ASIA COLLECTIVE 2025: POST-CONFERENCE REPORT

Event Overview

The event brought together senior military and law enforcement officers, government officials, experts and academics, researchers, business and industry leaders, and international organisations. We hosted nearly 200 international participants from 13 countries including officials from embassies and government/diplomatic organisations.

Program Topics

Opening Remarks

Mr. Goh Eng Choon, Executive Vice President, ST Engineering, emphasized that collaboration among governments, the military, the private sector, and experts is essential to address complex cyber threats amid rapid technological advances such as AI and quantum computing. He highlighted that cybersecurity is foundational to national resilience, economic stability, and public trust, stressing the necessity of collective action, shared intelligence, and innovation to build a proactive, adaptive cyber defence posture. ST Engineering is committed to co-creating solutions, investing in next-generation capabilities, and developing cyber talent, positioning the forum as a platform to transform ideas into partnerships and shared actions.

Asia Collective
e contact@asiacollective.org
w https://asiacollective.org

Panel 1: Industry Experts & Academics - *Moderated by Elliot Danker*

Panelists: **Daisy Radford** (Reversec), **Farlina Said** (ISIS Malaysia), **Lim Yihao** (Google), and **Professor Peixi Xu** (Communication University of China).

The first panel explored the private sector's role in securing public-private partnerships for cyber defence, examining the uneven cyber readiness across ASEAN member states and identifying pathways to close capability gaps.

Regional Cyber Readiness and Development

Professor Xu noted that uneven cyber capacity is typical even within China, where cybersecurity remains fragmented and provincial despite the market reaching $10 billion. He emphasized China's Global Data Security Initiative, which promises that Chinese companies operating abroad will not be obligated to share non-Chinese user data with Chinese authorities. Daisy Radford highlighted quantum computing as a critical example where the private sector should not run ahead without regulation, advocating for ASEAN to collectively establish regional standards rather than defaulting to external frameworks. Lim Yihao pointed out that threat intelligence data shows manufacturing and retail, not banks, as the most successfully targeted industries, emphasizing that cyber criminals are indiscriminate and exploit low-hanging fruit across all sectors.

Policy Development and Leadership

Farlina Said examined ASEAN's progress from the 2017 Cyber Security Cooperation Strategy to the current 2021-2025 framework, noting that while some countries are still drafting critical infrastructure protection and data protection regulations, significant progress has occurred. She emphasized that governments are both regulators and users, and that private sector leadership in establishing principles and management processes can shape governance landscapes. The discussion highlighted that successful partnerships require synergy between sectors, with private innovation potentially informing government guidelines while recognizing that regulations may not always align with all private sector developments.

Data Sovereignty and Cross-Border Cooperation

The panel debated data localization versus cross-border data flows. Lim Yihao noted Ukraine's success in maintaining operations during conflict by uploading critical applications to cloud infrastructure outside the country. Professor Xu distinguished between digital economy perspectives favoring globalization and cybersecurity concerns where fragmentation might offer protection. Farlina Said highlighted that AI development is driving renewed interest in maintaining data within borders to build local data assets for training models, particularly for localized languages and applications.

Technology Standards and Market Dynamics

Discussion centered on how market access influences standards adoption and the challenges of balancing innovation with security. Daisy Radford praised Singapore's Cybersecurity Act as a practical blueprint, citing its conditional approach where entities like the Shangri-La hotel must meet national infrastructure standards during high-security events but not during normal operations. The panel contrasted this with GDPR, which Professor Xu criticized as hurting European business through overly high standards, while Lim Yihao noted that GDPR makes cyber investigation more difficult by obscuring website registration information used by criminals.

Threat Intelligence Sharing

Singapore's announcement to share classified threat intelligence with critical infrastructure operators was highlighted as a significant development. Lim Yihao explained that while government threat intelligence is superior due to resources and collection capabilities, recipients must develop proper data management processes to prevent leaks that could create diplomatic crises. He also revealed that threat actors are increasingly using AI tools like Gemini for reconnaissance, phishing email creation, and even automated source code rewriting to evade signature-based detection, with one recent case showing malware calling Gemini API hourly to recompile and change signatures.

Building Trust and Collaboration

The panel identified matchmaking as a critical gap, with both governments and private sector interested in collaboration but often lacking communication channels. Farlina Said noted that researchers frequently discover both parties are interested but waiting for the other to initiate contact. Daisy Radford emphasized that financial institutions already report emerging threats to government agencies under strict timelines, and this relationship must be reciprocal to be effective. The discussion concluded that forums like Asia Collective provide essential spaces for convergence where stakeholders can discover mutual interests and establish connections.

Asia Collective
e contact@asiacollective.org
w https://asiacollective.org

Fireside Chat: Military, Civilian or Policy - Who Takes the Lead?

***Benjamin Ang** (RSIS) in conversation with **Nicholas Fang** (Black Dot)*

The fireside chat explored fundamental questions about leadership in cybersecurity, examining whether military, civilian, or policy sectors should drive cyber defence strategy and how to balance national security, privacy, and innovation.

Singapore's Regional Positioning

Benjamin Ang reflected on the 10th Singapore International Cyber Week, emphasizing its role as a platform for global cyber leaders to meet, build communication channels, and establish trust that enables mutual assistance during crises. He highlighted how Cyber Week facilitates not just learning about new developments but crucial bilateral meetings among top practitioners. Ang noted the blurring of lines between military and civilian cyber issues, citing how ransomware, once considered purely a law enforcement matter, has evolved into a state-to-state tactic, as seen in NotPetya and WannaCry attacks.

The Expanding Attack Surface

Ang emphasized that cyber threats ultimately target humans, not just systems. He explained that while movies portray exciting server hacking, real-world attacks primarily exploit human vulnerabilities through phishing and social engineering. Even when soldiers work on secure military networks, they return home to use personal devices, home computers shared with family, and internet-connected TVs, all potential infection vectors. He illustrated this with the deepfake Zoom call incident where a finance manager was fooled by AI-generated impersonations of executives and transferred millions, emphasizing that systems must include failsafes to catch human errors rather than relying solely on user vigilance.

Team Sport: Who Leads?

When pressed on whether military, civilian, or policy should take the lead, Ang invoked Cyber Security Commissioner David Koh's mantra: "Cybersecurity is a team sport." He explained that protection requires military systems for personnel, civilian infrastructure from telcos and

others, and policy incentives, such as requiring banks to implement safeguards preventing instant transfer of life savings. This coordination must extend beyond national borders to regional cooperation among law enforcement and militaries, given the interconnected nature of threats.

Centralized vs. Decentralized Models

Ang proposed a "team of teams" approach rather than strict centralization or decentralization. Different organizations have unique requirements, making identical rules impractical, but providing guidelines toward common goals allows flexibility. He cited Singapore's adaptive approach: operational technology cybersecurity guidelines have reached version 2.0 for emerging technologies, with separate frameworks for AI and generative AI cybersecurity. Rather than rigid laws that quickly become outdated, Singapore uses guidelines that can adapt as technology evolves, balancing security needs with innovation.

Whole-of-Nation Approach

Ang provided three examples of Singapore's integrated strategy: annual cyber exercises bringing together critical infrastructure owners, cyber defenders, and military personnel to build connections and practice joint response; Singapore's participation in NATO's Locked Shields exercise with a combined Singapore-Germany team that included private sector and civilian participants; and Minister Shanmugam's announcement that government would share classified threat intelligence with critical infrastructure operators, a significant shift from a decade ago when such sharing was considered impossible. Ang emphasized that mutual sharing between those with whole-country oversight and sector-specific visibility is essential for catching threats before they materialize.

Regional Trust and Confidence-Building

On building trust among potential rivals, Ang emphasized confidence-building measures (CBMs) within the region. The ASEAN point of contact database enables countries to reach out when detecting suspicious activity originating from another nation, facilitating cooperation rather than accusation. He stressed that bilateral meetings at events like Asia Collective and the ADMM Cyber Info Centre of Excellence's Digital Defense Symposium build familiarity, putting faces to names so that during conflicts, communication channels already exist. Regarding great power tensions, Ang acknowledged that every country must carefully balance relationships, but noted that non-state threats like ransomware gangs transcend geopolitical alignments, creating common ground for cooperation.

Cybercrime-as-a-Service Threat

Ang highlighted the alarming scale of cybercrime: Australia loses $600 million annually and Singapore loses $1 billion. These well-resourced cybercrime gangs possess sophisticated methods and captured data that they sell to the highest bidder. While cooperation against cybercrime gangs unites all nations regardless of geopolitical alignment, Ang warned that these groups function as mercenary cyber forces with no loyalty, working for anyone who pays, potentially switching sides overnight. This creates a complex threat environment

beyond traditional state-based polarization.

Future Regional Cooperation

Regarding ASEAN's cyber strategy for 2026-2030, Ang emphasized incorporating forward looking threat intelligence. While AI and quantum computing are current concerns, with quantum potentially breaking common encryption within 5-20 years, future strategies must remain adaptive through constant research and regular review periods. He pointed to the UN Open-Ended Working Group, which has transitioned from a five-year cycle to a permanent mechanism for annual multilateral cyber discussions. While acknowledging the idealism of global cooperation, Ang argued there's no alternative: incremental progress on shared concerns like ransomware, scams, and citizen protection offers the best path forward, even when complete agreement proves impossible.

Panel 2 Discussion: Defence Perspectives on Cyber Cooperation

Moderated by Muhammad Faizal bin Abdul Rahman, Research Fellow at S. Rajaratnam School of International Studies (RSIS), NTU

The panel opened with two key messages: secure cyberspace is central to trust in the digital economy, and strong cooperation between governments, industry, and technology sectors is essential for regional security. Each speaker outlined their cyber defence priorities:

- **Colonel Joey Fontiveros** stressed that growing interconnectivity drives more sophisticated cyber threats, making proactive protection and unhindered military freedom of action in cyberspace essential.
- **Rear Admiral Fadhil bin Abdul Rahman** highlighted Malaysia's focus on safeguarding command-and-control networks and ICT-dependent systems, noting that expanding responsibilities increasingly require national-level support and close cooperation with industry, government agencies, and academia.
- **Air Marshal Rudy Gultom** emphasized that cyberspace has become a fifth domain of

warfare, with Indonesia facing rising attacks. He explained that Indonesia's National Cyber and Encryption Agency (BSSN), established in 2016, leads national cyber defence and protects eight critical infrastructure sectors.

- **Colonel Clarence Cai** described Singapore's newly inaugurated Defence Cyber Command, which unifies existing SAF cyber units to secure military networks and bolster national cyber defence, leveraging substantial talent through Singapore's conscription system in partnership with the Cyber Security Agency.

Strategic Planning and Coordination

On how Southeast Asian countries should approach strategic cyber-defence planning across military, civilian agencies and private sector, panelists emphasized different frameworks: Colonel Joey highlighted balancing people, processes and technology; Admiral Fadhil argued for top-down political leadership with strong budget commitment; AM Rudy outlined three pillars; trust, transparency and technology, describing cybersecurity as requiring collaboration across government, industry, academia and users in a "quadruple helix"; and Colonel Clarence expanded on this inclusive approach, noting that clear boundaries between military and civilian responsibilities no longer hold.

Public-Private Partnership Challenges

Colonel Joey argued that military must actively engage and work alongside the private sector, with cyber defence exercises now including reservists, civilians, academia and other agencies. Admiral Fadhil emphasized that rapid technological change makes private-sector collaboration indispensable, though he noted cost challenges when products are tagged for military use. AM Rudy reiterated his three pillars for shifting from reactive defence to proactive resilience. Colonel Clarence highlighted that private companies often have far greater visibility of cyber activity than governments, making public-private partnership essential. Singapore's SIDEX exercises bring private firms into training scenarios so military can learn from real-world threats.

Intelligence Sharing

On sharing classified cyber-threat intelligence with the private sector, Colonel Joey argued that threat intelligence concerning critical infrastructure should ultimately not remain classified. Admiral Fadhil agreed, adding that intelligence sharing must be selective to avoid overwhelming operators with uneven defensive capacities. AM Rudy acknowledged it's a significant step that blurs boundaries between national-security institutions and commercial tech ecosystems. Colonel Clarence pointed to existing mechanisms like the ASEAN Cyber Defence Network and ADMM Cyber and Info Centre of Excellence, stressing the need for both bilateral exchanges and multilateral channels as "herd immunity" against threats.

Wartime Integration and Risk

Drawing on Ukraine's experience integrating civilian cyber experts during wartime, panelists discussed protecting private partners during crises. Colonel Clarence argued that nations should organize reservists and skilled civilian networks in peacetime for effective mobilization during conflict. Colonel Joey stressed that strict vetting is essential in the Philippines before

Asia Collective
e contact@asiacollective.org
w https://asiacollective.org

external partners support military cyber capabilities. Admiral Fadhil acknowledged the difficulty of safeguarding private-sector actors once they assist military in conflict. AM Rudy underscored the need for peacetime preparation through trust frameworks, secure data sharing mechanisms, and clear protocols.

Regional Exercise Feasibility

On conducting joint ASEAN cyber-defence exercises, Colonel Joey supported the idea but cautioned that ASEAN is not yet ready for a full joint exercise requiring mature, real-time collaborative platforms. However, Admiral Fadhil argued that regional cyber exercises are already feasible in technical formats like cyber-range activities or capture-the-flag simulations. AM Rudy endorsed the idea, emphasizing that cyber threats are borderless and can propagate across ASEAN within seconds. Colonel Clarence welcomed the prospect, noting many ASEAN militaries already conduct joint activities where cyber-defence elements can be integrated incrementally.

Cloud Infrastructure Resilience

Discussing lessons from recent cloud service disruptions, Colonel Joey emphasized the need to bolster defence through balanced people, processes and technology. Admiral Fadhil argued for sovereign cloud capabilities and separate defence clouds, noting no organisation is immune. AM Rudy proposed his Six-Ware Cyber Security Framework (brainware, hardware, software, infrastructure-ware, firmware and budgetware), stressing that adequate funding is essential. Colonel Clarence observed that whether outages are malicious or accidental, their effects are the same, urging investment in resilience through redundancy, graceful failure and contingency planning.

Closing Remarks by Farlina Said

Director of Cyber and Technology Policy Programme at ISIS Malaysia

Ms. Said thanked attendees for the insightful conversations throughout the event, highlighting the panels, fireside chat, and meals. She announced that the next Asia Collective Forum will be held in Kuala Lumpur next year and expressed eagerness to continue the discussions then.

Our Partners

M Group Asia

An established business solution service provider to a comprehensiverange of corporations to SMEs, MNCs, local and overseas companies and individuals, combining on-the-ground leg work with top-level strategic insights to deliver the highest quality analysis and value-added solutions. They provide unique insights into how governments, economies, companies and individuals in the Asia-Pacific converge and make decisions that impact businesses.

Semar Sentinel

A consulting firm specialised in security, defence and aerospace sectors. Semar Sentinel offers services and solutions to partners and clients, to get a better understanding of opportunities they might encounter and threats they might be confronted with, shedding light on security, defence and aerospace issues and matters.

International Development and Security Cooperation (IDSC)

A non-profit policy research organisation dedicated to advancing global development converging holistic, strategic, and progressive discourses on transnational development and regional security issues through collaboration, education, research, and training. IDSC helps policymakers make decisions based on evidence-based research and for academics to contribute to an alternative, balanced, and independent platform through shared intelligent conversations with premiere analysts across the globe.

United Peace Keepers Federal Council (UNPKFC)

They collaborate with UN Agencies and other International Organizations for supporting the Peacekeeping missions and mandates of the United Nations, engaging and promoting Peace Building process globally. As part of their UN-mandated responsibility to help prevent, mitigate, and resolve violent conflict abroad, the UNPKFC joins the efforts being undertaken by civil society organizations, elected officials and governments across the world to address issues of justice, diversity, equity, and inclusion in the field of peace-building.

Asia Collective
e contact@asiacollective.org
w https://asiacollective.org

Mirage Defence

A leading provider of comprehensive defence solutions, specialising in consultancy services, product distribution, and representation for defence and security industries. They work closely with government agencies, military organisations, and private sector clients to deliver tailored strategies and solutions that meet the ever-evolving challenges of today's defence landscape. Mirage Defence's consulting services encompass a wide range of areas, including threat assessment, risk analysis, strategic planning, and policy development.

ISIS Malaysia

As a premier think-tank, ISIS Malaysia engages actively in Track Two diplomacy, and promotes the exchange of views and opinions at both the national and international levels. The institute has also played a role in fostering closer regional integration and international cooperation through forums, such as the Asia-Pacific Roundtable, Asean Institutes of Strategic and International Studies, Pacific Economic Cooperation Council and the Network of East Asian Think-Tanks..