Narrative Report

Southeast Asia stands at a critical juncture as digital technology expands alongside rising cyber threats. The GFCE regional meeting addressed this challenge by fostering dialogue on regional cybersecurity capacity building and exploring AI's role in combating cybercrime. Aligned with GFCE's mission, the event emphasized tailored strategies for Southeast Asia, aiming to strengthen collective defenses through collaborative discussions on innovative solutions to protect the region's digital infrastructure and citizens.

The half-day event brought together nearly 100 representatives from ASEAN member states and other regional stakeholders in person in Singapore on Wednesday, October 16, alongside the Singapore International Cyber Week (SICW), to reflect on the evolution of the cybercrime landscape in the region and the role of AI in combating cybercrime and bridging the existing workforce capacity gap. The meeting also served to engage with regional stakeholders on activities of the SEA GFCE regional hub.

Welcome and Opening Remarks – Ms. Phua Puay Li, CSA, and Mr. David van Duren, GFCE

Ms. Phua Puay Li highlighted that in our interconnected world, a single cyber attack can disrupt economies and national security, making global cooperation essential to combat cyber threats. Cyber capacity building is critical, and multi-stakeholder engagement involving governments, industry, and civil society is needed to strengthen resilience. Programs like Singapore's ASEAN Cyber Security Center and the UN-Singapore Cyber Fellowship provide training across technical, legal, and policy domains, equipping leaders to address evolving threats. Collaborative initiatives are expanding globally, aiming to equip countries with the tools and strategies necessary to respond effectively to cyber risks. Ultimately, a unified, cooperative approach will build a secure and resilient digital environment.

Likewise, Mr. David van Duren emphasized the importance of collaboration, knowledge-sharing, and a regional approach to tackle cybersecurity fragmentation. GFCE regional hubs across Southeast Asia, Africa, and other regions focus on aligning cyber initiatives with local needs by fostering partnerships, identifying capacity gaps, and connecting expertise. Through a community-driven, demand-focused model, the GFCE aims to unify global cyber efforts for a resilient digital future.

Setting the stage for discussion – Mr. Allan Cabanlong, Director, GFCE Southeast Asia Hub

This year's Southeast Asia Regional Meeting focus on "Bridging Capacity for AI and Cybercrime Prevention" is timely for Southeast Asia, where rapid digital growth has created both opportunities and vulnerabilities. While digital advancements boost economic growth, they also increase exposure to AI misuse and cybercrime. The GFCE supports local capacity-building by fostering knowledge exchange and practical solutions across the region, helping strengthen cybersecurity readiness. Yet, Southeast Asia remains a target due to legal and governance gaps. This meeting promoted regional cooperation, best practices, and stakeholder empowerment to address these challenges and build a safer digital ecosystem for Southeast Asia.

(1) Panel Discussion: AI for Good: Leveraging AI to Combat Cybercrime

Moderator: Mr. Keith Detros, Programme Lead, Tech for Good Institute

Speakers:

- Ms. Lee Pei Ling, Head, Cyber Strategy and Capabilities Development, Cybercrime Directorate, INTERPOL
- Ms. Nina Bual, Co-Founder, Cyberlite
- Ms. Siti Liyana Azman, Junior Research Fellow, Global Research Network

The panel explored the intersection of technology and cybersecurity in Southeast Asia's digital landscape. With rapid digitalization posing significant challenges to secure digital environments, the discussion underscored the need for collaboration among stakeholders.

Panelists identified three factors complicating cybersecurity: the accelerated pace of technological innovation, the rise of mobile-first technologies, and AI's disruptive impact on traditional defenses. These elements contribute to a complex ecosystem where everyday online activities are vulnerable to sophisticated threats like phishing and deepfakes. Law enforcement agencies, including Interpol, are adapting by developing responsible AI toolkits that ensure ethical practices.

Education emerged as a critical concern, particularly for younger generations interacting with AI. Initiatives like Singapore's Tech30 Strategy aim to integrate AI safely in classrooms while promoting digital literacy and cybersecurity awareness. The discussion also emphasized regional cooperation to align local cybersecurity efforts with global standards.

Panelists argued for viewing AI not just as a facilitator of cybercrime but as a vital tool for law enforcement, aiding in tasks like vulnerability classification and anomaly detection. Innovative uses of large language models (LLMs) were explored, revealing their potential in creating deceptive phishing emails and countermeasures.

Moreover, AI's ability to analyze language patterns can help identify cyberbullying, enhancing child safety online. The panel called for greater community engagement and transparency regarding AI technologies. Ultimately, the discussion framed AI as a promising asset in the fight against cybercrime, advocating for public awareness campaigns to transform perceptions of AI into a beneficial tool for enhancing cybersecurity efforts.

(2) Panel Discussion: Bridging the Capacity Gap: Building a Regional AI and Cybersecurity Workforce

Moderator: Mr. Keith Detros, Programme Lead, Tech for Good Institute

Speakers:

- Ms. Lee Pei Ling, Head, Cyber Strategy and Capabilities Development, Cybercrime Directorate, INTERPOL
- Ms. Nina Bual, Co-Founder, Cyberlite
- Ms. Siti Liyana Azman, Junior Research Fellow, Global Research Network

The panel highlighted significant talent shortages in AI integration and cybersecurity across Southeast Asia, particularly in sectors such as FinTech and e-commerce. An estimated shortage of over 1.5 million cybersecurity roles underscores the rising demand for professionals in this field. Various initiatives, including those spearheaded by Singapore's cyber agency, aim to build regional capacities through educational programs and partnerships involving governments, the private sector, and academic institutions.

Experts noted a mismatch between rapid technological advancements in AI and the lack of relevant professional training, leaving graduates unprepared for the job market. This issue is exacerbated by the high costs of cybersecurity certifications, which many potential candidates find prohibitive. While there is a growing commitment to cybersecurity across Southeast Asian nations, implementing effective strategies remains challenging due to insufficient local expertise and funding. Models, such as public-private partnerships, are being explored to enhance training and education in cybersecurity. Improving coordination and resource allocation is seen as essential for developing a sustainable workforce in both AI and cybersecurity.

Furthermore, the urgent need for women's inclusion in the cybersecurity workforce was emphasized, as they currently represent less than 25% of the field. Initiatives like the Cyber Girls program by the Cyber Safe Foundation, which trains and mentors young women in Africa, serve as important examples of how to foster support systems such as mentorship and networking. This program not only trains women but also cultivates a supportive community, thereby enhancing their career growth and retention in the industry.

The conversation also addressed the necessity for political and cross-border collaboration in cybersecurity education, particularly in Southeast Asia and the Pacific Islands. Trust-building among countries is crucial for sharing information and resources. While establishing regional centers of excellence is proposed, challenges related to funding and sustainability persist.

International cooperation is further encouraged, with calls for developed countries to provide scholarships for students from low-income nations, enabling them to return home with skills to bolster their local cybersecurity workforce. Addressing issues like brain drain is critical for maintaining skilled talent within developing regions.

Closing remarks – Mr. Allan Cabanlong, Director, GFCE Southeast Asia Hub

During the meeting, participants reflected on the critical cybersecurity challenges facing Southeast Asia, particularly with the increasing influence of artificial intelligence and foreign

cyber threats. The discussions highlighted the urgent need for capacity building, emphasizing the importance of enhancing technical skills, legal frameworks, and public-private partnerships. It became clear that regional collaboration was essential, as cyber threats are transnational and require a united approach. Empowering stakeholders, including marginalized voices, was recognized as vital to fostering a safer digital future. In closing, the meeting underscored the commitment of all participants to translate insights into actionable steps, aiming for a more secure and resilient Southeast Asia through continued collaboration and support.