APAC Cybersecurity Fund

The Asia Foundation

EXPOSURE TO EMPOWERMENT

Strengthening Micro, Small, and Medium Enterprises in the Age of AI

in partnership with CyberPeace Institute GLOBAL CYBER ALLIANCE

with support from Google.org

Acknowledgments

This report was authored by the CyberPeace Institute, in collaboration with The Asia Foundation, supported by Google.org.

Research

CyberPeace Institute team: Adrien Ogee, Jim Boevink

Project Management

APAC Cybersecurity Fund Policy team: Anthea Mulakala, Rukshanie Vidyaratne, Diya Nag, Sandy Walsh, Sharifah Shahirah Idid, Syasya Roslan

Design

Syasya Roslan

Cover photo: Image altered using Canva AI tool.

Exposure to Empowerment
Strengthening Micro, Small, and Medium Enterprises in the Age of AI

KUALA LUMPUR, MALAYSIA. November 2025.

© The Asia Foundation 2025.

All rights reserved. No part of this report may be reproduced without written permission by The Asia Foundation.

Executive Summary

Across Asia-Pacific region, micro, small, and medium enterprises (MSMEs) are embracing AI tools to streamline operations, reach new markets, and serve customers more efficiently. However, this rapid uptake often happens without clear safeguards, exposing businesses to new cyber risks.

Malicious actors are now using AI to scale fraud, impersonation, and reputational attacks. In a region where MSMEs play a central role in powering most economies but face major cybersecurity gaps, this evolving threat landscape demands urgent attention. This policy brief explores the dual nature of AI for MSMEs—a powerful tool for growth and a sophisticated vector for new threats—and provides actionable recommendations for a safer, more resilient digital future.

"AI can empower MSMEs to grow and innovate, but only if scaled with foresight and safeguards. At CyberPeace Institute, we're committed to helping ensure that while AI reaches every corner of the Asia-Pacific economy, it does so within a governance framework that maps risk, secures deployment, and fosters trust."

Stéphane Duguin, CEO, CyberPeace Institute

Problem Overview and Context

The rapid adoption of AI is exposing MSMEs to unprecedented digital threats

The rapid adoption of AI across the Asia-Pacific region is exposing MSMEs to unprecedented digital threats. Although adoption levels vary across countries, the trend is clear: small businesses are adopting AI tools without adequate safeguards. A recent study found that AI adoption among MSMEs in India remains modest at 15% but is growing quickly, with 65% of firms experimenting with GenAI tools (National University Singapore, 2025).

This fast-paced and often unguided adoption creates critical vulnerabilities. As MSMEs integrate AI, they become targets for AI-enabled attacks that are increasingly sophisticated, scalable, and personalized. In Indonesia, where fewer than 5% of MSMEs are managed by digitally native generations (Y and Z), the rise of AI-driven scams, fraud, and document forgery poses an even greater risk to their resilience (BRIN, 2025).

The macro-economic context

MSMEs are the backbone of the Asia-Pacific economy, accounting for more than 90% of all businesses and employing more than 65% of the region's workforce. Their economic resilience is directly tied to national stability. While large corporations have the resources to invest in cybersecurity teams and AI governance, MSMEs operate with lean budgets and limited technical expertise. This disparity creates a significant attack surface for bad actors who are increasingly leveraging AI to exploit these vulnerabilities.

A report by the Economic Research Institute for ASEAN and East Asia (ERIA) projects that AI could contribute 10% to 18% of ASEAN's GDP by 2030, a potential uplift of nearly USD1 trillion. This opportunity, however, is contingent on a secure and trusted digital environment (ERIA, 2025).

AI Opportunities:

How APAC MSMEs are using AI

MSMEs across the region are leveraging AI to drive productivity and innovation, bridging the gap with larger competitors. They are not just using AI for cost savings; they are adopting it to create entirely new business models and customer experiences. As the adoption of AI deepens, MSMEs are discovering how digital tools can unlock efficiencies, enhance creativity, and open new market opportunities that were once out of reach.

Customer engagement :

Chatbots and virtual assistants handle customer inquiries 24/7, improving service efficiency and freeing up staff. In Vietnam, a logistics company uses a generative AI assistant for its restaurant partners to manage customer communication and orders, particularly during peak hours. This enables them to serve more customers with fewer resources (Quest Ventures, 2025).

Operational efficiency :

AI tools are used for inventory management, demand forecasting, and predictive analytics to optimize supply chains. In India, a fashion brand uses AI-based demand forecasting to minimize overstock and reduce waste (Quest Ventures, 2025).

Content creation :

Generative AI helps small businesses produce marketing copy, design assets, and social media content without costly outsourcing. Across the region, MSMEs are finding creative ways to use these tools in daily operations. In Thailand, small businesses use AI platforms to automate social media scheduling and generate real-time product creatives, helping lean teams reach wider audiences more efficiently (Quest Ventures, 2025). In Indonesia, where only one in five businesses use AI, early adopters already report strong gains. Tools such as chatbots, automated financial reporting, and AI-driven content generation have helped MSMEs cut costs by up to IDR15–25 million per month and reduce customer service workloads by 70 percent (Media Indonesia, 2025).

Sources: Desk research and key informant interviews conducted by the CyberPeace Institute (CPI) and The Asia Foundation (TAF). Unpublished internal research, year not specified.

Beyond the common use cases, MSMEs are finding innovative ways to apply AI to their businesses. From automating back-end operations to improving financial management and customer engagement, AI is reshaping how small enterprises operate and compete. These emerging applications illustrate how MSMEs are moving from basic adoption to strategic integration of AI across business functions.

Emerging AI applications for MSMEs

Financial management & fraud detection:

AI-powered accounting tools can reconcile transactions, flag anomalies, and support financial reporting with greater speed and accuracy. This helps small businesses detect and prevent fraudulent transactions in real time, providing a crucial safeguard against escalating threats.

Hyper-personalized marketing:

AI is enabling MSMEs to analyze customer behavior in real time and deliver hyper-targeted promotions. By leveraging the explosion of digital data from mobile payments and e-commerce platforms, small businesses in markets like the Philippines are now able to send personalized messages and offers, a capability once reserved for corporate giants (Tatler Asia, 2025).

Streamlined human resources:

AI is being used to automate recruitment tasks, improve employee engagement, and predict attrition. This helps small teams manage their most valuable asset, their people, more efficiently and strategically.

Source: As cited on page 5

While AI opportunities are being recognized globally, the way they are being embraced also depends on the digital maturity of countries, the sectors involved, and the level of 'AI readiness' they demonstrate. The following table provides a high-level overview comparing APAC countries in terms of AI readiness, digital maturity, and the digital support available to MSMEs

Countries	AI Readiness Level	Digital Maturity Level	Key Digital Supports for MSMEs
Singapore	High	High	Strong SME digitalization efforts
Japan	High	High	Rapidly evolving ecosystem
Korea	High	High	Fragmented digital landscape
Malaysia	Medium-High	Medium-High	Low digital literacy
India	Medium	Medium	Minimal AI policy framework
Thailand	Medium	Medium	Early-stage adoption
Vietnam	Medium	Medium	Extensive programs & grants
Philippines	Medium	Medium-Low	Strong regulatory oversight
Indonesia	Medium-Low	Medium-Low	Mature AI policies
Pakistan	Low	Low	Active government incentives
Bangladesh	Low	Low	Growing adoption, policy support
Sri Lanka	Low	Low	Limited infrastructure

Source: ERIA 2025, NUS 2025, Kearney 2025

AI Threats:

The Urgent Need for Platform-Provided Defenses

While AI creates immense opportunities for MSMEs, it also introduces new and complex challenges. As AI evolves, MSMEs increasingly rely on platform-enabled defenses and trusted AI solutions to safeguard their businesses against sophisticated threats. These attacks are becoming increasingly sophisticated and scalable, presenting urgent challenges for enterprises that lack robust, platform-enabled cybersecurity preparedness. As cybercriminals harness AI to automate scams, impersonation, and fraud, the financial and reputational consequences for MSMEs are growing rapidly. A UNODC report estimates that in 2023, financial losses from AI-driven scams in East and Southeast Asia alone ranged between USD18 billion and USD37 billion (UNODC, 2024).

Deepfake fraud & impersonation:

Sophisticated scams are emerging where malicious actors use AI to clone voices or create deepfake videos of business owners, staff, or customers. These convincing impersonations are used to authorize fraudulent transactions or demand sensitive information. This has been a particular concern in countries like India, Vietnam, and the Philippines, where a large portion of business is conducted through social and messaging platforms (CSIS, 2024, East Asia Forum, 2024). AI-driven scams targeting MSMEs have surged 115% in the past year, with perpetrators exploiting deepfake voices, fake transfer proofs, and AI-generated phishing messages. Indonesian MSMEs, already low in cyber preparedness, are now facing increasing fraud risks, with annual losses reaching IDR7.6 billion (Cyber Bulletins LinkedIn, 2025).

"In Vietnam, small businesses are facing **AI deepfake scams** that mimic the voices of their partners and clients to demand urgent payments or data." (CSIS, 2024)

"In 2025, the Financial Services Authority of Indonesia (OJK) received **over 70,000 reports of fraud** involving AI. Of these, **39,108 cases** were related to online trading scams, **20,628** involved fake calls where perpetrators impersonated others, and **14,533** were linked to investment fraud. AI misuse—most notably through voice cloning and deepfakes—is designed to deceive victims into believing what they see and hear, making them more likely to transfer money or fall for scams." (OJK, 2025)

Phishing-at-scale:

Generative AI allows criminals to create highly personalized, context-specific phishing emails and messages at an unprecedented scale. These scams are often localized by language and reference real-world events, making them much harder to detect than traditional phishing attempts. Europol has highlighted how large language models (LLMs) help scammers craft authentic-sounding messages to gain victims' trust, allowing them to operate much faster and at a greater scale (CSIS, 2024).

AI-powered reconnaissance:

Bad actors are using AI to automate the process of mapping a target's digital footprint. AI-powered tools can quickly scan an MSME's website, social media, and employee profiles to identify vulnerabilities, key personnel, and supplier relationships. This information is then used to craft highly targeted spearphishing attacks or to find weaknesses in their network.

AI-generated malware and code:

Generative AI is lowering the barrier to entry for cybercrime. Novice criminals can now use AI to generate malicious code, craft sophisticated malware, and build undetectable exploits without any prior coding knowledge. These tools are often available on dark web forums, creating a thriving criminal service economy. (CSIS, 2024)

WORMGPT AND DARKBARD

WormGPT and **DarkBard** are tools used to generate malicious code while enabling reconnaissance and social engineering at scale. They allow novice attackers to generate thousands of personalized phishing emails in different languages and with convincing local context–a task that previously required extensive human research and manual effort.

This enables wide-scale campaigns that are both massive and highly targeted, blurring the line between mass and personalized attacks.

Biometric exploitation:

AI's ability to create synthetic biometric data, such as deepfaked faces, poses a new threat. Scammers can use deepfaked faces to bypass biometric scanners on devices, gaining access to victims' personal and financial information. This is a critical concern for MSMEs that rely on mobile-first or app-based business models.

Source: As cited on page 5

AI Threats:

Brand Authority in the Age of Generative Search

AI also reshapes how MSMEs are seen and represented online. The way consumers discover and trust information is evolving rapidly, with AI-powered summaries and generative search now replacing traditional search engine optimization.

This shift creates new challenges for online visibility and brand reputation. As AI increasingly influences how content is produced, summarized, and surfaced, MSMEs must adapt their digital strategies to remain visible, credible, and trusted in this changing information landscape.

Brand sabotage

Unscrupulous competitors can manipulate AI outputs to damage a rival's reputation. They might publish false or defamatory content that AI models later ingest and present as fact in AI-generated summaries, bypassing traditional moderation systems. This is particularly concerning because AI-generated summaries often lack source citations, making it difficult for consumers to verify information.

Source: As cited on page 5

Loss of control

MSMEs face new challenges in managing their brand representation online. In the age of generative search, businesses can proactively strengthen brand authority by leveraging AI-enabled monitoring tools provided by trusted platforms, helping ensure accurate and positive representation. This shift means that an MSME's brand authority is no longer tied only to its own channels but also to a complex, opaque ecosystem of AI models.

Source: As cited on page 5

AI-enabled badmouthing

AI can be used to generate large volumes of negative reviews, forum posts, and social media comments about a competitor. The sheer speed and quantity of this content can overwhelm monitoring systems and quickly damage a business's reputation before they can respond.

Source: As cited on page 5

As AI-driven discoverability evolves, protecting brand integrity will require coordinated efforts between MSMEs, technology providers, and policymakers to strengthen verification systems, digital literacy, and accountability standards.

THE CASE OF "QUANTUM GLOBE" IN SINGAPORE

In a significant legal case, a company referred to as **"Quantum Globe"** was found to have used generative AI to create fake positive reviews to boost its ratings. While this was not a direct case of sabotage, it demonstrated how AI can be used to manipulate online reputation.

The company used AI to generate human-like, fabricated reviews posted under real customer names, showing how **AI enables the creation and scaling of deceitful content** that undermines brand trust. The same tactic could easily be reversed to generate fake negative reviews about a rival.

AI Threats:

Internal Vulnerabilities from Misuse of AI

Beyond threats posed by external actors, the unregulated use of AI within businesses can create major internal vulnerabilities. When employees experiment with AI tools without proper guidance, they may unintentionally expose sensitive information or rely on inaccurate outputs.

These internal risks highlight the need for MSMEs to establish clear policies and build awareness around the responsible use of AI technologies. One growing example of this challenge is seen in the rise of Shadow AI.

Rise of Shadow AI: More than **one-third of employees** share sensitive work information with AI tools without their employer's permission (Infosec Magazine, 2024). This widespread use of unauthorized AI applications, known as "Shadow AI," exposes businesses to significant risks, including:

Data leaks:

Employees may feed confidential customer data, financial reports, or trade secrets into public AI models, which can be stored or used for future training without the business's consent. These public models are often unsecured and can be exploited by data scrapers.

Unsecured tools:

Employees may use third-party browser plugins or applications that act as backdoors for hackers, introducing vulnerabilities into the company's network. These tools often request broad permissions, giving bad actors access to sensitive data.

Alongside Shadow AI, the absence of proactive AI governance policies exposes MSMEs to systemic vulnerabilities.

Lack of governance policies:

Many MSMEs do not have clear or simple policies on AI usage. Without guidelines, employees are left to make their own judgments, leading to inconsistent security practices and a higher risk of data breaches.

The talent and knowledge gap:

MSMEs often lack the internal expertise to vet AI tools, train employees on secure usage, or respond effectively to AI-enabled attacks. This knowledge gap is a primary reason for low adoption of secure, enterprise-grade tools, as the complexity and cost are seen as prohibitive.

Reliance on unverified content:

When MSMEs use AI to generate legal, financial, or medical content without human oversight, they risk spreading misinformation or making decisions based on inaccurate data. This not only poses a reputational risk but also exposes them to legal and financial liabilities.

Source: As cited on page 5

THE CASE OF AUSTRALIAN GOVERNMENT AI GUIDELINES:

The Australian Signals Directorate and the Australian Cyber Security Centre have repeatedly warned Australian businesses about AI risks. A 2024 report revealed that while **79%** of organizations in the APAC region are using or planning to use AI, only **32%** have a formal inventory of these tools. This gap demonstrates a systemic failure to manage and secure AI adoption, leaving a massive internal security risk. Many MSMEs lack even the basic awareness of what AI tools are being used, compounding their vulnerability.

Recommendations

To address these challenges, a multi-stakeholder approach is required to build a resilient and trusted AI ecosystem for MSMEs in the Asia-Pacific region. **Governments, technology providers, financial institutions, and business networks** must work together to ensure that MSMEs have the tools, knowledge, and support needed to adopt AI safely and effectively.

For MSMEs with relatively low digital maturity:

- **Set up a simple AI policy:** Share a short staff note or pinned chat message outlining three key rules: which tools are allowed, a reminder not to upload customer or sensitive data, and to ask management if unsure.

- **Micro-trainings:** Dedicate 5–10 minutes during regular staff meetings to show a recent scam example and discuss how to identify it. Use free resources from government agencies, chambers of commerce, or industry associations.

- **Basic online checks:** Once a month, search your business name on Google, Facebook, or WhatsApp groups relevant to your sector to spot misinformation or impersonation.

- **"Verify, Don't Trust" rule:** Require staff to confirm all payment or data requests through a second channel, such as a phone call or face-to-face confirmation, before acting.

For MSMEs with relatively high digital maturity:

- **Develop a living AI policy:** Create a short, regularly updated document that lists approved AI tools, defines data protection practices, and explains escalation procedures.
- **Structured training:** Organize short interactive sessions with case studies and role-playing. Track participation and provide annual refreshers.
- **Brand monitoring:** Use affordable AI-enabled tools to track how your business appears in search results and generative platforms, and review them regularly.
- **Formal verification controls:** Add written procedures for the "Verify, Don't Trust" rule, include it in onboarding, and where possible, use simple tools like call-back systems or two-person approvals for financial transactions.

For Tech Companies and Platforms:

- **Provide accessible, secure tools:** Develop affordable, easy-to-use and robust, security protections baked into product offerings. These tools should be "secure by design" and "secure by default" and not require extensive technical knowledge to use safely
- **Collaborate on threat intelligence:** Regularly publish threat intel resources through publicly available, free-of-charge channels such as blog posts, quarterly reports to enable security researchers, practitioners, and the public to share information and expertise on the latest, evolving tactics on AI threats
- **Empower MSMEs with AI-enabled solutions:** Develop affordable tools that help MSMEs manage their digital reputation, detect security threats, and protect their brands from manipulation.

For Governments and Policymakers:

- **Fund targeted training programs**: Launch government-funded initiatives and grants to support MSMEs in AI literacy, cybersecurity, and secure implementation. Singapore's Digital Enterprise Blueprint is a strong model, subsidizing up to 50% of tech expenses for SMEs (The Straits Times, 2024).

- **Foster AI Sandboxes:** Establish regulatory sandboxes that allow MSMEs to test new AI technologies safely and understand risks before full adoption.

- **Develop clear ethical and regulatory frameworks:** Provide clear, guidelines for AI use that protect against data misuse and brand manipulation, while supporting innovation. Singapore's regulatory approach of relying primarily on guidelines for AI governance can serve as a model for other nations in the region. (Xenoss, 2025)

- **Promote international and regional collaboration:** As AI-enabled cybercrime is a transnational problem, governments must work together to share intelligence, harmonize policies, and prosecute cross-border crimes. Regional bodies like ASEAN should establish a dedicated AI working group to lead this effort.

Call to Action

The rise of AI presents both a monumental opportunity and a significant threat to MSMEs. It is imperative that all stakeholders – governments, tech companies, and MSMEs – act now to build a secure, resilient, and inclusive digital ecosystem that allows these vital enterprises to thrive. The time to move from observation to action is now, ensuring that AI becomes a catalyst for growth rather than a vector for exploitation.

References

Badan Riset dan Inovasi Nasional (BRIN). (2025). BRIN soroti rendahnya adopsi teknologi digital oleh UMKM Indonesia. Retrieved from: https://brin.go.id/news/124058/brin-soroti-rendahnya-adopsi-teknologi-digital-oleh-umkm-indonesia

Bisnis.com. (2025). OJK: Puluhan ribu orang jadi korban penipuan AI, wajah dan suara dipakai tarik uang. Retrieved from: https://finansial.bisnis.com/read/20250804/563/1899254/ojk-puluhan ribu-orang-jadi-korban-penipuan-ai-wajah-dan-suara-dipakai-tarik-uang

Center for Strategic and International Studies (CSIS). (2024). Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories.

Cyber Bulletins – Linkedin. (2025). Serangan siber bermodus AI meningkat 115%, UMKM jadi sasaran empuk. Retrieved from: https://www.linkedin.com/pulse/serangan-siber-bermodus-ai-meningkat-115-umkm-jadi-sasaran-empuk-zlosc/

East Asia Forum. (2024). Tempering the Philippines' AI disinformation storm.

Economic Research Institute for ASEAN and East Asia (ERIA). (2025). AI to Transform 3 Key Sectors in ASEAN. Policy Brief.

Infosecurity Magazine. (2024). Over a third of employees secretly sharing work info with AI.

Kearney. (2025). Racing Toward the Future: Artificial Intelligence in Southeast Asia. Singapore: Kearney Insights Series.

Media Indonesia. (2025). AI bantu UMKM hingga korporasi tekan biaya operasional. Retrieved from: https://mediaindonesia.com/ekonomi/798039/ai-bantu-umkm-hingga-korporasi-tekan-biaya-operasional#google_vignette

Nasscom. (2025). Unlock AI's Potential for Tech-Enabled MSMEs. Whitepaper.

National University of Singapore (NUS). (2025). AI Adoption in India: Moving the Needle Forward. Singapore: NUS Digital Transformation Centre.

Quest Ventures. (2025). AI and the Future of SMEs in Asia.

Tatler Asia. (2025). How AI is helping small businesses punch above their weight in emerging markets.

The Straits Times. (2024, May 29). SMEs to get help in using generative AI, tech workers to be upskilled.

United Nations Office on Drugs and Crime (UNODC). (2024). Billion-dollar cyberfraud industry expands in Southeast Asia as criminals adopt new technologies.

Xenoss. (2025). APAC AI regulations 2025: China, Japan, Korea, India, Australia.

The APAC Cybersecurity Fund

The APAC Cybersecurity Fund is an initiative by The Asia Foundation, supported by Google.org, Google's philanthropic arm, designed to build inclusive and sustainable cybersecurity ecosystems across the Asia-Pacific region. Through cyber hygiene training, policy research, and stakeholder engagement, the program helps micro and small businesses, nonprofits, and social enterprises strengthen their cyber resilience. It also invests in long-term capacity by establishing more than 20 university-based cyber clinics to expand outreach and develop the region's cybersecurity workforce. The initiative spans across 13 countries including Australia, Bangladesh, India, Indonesia, Japan, Korea, Malaysia, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam.

CyberPeace Institute

The CyberPeace Institute protects the most vulnerable in cyberspace. We deliver cybersecurity assistance and hold all actors accountable for ensuring peace in cyberspace by exposing the human harm caused by cyberattacks and disinformation. We advocate against the unacceptable use of artificial intelligence to threaten international peace and security, while promoting the responsible development and use of AI.

The Asia Foundation

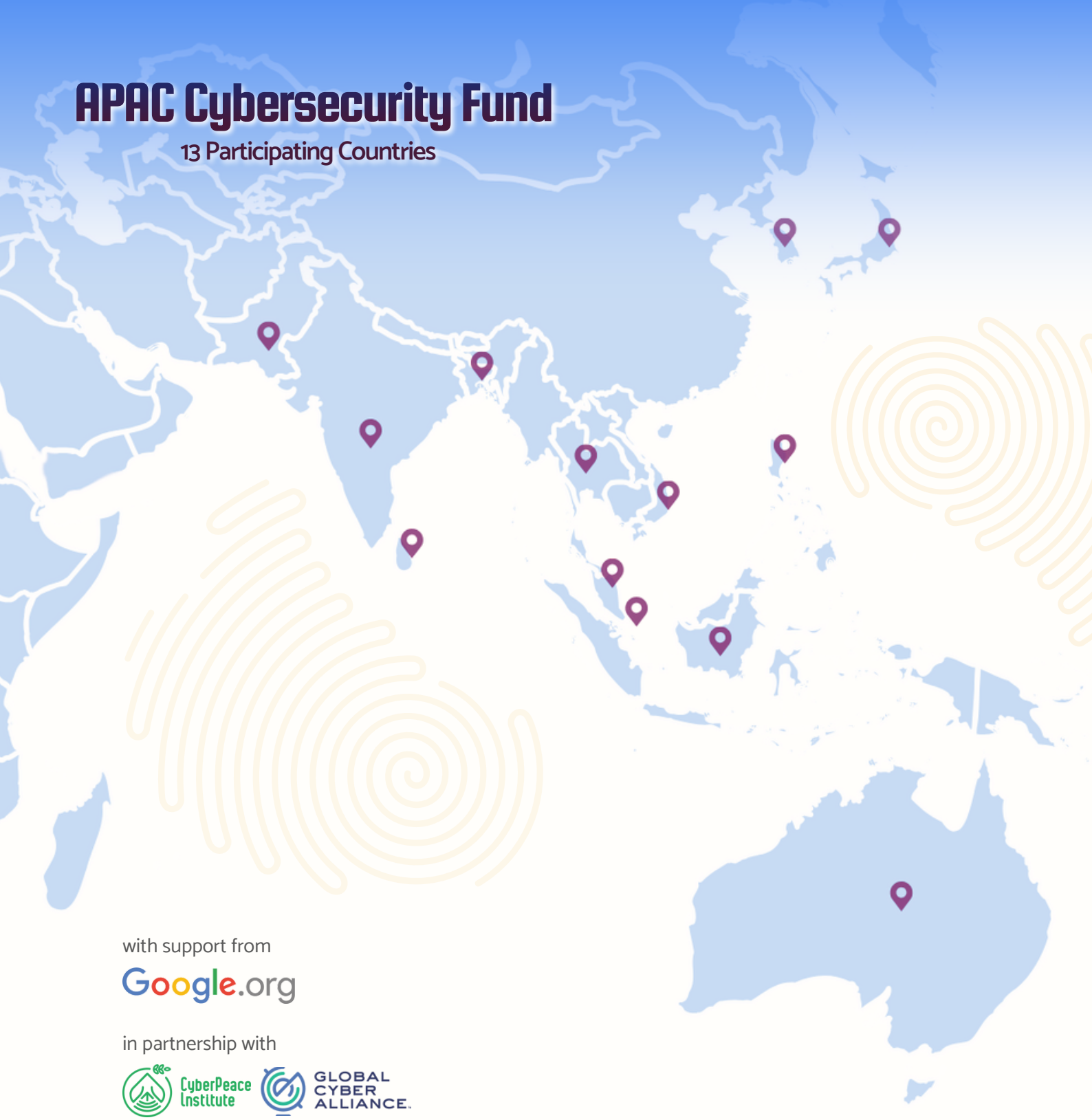
The Asia Foundation is an international nonprofit organization working to solve the toughest social and economic challenges in Asia and the Pacific. Informed by more than 70 years of experience and deep local knowledge, we work with partners across more than 20 countries to improve lives and expand opportunities.

Google.org

Google.org, Google's philanthropy, brings the best of Google to help solve some of humanity's biggest challenges combining funding, product donations and technical expertise to support underserved communities and provide opportunity for everyone. We engage nonprofits, social enterprises and civic entities who make a significant impact on the communities they serve, and whose work has the potential to produce scalable, meaningful change.

APAC Cybersecurity Fund

13 Participating Countries



with support from

Google.org

in partnership with

CyberPeace Institute

GLOBAL CYBER ALLIANCE

The Asia Foundation

The Asia Foundation
Kuala Lumpur, Malaysia
www.asiafoundation.org

© The Asia Foundation 2025