SINGAPORE'S CYBERSECURITY STRATEGY 2026

SINGAPORE'S CYBERSECURITY STRATEGY 2026

CSA
SINGAPORE

CONTENTS

Acknowledgements	6
Foreword by Prime Minister	7
Chapter 1: Our Changing Landscape	10
Chapter 2: Singapore's Strategic Response	16
Chapter 3: Pillar 1 – Defend Critical Infrastructure	20
Chapter 4: Pillar 2 – Secure our Wider Cyberspace	26
Chapter 5: Pillar 3 – Strengthen Capabilities for AI and Quantum	34
Chapter 6: Pillar 4 – Enhance Resilience through Global Partnerships	42
Chapter 7: Enabler 1 – Build a World-Class Cybersecurity Ecosystem	48
Chapter 8: Enabler 2 – Level Up our Cyber Workforce	54
Chapter 9: Everyone Has a Role To Play	60

BUILDING A SECURE, TRUSTED AND RESILIENT DIGITAL FUTURE FOR SINGAPORE.

ACKNOWLEDGEMENTS

We would like to thank the following groups for their valuable input and support over the course of developing Singapore's Cybersecurity Strategy 2026:

Agencies

- Centre for Strategic Infocomm Technologies
- Defence Science and Technology Agency
- Digital and Intelligence Service
- Government Technology Agency of Singapore
- Home Team Science and Technology Agency
- Infocomm Media Development Authority
- Internal Security Department
- Ministry of Digital Development and Information
- Ministry of Defence
- Ministry of Home Affairs
- Singapore Police Force

Industry and Ecosystem Partners

- Amazon Web Services
- Booz Allen
- Cisco Systems, Inc.
- Cyber Security Awareness Alliance
- CyberSG TIG Collaboration Centre
- CyberSG R&D Programme Office
- Dragos, Inc.
- Ensign InfoSecurity Pte. Ltd.
- Ernst & Young Advisory Pte. Ltd.
- Google
- Microsoft Corporation
- Recorded Future
- Schneider Electric
- ST Engineering Info-Security Pte. Ltd.
- Zscaler, Inc.

Industry Associations

- Association of Information Security Professionals
- Centre for Strategic Cyberspace and International Studies
- Cloud Security Alliance Singapore Chapter
- Digital Defence Alliance Singapore
- ISACA Singapore Chapter
- ISC2 Singapore Chapter
- OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC)
- SGTech
- Singapore Computer Society
- The Law Society of Singapore

FOREWORD BY PRIME MINISTER

Singapore has embraced digital technologies to grow our economy, improve public services and create better opportunities for our people. Today, digital systems keep our essential services running and support the way we work and connect. But the more we depend on them, the greater the impact when things go wrong. That is why we have always taken cybersecurity seriously.

We launched our first Singapore Cybersecurity Strategy in 2016, bringing together efforts to protect essential services, build capabilities and strengthen international partnerships. We refreshed it in 2021 to extend our focus beyond critical infrastructure, and to grow our cybersecurity ecosystem and workforce.

Over the past decade, we have made steady progress. We have strengthened the resilience of our critical infrastructure and wider economy, deepened cooperation with industry and international partners, and more than doubled our cybersecurity workforce.

But the landscape continues to evolve. Cyber threats are becoming more frequent and sophisticated. AI is enabling attacks to be carried out at greater speed and scale, even as it becomes essential for cyber defence. Advances in quantum computing could eventually undermine today's encryption. Technology supply chains are becoming complex, spanning multiple jurisdictions. And even as international cooperation becomes more important, geopolitical tensions are making it harder to build trust.

The Singapore Cybersecurity Strategy 2026 sets out our next phase of work. We will strengthen our ability to detect risks earlier and act in a more coordinated way. We will move safeguards further upstream and build security into systems from the outset, so that organisations and users are better protected by default. We will develop the capabilities to use AI securely and effectively, prepare for quantum-enabled threats and deepen trusted partnerships at home and abroad. We will also continue to strengthen the ecosystem and workforce needed to sustain these efforts in the long term.

Cybersecurity cannot be the work of specialists alone. The Government will lead, but everyone has a part to play. Organisations must take responsibility for securing their systems and services. Technology providers must build security into their products from the start. And all of us must stay vigilant and practise good cyber habits. In an interconnected digital world, what each of us does affects the security of others.

By working together, we can keep Singapore's cyberspace secure, trusted and resilient, and continue harnessing technology with confidence – to improve lives and create new opportunities for our people.

Lawrence Wong
Prime Minister

STRATEGIC PILLARS

Defend Critical Infrastructure

Anticipate, detect, and defend against threats to our critical infrastructure

Strengthen national cyber defence

- Establish the National Cybersecurity Command Centre and Digital Defence Hub
- Review national concept of operations and legislation
- Strengthen national readiness through cyber exercises

Uplift the capabilities of Critical Information Infrastructure (CII) owners

- Enhance threat intelligence sharing, attack surface monitoring and threat detection
- Accelerate adoption of AI-enabled cyber defence capabilities
- Strengthen leadership and workforce capabilities

Secure our Wider Cyberspace

Protect upstream and make our digital environment safer by default

Protect upstream and build security by default

- Develop a national Protective Domain Name Service
- Set minimum requirements for higher-risk IoT devices

Disrupt scams and cybercrime

- Establish the SPF Cyber Command
- Develop National Scams List

Drive organisations to strengthen cybersecurity posture

- Raise cybersecurity standards for higher-risk organisations
- Explore cyber insurance pilots

Strengthen cyber-safe habits together

- Strengthen public-private partnerships

FOUNDATIONAL ENABLERS

Build a World-class Cybersecurity Ecosystem

Strengthen local capabilities while pursuing global competitiveness

Grow local capabilities from research to market

- Focus CyberBoost, CyberCall, and CyberGrowth on developing priority capabilities
- Explore a new bridging programme from early-stage research to product development

Accelerate capability building through co-development

- Launch two Signature Programmes in AI and OT security under the National Cyber R&D Programme
- Enhance national testbeds and infrastructure
- Strengthen industry-academia collaboration through CyberSG Consortium
- Attract leading international cybersecurity firms to Singapore

VISION: **A Secure, Trusted, and Resilient Cyberspace to Empower our Digital Way of Life**

Strengthen Capabilities for AI and Quantum

Secure the next technological frontier

Leverage AI to strengthen cyber defence

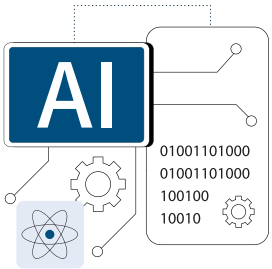
- Build expertise to use AI models for cybersecurity
- Promote adoption of AI tools for cyber defence

Enable secure adoption of AI

- Develop guidance for organisations to adopt AI securely

Prepare for quantum-enabled threats

- Accelerate national quantum-safe migration



Enhance Resilience through Global Partnerships

Collaborate and co-create with states and tech firms

Strengthen Singapore's position as a trusted convenor in cyber diplomacy

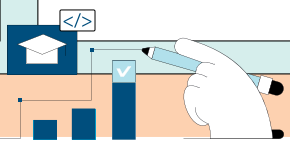
- Continue to organise the Singapore International Cyber Week
- Establish the Digital Defence Symposium

Advance rules-based cyber cooperation

- Support cybersecurity cooperation within ASEAN
- Support the Counter Ransomware Initiative

Partner major technology firms

- Provide a trusted testbed for experimentation of solutions
- Co-create solutions in priority areas



Level Up our Cyber Workforce

Professionalise and deepen the skills of cybersecurity practitioners

Professionalise cybersecurity workforce

- Establish a Cybersecurity Professional Accreditation Framework

Deepen cyber capabilities

- Synergise skills frameworks
- Support leadership development through the Cybersecurity Strategic Leadership Programme

Broaden Singapore's cyber talent pipeline

- Strengthen cybersecurity education and talent attraction through the SG Cyber Talent programme and Sentinel programme
- Equip full-time National Servicemen with cybersecurity skills and experience through the Cyber Work Learn Scheme
- Mobilise civilian cybersecurity expertise through Sectoral Cyber Defence Teams

CHAPTER 1

OUR CHANGING LANDSCAPE

Why Cybersecurity Matters

Cybersecurity is critical to our national security, economic growth, and public trust. We rely on digital systems to deliver essential services, power business growth, and communicate securely. Without cybersecurity, these systems are vulnerable to compromise or disruption, carrying serious consequences for Singapore.

Therefore, cybersecurity is no longer only about protecting systems from attack. It has become a strategic capability that enables Singapore to adopt emerging technologies confidently, preserve trust in our digital economy, and remain resilient in a more contested world. As Singapore pushes forward with its Smart Nation ambitions and embraces artificial intelligence (AI), cybersecurity will become ever more critical.

Since the launch of Singapore's Cybersecurity Strategy 2021, we have made significant progress in strengthening our national cybersecurity posture and reinforcing our position as a trusted digital hub. Together with industry and international partners, we have raised the resilience of our critical infrastructure and the wider economy, enhanced international cooperation on cybersecurity, developed a vibrant cybersecurity ecosystem, and nurtured a growing pipeline of cybersecurity talent.

However, the cyber threat landscape has evolved significantly in the past five years, and requires a refreshed approach.

A Changing Cyber Landscape

Four major developments have reshaped the cybersecurity landscape.

Cyber threats are becoming more severe

Cyber threats are growing in frequency and sophistication. Threat actors are operating with greater speed and scale, leveraging AI to conduct their attacks, while exploiting supply chain weaknesses and zero-day vulnerabilities to compromise organisations.

The nature of threats has shifted from opportunistic cybercrime to **persistent campaigns by Advanced Persistent Threat (APT) actors**[1] against Critical Information Infrastructure (CII). Between 2021 and 2024, suspected attacks by APT actors increased more than four-fold.

APT activity is also **shifting beyond espionage and data exfiltration towards pre-positioning for disruption**. This involves APT actors infiltrating critical infrastructure and remaining dormant for prolonged periods, waiting for an opportune time to launch an attack.

Operation CYBER GUARDIAN: A Turning Point in Singapore's Cyber Defence

In July 2025, the Government revealed that UNC3886, a sophisticated APT actor, was conducting attacks on high-value targets in Singapore[2].

In February 2026, the Government further revealed that UNC3886 had launched a deliberate campaign against Singapore's telcos, using a zero-day exploit and deploying advanced rootkits and other tools to gain limited access to CII systems.

Minister-in-charge of Cybersecurity Josephine Teo being briefed on Operation CYBER GUARDIAN

The Government mounted a coordinated response, **Operation CYBER GUARDIAN**, which prevented UNC3886 from gaining further access to our telco networks. This was Singapore's largest cyber response to date, bringing together more than 100 cyber defenders from government agencies in close partnership with the telcos.

This was a significant milestone in Singapore's cyber defence journey, making it clear that Singapore must be prepared for sustained campaigns by APT actors.

[1] APT actors are highly skilled, sophisticated and well-resourced cyber threat actors that typically act on State objectives and conduct targeted and sustained cyber operations to advance strategic objectives. Unlike opportunistic cybercriminals, APTs deliberately target high-value organisations and critical infrastructure, seeking to steal sensitive information, conduct espionage, or disrupt essential services.

[2] 'UNC' stands for 'uncategorised' and 'unclassified'. Industry experts have identified UNC3886 as a highly sophisticated threat actor, deploying advanced tools to compromise systems. The group has also been associated with attacks against critical entities such as defence, telcos, and technology organisations in the United States and Asia.

2 Disruptive technologies are transforming cybersecurity

AI represents one of the most revolutionary technological shifts in decades. It is transforming how we operate – automating complex tasks, improving productivity, and unlocking new forms of innovation. It is also reshaping the cybersecurity landscape. From a cybersecurity perspective, **AI plays three distinct roles – as a threat, a tool, and a target**.

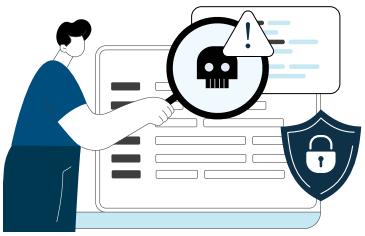
The "3Ts" of AI

AI as a threat

AI dramatically increases the speed, scale, and sophistication of cyberattacks. It does this by significantly compressing the time needed to turn software vulnerabilities into exploits, lowering the expertise needed to exploit specialised systems, and carrying out tasks autonomously with little human supervision needed. As agentic AI systems advance rapidly, they could be manipulated to circumvent safeguards, deceive users, or cause unintended actions, outpacing AI governance.

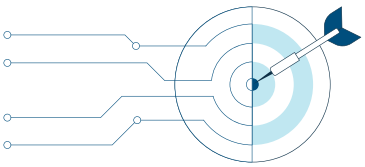
AI as a tool

AI can also strengthen cyber defence by enabling earlier threat and vulnerability detection, faster analysis, and more effective response. As the speed and scale of AI-enabled threats will overwhelm traditional cyber defences, AI is no longer optional but essential in cyber defence.



AI as a target

As AI becomes embedded across organisations and critical systems, it will increasingly become a target for cyberattacks. Vulnerabilities in AI systems could be exploited to manipulate their data and behaviour, undermining the security and reliability of systems that depend on them.



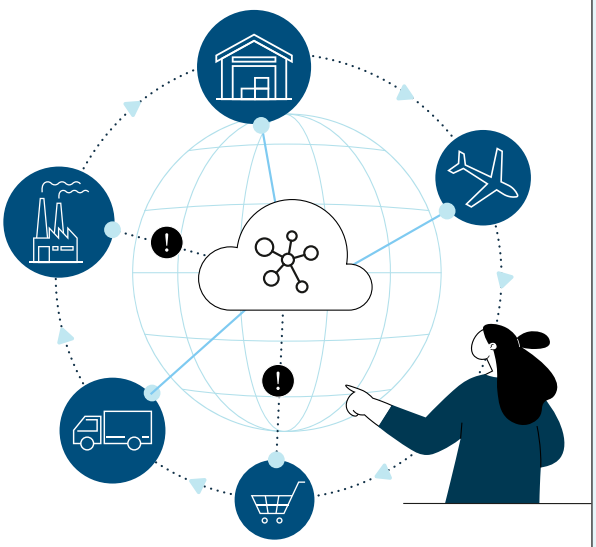
Looking ahead, advances in **quantum computing may render current encryption methods obsolete**, potentially exposing sensitive data and communications that are secure today. This makes an early transition to quantum-resistant cryptography critical, given the time required to upgrade systems and the risk that encrypted data stolen today could be decrypted in future.

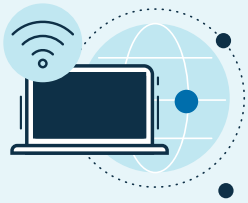
3 Technology dependencies are becoming more complex

Singapore's digital economy depends on interconnected technology supply chains. Organisations are relying more on cloud services, open-source software, AI models, and digital platforms developed across multiple jurisdictions.

While these technologies create significant opportunities, they introduce new dependency risks. Software vulnerabilities, compromised supply chains, and digital disruptions can have cascading consequences across sectors and national borders.

Singapore must therefore strengthen the resilience of our digital ecosystem by promoting secure-by-design principles, improving visibility over technology risks, and preserving access to technologies.





Building Resilience Against Digital Disruptions

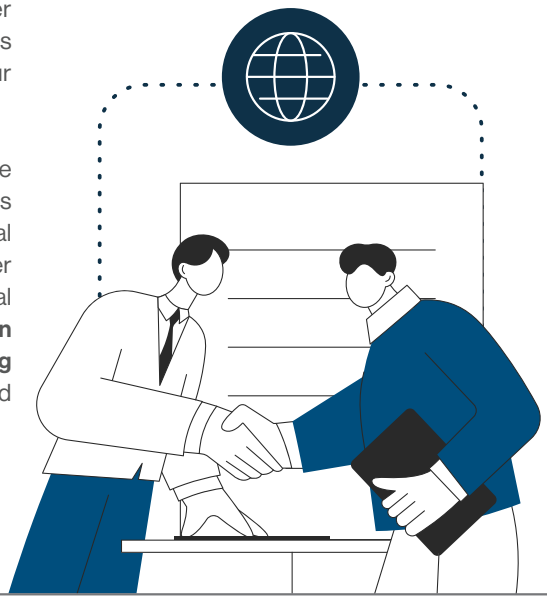
The **2024 CrowdStrike outage** demonstrated how a disruption to widely used technology can cascade across organisations and sectors. A faulty software update affected an estimated **8.5 million Windows devices globally,** disrupting airlines, airports, banks, healthcare providers, and other services. In Singapore, airline check-in systems were affected and more than **100 departing flights at Changi Airport were delayed.**

While not a cybersecurity incident, the disruption showed how failures in widely used technologies can cascade across organisations and sectors. Organisations must therefore have visibility of their technology dependencies, assess the risks they create, and put in place appropriate business continuity plans to remain resilient when, not if, disruptions occur.

International cooperation is becoming more important—and more challenging

Cyberspace transcends national borders. Cyber threats routinely originate outside Singapore's jurisdiction, while digital technologies connect our economy and society with the world.

Maintaining an open, secure, and interoperable digital environment requires strong partnerships between governments, industry and the international community. This is especially important at the frontier of technological innovation, where international regulations are still being shaped. Yet, **precisely when collective action matters most, trust is becoming harder to build** as technological competition and geopolitical tensions become more pronounced.



THESE DEVELOPMENTS REQUIRE SINGAPORE TO REFRESH OUR NATIONAL CYBERSECURITY STRATEGY

CHAPTER 2

SINGAPORE'S STRATEGIC RESPONSE

Singapore's Cybersecurity Strategy 2026 responds decisively to our rapidly evolving cyber landscape, building on the strong foundations established over the past decade. It reflects a shift from strengthening resilience alone towards proactively securing Singapore's digital future.

The Strategy is guided by a renewed vision:

A secure, trusted, and resilient cyberspace to empower our digital way of life.

Our Vision

A secure, trusted, and resilient cyberspace to empower our digital way of life.

Secure

Singapore must take a more proactive approach to cybersecurity – to anticipate, prevent, and disrupt threats before they disrupt critical systems. This means strengthening the protection of our critical infrastructure, securing emerging technologies and investing in advanced national cyber defence capabilities that keep pace with the evolving threat landscape.

Trusted

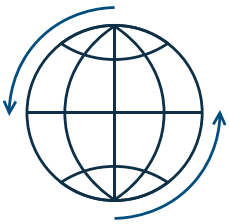
Trust underpins Singapore's digital economy. Citizens must have confidence that digital services are safe to use. Businesses must trust that they can innovate, invest, and operate securely. International partners must continue to view Singapore as a trusted location for technology development, digital trade and cross-border collaboration.

Maintaining this trust requires more than strong technology. It also depends on sound governance, responsible innovation, international cooperation, and a collective commitment to cybersecurity across Government, industry and society.

Resilient

No system can ever be completely immune from attack. Singapore must therefore ensure that our digital systems and essential services can **withstand disruption, respond effectively to incidents, and recover quickly** when attacks occur.

Resilience requires organisations to continuously strengthen their cyber posture, develop robust response capabilities, and recover quickly from incidents. At the national level, resilience also depends on strong partnerships, coordinated action, and the ability to adapt quickly as threats evolve.



Empower our Digital Way of Life

Cybersecurity enables Singapore to **embrace technology with confidence**. It allows businesses to transform and innovate, enables the secure adoption of emerging technologies, and strengthens Singapore's Smart Nation ambitions.

By building a secure, trusted, and resilient digital environment, cybersecurity enables technological innovation, economic growth, and better public services, while protecting our national security and the interests of citizens and businesses.

Our Response

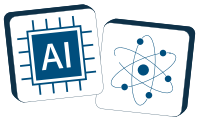
Guided by this vision, the Strategy sets out four strategic pillars:

Defend Critical Infrastructure

Strengthen the security of Singapore's critical infrastructure through proactive national cyber defence and uplifting our critical infrastructure's cyber posture against sophisticated threats.

Secure our Wider Cyberspace

Raise cyber resilience across organisations, businesses, and individuals through secure-by-design practices, stronger governance, and widespread adoption of good cyber hygiene.



Strengthen Capabilities for AI and Quantum

Secure emerging technologies while leveraging AI and other frontier technologies to strengthen Singapore's cyber defence capabilities and prepare for a quantum future.

Enhance Resilience through Global Partnerships

Strengthen international partnerships, deepen collaboration with industry, and contribute to an open, secure and interoperable cyberspace that enhances Singapore's resilience.

These pillars are underpinned by two foundational enablers:

Build a World-class Cybersecurity Ecosystem

Develop world-class cybersecurity capabilities by strengthening research, innovation, entrepreneurship, and industry partnerships that support Singapore's national interests.

Level Up our Cyber Workforce

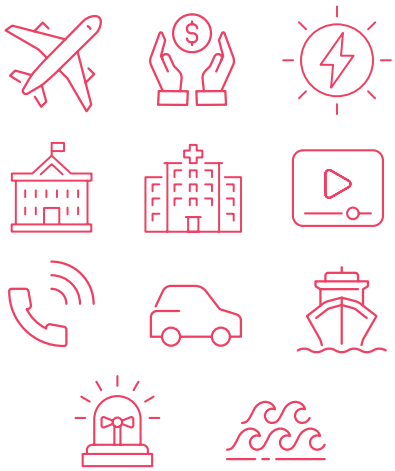
Build, attract, and continually develop a highly skilled cybersecurity workforce equipped to address increasingly sophisticated cyber threats and emerging technologies.

CHAPTER 3

PILLAR 1 – DEFEND CRITICAL INFRASTRUCTURE

Protecting Our Essential Services

Singapore's Critical Information Infrastructure (CII) provides the essential services that Singaporeans rely on every day—from electricity, water, and healthcare to banking, telecommunications, and transport. A successful cyberattack on our CII could disrupt these essential services. It could also steal sensitive data which could be used to undermine national security or public order. The Government must strengthen the cybersecurity of our CII, especially as these essential services become increasingly digital and interconnected.



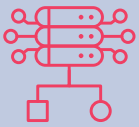
Critical Information Infrastructure in Singapore

CIIs are digital systems that support the delivery of essential services.

Today, CIIs have been identified from 11 critical sectors — Aviation, Banking and Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security and Emergency Services, and Water.

CSA works closely with sectoral agencies and CII owners to strengthen the cyber resilience of our CIIs.

Over the next five years, the Government will:



Strengthen national cyber defence through building centralised national cyber defence capabilities. This will allow us to anticipate emerging risks, detect malicious activity earlier, and disrupt cyber threats before they can compromise critical systems or disrupt essential services.

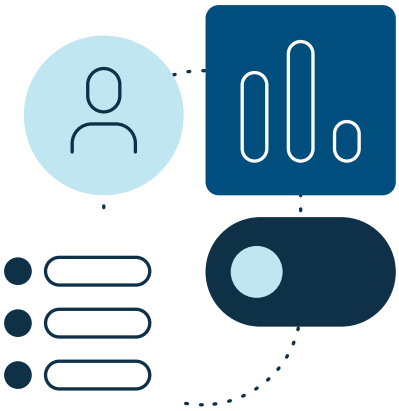
Uplift our CII owners' capabilities, so they can defend against APT-level and AI-enabled attacks. Organisations are the first line of defence and should continue to remain responsible for securing their own systems.

As Singapore faces a more dangerous cyber threat landscape, CII owners will need to ramp up their defences. The Government will lean forward by strengthening national cyber defence and supporting our CII owners in capability development.

Strengthen National Cyber Defence

Amid intensifying cyber threats, Singapore needs **stronger national capabilities** to enhance national cyber situational awareness, accelerate operational responses, and defend against sophisticated cyber threats.

Anchoring this effort is Cyber Security Agency of Singapore (CSA)'s **National Cybersecurity Command Centre (NC3)**. The NC3 will fuse cyber threat information across multiple sources to develop a comprehensive national cyber situational picture and facilitate national coordination of cyber operations.



The Centre for Strategic Infocomm Technologies (CSIT)'s **Digital Defence Hub (DDH)** supports Government agencies and CII owners in defending against sophisticated cyber threats such as Advanced Persistent Threats (APTs). It brings together deep technical expertise in cyber threat research, malware analysis, threat hunting, and red teaming to develop and deploy advanced cyber defence capabilities, while working closely with industry partners to co-develop new capabilities, exchange cyber threat intelligence, and strengthen Singapore's national digital defence.

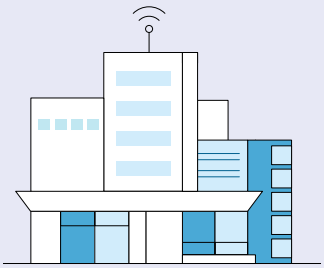
The Government will also review **our national concept of operations and legislative frameworks** to ensure they remain fit for purpose.

- On the concept of operations, the Government will explore how capabilities, processes and resources can be strengthened to **enable timelier, intelligence-driven action**.

- On legislation, the Government will ensure that cybersecurity standards keep pace with the evolving threat landscape. This includes strengthening the **Cybersecurity Act and Cybersecurity Code of Practice (CCoP)**, which set the baseline expected of all CII owners. The Government will also strengthen **sector-specific cybersecurity obligations** and move towards a more **continuous, risk-based approach to cyber supervision and assurance.**

- The Government will **review the powers required to enhance our national cybersecurity posture**, in particular the resilience of our systems, and to take pre-emptive action such as through proactive scanning and the takedown of malicious infrastructure.

The Government will continue to **organise national cyber exercises**. This includes the CSA-organised Exercise Cyber Star, and the Critical Infrastructure Defence Exercise (CIDeX) co-organised by CSA and Digital and Intelligence Service (DIS). These exercises strengthen the readiness of CII owners and Government agencies to detect, respond to, and recover from cyber incidents, including those affecting operational technology (OT) environments. **National cyber exercises bring together cyber defenders from across Government, critical sectors, and industry** to validate incident response plans, strengthen technical proficiency, improve operational coordination and reinforce information sharing under realistic attack scenarios.



National Cybersecurity Command Centre (NC3)

The Cyber Security Agency of Singapore (CSA) is building the NC3 as the nerve centre for national cyber defence operations.

It will fuse intelligence from Government, CII owners, commercial cybersecurity firms, and trusted international partners.

NC3 will help us better coordinate a national response to cyber threats, just like Operation CYBER GUARDIAN.

This will enable earlier detection of emerging threats, more informed assessments, and faster, more coordinated operational responses.

Uplift the Capabilities of our CII owners

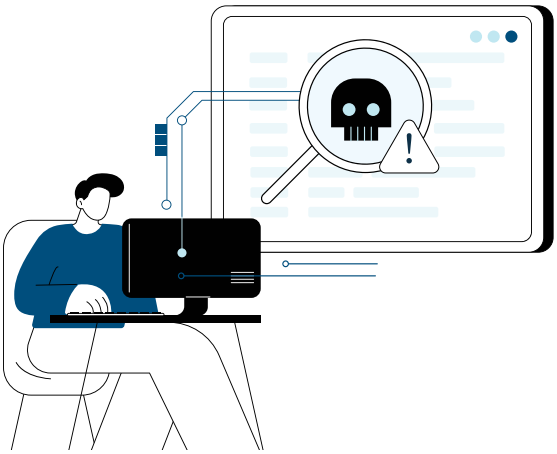
As APTs and AI-enabled threats become more sophisticated, CII owners must continually strengthen their organisational capabilities, readiness, and leadership to defend themselves.

Building Technical and Operational Capabilities

Traditional cyber defence has relied heavily on periodic assessments and reactive responses. APTs and AI-enabled threats demand a more proactive approach from CII owners to detect threats earlier, identify vulnerabilities before attackers do, and respond more quickly. This includes OT environments, where growing connectivity between operational systems, IT networks, and external parties is creating new attack paths and increasing the need for network visibility.

The Government will support CII owners in building up their threat detection, mitigation and response capabilities:

- The Government will **continue to share classified threat intelligence** with CII owners where it is operationally relevant to enable earlier awareness of emerging threats and support timely risk mitigation.

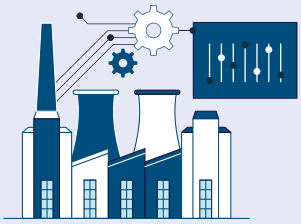


- The Government will **conduct attack surface monitoring of CII networks**, to help CII owners identify weaknesses before attackers do. The Government will also complement this with regular **security testing**, such as through piloting tools that continuously validate the effectiveness of CII owners' cybersecurity controls under simulated attack scenarios.

- The Government will **deploy a CSIT-developed threat detection system** in our CII owners to facilitate the detection of APT-level threats. The Government will also co-fund the adoption of **commercial network detection and response tools** for CII owners, where appropriate. This helps to create a cycle of two-way intelligence sharing, where CII owners benefit from the Government's threat insights while the Government gets greater visibility of threats observed across the critical sectors.

- The Government will work with industry and technology partners to **accelerate the adoption of AI-enabled cyber defence capabilities across critical sectors.** This includes **leveraging frontier AI models and model-agnostic AI harnesses** to strengthen vulnerability discovery, analyse large volumes of security data, prioritise remediation, and automate routine investigative tasks (see **Chapter 5** for more details).

Together, these investments **will strengthen CII owners' ability to detect, investigate, and respond to** increasingly sophisticated cyber threats more quickly, while enabling cyber defenders to focus on higher-value investigative and decision-making activities. The Government will facilitate the adoption of these capabilities, including providing funding support, where appropriate.



Securing Operational Technology Environments

Operational Technology (OT) systems, which control industrial operations and are typically harder to exploit due to their complexity, have become more vulnerable.

As OT systems become increasingly connected to IT networks, remote services and external vendors, their attack surfaces are expanding.

AI further lowers the barriers for threat actors to understand complex OT environments and identify vulnerabilities.

System owners can therefore **no longer rely on isolation or "security by obscurity"**. Securing OT also requires stronger visibility and clearer accountability across the technology lifecycle, not just relying on security-by-design. Manufacturers should build secure products and provide secure defaults, while system integrators and asset owners must ensure that OT systems are securely configured, deployed, operated and maintained.

Deepening Leadership and Workforce Capabilities

Effective cyber defence depends on capable leadership and a highly skilled cybersecurity workforce that keeps abreast of the latest tech developments.

The Government will continue working with CII owners to strengthen leadership and workforce capabilities at every level:

- CSA will **curate training offerings for CII owners board members and senior executives** to help them make informed decisions on cybersecurity risk, technology adoption, investment and accountability.
- CSA will also continue to support **leadership programmes for cybersecurity practitioners.** For instance, CSA partners **Singapore Management University** to deliver the **Cybersecurity Strategic Leadership Programme.** This aims to equip participants to effectively shape and uplift their organisations' cybersecurity posture and resolve cybersecurity challenges through innovation and partnership.

Please refer to **Chapter 8** for more details of workforce development initiatives.

CHAPTER 4

PILLAR 2 – SECURE OUR WIDER CYBERSPACE

Building a Safer and Trusted Cyberspace for Everyone

Every day, Singaporeans bank, shop, work, learn, and connect online. Businesses run on digital services, while homes and workplaces are filled with connected devices. These technologies make life easier, but they also expand the attack surface, giving threat actors more avenues to deceive users and launch cyberattacks.

Organisations and individuals face greater risks from phishing, scams, ransomware, and malware. From 2024 to 2025, the number of malware-infected systems detected more than doubled, from 117,300 to 284,300. The impact can also extend beyond the immediate victim.

Poorly secured devices and systems can be compromised and used as launchpads for attacks against other targets, including critical systems.

Singapore must raise the level of cybersecurity across our entire ecosystem, beyond just Critical Information Infrastructure (CII) owners.

Over the next five years, the Government will:

Protect upstream to minimise organisations' and individuals' exposure to cyber threats.

Drive organisations to strengthen their cybersecurity posture, beyond just voluntary adoption.

Equip Singaporeans with the knowledge to protect themselves online through **public education and outreach**.

Protect Upstream

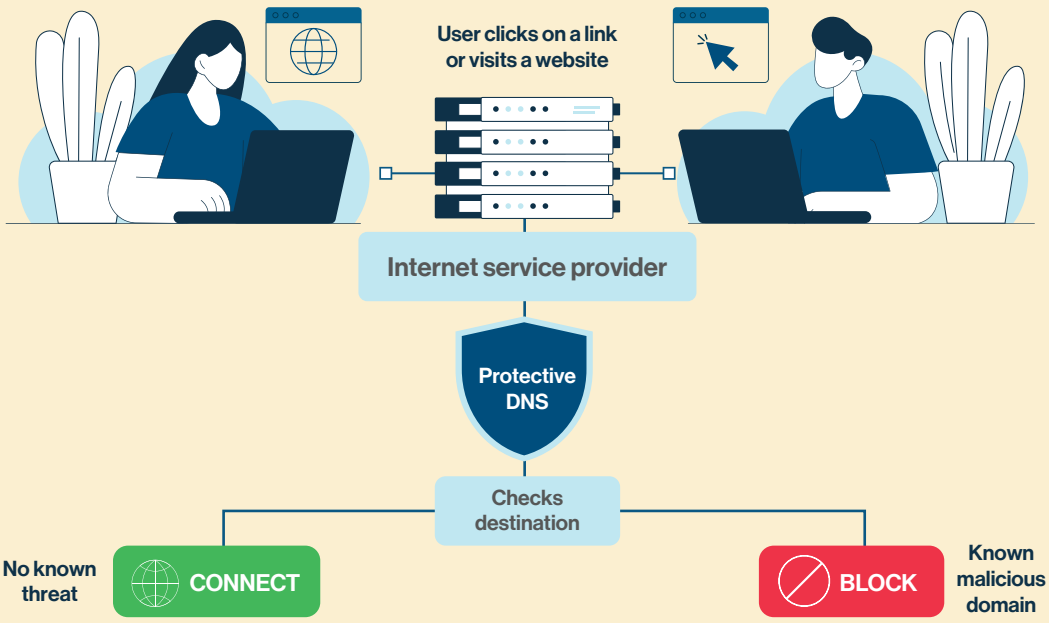
National-level Protections

The Government will strengthen upstream national-level protections to reduce cyber risks before they reach users.

- The Government will develop a **national Protective Domain Name Service (PDNS)**, which will provide a foundational layer of protection across Singapore's digital ecosystem by automatically blocking access to known malicious domains and reducing exposure to phishing, scams, malware, and other cyber threats before users interact with them.
- The Government will also strengthen our ability to detect and disrupt malicious websites at scale. **Singapore Police Force (SPF)'s Scam Analytics and Tactical Intervention System (SATIS)**, jointly developed with Home Team Science and Technology Agency (HTX) and Government Technology Agency of Singapore, uses AI and machine-learning capabilities to prioritise, evaluate, and disrupt scam sites. This helps to reduce public exposure to cyber-enabled harms before they reach more users.

Stopping Threats Before They Reach You

When you enter a website address or click a link, your device first needs to locate that website on the Internet. The **Protective Domain Name Service (PDNS)** acts at this point, checking the destination before connecting your device to it. If the destination is known to be malicious, the connection is stopped.



How PDNS serves upstream protection for users.

Build Security by Default

As Singapore deploys more Smart Nation projects, **cybersecurity must be built in from the start**. Initiatives like autonomous vehicle deployment can demonstrate how Singapore can adopt new technologies securely and confidently through a secure-by-default approach.

- The Government will identify the cybersecurity risks of novel technologies early, conduct threat analysis and risk assessments, and address gaps in existing standards where needed.

Connected devices are another important part of the wider digital ecosystem. Commonly used Internet of Things (IoT) devices, such as home routers and IP cameras, can become entry points into home and enterprise networks if they are not adequately secured. Compromised devices can also be harnessed into botnets to launch large-scale cyberattacks against other organisations and individuals.

- To strengthen the security of higher-risk IoT devices, the Government will set minimum standards for such devices under the **Cybersecurity Labelling Scheme (CLS)**. By end 2027, all home routers sold in Singapore must attain at least CLS Level 2. The Government is considering imposing a minimum CLS level for IP cameras, and will review how requirements can be extended to other IoT devices over time.

Disrupt Scams and Cybercrime

Scammers and cybercriminals move quickly. The Government must strengthen our ability to prevent, deter, and disrupt scams and cybercrime at scale.

- **The SPF Cyber Command** achieves this by bringing together SPF's anti-scam and cybercrime capabilities across operations, investigations, intelligence, and policy, enabling a more coordinated and effective response to cyber-enabled and cyber-dependent crime.
- SPF and HTX will develop the **National Scams List** to support the timely exchange of scam and cybercrime indicators between Government and industry partners, including banks, telcos, and digital service providers. This will allow malicious entities, scam enablers, and criminal infrastructure to be detected and disrupted more quickly across Singapore's digital ecosystem.

Singapore Police Force (SPF) Cyber Command

Established on 3 July 2026, the SPF Cyber Command will be the "tip of the spear" in Singapore's fight against scams and cybercrime, bringing together capabilities across operations, investigations, intelligence, and policy. This will enable SPF to act further upstream against malicious infrastructure, scam enablers, and criminal syndicates, while strengthening real-time detection and disruption, cybercrime investigations, cryptocurrency tracing and fund recovery, and coordination against transnational threat actors.

Prime Minister Lawrence Wong and Senior Minister of State for Home Affairs Goh Pei Ming visited the SPF Cyber Command, where they were briefed on Singapore's anti-scam strategy.

Drive Organisations to Strengthen their Cybersecurity Posture

Organisations are integral to Singapore's cyber resilience. As they become increasingly interconnected through digital services and supply chains, a compromise in one organisation can have cascading effects across the wider digital ecosystem, impacting other businesses and disrupting services.

The Government will take a systematic approach to raising cybersecurity across organisations: introducing targeted requirements where risks are higher, while providing practical support to help organisations strengthen their cybersecurity.

For higher-risk organisations, such as Government vendors that manage critical systems and sensitive data, the Government will **require the adoption of cyber standards commensurate with the risks they face** – for example, **the Cyber Essentials Mark (CEM), Cyber Trust Mark (CTM)**, and equivalent standards. The Government will explore appropriate regulatory levers to achieve this, such as procurement rules.

The Government will also continue to work with industry partners to **make cybersecurity support more accessible.** For instance, the Singapore Business Federation's Cyber Resilience Centre serves as a one-stop hub to help businesses strengthen their cyber resilience through workshops, system evaluations, cyber drills, and post-incident recovery support.

The Government will continue to **equip organisations with practical tools and support to uplift their own cybersecurity posture.** Initiatives such as **CISO-as-a-Service** and **Infocomm Media Development Authority (IMDA)'s SMEs Go Digital** platform provide expert guidance, funding support, and pre-approved cybersecurity solutions, helping organisations strengthen their defences more easily.

Beyond certification and support, organisations must also strengthen their ability to understand and manage risks and recover quickly from cyber incidents. The Government will **explore cyber insurance pilots** that encourage good cybersecurity practices while strengthening organisational resilience. Well-designed cyber insurance can improve cyber risk visibility, encourage stronger security controls, accelerate incident response, and support faster recovery following cyber incidents.

These efforts will help move Singapore from awareness to sustained adoption, making cybersecurity a more consistent part of organisational risk management, procurement, leadership, and operations.

Strengthening Cyber Resilience of Businesses

Established in October 2025, the **Cyber Resilience Centre (CRC)** — operated by the Singapore Business Federation (SBF) in partnership with Singapore Chinese Chamber of Commerce and Industry (SCCCI) and SGTech, and supported by CSA, serves as a central node to strengthen cyber defences and provide recovery assistance to organisations, particularly Small and Medium Enterprises (SMEs) when incidents occur.

The CRC offers a range of support, including cybersecurity health clinics and workshops, access to the CISO-as-a-Service programme, and cyber drills to build incident response capabilities. Since its inception, the CRC has supported close to 300 SMEs. A Cyber Incident Helpline will be launched in 2026.

By providing practical tools, expert guidance, and timely support, the CRC aims to strengthen the collective cyber resilience of Singapore's business ecosystem.

Cybersecurity Health Clinic in progress

Strengthen Cyber-Safe Habits Together

Individuals can do their part by staying vigilant and practising safe online habits.

The Government will drive national campaigns and targeted outreach to help different segments of society build safer digital habits. This will include broad-based public campaigns, as well as dedicated programmes for students and seniors.

Students from Jurong West Primary School taking part in the Be Cyber Safe Cyber Quest, an interactive trail where students navigate key cybersecurity concepts, from securing online accounts and safeguarding personal information, to staying safe online.

Industry and community partners also play an important role in reinforcing cyber awareness and helping individuals and organisations adopt good cyber practices.

The Government will **strengthen public-private partnerships to expand public outreach** and deepen awareness of cyber threats. This includes working with 3P (People, Public, Private) partners such as the Cyber Security Awareness Alliance (CSAA), whose members help promote good cybersecurity practices across organisations and the wider community.

[3] The three Cyber Tips are:
- Enable Two-Factor Authentication (2FA) and Use Strong Passphrases
- Update Software Promptly
- Add ScamShield and Anti-Virus Apps

Cyber Safe at Every Age

Jaga, the Cybersecurity Hedgehog

National Cybersecurity Campaigns promote simple, practical cyber-safe behaviours across the population. The latest **"Stop and Check"** campaign encourages people to take a cognitive break to pause and check if unsolicited requests and messages are genuine before acting. Fronted by Jaga, the Cybersecurity Hedgehog, the campaign also promotes CSA's three Cyber Tips[3] to stay safe online.

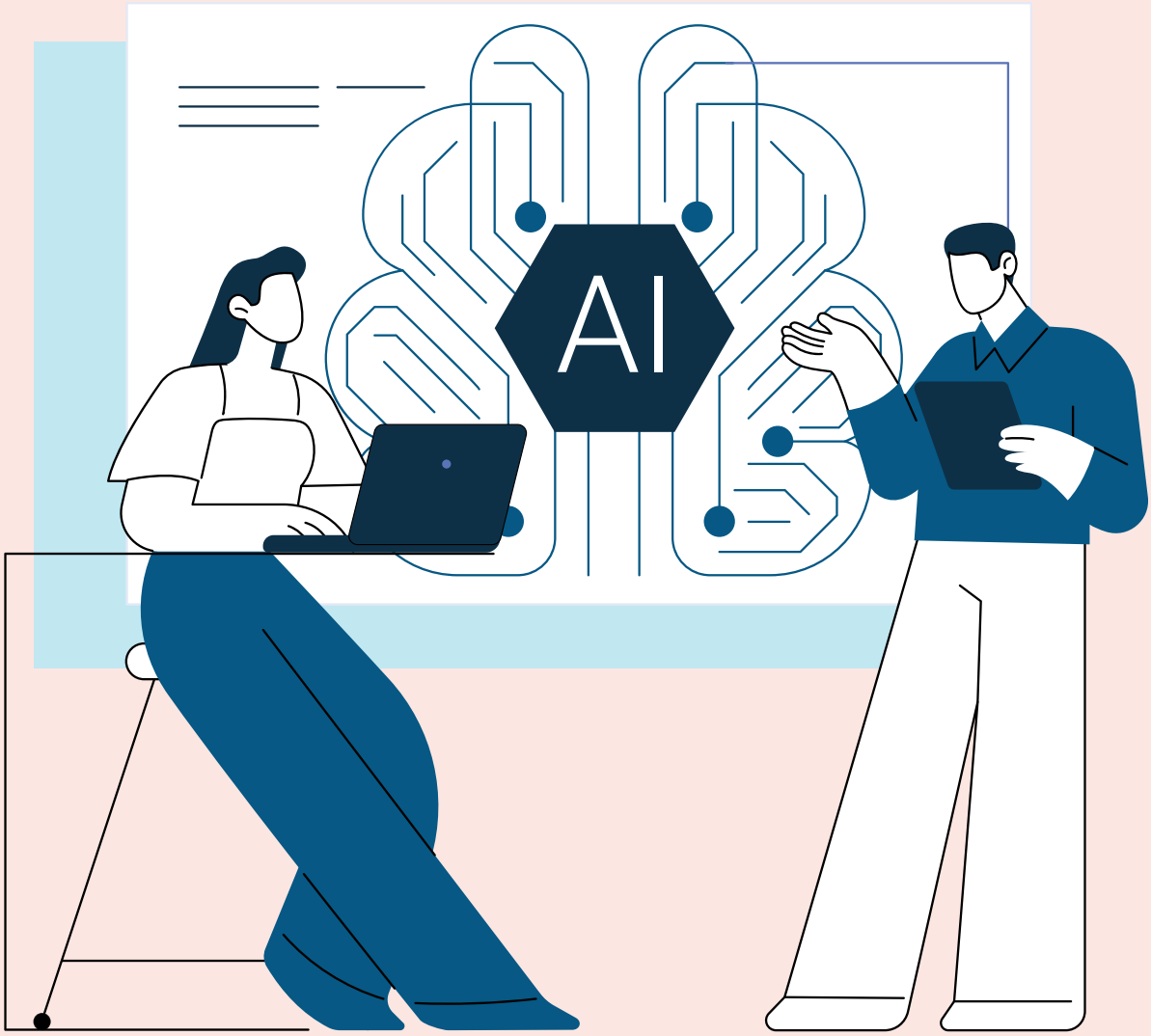
SG Cyber Safe Students Programme helps young people build good cyber habits through initiatives and resources developed with Ministry of Education and aligned with the school curriculum.

SG Cyber Safe Seniors Programme helps seniors use digital services safely through guided learning and community outreach, working with partners across the public, private, and community sectors. Be Cyber Safe workshops are conducted in the community with various partners including Infocomm Media Development Authority (IMDA)'s SG Digital Office, Central Provident Fund Board, and banks with the support of student volunteers from various Institutes of Higher Learning. Digital skills and online safety tips are also taught by IMDA's SG Digital Ambassadors at community hubs. The initiatives have reached more than 253,000 seniors over the past five years.

Together, these efforts will make Singapore's digital ecosystem safer by default, reducing exposure to cyber threats, strengthening cybersecurity across organisations, and helping everyone stay safe online. This will enable Singaporeans and businesses to embrace our digital future with greater confidence.

CHAPTER 5

PILLAR 3 – STRENGTHEN CAPABILITIES FOR AI AND QUANTUM



Harnessing and Securing Disruptive Technologies

Disruptive technologies such as **AI and quantum computing** are reshaping cybersecurity. AI can strengthen cyber defence, but can also enable malicious actors to conduct faster and more sophisticated attacks. As AI becomes embedded in critical systems and business processes, AI systems themselves must also be secured. Advances in quantum computing could similarly create new security risks.

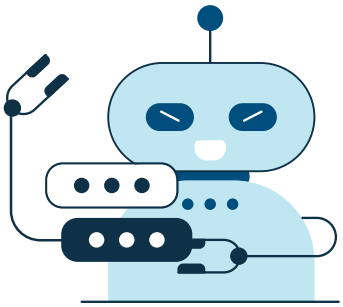
Over the next five years, the Government will:

Leverage AI to strengthen cyber defence.

Support the secure adoption of AI.

Prepare upstream for quantum-enabled threats.

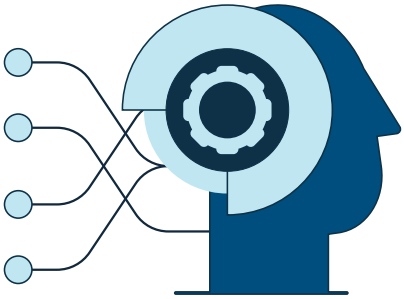
Leverage AI to Strengthen Cyber Defence



Cyber defenders will need to use AI effectively to keep pace with AI-enabled threats. AI can significantly enhance the **identification of threats** through rapid analysis of threat intelligence; the **detection of threats** through analysing large volumes of alerts and telemetry to surface malicious activity and reduce false positives; and **incident response** by accelerating digital forensics and analysing evidence at scale to shorten investigation timelines.

The Government will pursue three complementary approaches.

First, the Government will invest in building the expertise and capabilities needed to use leading AI models securely for cyber defence.

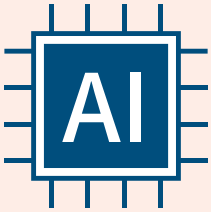


Within Government, Cyber Security Agency of Singapore (CSA) and Government Technology Agency of Singapore (GovTech) will **build expertise to evaluate, adapt, and securely operate AI systems for cybersecurity**. This will enable us to select suitable models, integrate them into operational workflows, and remain agile as AI technologies continue to evolve.

The Government will continue to deepen partnerships with leading technology companies, research institutions, and international partners to access advanced AI capabilities, keep pace with frontier developments, and accelerate their secure adoption for cyber defence.

Second, the Government will invest in AI harness engineering as a strategic capability.

Singapore will take a pragmatic approach. Rather than investing in developing frontier AI models, the Government will focus on building the capabilities needed to securely **deploy, integrate, and operate the best available models for our operational needs**. This provides enduring value regardless of which foundation models emerge as market leaders.



What is an AI harness?

AI harnesses comprise the software, workflows, and orchestration layers that transform one or more AI models into operational cyber capabilities. These harnesses determine how AI models interact with users, tools, enterprise systems, and operational workflows. They also provide important safeguards, evaluation mechanisms, and governance that enable AI systems to be used safely and effectively.

GovTech's Vanguard is one example of an AI harness. It orchestrates AI agents to identify software vulnerabilities, validate findings independently, and recommend practical fixes, enabling faster and more reliable code security reviews while remaining adaptable as AI models improve.

Third, the Government will promote the adoption of AI cyber defence tools within the wider cybersecurity ecosystem. The Government will lead by example through early adoption of AI-enabled cybersecurity capabilities. Successful operational use within Government will provide practical lessons that can subsequently be shared with CII owners and the wider cybersecurity ecosystem.

The Government will progressively deploy AI across our national cyber defence operations, including within the National Cybersecurity Command Centre (NC3) and Government Cyber Security Operations Centre (GCSOC), to strengthen how the Government identifies, detects, and responds to cyber threats.

Government agencies are already applying AI across a range of cybersecurity functions.

Government-Developed AI Tools for Cyber Defence

AEGIS is CSA's AI-powered attack surface scouting tool that discovers and maps exposed assets and vulnerabilities, including unknown and shadow assets. It investigates and correlates these findings to build a **holistic view of an organisation's external attack surface**, helping defenders identify and address exposure before attackers can exploit it.

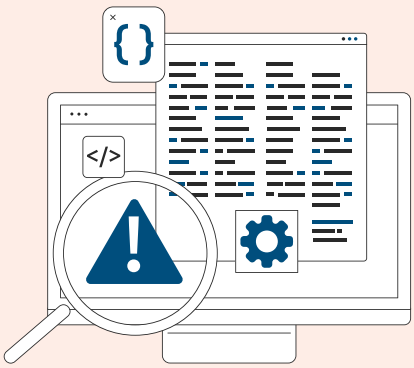
JEWEL is CSA's AI-assisted web testing specialist for expert-led testing of complex vulnerabilities in web applications. It combines AI assistance with human expertise to test application workflows, user roles, and business logic, helping to uncover issues that automated scanners may miss. This enables cybersecurity specialists to **steer AI towards areas of concern and investigate potential issues more efficiently**, while retaining oversight of the testing process.

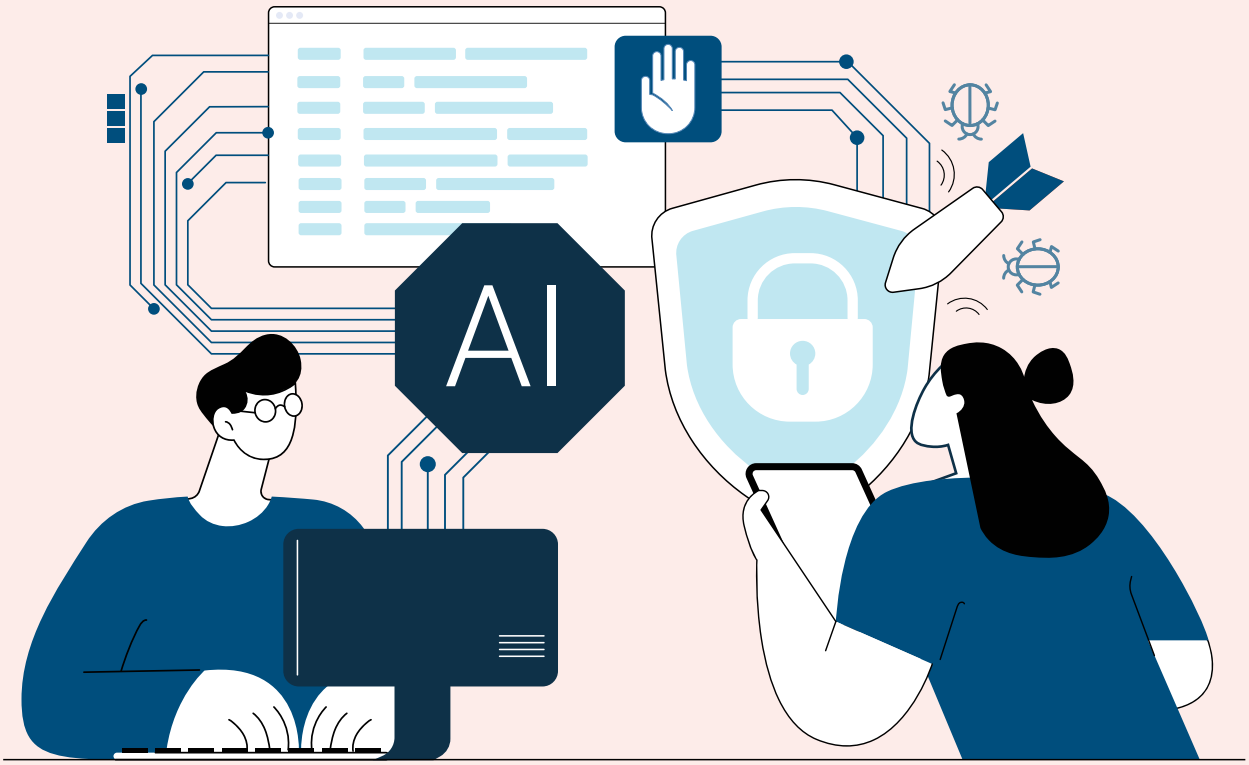
MAIA is GovTech's AI-assisted penetration testing capability that leverages AI agents to accelerate vulnerability discovery within Government systems, helping defenders identify and remediate weaknesses before attackers can exploit them. It also **strengthens Singapore's sovereign AI cybersecurity capabilities and reduces dependence on any single AI provider**, enhancing resilience in an increasingly complex global landscape.

AEGIS, MAIA, and JEWEL complement each other by helping teams discover exposed systems, automate vulnerability testing at scale, and carry out deeper expert-guided testing where needed. Together, they enable cybersecurity teams to assess significantly more systems than traditional approaches.

AETHER is Centre for Strategic Infocomm Technologies (CSIT)'s malware analysis tool that uses AI to automate complex and time-consuming analysis tasks, helping cybersecurity experts analyse malware faster and more accurately. **AETHER has been made open source, making advanced malware analysis more accessible to the wider cybersecurity community.**

The Digital and Intelligence Service (DIS)'s **Cyber Defence Test and Experimentation Centre (CyTEC)** provides a high-fidelity environment for **developing, testing and validating AI-enabled cybersecurity capabilities**. It has demonstrated the use of AI agents in digital forensics to accelerate anomaly detection, investigative analysis, and other labour-intensive forensic tasks.





The Government will also support wider adoption of AI-enabled cybersecurity capabilities across organisations, with priority given to Critical Information Infrastructure (CII) owners. This includes providing funding support through initiatives such as the **AI for Cyber Experimentation Sandbox,** making Government-developed tools and AI harnesses available where appropriate, publishing practical guidance, and potentially recommending suitable AI-enabled cybersecurity tools to accelerate adoption of proven capabilities.

The Government will also support CII owners and other organisations in building AI capabilities for cybersecurity through training, technical guidance, and opportunities for practical experimentation. These efforts will strengthen the cybersecurity workforce and help organisations confidently adopt AI in cyber operations (see **Chapter 8**).

Support the Secure Adoption of AI

AI is not only a tool for defenders – it is also a technology that must be secured.

AI systems face a growing range of cybersecurity threats. These include data poisoning and adversarial attacks that can exfiltrate sensitive data or provide a pathway into connected systems. These risks will become more complex and potentially more severe as agentic AI systems become more autonomous, interact with other AI agents, and operate across multiple systems. These risks can undermine the security, reliability, and trustworthiness of AI, particularly as it is deployed in critical sectors.

The Government will enable the secure adoption of AI by developing baseline security requirements and practical implementation guidance that organisations can confidently adopt.

- **The Government will lead by example in adopting AI securely.** Singapore will adopt a risk-based, defence-in-depth approach to AI adoption, calibrated to the sensitivity of the data and impact of the use case. Higher-risk deployments, such as those involving classified data, public-facing systems or agentic capabilities, require stronger controls, safety testing, and guardrails. The intent is that digital transformation is matched by a robust security posture that protects trust at every layer, which in turn enables our agencies to innovate with confidence.

- **The Government will provide practical guidance for the wider ecosystem.** CSA will develop practical guidance and implementation resources that enable organisations to adopt AI securely across the entire development and deployment lifecycle. As AI technologies continue to evolve, Singapore will regularly review and update its guidance to address new risks, including those arising from increasingly autonomous AI systems and emerging AI architectures.

Government Resources on Securing AI

1. **Guidelines and Companion Guide on Securing AI Systems** – Published in 2024, the Guidelines and Companion Guide on Securing AI Systems were developed to help organisations adopt AI in a secure manner. The Guidelines lay out the foundational security principles for system owners to secure the use of AI throughout its lifecycle. The Companion Guide complements the Guidelines and provides practical measures and controls that system owners may consider as part of implementing the guidelines.

2. **Addendum on Securing Agentic AI** – Published in June 2026, the Addendum outlines how risks can be identified and assessed based on the capabilities of Agentic AI systems, and provides practical controls to mitigate relevant risks across the development lifecycle.

3. **TR 147: Cybersecurity Practices for Large Language Model (LLM) Applications** – Published in June 2026, TR 147 provides practical cybersecurity practices for organisations developing, deploying, integrating or maintaining LLM-based systems, whether in-house or through third-party providers. It adopts a structured, lifecycle-based approach to identifying, assessing, and mitigating cybersecurity risks across the development and operational stages of LLM systems. To support practical implementation, TR 147 includes illustrative examples such as an internal coding assistant, an enterprise knowledge agent, and a national healthcare chatbot. TR 147 is designed to be adapted to different operational contexts, enabling organisations to incorporate LLM-specific cybersecurity practices into their AI risk management and governance frameworks.

Prepare Upstream for Quantum-Enabled Threats

Advances in quantum computing may put today's encryption methods at risk and challenge current cybersecurity assumptions.

The Government will accelerate national quantum-safe migration by working with industry, sector leads, and public agencies to plan, prioritise, and execute the transition. This includes setting timelines for migration planning, publishing practical guidance and support for organisations, and coordinating implementation across Government and sectors. Beyond these systems, the Government will raise awareness among organisations on the potential impact of the quantum threat and the need to undertake migration.

The Government has issued guidance to CII owners, setting out three milestones, which are aligned with international references.

By 31 March 2027

Submit quantum-safe migration plans to CSA.

From 1 January 2028

Factor quantum-safe considerations into the procurement and implementation of new CII systems.

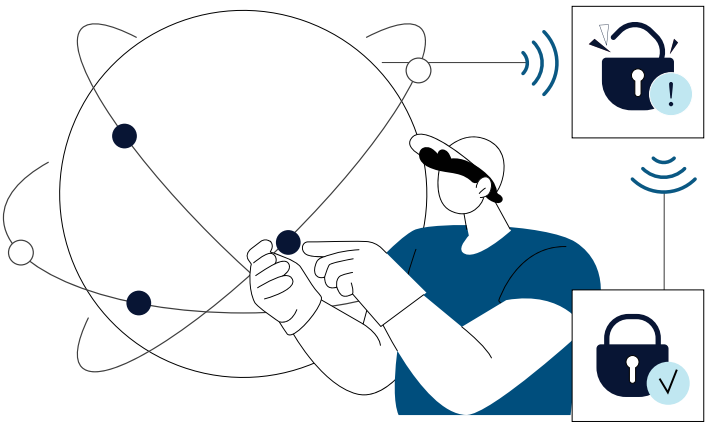
By 31 December 2031

Complete quantum-safe migration for CII systems.

- While these requirements apply specifically to CII owners, other organisations exposed to quantum risks are encouraged to complete migration by 2035. This timeline provides organisations with a realistic planning horizon for what will be a multi-year transition. The Government will progressively issue targeted guidance to equip organisations with clear pathways to meet these milestones.

- To support this transition, the Government will continue developing and updating practical resources such as the **Quantum-Safe Handbook** and **Quantum Readiness Index**. The Government is exploring funding and training support to help organisations build experience and kickstart quantum-safe migration.

By investing early, Singapore can remain resilient against future technology-enabled cyber threats while continuing to embrace innovation with confidence.



CHAPTER 6

PILLAR 4 – ENHANCE RESILIENCE THROUGH GLOBAL PARTNERSHIPS

Strengthen Singapore's Position in a Fragmented Digital World

The global digital landscape is becoming more fragmented as major powers seek to develop their own technology ecosystems and exert greater control over their frontier technologies, especially in AI. Small states like Singapore will find it more challenging to preserve neutrality and the policy space to choose between technology systems.

At the same time, the rules-based multilateral order is fraying, making it more difficult to forge international consensus and cooperation in the cyber domain. Singapore must continue to invest in international cybersecurity cooperation – advancing norms of responsible behaviour in cyberspace, and strengthening collective action against cross-border threats.

We must build up our resilience by enhancing our global partnerships. These must go beyond states.

The Government will deepen collaboration with major technology firms and other non-state actors which already wield significant influence in the digital landscape, and will grow in heft amidst weaker multilateralism.

Over the next five years, the Government will:

Secure Singapore's position as a trusted convenor in cyber diplomacy.

Advance rules-based cyber cooperation.

Partner major technology firms to co-create solutions.

Secure Singapore's Position as a Trusted Convenor in Cyber Diplomacy

In the past decade, Singapore has built a reputation for fostering international engagement across different blocs on cyber issues.

- The Government will continue to organise the **Singapore International Cyber Week (SICW)** annually. SICW has established itself as a premier international forum for bringing together governments, industry, researchers, and civil society to tackle emerging cyber challenges. SICW will remain a **non-partisan and inclusive forum** that can bring together diverse perspectives across different blocs and facilitate international dialogue on contentious issues.

- The Government will also work to establish the **Digital Defence Symposium (DDS)** as a key defence platform for senior defence officials, academics, industry experts, and international partners from Association of Southeast Asian Nations (ASEAN) and key partner nations, to discuss common digital and information security challenges in the defence sector.

Singapore International Cyber Week (SICW)

Since its debut in 2016, the SICW has grown into a premier cybersecurity event both in Asia and internationally for governments, industry, academia, and international organisations. In 2025, over 13,000 delegates from more than 90 countries and regions attended.

SICW will continue to be an inclusive and non-partisan forum where difficult issues can be discussed candidly, new partnerships can be formed, and practical initiatives can be launched.

In 2026, the SICW Ministerial Roundtable will be organised for the first time, bringing together Ministers, senior government officials, and industry leaders in a closed-door setting for candid discussions on emerging cyber and digital security challenges.

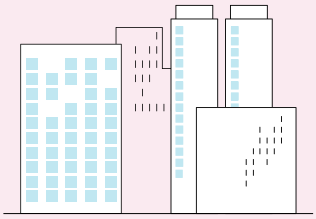
Advance Rules-Based Cyber Cooperation

Singapore will maintain its commitment to advance rules-based cyber cooperation through multilateral and plurilateral platforms. This means contributing to norms, standards, and practical initiatives that support responsible behaviour in cyberspace, while also helping to raise the global cybersecurity baseline.

A priority is to work through the ASEAN to advance initiatives that support regional cooperation on cybersecurity and future technologies, including cyber-related deliverables for Singapore's 2027 ASEAN Chairmanship. These initiatives would strengthen regional cyber resilience and capabilities in the face of current and emerging threats.

- Since 2018, Singapore has invested $30 million in the **ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)**. We will continue to support the ASCCE.

Singapore is also an active member of the **Counter Ransomware Initiative (CRI)**. Established in 2021, the CRI is a multilateral platform that brings together over 70 countries and organisations. The CRI efforts are led by a steering committee comprising Australia, Germany, Singapore, the United Kingdom, and the United States. The CRI is dedicated to fostering international collaboration to combat ransomware, including through practical cooperation, the sharing of best practices, and the development of common frameworks to strengthen collective resilience against ransomware threats. Singapore hosted the CRI Summit in conjunction with the SICW in 2025 and 2026.



Singapore as a Trusted Regional Cybersecurity Capacity Building Hub

Since 2017, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) has delivered 83 programmes for more than 2,200 participants from 101 countries and partnered 33 international and multi-stakeholder partners, providing training, research, and cyber defence exercises for ASEAN member states.

The ASCCE fulfils three main functions:

- Conduct research and provide training in areas spanning international law, cyber strategy, legislation, cyber norms, and other cybersecurity policy issues.
- Provide Computer Emergency Response Team (CERT)-related technical training and facilitate the exchange of open source information and best practices.
- Conduct virtual cyber defence training and exercises.

ASCCE will continue to refresh Singapore's capacity-building offerings to address emerging cybersecurity priorities and deliver more targeted, high-quality, and demand-driven programmes.

Partner Major Technology Firms to Co-Create Solutions

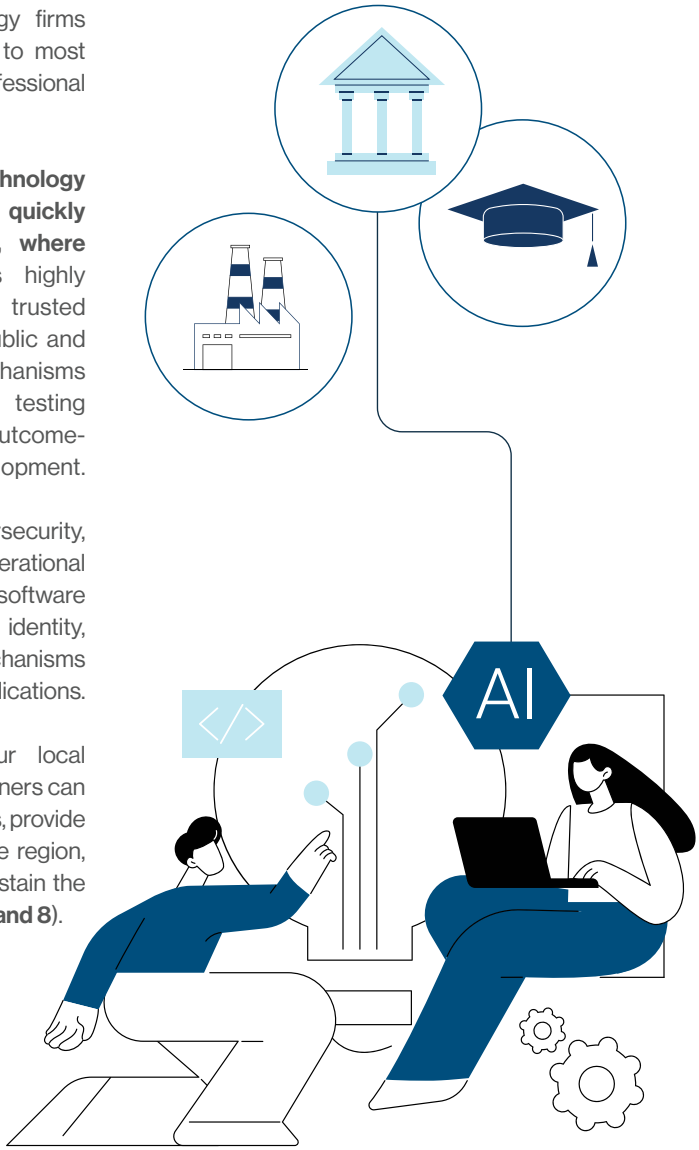
Major technology firms, global cybersecurity companies, and research partners have capabilities, telemetry, and technical expertise that are essential to addressing modern cyber threats.

The private sector owns and operates much of the infrastructure, platforms, software, and data that shape cybersecurity outcomes. Leading technology firms can observe threats at a scale unavailable to most governments, while researchers and professional communities often identify emerging risks first.

- **The Government will work with technology partners to move promising ideas quickly from concept to controlled trial and, where effective, to deployment.** Singapore's highly digitalised environment can serve as a trusted testbed for solutions that address real public and national security needs. Suitable mechanisms include regulatory sandboxes, shared testing environments, innovation challenges, outcome-based procurement, and joint product development.

- Priority areas will include AI-enabled cybersecurity, the security of agentic AI, protection of operational technology (OT), cloud resilience, software supply-chain assurance, secure digital identity, quantum-safe migration, and mechanisms to reduce scams and malicious applications.

These firms can also contribute to our local cybersecurity ecosystem. Global industry partners can partner the Government to, among other things, provide capacity building in Singapore and across the region, co-develop standards, and raise, train, and sustain the cybersecurity talent required (see **Chapters 7 and 8**).



Partnering for Cyber

The Singapore Government will collaborate with industry partners to co-create solutions. In 2023, Google worked with Cyber Security Agency of Singapore (CSA) to pilot **Google Play Protect**, which serves to keep Google Play and Android app ecosystems safe by automatically scanning every application on Android devices, regardless of the source, for malicious behaviour, helping to protect users against malware, harmful applications, and financial fraud. As of August 2026, in Singapore, Google Play Protect has blocked more than 68,000 apps from being potentially misused for financial fraud and scams. Google Play Protect has also blocked more than 3.34 million installation attempts of potentially malicious applications across 774,000 devices, warning users or blocking the app to neutralise the threat.

To support CSA's capacity building efforts in ASEAN, CSA and Microsoft co-hosted the inaugural **ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)-Microsoft Cybersecurity Roundtable** in June 2025. The Roundtable contributed to regional efforts in addressing cyber threats by providing valuable insights and perspectives from both the public and private sectors. With the success of the inaugural roundtable, CSA and Microsoft agreed at Singapore International Cyber Week (SICW) 2025 to conduct the Roundtables annually for up to two years.

CSA also worked with Cloud Service Providers (CSPs) — Amazon Web Services, Microsoft Azure, and Google Cloud — to co-develop CSP-specific guides to the **Cybersecurity Code of Practice for Cloud Services**, or "CCoP (Cloud)". The CCoP (Cloud) establishes cybersecurity requirements governing the secure deployment, operation, and management of Critical Information Infrastructure (CII) systems hosted on the cloud. CSP-specific guides are intended to help CII owners reduce compliance burden and uncertainty by giving them a set of outcome-based, explicit, actionable, and cloud-centric controls.

Participants of the 2026 edition of the ASCCE - Microsoft Roundtable

CHAPTER 7

ENABLER 1 – BUILD A WORLD-CLASS CYBERSECURITY ECOSYSTEM

Building the Capabilities Singapore Needs

Singapore has made significant progress in developing a vibrant cybersecurity ecosystem over the past decade, with nearly five-fold growth in our cybersecurity market from $570 million in 2015 to $2.7 billion in 2024. By 2030, Singapore's market size is expected to reach approximately $5 billion[4]. These efforts have helped position Singapore as a trusted cyber hub and supported the growth of Made-in-Singapore cybersecurity products and services. This has also created new economic opportunities and jobs.

In the next bound of industry growth, the Government will focus on establishing Singapore as **Asia's leading innovation hub**, where globally competitive and trusted cybersecurity capabilities for critical infrastructure are built, validated, and deployed.

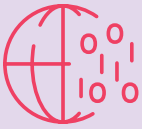
[4] Deloitte's Cybersecurity Landscape Study 2025

The Government aims to develop **stronger local capabilities for national resilience** amidst greater geopolitical contestation in the tech domain. The Government will also continue to pursue **global competitiveness**, recognising that commercial success is essential to sustaining our ecosystem.

A key shift is to move from broad-based industry support to a **targeted capability-driven strategy,** focussed on capabilities that meet national security objectives and emerging strategic technologies.

Over the next five years, the Government will:

Grow local capabilities from research to market.



Accelerate capability building through co-development.

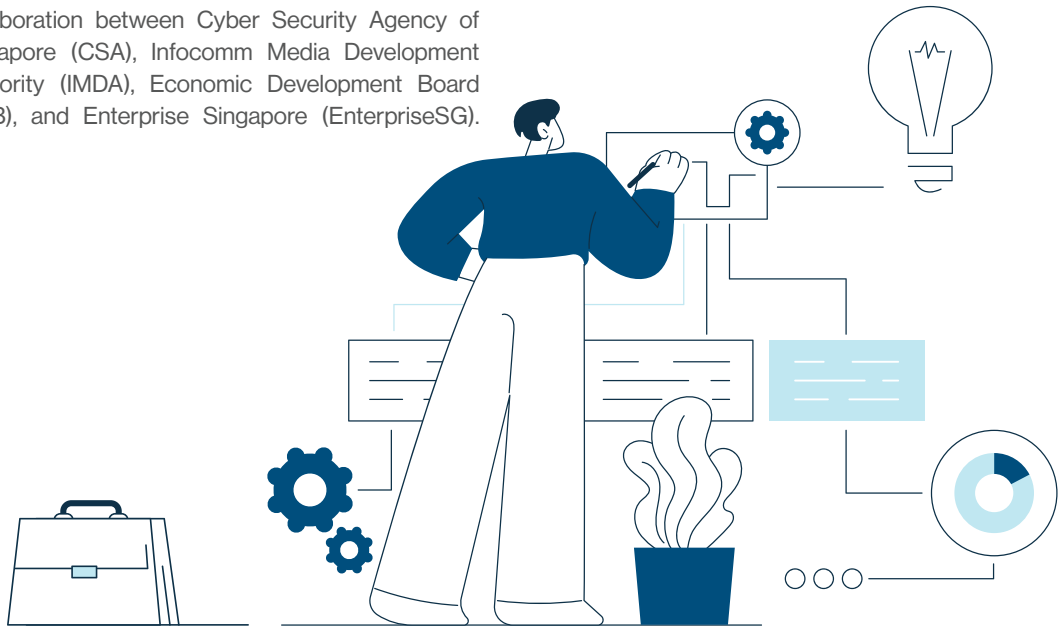
Grow Local Capabilities from Research to Market

The Government will strengthen pathways that translate research into practical capabilities that benefit industry, Government, and the wider economy.

- Today, the **CyberSG R&D Programme Office (CRPO) Grant Call** supports early-stage research, while CyberCall supports product development. The Government will explore a new bridging programme that supports translation from the former to the latter.

The Government will also strengthen support for cybersecurity entrepreneurs and companies across their venture journey, with a focus on developing strategic cybersecurity capabilities.

- The Government will focus existing programmes under the **CyberSG Talent, Innovation and Growth Collaboration Centre (TIG Centre)** – such as **CyberBoost, CyberCall,** and **CyberGrowth** – on priority capabilities including AI-enabled security and quantum-safe migration. The enhanced programmes will provide more targeted support for companies developing solutions in these areas, including commercialisation, enterprise scaling, and overseas expansion. This effort will involve collaboration between Cyber Security Agency of Singapore (CSA), Infocomm Media Development Authority (IMDA), Economic Development Board (EDB), and Enterprise Singapore (EnterpriseSG).
- The Government will help Singapore-based companies grow globally by connecting them with investors, customers, and technology partners, providing opportunities for mentorship and expert guidance to bring their products to market faster, and opening doors to international markets through business missions and global industry events.
- Beyond ongoing cyber community building efforts, the TIG Centre will introduce a new **CyberSG CISO Advisory Committee,** comprising senior cybersecurity leaders from Critical Information Infrastructure (CII) sectors, government agencies, academia, and industry. The Committee will help startups, researchers, and ecosystem partners better align innovation with real-world industry needs, adoption barriers, and future capability gaps. Thematic community workshops and networking opportunities focussing on prioritised capability areas will also be organised to strengthen collaboration and knowledge-sharing across the ecosystem.



Growing Cyber Companies from Singapore

The Government supports cybersecurity companies from innovation to international growth through programmes tailored to different stages of their journey.

CyberBoost

Helps cybersecurity companies become ready to grow and scale through tailored support.

Tailored mentorship to build capabilities and readiness

Access to industry networks to connect and collaborate

Investor engagements to unlock funding opportunities

Since 2024, the CyberSG Talent, Innovation and Growth (TIG) Collaboration Centre has

Delivered **5** CyberBoost cohorts since 2024

Supported **40+** local and overseas cybersecurity companies

CyberCall

Advances the translation of industry problem statements into deployable cybersecurity solutions through close partnerships with end-users and industry stakeholders.

Betterdata
CyberCall supported this Singapore-based AI company in developing an AI model for data.

Privacy-Preserving AI
This allows Betterdata to develop high-quality synthetic data without exposing personal information.

Global Recognition
Betterdata secured a US Department of Homeland Security contract for cyber defence simulations.

CyberGrowth

Supports companies expanding into new markets by lowering market entry barriers and facilitating business connections.

Connected **50+** local cybersecurity companies through curated business matching opportunities and participation in global events such as RSA Conference.

Accelerate Capability Building through Co-development

The Government will convene multiple ecosystem players such as Institutes of Higher Learning (IHLs), industry partners, and end-users from the outset to jointly develop capabilities.

To support this, the Government will introduce **two Signature Programmes in AI and Operational Technology (OT) security under the National Cyber R&D Programme (NCRP).** These programmes will actively work across the research-to-deployment lifecycle to systematically build world-class capabilities that will enhance our national security and resilience.

- The **AI Security Signature Programme** supports the development of secure systems underpinning Smart Nation initiatives. AI is crucial to cybersecurity as it enables faster threat detection, automated response, and adaptation to evolving attacks.

- The **OT Security Signature Programme** will focus on sectors where Singapore can lead globally (e.g. maritime, water, and energy), as well as in areas where we can develop new methods and solutions to secure OT systems for our critical infrastructure.

The Government will also enhance our national testbeds and infrastructure as enablers for capability development.

- The Government will enhance testbeds such as **iTrust** at the **Singapore University of Technology and Design** and the **National Cybersecurity Lab** at the **National University of Singapore** to better support the testing and validation needs of CII owners and industry partners.

- The **National Integrated Centre for Evaluation (NiCE)** at **Nanyang Technological University** will complement these capabilities by providing testing, inspection, and certification services. Together, these platforms will strengthen the translation of research into deployable cybersecurity capabilities.

The **CyberSG Consortium**, a platform that brings together researchers and go-to-market partners, will continue to support industry-academia collaboration to drive research translation, product development, and commercialisation. These efforts will strengthen Singapore's ability to translate promising innovation into deployable products that address real-world cybersecurity challenges.

The Government will also attract leading international firms to embed sophisticated cybersecurity capabilities within the local ecosystem, where building them locally may not be efficient. The Government will do so by:

- Using government use cases to attract and anchor leading global cyber companies in Singapore, and formalise arrangements through MoUs where appropriate.

- Providing economic incentives to deepen local R&D and technical capabilities, including schemes such as EDB's Research and Innovation Scheme for Companies.

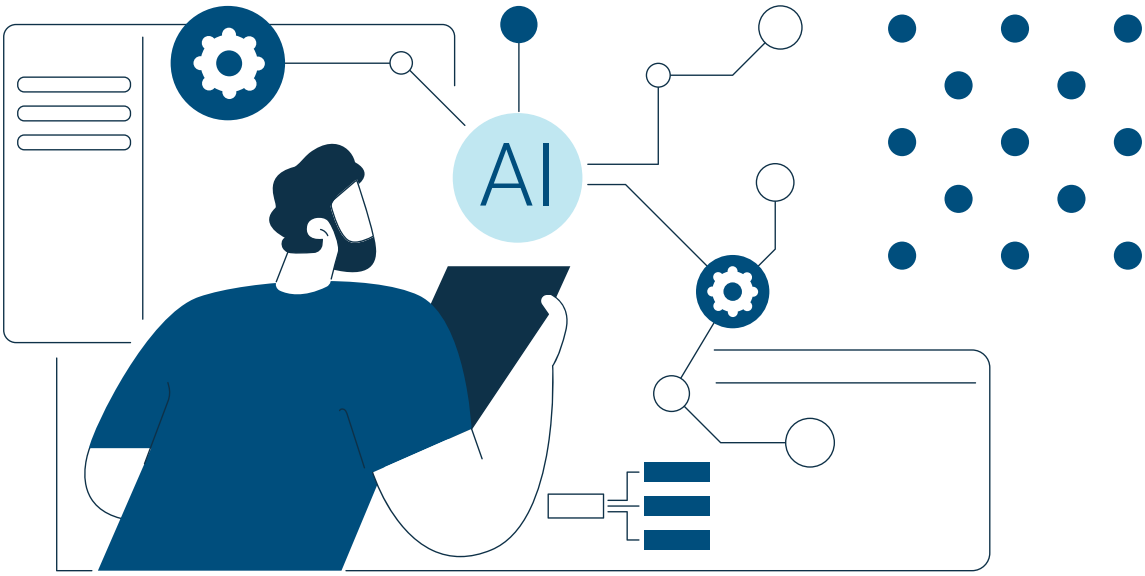
From Research to Real-World Impact

National testbeds and infrastructure such as iTrust provide the environments for researchers, industry, and end-users to jointly develop, validate, and commercialise innovative cybersecurity technologies.

iTrust has established itself as a world-recognised centre for Operational Technology (OT) cybersecurity research. Its high-fidelity cyber twins spanning water, energy, and maritime environments, alongside the availability of operational technology datasets, have drawn over 15,000 downloads from nearly 1,900 organisations across 90 countries, demonstrating the international reach and relevance of Singapore's research capabilities.

These capabilities have supported more than 100 researchers locally and internationally, providing realistic environments to validate new technologies and operational use cases, and helping promising research move closer to real-world adoption. We will broaden access to these facilities by connecting research institutions, Institutes of Higher Learning, and industry partners with relevant testbeds and operational use cases.

Building on this foundation, iTrust will deepen its role as a key translation and validation partner for both the AI and OT Security Signature Programmes. This includes stress-testing AI-driven threat detection and response solutions, as well as validating OT security research outputs against realistic cyber-physical environments.



CHAPTER 8

ENABLER 2 – LEVEL UP OUR CYBER WORKFORCE

Building the Cyber Workforce for the Next Frontier

Human capital remains Singapore's decisive cybersecurity advantage. Technology can automate analysis, detection, and response, but it cannot replace trusted judgment, deep operational experience, ethical responsibility or leadership during a crisis.

Over the past decade, Singapore has made significant progress in building a strong cybersecurity workforce. The number of cybersecurity professionals has more than doubled from 4,000 in 2016 to more than 10,000 in 2025. Programmes such as **SG Cyber Talent** have helped attract young Singaporeans to the profession, supported mid-career transitions, and strengthened leadership development across the cybersecurity ecosystem.

Looking ahead, the challenge is no longer simply to grow the workforce but to deepen its capabilities. Advanced Persistent Threats (APTs), AI-enabled threats, and emerging technologies require highly skilled and experienced practitioners capable of defending critical systems, integrating AI into cyber operations, and responding to complex cyber incidents.

Singapore must build a future-ready workforce with deep technical expertise, recognised professional standards, and the ability to operate in a new environment where cyber threats are increasingly sophisticated.

Over the next five years, the Government will:

Professionalise the cybersecurity workforce.

Deepen national cyber capabilities.

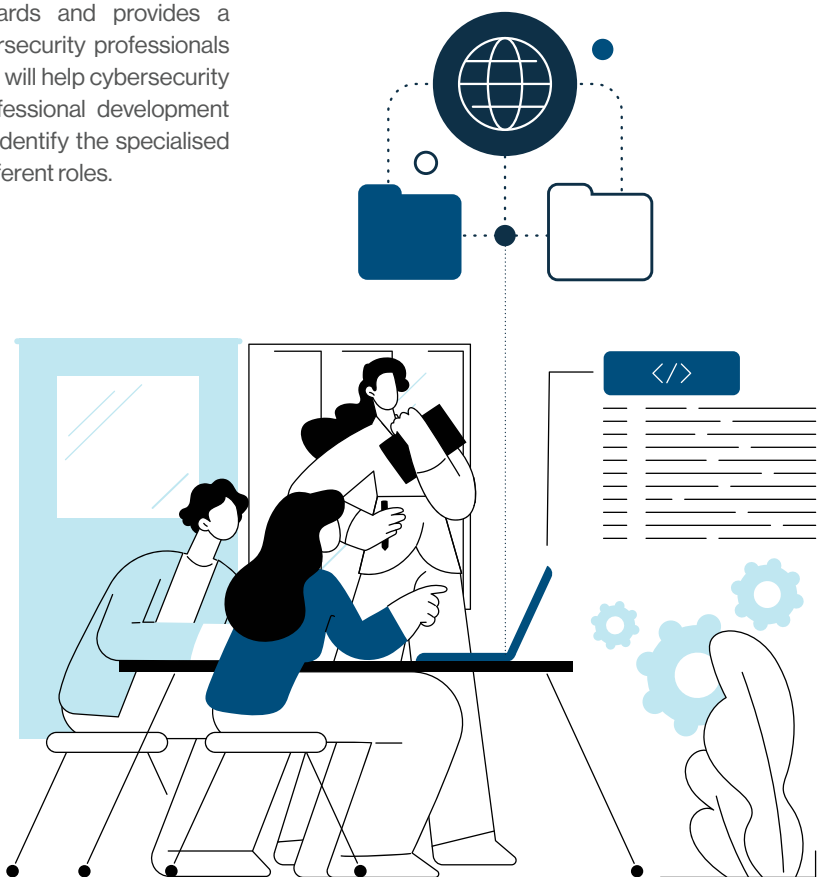
Broaden the national cyber talent pipeline.

Professionalise the Cybersecurity Workforce

Professionalisation will raise the quality of Singapore's cybersecurity workforce to address increasingly complex cybersecurity threats and strengthen recognition of professional expertise.

The Government will introduce professional accreditation for the cybersecurity workforce. A Cyber Security Agency of Singapore (CSA)-commissioned consultancy study conducted by Ernst & Young in 2024/25 found that 67 per cent of stakeholders considered the industry ready for professional accreditation. We will take a phased approach to implementation, allowing refinements to be made based on industry feedback and evolving needs.

- The Government will establish a **Cybersecurity Professional Accreditation Framework** which defines the national standards and provides a structured pathway for cybersecurity professionals throughout their careers. This will help cybersecurity practitioners chart their professional development while enabling employers to identify the specialised competencies required for different roles.
- The framework will include requirements for continuing professional development and periodic renewal. This will help cybersecurity practitioners chart their professional development and remain current with the evolving operating environment, while enabling employers to identify the specialised competencies required for different roles. A professional panel will be established to guide the evolution of professional standards and ensure that the framework remains relevant.



Deepen Cyber Capabilities

The Government will expand and refresh cybersecurity training programmes to equip cyber defenders with the knowledge and skills to address APT-level threats and leverage AI-enabled cyber tools.

- The Government will refresh and harmonise the **ICT Skills Framework for Cybersecurity** and the **Operational Technology (OT) Cybersecurity Competency Framework** to reflect emerging technologies and evolving industry needs. Notably, **AI-related competencies** will be incorporated into these skills frameworks and training pathways.

- Within Government, the Government Technology Agency of Singapore will work to establish a new **Cybersecurity Training School** for cybersecurity professionals across the public service. The Training School will provide structured, role-based pathways for specialised functions such as digital forensics and incident response, threat hunting, penetration testing, red teaming, secure architecture, cloud security, and cybersecurity engineering.

CSA Academy will continue to support the professional and leadership development of cybersecurity leaders in Singapore through the **Cybersecurity Strategic Leadership Programme.** CSA is also rolling out a series of training programmes with training partners for CII owners to strengthen their abilities to defend against APTs and AI-enabled threats, including training for Board, Chief Information Security Officers, and practitioners.

These investments ensure that Singapore's cyber defenders remain equipped to address today's and tomorrow's threats and technologies.

Broaden Singapore's Cyber Talent Pipeline

The Government will build on the success of **CSA's SG Cyber Talent programme** and **Digital and Intelligence Service (DIS)'s Sentinel Programme** to offer multiple pathways for talent to enter the cybersecurity field across all life stages.

- The Government will continue working closely with schools, Institutes of Higher Learning (IHLs), and industry partners to strengthen cybersecurity education and attract more young Singaporeans into cybersecurity careers.

- Beyond students and fresh graduates, the Government will continue running programmes to facilitate mid-career conversions into the cybersecurity field. These include tailor-made programmes for specific demographics such as women, individuals from adjacent technology disciplines, and persons returning to the workforce.

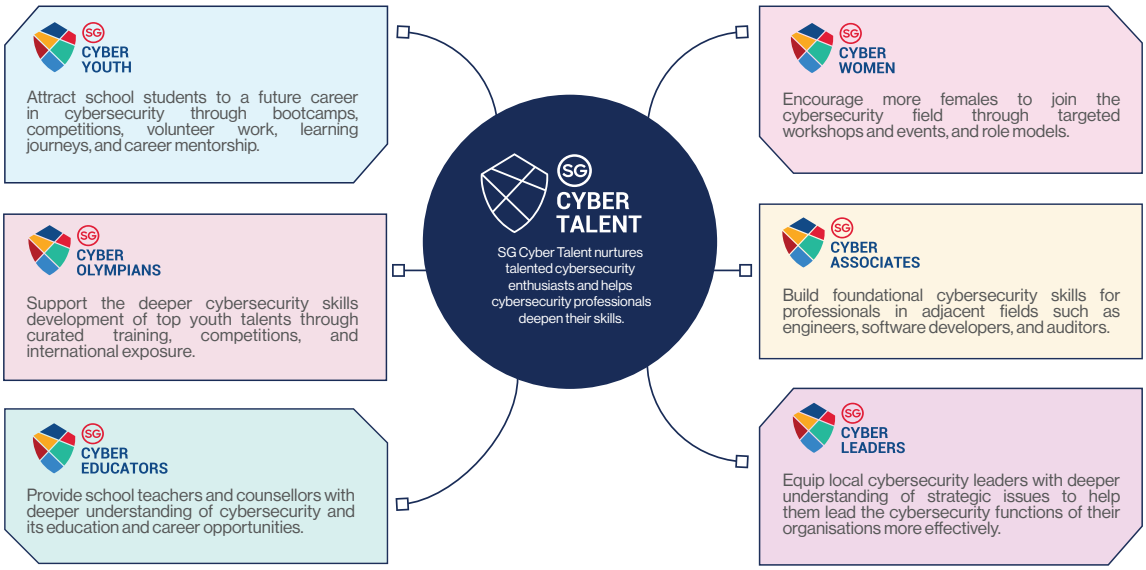
These efforts are complemented by other Government initiatives such as Skills and Workforce Development Agency (SWDA)'s SkillsFuture programmes, and Infocomm Media Development Authority (IMDA)'s TechSkills Accelerator, which both support continuous education and training.

Specifically for full-time National Servicemen (NSmen), **the Cyber Work Learn Schemes** will allow them to gain knowledge for crucial roles in cyber defences while gaining practical experience. Vocational training, on-the-job training, and academic training equip them with vocational knowledge and skills that prepare them well for a future in the cybersecurity industry.

Participants at the Sentinel Challenge, a capstone exercise as part of the Sentinel Programme for secondary school, junior college, polytechnic and Institute of Technical Education (ITE) students

CSA's SG Cyber Talent Programme

Building an effective talent pipeline for Singapore's cybersecurity ecosystem



As we grow our domestic talent pool across Government and the private sector, we should develop ways to draw upon this distributed expertise in times of crisis. In the event where multiple critical sectors are affected simultaneously, the Government must be able to mobilise talents across the public and private sectors to address cyber threats.

- A key initiative in achieving this is the deployment of the **Singapore Armed Forces (SAF) Sectoral Cyber Defence Teams (SCDTs)**.
- The SCDTs provide an additional layer of national capability that complements Government agencies and CII owners, ensuring Singapore has access to specialised expertise to defend our CIIs when responding to significant cyber events.

Sectoral Cyber Defence Teams (SCDTs)

To strengthen cyber defence and resilience of key CIIs against advanced persistent threats, SCDTs were set up by the Singapore Armed Forces to leverage the civilian cybersecurity expertise of our Operationally Ready National Servicemen (NSmen) in support of CSA's national efforts to strengthen the protection of Singapore's Critical Information Infrastructure against sophisticated cyber threats.

CHAPTER 9

EVERYONE HAS A ROLE TO PLAY

A Shared Responsibility in an Interconnected Digital World

Singapore's cybersecurity depends on the resilience of our entire digital ecosystem. As organisations, technology providers, and individuals become increasingly interconnected online, vulnerabilities can cascade from one part of the ecosystem to many others, while stronger cyber resilience benefits the ecosystem.

Singapore's Cybersecurity Strategy 2026 therefore adopts a whole-of-ecosystem approach. Each stakeholder has distinct but complementary roles in strengthening our collective resilience. Cybersecurity is not only a shared responsibility – it is a shared endeavour in which everyone has a part to play.

The Government
Leads in national cyber defence and capability building by:

- Strengthening national cyber defence capabilities, protecting critical infrastructure, and coordinating responses to significant cyber threats.
- Providing enhanced national threat detection capabilities and stronger partnerships with Critical Information Infrastructure (CII) owners through the National Cybersecurity Command Centre.
- Strengthening legislation, investment in research and innovation, talent development, and working with international partners to ensure Singapore's cyberspace remains secure, trusted, and resilient.

A Critical Information Infrastructure (CII) owner
Enhances the security of CIIs by:

- Taking a proactive approach to cybersecurity by integrating security into business decisions and fostering a strong security culture across the organisation.
- Adopting a mindset of continuous defence by continuously monitoring for threats and vulnerabilities, strengthening defences as risks evolve, and addressing weaknesses promptly.
- Adhering to the updated Cybersecurity Code of Practice for relevant CII systems and systems linked to them, including systems hosted in the cloud.
- Securing their supply chains. This includes ensuring that their suppliers, vendors, and other third-party system providers they work with meet baseline cybersecurity requirements, such as through the Cyber Trust Mark and Cyber Essentials Mark.

A Business Owner
Strengthens the organisation's cybersecurity by:

- Embedding security in digital transformation and strengthening cyber risk management to protect customers, suppliers, and partners.
- Investing in cyber leadership and workforce personnel development to groom leaders and practitioners that can oversee security-by-default, monitoring and detection, incident response, and business continuity recovery.
- Adopting baseline cybersecurity measures, such as through the Cyber Trust Mark, Cyber Essentials Mark, and CISO-as-a-Service.

A Technology Company and Researcher
Contributes to a safer digital environment by:

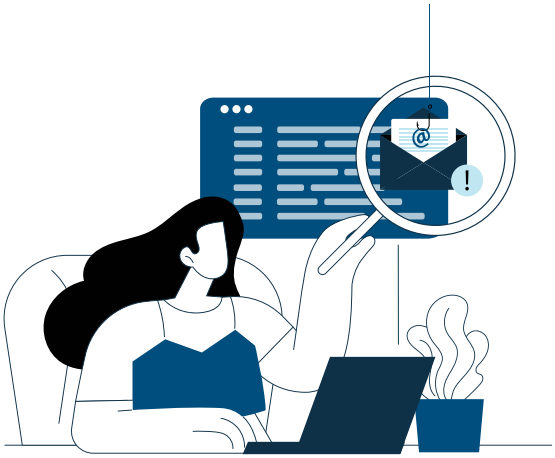
- Developing the tools, capabilities, and standards that underpin Singapore's cyber resilience.
- Translating research and innovation into deployable products that address national priorities through initiatives such as the National Cyber R&D Programme, CyberBoost, CyberCall, and CyberGrowth.
- Partnering with global technology firms to bring frontier technologies to Singapore and co-create cybersecurity solutions.

A Cybersecurity Professional
Contributes to our ecosystem by:

- Providing expertise needed to design secure systems, detect sophisticated threats, investigate incidents, and respond effectively when attacks occur.
- Leveraging new training opportunities and capability development programmes under the Cybersecurity Professional Accreditation Framework to keep their skills current as technologies and threats evolve.

A Student
Learns more about cybersecurity by:

- Building cybersecurity knowledge through education and lifelong learning.
- Participating in competitions, internships, and industry opportunities to be equipped for relevant skills in an increasingly digital future.
- Considering cybersecurity qualifications and careers to contribute to Singapore's cyber workforce.



An Individual who uses technology for work or play
Practices good cyber habits by:

- Remaining vigilant against scams and cyber threats by practising the three Cyber Tips:
  - Enabling two-factor authentication and using strong passphrases,
  - Updating software promptly, and
  - Adding ScamShield and anti-virus apps.
- Using AI tools responsibly, and checking the authenticity and accuracy of content before sharing it.
- Reporting harmful online content to platform providers.

Stronger Together

Singapore's Cybersecurity Strategy 2026 reflects a shift in how Singapore approaches cybersecurity. Cybersecurity is a national capability built upon strong partnerships, shared responsibility and mutually reinforcing efforts across Government, industry and society. It demands a collective response.

Together, we can build **a secure, trusted, and resilient cyberspace that empowers our digital way of life** — a cyberspace where the Government, businesses, researchers, technology companies, and every Singaporean can protect our shared digital commons.

Singapore's Cybersecurity Strategy 2026
Copyright © 2026
by Cyber Security Agency of Singapore
All rights reserved.

ISBN: 978-981-94-7721-0

If you have any feedback on this publication,
or wish to find out more about
Singapore's efforts in cybersecurity,
please visit the following websites or contact us:

Cyber Security Agency of Singapore
Website: www.csa.gov.sg

General enquiries/feedback: contact@csa.gov.sg
SingCERT (for incident reporting and other resources):
https://www.csa.gov.sg/resources/singcert/

Designed by:
SiliconPlus Communications Pte. Ltd.

CSA
SINGAPORE