ASEAN REGIONAL FORUM

Promoting peace and security through dialogue and cooperation in the Asia Pacific

Co-Chairs' Summary Report

ASEAN Regional Forum Workshop

on Fostering Professionals on Security of and in the Use of ICTs

13 June 2023, Hanoi, Viet Nam

Introduction

1. The ARF Workshop on Fostering Professionals on Security of and in the Use of ICTs, co-chaired by the Republic of Korea (ROK) and the Socialist Republic of Vietnam, was held on 13 June, 2023, in Hanoi. The workshop was attended by ASEAN Regional Forum participating countries, Brunei Darussalam, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand, the Commonwealth of Australia, the People's Republic of Bangladesh, Canada, the European Union, the Republic of India, Japan, the Russian Federation, and the United States of America, which were represented by government officials and cybersecurity professionals from industry and academia. The list of attendance appears in **ANNEX 1**.

2. The workshop was divided into three sessions:
   A. *Session I: The current status of fostering cybersecurity professionals in the region*
   B. *Session II: The private sector's system of training cybersecurity experts*
   C. *Session III: The ASEAN-targeted cybersecurity capacity building programs*

   The final agenda appears in **ANNEX 2.**

Opening Remarks

3. In his opening remarks, H.E. Hyun Woo Cho, Ambassador for International Security Affairs of the ROK, highlighted that malicious cyber activities threaten not only individuals and businesses, but also international security. He emphasized that the Democratic People's Republic of Korea (DPRK) is securing funds for its nuclear and missile program by stealing cryptocurrency, which threats the ASEAN countries. In this regard, he noted the importance of strengthening the capabilities of partner countries in the region to respond to

these threats effectively. Furthermore, he announced that the ROK wants to actively contribute to this, based on its technological advancements, government policies, and practical experiences cumulated while responding to the DPRK's malicious cyber activities.

4. In his opening remarks, H.E. Vu Ho, Acting SOM Leader and the Director-General of the ASEAN Department of the Socialist Republic of Vietnam's Ministry of Foreign Affairs, mentioned that as the world is connected through the internet in cyberspace, it is important to prevent conflicts in cyberspace and promote the prosperity of all nations. He emphasized the contribution of the workshop and the ARF ISM ICTs in general to this effort, as the workshop aims to enhance the ICT security capabilities of member countries of the ARF and seeks to lay the groundwork for future collaborations among ARF members, specifically in training professionals in the field of ICT security and the safe utilization of ICTs.

Session I: The current status of fostering cybersecurity professionals in the region

Moderator: Mr. Nguyen Huu Phu, Deputy Director General of Law and International Treaties Department, Ministry of Foreign Affairs.

Speakers

- Ms. Nguyen Thi Minh Thu, Deputy Head of Division, Information and International Cooperation Division, Authority of Information Security, Ministry of Information and Communication, Vietnam
- Ms. Hyun-O Kwon, Vice President, Korea Internet & Security Agency (KISA), ROK
- Ms. Lim Shin Yi, Senior Assistant Director, Cyber Security Agency (CSA) of Singapore

Speaker 1: Ms. Nguyen Thi Minh Thu

5. Ms. Nguyen Thi Minh Thu briefed on Vietnam's policy related to strengthening cybersecurity and fostering experts. She elaborated on the Law on Information Security in 2015, the Law on Cybersecurity in 2018, and several of the Prime Minister's Decisions related to training and developing cybersecurity human resources, such as the PM Decision 21 (approving the project on "Training and development cybersecurity human resources" for the 2021-2025 period). Furthermore, she briefed on the main activities conducted under PM Decision 21, such as short-term training courses, standardization of cybersecurity skills, and overseas training courses for university lecturers and researchers. Despite these endeavors, she also mentioned the challenges that Vietnam is encountering, such as the shortage of cybersecurity experts, limited practical training environment, and lack of close cooperation on human resource needs between training institutions, enterprises, and organizations.

Speaker 2: Ms. Hyun-O Kwon

6. Ms. Hyun-O Kwon briefed on the ROK's basic system of promoting cybersecurity and its plan to foster 1 million cybersecurity talents, which was announced in July 2022. In addition, she elaborated on the ROK's projects for fostering domestic cybersecurity professionals, such as K-Shield and Security-Gym. K-Shield is a program run by the Korea Internet & Security Agency (KISA) to foster experts in the field of cybersecurity. It is divided into K-Shield for cybersecurity-related employees and affiliated companies and K-Shield Junior for high school graduates. Security-Gym is a training facility designed to enhance incident response capabilities by simulating various attacks and conducting practical defense training in a virtual breach incident environment.

7. In addition, she introduced the ROK's initiatives for global cooperation, such as ASEAN Cyber Shield and the Cybersecurity Alliance for Mutual Progress (CAMP). ASEAN Cyber Shield is an initiative to apply the successful model of K-Shield to ASEAN countries. CAMP is a network platform for the capacity building of the participants. It has 64 organizations from 48 countries as members and holds annual meetings and regional forums. The ASEAN Cyber Shield project was elaborated more in Session 3 by Ms. Hye-in Song of KISA.

Speaker 3: Ms. Lim Shin Yi

8. Ms. Lim Shin Yi said that growing a robust cyber talent pipeline is one of the foundational enablers for Singapore Cybersecurity Strategy 2.0. She introduced three strategic thrusts for building a robust cyber talent pipeline: (a) Supporting youths, women, and mid-career professionals in pursuing a cybersecurity career; (b) Creating an upskilling culture for a globally competitive workforce; and (c) Fostering a dynamic sector with strong professional communities. Furthermore, she elaborated on Singapore's initiative, SG Cyber Talent, that nurtures talented cybersecurity enthusiasts from a young age and helps cybersecurity professionals deepen their skills. The programmes for building cybersecurity talent development pipeline are developed with the key target groups, such as pre-tertiary students, tertiary students national servicemen, fresh professionals and mid-careerists. In addition, she introduced projects that Singapore is running, such as scholarships, degree programmes, and the Cyber NSF Scheme to build up cyber talent through training the full-time National Servicemen with requisite aptitude and skills.

Panel Discussion

Moderator: Mr. Nguyen Huu Phu

Panelists

- Ms. Nguyen Thi Minh Thu, Deputy Head of Division, Information and International Cooperation Division, Authority of Information Security, Ministry of Information and Communication, Vietnam
- Ms. Hyun-O Kwon, Vice President, Korea Internet & Security Agency (KISA), ROK
- Ms. Lim Shin Yi, Senior Assistant Director, Cyber Security Agency (CSA), Singapore
- H.E. Hyun Woo Cho, Ambassador for International Security Affairs of the ROK

Theme: How to bridge the cybersecurity capacity gap in the region, especially by applying the examples presented by the speakers?

9. The moderator asked Ms. Nguyen Thi Minh Thu which projects of the ROK and Singapore mentioned during the presentations could be referenced by Vietnam. She replied that Vietnam can learn from the ROK's K-Shield and Singapore's Skills Framework for ICT.

10. The moderator asked Ms. Hyun-O Kwon which was the most successful policy for fostering cybersecurity professionals in the ROK. She replied that proper wages, improving working conditions, and developing a career path model are needed to foster cybersecurity experts, among which she emphasized the importance of proper wages.

11. The moderator asked Ambassador Hyun Woo Cho for his take on the role of the ROK in complementing the existing cyber capacity-building programs for partner countries. He suggested two points. First, he mentioned that the DPRK is diversifying its target to ASEAN countries, as we can see from the example of the DPRK stealing 6.2 billion dollar-worth of cryptocurrency from a Vietnamese gaming company. In this regard, he emphasized the importance of the ROK's sharing of experiences and best practices in responding to the DPRK's malicious cyber activities and introduced the ROK's relevant efforts, such as the hosting of symposiums. Second, he explained that the ROK has outstanding cybersecurity companies and has incorporated them in cyber capacity-building projects, such as ASEAN Cyber Shield.

12. The moderator asked Ms. Lim Shin Yi about the process Singapore has gone through to achieve the current level of the cybersecurity workforce. She replied that Singapore began to foster cybersecurity professionals since CSA was

established in 2015 has developed SG Cyber Talent, to develop programs for each target audience by closely cooperating with stakeholders through various government-to-government and government-to-private sector channels.

Question and Answer Session

13. The moderator opened the floor for questions. A participant from the Philippines asked how each country has persuaded high government officials or parliament to enact laws or make policies to strengthen cybersecurity.

14. Ms. Hyun-O Kwon answered that the ROK didn't need serious persuasion as it already had a nationwide consensus on strengthening cybersecurity and fostering experts. Ambassador Hyun Woo Cho added to this and explained one example: the revision of the Act on Reporting and Using Specified Financial Transaction Information. He mentioned that the ROK also experienced a conflict of interest with regard to the need to regulate cryptocurrency exchanges. He said the ROK had assessed the need for and possible problems of regulation and figured out a balance.

15. Ms. Lim Shin Yi mentioned that in Singapore, CSA which is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information, was set up to provide dedicated and centralized oversight of national cybersecurity functions. CSA also works with sector leads, which are other government agencies, to protect Singapore's critical services. The Cybersecurity Act is one example of cybersecurity legislation that was tabled in the Parliament. There is also constant consultation with both the private and public sector organisations for new policies/programmes to be developed. Policies for other programmes such as cybersecurity ecosystem development will be guidelines.

16. Ms. Nguyen Thi Minh Thu reiterated the importance of evidence and public opinion when persuading high-ranking officials and parliament. Mr. Nguyen Huu Phu emphasized that it is important for one ministry to take the initiative in bolstering the legislation process by taking examples of Vietnam's two relevant laws (the Law on Information Security and the Law on Cybersecurity). In addition, he noted the importance of learning from the experiences of other countries on how they resolved conflicting interests and found balance.

Session II: The private sector's system of training cybersecurity expert

Moderator: Ms. Minhye Park, Senior Researcher, KISA

Speakers:

- Mr. Jin Won Choi, CEO, ALL iT ONE, ROK
- Dr. Cheol Ho Lee, Research Director, ENKI, ROK

- Ms. Hoang Phuong Linh, Marketing Director, Viet Nam Cecomtech Technology Coporation
- Mr. Huy (Dob) Nguyen, Professional Services Manager, Vietnam Network Security Joint Stock Company (VSEC)

Speaker 1: Mr. Jin Won Choi

17. Mr. Jin Won Choi began his presentation with a brief on the two generations of cybersecurity training, with the COVID-19 pandemic as a milestone. Before COVID-19, most cybersecurity education was focused on offline platforms, such as classroom training and computer -based classes. After COVID-19, as society became less face-to-face oriented and people began to rely more on online services, cybersecurity training paradigms shifted to more online-focused.
18. He then made the observation that due to the shift in the way cybersecurity training is delivered, its future will revolve around four tools - enhanced Learning Management System (LMS), cloud-based virtual training, attack simulators, and AI-based automatic scenario creation - which tech companies are accelerating investment and research into developing.
19. In conclusion, he said that by utilizing online education platforms, we can overcome the limitations of traditional offline education and offer high-quality education in every country, which will shape the future of cybersecurity education.

Speaker 2: Dr. Cheol Ho Lee

20. Dr. Lee presented on the topic of Fostering Cybersecurity: Up-Skilling Through Attack and Defense Training. He opened with numerous statistics to show the growth of the global cybersecurity training market in size and scope. He also gave the definition, simulation environment, target users, and use cases of Cyber Range to provide background knowledge.
21. Next, he introduced some global activities for cybersecurity training, such as the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity (NICE) Framework (USA), Locked Shields (NATO), and Cyber Storm (USA). He concluded by briefing about ENKI's Training Platform (the "VATE") and its outstanding features, including the simulated virtual training environment for various infrastructures, real-time attack and defense, gamification and career management.

Speaker 3: Ms. Hoang Phuong Linh

22. To begin with, she gave an overview of the roles of the private sector in cybersecurity training in Viet Nam. Most organizations, including the government sector, the financial banking system, and business sectors have gradually transformed their business models. The application of digital programs is accelerating, especially after the COVID-19 pandemic, and overcoming the difficult stages of this epidemic. However, the dependence on the internet also creates opportunities for cyber crimes to exploit, which further increases the demand for cybersecurity and the role of IT security workforce.

23. She also elaborated on the current frameworks and recent improvements in cybersecurity labor force training in Viet Nam. As part of this effort, Cecomtech has actively contributed by conducting training courses, organizing learning and international certification exams on security and cybersecurity, and establishing partnerships with international and national stakeholders.

Speaker 4: Mr. Huy (Dob) Nguyen

24. Mr. Dob shared his perspective on the relations between the state, the private sector, and communities in training cybersecurity experts in Viet Nam. As each stakeholder has its role and responsibility, understanding of cyberspace, and authority and capabilities for implementation, it is important to balance government and end-user demands, globally and among multiple stakeholders.
25. Furthermore, he took the VSEC as an example of how the private sector can contribute through both security professionals and security operation center services, especially the mentorship program to create an environment where everyone can grow. He emphasized that the contribution is not just about revenue but more about conveying value to the community.

Session III: Discussion on the ASEAN-targeted cybersecurity capacity building programs

Moderator: Ms. Minhye Park, Senior Researcher, KISA

Speakers

- Ms. Hye In Song, Manager, Korea Internet & Security Agency, ROK
- Mr. Nam-hyun Kim, Investigator, Supreme Prosecutor's Office, ROK
- Dr. Nguyen Viet Hung, Deputy Director of Information & Communications Technologies Institute, Le Quy Don Technical University

Speaker 1: Ms. Hye In Song

26. Ms. Hye In Song elaborated on two KISA cyber security capacity- building programs: the ASEAN Cyber Shield Project and the Global Cybersecurity Center for Development (GCCD). She explained the objectives, programs, types of activities, and plans of each initiative.
27. Regarding the ASEAN Cyber Shield Project, it has three missions: education, competition, and scholastic exchange. Through different activities such as R&D, seminars, competitions, networking, mentorships, internships, it aims to reinforce ASEAN cybersecurity capability and contribute to realizating of the Korea-ASEAN Solidarity Initiative.
28. She also briefed the Workshop on the GCCD. Established in 2015 under KISA, its objective is to enhance the information security capacity of emerging economies in collaboration with the Multilateral Development Bank. In 2023, several programs will be conducted, such as joint seminars, invitation-based

training, CIP consulting, and hands-on exercises in countries like Indonesia and Viet Nam.

Speaker 2: Mr. Nam-hyun Kim

29. Mr. Nam-hyun Kim introduced the APC-HU, a capacity-building training institution that offers comprehensive training on combating cybercrime to lawmakers, policymakers, judges, prosecutors, investigators, and other stakeholders across the Asia-Pacific region. He highlighted that APC-HUB has successfully organized its first training session, with delegations ranging from policymakers to law enforcement officers and from diplomats to judiciaries. The agenda included national cyber policies, cybercrime legislation, incident response, and international cooperation. He also shared that the preparation for the second training session is now underway.

Speaker 3: Dr. Nguyen Viet Hung

30. The final speaker, Dr. Nguyen Viet Hung, presented Information Security training programs at Le Quy Don Technical University (LQDTU). Viet Nam is a frequent target of spy operations yet faces a cybersecurity workforce shortage. Against this backdrop, the Government launched PROJECT 99 for education in cybersecurity, in which LQDTU was selected as a member of eight elite universities to carry out undergraduate and postgraduate training. Moreover, the University also promoted research areas such as smart malware analysis and detection, data loss prevention, and anomaly detection.