. It will advance international norms and standards that reflect these EU core values, by working with its international partners in the United Nations and other relevant fora

3.2 Cooperation with partners and the multi-stakeholder community - cyber dialogues with third countries, regional and international organisations as well as the multi-stakeholder community will be intensified. The EU will also form an EU Cyber Diplomacy Network around the world to promote its vision of cyberspace

3.3 Strengthening global capacities to increase global resilience - the EU will further strengthen its EU Cyber Diplomacy Toolbox and increase cyber capacity-building efforts to third countries by developing an EU External Cyber Capacity Building Agenda.

China

(9 strategic tasks) - 2016

Task 9

Strengthening international cooperation in cyberspace

On the basis of mutual respect and mutual trust, strengthen international cyberspace dialogue and cooperation, and promote the reform of the global internet governance system. Deepen bilateral and multilateral cyber security dialogues, exchanges and information communications with all countries, effectively manage and control differences, vigorously participate in cyber security cooperation in global and regional organisations, promote the internationalisation of the management of Internet addresses, domain name servers and other such basic resources.

Support the United Nations to play a leading role, promote the formulation of international norms for cyberspace that are universally recognised by all sides, and an international treaty on anti-terrorism in cyberspace, complete judicial assistance mechanisms to attack cyber crime, deepen international cooperation in areas such as policies and laws, technological innovation, standards and norms, emergency response, critical information infrastructure protection, etc.

Strengthen support and assistance to developing countries and backward regions to disseminate internet technology and construct infrastructure, and strive to close the digital divide. Promote the construction of “One Belt, One Road”, raise international telecommunications interconnection and interaction levels, and pave a smooth information silk road. Set up the World Internet Conference and other such global internet sharing and common governance platforms, and jointly promote the healthy development of the internet. Through vigorous and effective international cooperation, establish a multi-lateral, democratic and transparent international internet governance system, and jointly build a peaceful, secure, open, cooperative and orderly cyberspace.