

Home > News & Events > Press Releases >

Singapore Launches Cybersecurity Strategy 2026 to Strengthen National Cyber Resilience

Singapore Launches Cybersecurity Strategy 2026 to Strengthen National Cyber Resilience

13 October 2026

Singapore plans a national filter to block malicious websites under a cybersecurity strategy launched on 13 October

Description

Singapore will build a national filter that stops computers and phones from connecting to known malicious websites, under a new cybersecurity strategy that also puts artificial intelligence at the centre of national cyber defence. The [Cyber Security Agency of Singapore](#) released Singapore's Cybersecurity Strategy 2026 on Tuesday 13 October, launched by Senior Minister and Coordinating Minister for National Security K Shanmugam at the opening of the 11th Singapore International Cyber Week at Sands Expo and Convention Centre.

Home > News & Events > Press Releases >

Singapore Launches Cybersecurity Strategy 2026 to Strengthen National Cyber Resilience

Singapore Launches Cybersecurity Strategy 2026 to Strengthen National Cyber Resilience

13 October 2026

Photo: Cyber Security Agency of Singapore

It is the third version of the strategy, after the first in 2016 and a refresh in 2021, and it sets the Government's cyber agenda for the next five years.

Blocking bad sites before they load

The new filter is called a national Protective Domain Name Service, or PDNS. When someone tries to reach a domain already known to be malicious, the service stops the connection before the threat reaches the user. The Government expects it to cut exposure to phishing sites, scams and malware.

It is part of a wider push to “secure the wider cyberspace” beyond the operators of critical information infrastructure, alongside public education on staying safe online.

AI on the defending side

The Government will progressively deploy AI across its national cyber defence operations, including the National Cybersecurity Command Centre (NC3), CSA’s operations hub, and the Government Cyber Security Operations Centre. CSA already uses AI tools to find and map exposed systems and weaknesses, and GovTech uses AI agents to speed up security testing.

Singapore will not build its own AI model for every task. It will instead invest in what Mr Shanmugam called “AI harness engineering”, so that defenders can test the best available models and plug them securely into their own tools and data.

NC3 gives the Government a national picture of threats and vulnerabilities, supports continuous monitoring of critical infrastructure and is meant to spot advanced persistent threat groups earlier. It grew out of lessons from Operation CYBER GUARDIAN, Singapore’s largest cyber response to date, which was mounted against UNC3886, a group that had gained access to Singapore’s telecom networks.

Four pillars, two enablers

The strategy rests on four pillars:

- Defend critical infrastructure
- Secure the wider cyberspace
- Strengthen capabilities for AI and quantum computing
- Enhance resilience through global partnerships

Two enablers sit underneath: growing Singapore into Asia’s leading cybersecurity innovation hub, and professionalising and widening the cyber workforce. On quantum computing, which could one day break today’s encryption, the Government will speed up a national move to quantum-safe systems with industry and public agencies.

In his foreword, Prime Minister Lawrence Wong wrote that “what each of us does affects the security of others”.

The Cyber Week opening also cited recent attacks abroad: coordinated strikes on more than 30 wind and solar installations in Poland in December 2025, a breach that exposed close to 27 million user records at South Korea’s largest mobile carrier in April 2025, and an AI agent that reached non-public data on an Australian government portal in September 2026.

Date Created

14/10/2026

Author

claratan

default watermark