

Singapore launches Cybersecurity Strategy 2026, with AI in national cyber defence

Source copy kept by wheresthe.ai for the story "Singapore launches Cybersecurity Strategy 2026, with AI in national cyber defence" (<https://wheresthe.ai/d/sg-singapore-launches-refreshed-cybersecurity-strategy-with-2026-10/>).

Source: <https://www.csa.gov.sg/news-events/press-releases/singapore-launches-cybersecurity-strategy-2026-to-strengthen-national-cyber-resilience/>

Text saved 25 Oct 2026 (the page as published).

SHA-256 of the saved text: 33e4d2be7f00432e7f0b7f13e4e589b84a32e72833fc71e088b4be55b1c372f5

Home News & Events Press Releases Singapore Launches Cybersecurity Strategy 2026 to Strengthen National Cyber Resilience

Press Releases Singapore Launches Cybersecurity Strategy 2026 to Strengthen National Cyber Resilience

13 October 2026 Singapore's Cybersecurity Strategy 2026 sets out a whole-of-nation approach to strengthening cyber resilience. It focuses on defending critical infrastructure, securing the wider digital ecosystem, preparing for AI and quantum risks, strengthening global partnerships, building cybersecurity capabilities and developing a future-ready cyber workforce.

1. [Singapore, 13 October 2026] Singapore's Senior Minister, Coordinating Minister for National Security, and Minister for Home Affairs Mr K Shanmugam launched Singapore's Cybersecurity Strategy (SCS) 2026 today at the Opening Ceremony of the 11 th Singapore International Cyber Week (SICW) at the Sands Expo and Convention Centre. 2. The SCS guides Singapore's whole-of-nation approach to cybersecurity. SCS 2026 is guided by the vision of a secure, trusted and resilient cyberspace that empowers our digital way of life. In his foreword to SCS 2026, Prime Minister Lawrence Wong underscored the importance of shared responsibility and collective action to achieve this. He wrote: "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." – Prime Minister Lawrence Wong Foreword to the Singapore Cybersecurity Strategy 2026 3. SCS 2026 responds to a more challenging cyber landscape. Cyber threats are growing more severe, with Advanced Persistent Threat (APT) actors increasingly targeting critical infrastructure and preparing for potential disruption. Frontier Artificial Intelligence (AI) is transforming cyber offence and defence, while advancements in quantum computing could eventually undermine today's encryption. Growing digital interdependencies mean that vulnerabilities and disruptions can have cascading effects across sectors and borders. At the same time, geopolitical tensions and technological competition are making international cooperation on cybersecurity more challenging. 4. First launched in 2016 and refreshed in 2021, SCS 2026 builds on foundations established over the past decade while sharpening Singapore's response to new and emerging challenges. The refreshed Strategy places greater emphasis on strengthening national-level cyber defence, raising cybersecurity standards across the wider digital ecosystem, and preparing Singapore for emerging technological threats. It sets out four strategic pillars, supported by two foundational enablers, which are summarised below. An infographic outlining the pillars, enablers and key initiatives is in the Annex . Pillar 1: Defend Critical Infrastructure 5. Singapore's Critical Information Infrastructure (CII) provides the essential services that Singaporeans rely on every day. A successful cyberattack on our CII could disrupt essential services, or steal sensitive data which could be used to undermine national security or public order. The Government will strengthen national cyber defence by developing centralised capabilities to better anticipate, detect and respond to sophisticated cyber threats, while strengthening CII owners' capabilities to defend their systems against advanced and AI-enabled attacks. These efforts will reinforce the resilience of essential services on which Singaporeans depend. Pillar 2: Secure our Wider Cyberspace 6. Singapore must raise the level of cybersecurity across our entire ecosystem, beyond just CII owners, to protect businesses, organisations and individuals from cyber harms. The Government will strengthen upstream protection measures to minimise overall exposure to cyber threats; and drive and support organisations to strengthen their cybersecurity posture . The Government will also continue its public education and outreach efforts to equip Singaporeans with the knowledge to protect themselves online. Pillar 3: Strengthen Capabilities for AI and Quantum 7. AI is transforming the cybersecurity landscape. The Government will leverage AI to enhance cyber defence by strengthening in-house capabilities and promoting the wider adoption of AI-enabled cyber tools. The Government will also support organisations to adopt AI systems securely by developing practical implementation

guidance and leading by example. 8. The impact of quantum computing may be further away, but Singapore must prepare early for quantum-enabled threats. The Government will accelerate national quantum-safe migration by working with industry and public agencies to plan, prioritise and execute the transition; and by developing and updating practical resources to support the transition. Pillar 4: Enhance Resilience through Global Partnerships 9. As cyber threats transcend national borders, Singapore will deepen international cooperation even as geopolitical tensions and technological competition make such cooperation more challenging. The Government will strengthen Singapore's role as a trusted convenor for international cybersecurity dialogue through platforms such as SICW, continue advancing rules-based cooperation in cyberspace, and partner major technology firms to co-develop solutions in priority areas such as AI-enabled cybersecurity, operational technology (OT) security, and quantum-safe migration. Enabler 1: Build a World-class Cybersecurity Ecosystem 10. Singapore will strengthen its cybersecurity industry and innovation ecosystem to develop the capabilities needed for long-term national cyber resilience. The Government aims to establish Singapore as Asia's leading cybersecurity innovation hub where globally competitive and trusted cybersecurity capabilities for critical infrastructure can be developed, validated, and deployed. To achieve this, the Government will focus on growing local capabilities from research to commercialisation, and accelerate the co-development of cybersecurity solutions with academia and industry, including international firms operating in Singapore. Enabler 2: Level Up our Cyber Workforce 11. People remain central to Singapore's cybersecurity efforts. As cyber threats become more sophisticated and emerging technologies reshape the profession, Singapore will need a workforce with deep technical expertise, strong professional standards, and the ability to adapt to new challenges. The Government will professionalise the cybersecurity workforce, deepen cybersecurity capabilities, and broaden the national cyber talent pipeline to build a future-ready workforce. Invitation to Collaborate 12. Over the next five years, the Government will work with relevant stakeholders to implement the key initiatives outlined in SCS 2026. We invite stakeholders across governments, industry, academia and the wider cybersecurity community to partner us in taking these initiatives forward and building a secure, trusted and resilient cyberspace for Singapore. Annex

[Back to top](#)