ASEAN THAILAND 2019
ADVANCING PARTNERSHIP FOR SUSTAINABILITY

CYBERSECURITY

IMPLICATIONS ON PEACE & SECURITY IN THE ASEAN REGION

10-11 MAY 2019
SHANGRI-LA HOTEL
BANGKOK, THAILAND

FINAL REPORT

Microsoft cisco paloalto NETWORKS UNODC United Nations Office on Drugs and Crime Symantec

CONTENTS

Concept of the Conference	4
Programme	10
Speakers & Panelists	16
Summary of Conference	24
Photo Gallery	34
Conference Organisers & Sponsers	44

ASEAN
THAILAND 2019
ADVANCING PARTNERSHIP
FOR SUSTAINABILITY

CONCEPT OF THE CONFERENCE

CONCEPT OF THE CONFERENCE

International Conference on "Cybersecurity: Implications on Peace and Security in the ASEAN Region" 10-11 May 2019, Shangri-La Hotel, Bangkok

BACKGROUND

Threats to Cybersecurity is increasingly sophisticated, transboundary and multi-dimentional. Cyberspace and Cybersecurity are now playing an increasingly important role in international peace and security, including in the ASEAN region. Cyberspace can be used to either strengthen or undermine peace and security of individual countries or of the overall region. For instance, at the regional and international levels, the Internet and social media are now widely used by extremist groups to recruit new followers across borders or even to signal attacks. At the national level, extensive studies revealed how the Internet and social media propaganda are being used to influence, distort or disrupt politics, as well as the peace and conflict management processes, in many countries, including those in the ASEAN region.

At the same time, due to advancement in technology, critical infrastructure and digital economies of countries, as well as the livelihood of their citizens, have become increasingly vulnerable to various forms of cyber threats, some of which are suspected to be state sponsored.

ASEAN Leaders see the need for ASEAN Member States to prepare themselves for the future and work closely with one another in working towards a common policy on cybersecurity.

At the 32nd ASEAN Summit in April 2018, the ASEAN Leaders issued their first-ever statement on **Cybersecurity Cooperation**. In the Statement, the ASEAN Leaders reaffirmed the need to build closer cooperation and coordination among ASEAN Member States on cybersecurity policy development and capacity building initiatives, including through the ASEAN Cyber Capacity Programme, the ASEAN Ministerial Conference on Cybersecurity (AMCC) and the ASEAN-Japan Cybersecurity Capacity Building Centre, towards the promotion of voluntary and non-binding cyber norms, as well as the development of a peaceful, secure and resilient rules-based cyberspace that will contribute to continued economic progress, enhanced regional connectivity within and improved living standards across ASEAN.

The ASEAN Leaders also recognised the need for all ASEAN Member States to implement **practical confidence-building measures** and adopt a set of common, voluntary and non-binding norms of responsible State behaviour in cyberspace, so as to enhance trust and confidence in the use of cyberspace to its full potential to bring about greater regional economic prosperity and integration.

The ASEAN Leaders further recognized the value of enhanced dialogue and cooperation on cybersecurity issues with Dialogue Partners and other External Parties, and in other ASEAN-led

platforms, including the ASEAN Regional Forum (ARF) and the ASEAN Defence Ministers' Meeting, together with the eight Dialogue Partners (ADMM-Plus).

The ASEAN Leaders also recognized the need for all ASEAN Member States to implement **practical confidence-building measures and adopt a set of common, voluntary and non-binding norms of responsible State behavior in cyberspace, in order to enhance trust and confidence in the use of cyberspace** to its full potential to bring about greater regional economic prosperity and integration.

The ASEAN Leaders tasked relevant Ministers from all ASEAN Member States to closely consider and **submit recommendations on feasible options of coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts among various platforms of the three pillars of ASEAN, so that ASEAN's efforts are focused, effective, and coordinated holistically** on this important cross-cutting issue.

They further tasked relevant Ministers from all ASEAN Member States to make progress on discussions by ASEAN ICT and Cybersecurity Ministers at the AMCC, the ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), as well as other relevant sectoral bodies such as the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), **to identify a concrete list of voluntary, practical norms of State behaviour in cyberspace that ASEAN can work towards adopting and implementing**, and to facilitate cross-border cooperation in addressing critical infrastructure vulnerabilities, as well as to encourage capacity-building and cooperative measures to **address the criminal or terrorist use of cyberspace, taking reference from the voluntary norms recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE)**.

PROPOSAL

Thailand attaches great importance to advancing cooperation within ASEAN and with external partners to address **non-traditional security challenges**. Most recently, on Cybersecurity, the **Ministry of Foreign Affairs and the Ministry of Digital Economy and Society** of Thailand, together with the government of Australia, co-hosted the ASEAN-Australia Cybersecurity Workshop entitled **"Strengthening Legal Implementation in Tackling Cybersecurity Challenges in the Region"** in Bangkok, on 13 February 2018, in order to promote the monitoring and tackling of cyber threats and enhancing coordination between cybersecurity-related agencies.

For this year, the **Ministry of Foreign Affairs and the Ministry of Digital Economy and Society of Thailand** are proposing to hold an International Conference entitled **"Cybersecurity: Implications on Peace and Security in the ASEAN Region"** in Bangkok, on 10-11 May 2019. The Conference will be in line with the ASEAN Leaders' Statement on Cybersecurity Cooperation which tasks relevant Ministers from all ASEAN Member States to closely consider and **submit recommendations on feasible options of coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts among various platforms of the three pillars of ASEAN,** while recognizing the value of

enhanced dialogue and cooperation on cybersecurity issues with Dialogue Partners and other External Parties. More importantly, **the Conference will also be in line with the activities agreed in the ASEAN Political-Security Community Blueprint which attaches importance to addressing issues of cybercrime and cybersecurity.**

OBJECTIVES

This Conference is designed to support and complement the on-going efforts of existing ASEAN frameworks, platforms, bodies and mechanisms on Cybersecurity.

The objectives of the proposed conference are:

1. Promote better understanding about cybersecurity and its impact on peace, security and conflict management in ASEAN and the Asia-Pacific region.
2. Provide global and regional perspectives on how international cooperation and collaboration on cybersecurity can be better managed for the benefit of all involved.
3. Discuss global and regional perspectives on the emerging international legal and normative frameworks on cybersecurity, especially the 2001 Budapest Convention on Cyber Crime, the 2015 Report of the United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (UNGGE), and the proposed **"Digital Geneva Convention"** to protect cyberspace and how they can be applied to the ASEAN region
4. Discuss how to build closer cooperation and coordination among ASEAN Member States, and beyond, on cybersecurity policy development and capacity building initiatives. And, to learn from the experience of other regions in this endeavor.
5. Discuss how to efficiently support existing ASEAN frameworks, bodies and mechanisms, such as the AMCC, TELMIN and AMMTC, in their efforts to coordinate and to make progress toward the creation and promotion of voluntary and non-binding cyber norms and rule-based cybersecurity environment for the ASEAN region and beyond.
6. Discuss possible recommendations on the above, which relevant ASEAN bodies could consider adopting as part of their recommendations to relevant ASEAN Ministers and ASEAN leaders for consideration.

PARTICIPATION

The International Conference on **"Cybersecurity: Implications on Peace and Security in the ASEAN Region"** is expected to be attended by representatives from ASEAN governments, ASEAN dialogue partners and other interested countries. Representatives

from relevant ASEAN bodies, international organizations, businesses and non-government organizations, both within and outside the ASEAN region, are also expected to participate. Altogether,

approximately 120 high-level participants are expected at this Conference. Some of the participants will be invited to form the core part of this Conference in the role of Moderators, Presenters and Commentators, in the various sessions of the Conference.

EXPECTED OUTCOMES

1. It is expected that the Conference will result in increased awareness about the importance of cybersecurity in the context of regional peace and conflict management.
2. It is also hoped that the discussions during the Conference could help support the on-going activities by existing ASEAN frameworks, platforms, bodies, mechanisms and ASEAN Member States in their efforts toward creating and coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building among various platforms of the three pillars of ASEAN, especially in relation to regional peace and conflict management.
3. In addition, it is expected that the discussions at the Conference will be able to help provide support to the on-going activities of relevant ASEAN frameworks, platforms, bodies and mechanisms, towards **identifying a proposed concrete list of voluntary, practical norms of State behavior on cyberspace, especially in relation to regional peace and stability,** that ASEAN can consider working towards adopting and implementing.
4. It is also expected that the Conference will be able to help contribute to efforts of ASEAN to enhance its cooperation and collaboration with the international community in the area of cybersecurity and non-traditional security issues, especially in aspects which are directly relevant to regional and international peace and conflict management.
5. It is expected that the Conference would serve as a vehicle whereby ASEAN Member Countries could promote closer functional relations with Dialogue Partners, businesses, the Civil Society community and all interested parties, especially in the area of cybersecurity.

FUNDING

The **Ministry of Foreign Affairs** and the **Ministry of Digital Economy and Society** of Thailand will be responsible for the management and costs of the International Conference on **"Cybersecurity: Implications on Peace and Security in the ASEAN Region"**. Financial Contributions and material support from interested parties are welcomed, although not a requirement for participating in the Conference. The Ministry of Foreign Affairs and the Ministry of Digital Economy and Society of

Thailand will also be responsible for administrative costs, as well as the cost of the publication of the report of the outcome of the Conference.

******

Contact Persons:

Ms. Bheraya Homkosol
Department of ASEAN Affairs
Ministry of Foreign Affairs of Thailand
Tel: +6686-886-3698
Email: bheraya@gmail.com; bhomkosol@gmail.com

Mr. Intouch Namsaengwanich
Department of ASEAN Affairs
Ministry of Foreign Affairs of Thailand
Tel: +662-203-5000 Ext. 14397
Email: intouch23.n@gmail.com

ASEAN
THAILAND 2019
ADVANCING PARTNERSHIP
FOR SUSTAINABILITY

PROGRAMME

INTERNATIONAL CONFERENCE ON CYBERSECURITY: IMPLICATIONS ON PEACE AND SECURITY IN THE ASEAN REGION 10-11 MAY 2019, SHANGRI-LA HOTEL, BANGKOK

PROGRAMME
VENUE: GRAND BALLROOM III, 2ND FLOOR (LOBBY FLOOR), SHANGRI-LA WING

Friday, 10 May 2019

0800- 0900	Registration
0900- 0910	Opening Remarks by **H.E. Ambassador Mr. Chaisiri Anamarn, Advisor to the Foreign Minister of Thailand**
0910- 0930	Group Photo
0930- 1000	Coffee Break

Session 1

As the first session of the Conference, the purpose of the session is to set the tone of the Conference by conducting a survey of the current cybersecurity eco-system and situations at the global and regional levels

1000- 1200 **Overview: Global & Regional Cybersecurity Situation**

- **Mr. Timothy Snow**, Security Advisor – Security Asia Pacific, CISCO
- **Mr. Kevin O'Leary**, Chief Security Officer, Asia Pacific, Palo Alto Networks
- **Ms. Edna Yap**, Cyber Partner, Deloitte Singapore
- **Dr. Rattipong Putthacharoen**, System Engineers Lead – Symantec (Thailand) Ltd.

Moderator: **Dr. Darmp Sukontasap**

1200- 1300 **Lunch Break**

Session 2

This session explores current global and regional efforts towards a legal and normative framework on the behavior of states on cyberspace and cybersecurity issues

1300- 1500 **Overview: Global & Regional Efforts toward an International Framework for Responsible State Behavior in Cyberspace**

- **Mr. Alexandru Caciuloiu**, Cybercrime and Cryptocurrency Advisor,Programme Coordinator for Southeast Asia and Pacific, UNODC
- **Mr. Jonghyuk Ro**, Director of Cybersecurity Policy, Microsoft Corp.
- **Mr. Guy Segal**, General Manager, Custodio Technologies Ltd. Pte.
- **Ms. Johanna Weaver**, Director Cyber Affairs Section, Australian Department of Foreign Affairs and Trade

Moderator: **Dr. Suriya Chindawongse**

1500- 1520 **Coffee Break**

Session 3

This session focuses on current developments in the Asia-pacific region, and ASEAN in particular, on efforts to enhance the cooperation and coordination of states on cybersecurity, in the promotion of peace and trust in the region and in efforts to combat all forms of cybersecurity threats; Capacity Building efforts are also an important part in cooperation between states and within the region

1520- 1730 **National and Regional Experience in Promoting Peace, Security and Capacity Building thru Cybersecurity**

- **Dr. Hoang Anh Tuan**, Deputy Secretary-General of ASEAN for Political-Security Community
- **Ms. Johanna Weaver**, Special Adviser to Ambassador for Cyber Affairs, Australian Department of Foreign Affairs and Trade
- **Ms. Ajarin Pattanapanchai**, Permanent Secretary, Ministry of Digital Economy and Society, Thailand
- **Dr. Paiboon Amornpinyokiat**, Qualified Expert, National Cybersecurity Preparation Committee

Moderator: **Group Captain Amorn Chomchoey**

1830 – 2030 **Welcome Dinner** Hosted by **Dr. Suriya Chindawongse**, Director-General of ASEAN Affairs Department, Ministry of Foreign Affairs of Thailand

Saturday, 11 May 2019

Session 4

This session discusses the importance of closer partnerships, cooperation and coordination, as well as support, between governments, regulators, businesses and the civil society on cybersecurity and to learn from the experiences of the parties involved

0900- 1100 **Public & Private Partnership on Cybersecurity, in the Aspects of building international legal and normative frameworks**

- **Ms. Atsuko Okuda**, Chief, ICT and Development Section, United Nations ESCAP
- **Mr. Mier Avidan**, Vice President, Cellebrite, Israel
- **Mr. Edgar H. McConnell**, Legal Attache, Federal Bureau of Investigation, US Embassy Bangkok
- **Dr. Prinya Hom-anek**, President and CEO, ACIS Professional Center

Moderator: **Mr. Narinrit Prem-apiwatthanokul**

Coffee Break/Health Break as needed

Session 5

As the last session of the conference, this session will attempt to summarize the lessons learned, as well as to map out recommended next steps for all stakeholders, in order to help move forward the global and regional agenda on international cooperation on cybersecurity issues

1100- 1230 **Summary and Recommendations**

- Lessons Learned: How can the ASEAN region efficiently move towards (a) adopting a regional Cybersecurity Policy, (b) developing a legal and normative framework on cybersecurity, as well as creating a rule-based cybersecurity environment, both independently and working together with the international community

Next Steps

- **Dr. Suthad Setboonsarng**, Chair, Audit Committee, Bank of Thailand
- **H.E. Ms. Arjaree Sriratanaban**, Ambassador Attached to the Ministry of Foreign Affairs of Thailand
- **Mr Nguyen Huu Phu**, Director of Political-Security Division, Department of International Law and Treaties, Ministry of Foreign Affairs of Vietnam
- **Mr. Desarack Teso**, Corporate, External & Legal Affairs Director, Microsoft Thailand

Moderator: **Dr. Darmp Sukontasap**

Session 6

1230- 1300 **Closing Remarks**

- **Ms. Usana Berananda**, Deputy Director General of ASEAN Affairs Department, Thailand

1300- 1430 **Lunch Break**

End of Conference

Departure of Participants

ASEAN
THAILAND 2019
ADVANCING PARTNERSHIP
FOR SUSTAINABILITY

SPEAKERS & PANELISTS

INTERNATIONAL CONFERENCE
ON
CYBERSECURITY: IMPLICATIONS ON PEACE AND SECURITY IN THE ASEAN REGION
10-11 MAY 2019, SHANGRI-LA HOTEL, BANGKOK

SPEAKERS & PANELISTS

Opening Session

H.E. Ambassador
Mr. Chaisiri Anamarn
Advisor to the Foreign Minister of Thailand

Dr. Suriya Chindawongse
Director-General, ASEAN Affairs Department, Ministry of Foreign Affairs of Thailand

Session 1

Mr. Timothy Snow
Security Advisor –
Security Asia Pacific,
CISCO

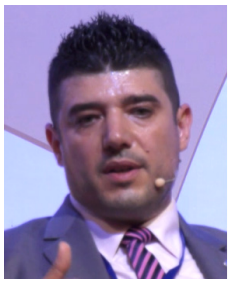
Mr. Kevin O'Leary
Chief Security Officer,
Asia Pacific, Palo Alto
Networks

Ms. Edna Yap
Cyber Partner,
Deloitte Singapore

Dr. Rattipong Putthacharoen
System Engineers Lead –
Symantec (Thailand) Ltd.

Moderator
Dr. Darmp Sukontasap
Chair and Representative of
Thailand to the Governing
Council of the ASEAN-IPR

Session 2



Mr. Alexandru Caciuloiu
Cybercrime and Cryptocurrency Advisor, Programme Coordinator for Southeast Asia and Pacific, UNODC

Mr. Jonghyuk Ro
Director of Cybersecurity Policy, Microsoft Corp.

Mr. Guy Segal
General Manager, Custodio Technologies Ltd. Pte.

Ms. Johanna Weaver
Director Cyber Affairs Section, Australian Department of Foreign Affairs and Trade

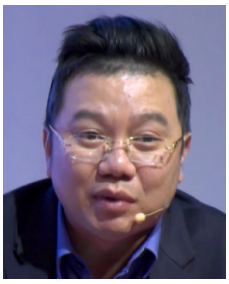
Moderator
Dr. Suriya Chindawongse
Director-General, ASEAN Affairs Department, Ministry of Foreign Affairs of Thailand

Session 3

Dr. Hoang Anh Tuan
Deputy Secretary-General of ASEAN for Political-Security Community

Ms. Johanna Weaver
Special Adviser to Ambassador for Cyber Affairs, Australian Department of Foreign Affairs and Trade

Ms. Ajarin Pattanapanchai
Permanent Secretary, Ministry of Digital Economy and Society of Thailand

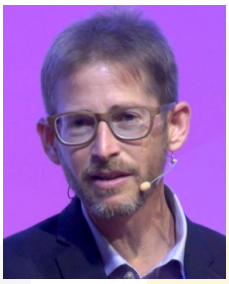


Dr. Paiboon Amornpinyokiat
Qualified Expert, National Cybersecurity Preparation Committee of Thailand

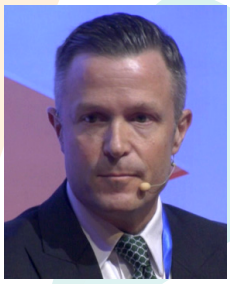
Moderator
Group Captain
Amorn Chomchoey
Division Chief, Royal Thai Air Force Cyber Warfare Division

Session 4

Ms. Atsuko Okuda
Chief, ICT and Development Section, United Nations ESCAP

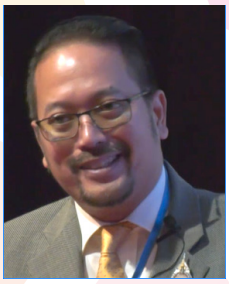


Mr. Mier Avidan
Vice President, Cellebrite, Israel



Mr. Edgar H. McConnell
Legal Attache, Federal Bureau of Investigation, US Embassy Bangkok

Dr. Prinya Hom-anek
President and CEO, ACIS Professional Center

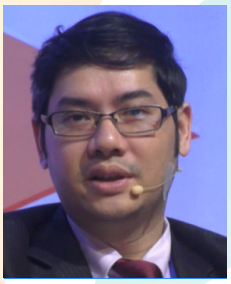


Moderator
Mr. Narinrit Prem-apiwatthanokul
Committee Member, Thailand Information Security Association (TISA)

Session 5

Dr. Suthad Setboonsarng
Chair, Audit Committee,
Bank of Thailand

H.E. Ms. Arjaree Sriratanaban
Ambassador Attached to the
Ministry of Foreign Affairs
of Thailand



Mr Nguyen Huu Phu
Director of Political-Security
Division, Department of
International Law and
Treaties, Ministry of Foreign
Affairs of Vietnam

Mr. Desarack Teso
Corporate, External & Legal
Affairs Director, Microsoft
Thailand

Moderator
Dr. Darmp Sukontasap
Chair and Representative of
Thailand to the Governing Council
of the ASEAN-IPR

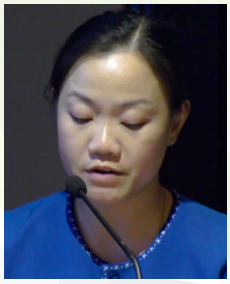
Closing Session

Ms. Usana Berananda
Deputy Director General,
ASEAN Affairs Department,
Ministry of Foreign Affairs
of Thailand

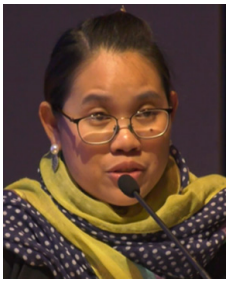
Conference Coordinators

Mrs. Hathaichanok Riddhagni Frumau
Chief, Political and Security Division, Department of ASEAN Affairs

Ms. Piyaporn Putanapan
Member, ASEAN Chairmanship Task Force, Department of ASEAN Affairs



Ms. Nattaporn Phromlert
Political and Security Division, Department of ASEAN Affairs



Ms. Bheraya Homkosol
Political and Security Division, Department of ASEAN Affairs

Mr. Intouch Namsaengwanich
Political and Security Division, Department of ASEAN Affairs

ASEAN
THAILAND 2019
ADVANCING PARTNERSHIP
FOR SUSTAINABILITY

SUMMARY OF CONFERENCE

SUMMARY OF CONFERENCE
INTERNATIONAL CONFERENCE ON CYBERSECURITY: IMPLICATIONS ON PEACE AND SECURITY IN THE ASEAN REGION
10-11 MAY 2019, BANGKOK

Opening Session

- H.E. Mr. Chaisiri Anamarn, Advisor to the Minister of Foreign Affairs of Thailand delivered opening remarks. He stressed the priority of cybersecurity which underpins the development of a sustainable ASEAN Community in an age of digital and technological disruption. He noted the need to pay adequate attention to building resilience against growing cybersecurity threats and cybercrimes through a "Unified ASEAN" approach in order to be able to realize a truly "Seamless Digital ASEAN," in a sustainable manner, which is one of Thailand's goals under her ASEAN Chairmanship.

- He argued that ASEAN Leaders' Statement on Cybersecurity Cooperation adopted during the 32nd ASEAN Summit in 2018 was an important milestone that accentuated ASEAN's political commitment to advance closer cooperation and coordination on the development of a cybersecurity policy and capacity-building initiatives. He emphasized Thailand's contributions, such as the hosting of the ASEAN-Japan Cybersecurity Capacity-Building Centre in Bangkok, and her commitment to work in partnership with other ASEAN Member States, ASEAN organs and mechanisms in a complementary manner.

SESSION 1: Overview: Global and Regional Cybersecurity Situation

Session 1 aims at setting the tone by illustrating the overview situation of cybersecurity from multiple perspectives. Key questions included the current state of cybersecurity technical development and applications, the seriousness of evolving threats including against Critical Infrastructures, and the assessment on levels of preparedness among various stakeholders.

- According to the Panelists, there are multifaceted challenges on cybersecurity; cyber attacks are at every level, from individuals to states. While several traditional challenges have yet to be adequately addressed, new threats are constantly emerging. The level of risk is, therefore, being constantly elevated, while large segments of public and private sectors are not well prepared.

- Technology is constantly evolving. Therefore, cyber threats will always be there and will become increasingly sophisticated. To do nothing to prepare oneself to counter the evolving threat is not an option. Since every organization encounters different sets of risk, each has to assess and mitigate one's own risks accordingly. Information sharing among industries and with government is therefore crucial to bridge knowledge gaps.

- With regard to new technology such as the 5th Generation Mobile Network Technology (5G), cloud computing and Internet of Things (IoT), there is the need to find a good balance between "convenience and acceptable risks."

- There is a particularly high level of concern over attacks against Critical Infrastructures, such as electricity, public utilities, hospitals and public transports, which would affect a large group of the population. The more IT equipment is linked, the higher the risks. Operators of Critical Infrastructures should prioritize and innovative cybersecurity solutions to keep up with the pace of increasing connectivity among electronic devices.

- Even though digital forensics is continuously advancing, accuracy of attribution remains a challenge. One should be extremely careful in making attributions. Rather, focus of the efforts should be on developing capabilities to detect and prevent breaches. Post-event information sharing should also be encouraged to help analyze the methodology and possible motives of those who were responsible.

SESSION 2: Overview: Global and Regional Efforts toward an International Framework for Responsible State Behaviour in Cyberspace

Session 2 aims at exploring current global and regional efforts being taken to address responsible State behaviour in cyberspace, assuming that States are critical players in shaping the landscape of cyberspace and are also particularly vulnerable to cyber threats or malicious undertakings in cyberspace that could affect the safety, security and well-being of their citizens.

- At the UN level, in December 2018, two UN General Assembly resolutions were adopted establishing the new UN Group of Governmental Experts **(UNGGE)**, on one hand, and the **Open-Ended Working Group (OEWG)** proposed by Russia to work on responsible State behavior in cyberspace in the context of international security, on the other. The process is likely to be a long one before we see any tangible results because a wide divergence of views still exist over how international law should be applied to cyberspace.

- A panelist expressed support for a **Digital Geneva Convention**, emphasizing the promotion of safe usage of cyberspace. The idea was inspired by the 1949 Geneva Convention. Such panelist also informed the Conference that his organization is a main supporter of the **"Paris Call for Trust and Security in Cyberspace". The Cybersecurity Tech Accord** is another concrete example of private sector-led initiative and self-regulated mechanism to prevent and fight against cyber attacks.
- Another speaker suggested that countries should focus on the implementation of existing international norms/laws which are also applicable on cyberspace, rather than to negotiate a new normative or legal framework, which would take years to accomplish. In this regard, the eleven voluntary norms recommended in the 2015 Report of the UNGGE were highlighted as reference. The view was expressed that ASEAN Member States should discuss and identify a concrete list of practical norms suitable for ASEAN's context.

- The main idea is to take action, not more talks. In other word, ASEAN Member States could not afford to passively wait for global discussions on a normative or legal framework to materialize. Rather, they should take a proactive course of action to promote stability and predictability in cyberspace, through confidence-building measures and capacity-building, which would lead to the implementation certain international and regional norms.

SESSION 3: National and Regional Experience in Promoting Peace, Security and Capacity-Building thru Cybersecurity

Session 3 aims to provide tangible examples of national and regional efforts in promoting cybersecurity, i.e., ASEAN, Thailand and Australia. Key points that emerged were the importance of capacity-building, striking the right balance between regulation and incentivizing, and close and interactive relations among all stakeholders.

- There are several factors contributing to potential risks on cybersecurity in ASEAN, including the constantly growing economy, the inter-connectedness of its Member States, the high degree of accessibility to the Internet, etc. Moreover, ASEAN still faces several hurdles such as the lack of digital workforce, development gaps, differing priorities and underdeveloped infrastructures and legal frameworks.

- In response, ASEAN has made several efforts such as the implementation of the ASEAN ICT Masterplan 2020 (AIM2020), setting up of the ASEAN-Japan Cybersecurity Capacity-Building Centre in Bangkok, and the carrying out of the feasibility study on establishing an ASEAN

Computer Emergency Response Team (CERT). In March 2019, Thailand also hosted the ASEAN Digital Ministers' Retreat which agreed to rename the ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN) as "the ASEAN Digital Ministers' Meeting" to accommodate the evolving nature of its mandates. The Conference also noted the good progress on cybersecurity that is being made in individual ASEAN Member States.

- As for Thailand national experience, the new Cybersecurity Act was adopted primarily for protecting the country's Critical Information Infrastructures (CIIs). The Act is based on three concepts: self-regulation, information sharing and balance between enforcement and incentives for voluntary compliance.
- Australia has no overarching cybersecurity legislation, Rather, it adopts a principle-based approach, looking at what needs to be put in place. Australia Cybersecurity Centre (ACSC) was established to provide guidelines to encourage government agencies and industries to follow. Australia is also attempting to increase awareness amongst stakeholders through education, in order to create demand for IT specialists and in order for the IT industry to be more responsible in helping to fill the capability gap.

SESSION 4: Public and Private Partnership on Cybersecurity, in the aspects of building international legal and normative frameworks

Session 4 aims at highlighting the importance of inclusive partnerships among broad spectrum of stakeholders involved in promoting cybersecurity. Panelists were invited to share their views, experience and recommendations on Public-Private Partnership, as well as the involvement of all stakeholders in the drawing up of cybersecurity policy and its implementation.

- A panelist expressed the view that Public-Private Partnership (PPP) is essential in preventing, responding to and building resilience against cyber threats. However, PPP could not be achieved without "trust" and "confidence" that should be promoted through regular sharing of information and best practices.

- A view was expressed that a "top-down" approach by the public sector is more effective in achieving tangible results. However, this would require strong political commitment and general public support to sustain the reform of public sector's approach and mindset.

- A panelist also pointed out that the public and private sectors need to develop a common language, terminology and understanding on technical topics, in order to be able to come up with practical cyber regulation/legislation.

- A view was expressed that it is imperative for the public sector to firstly identify and assess each industry's specific needs before matching them with suitable support. Public sector should provide support to efforts to promote cybersecurity awareness and capacity-building.

- Collective efforts and long-term cooperation are crucial for ASEAN Member States to narrow their gaps regarding legislation, law enforcement, human resources, capabilities and knowledge on cybersecurity.

SESSION 5: Summary and Recommendations

Session 5 attempts to summarize some key takeaways of the Conference to create a list of practical recommendations for ASEAN's policymakers, bearing in mind that cybersecurity concerns all spectrums of the society and therefore needs to be addressed at multiple fronts in a calibrated and concerted manner.

- Close cooperation between public and private sectors, as well as with all relevant parties, such as academics and civil society, is indispensable in addressing cyber threats. Private sector should take the lead in making available the necessary technical know-how, while the public sector plays a supportive role and focuses on ensuring public awareness and preparedness for possible cyber incidents.

- Likewise, there should be close consultation among government agencies, the private sector, academics, the civil society, as well as all interested parties in legislating and regulating cybersecurity.

- Government agencies also need to adequately improve their own cyber capabilities to ensure continuity and reliability of their services.

- Raising Awareness, capacity-building, information-sharing and Public-Private Partnership on cybersecurity are key priorities that should be urgently established.

- ASEAN Leaders need to better understand the importance of cybersecurity issues and the need to have adequate protection.

- As one of the fastest growing economic regions of the world, ASEAN should elevate its role on cybersecurity in the international arena and cooperate more actively with major global players.

- By involving the private sector, international organizations, academics and cybersecurity experts from various countries outside of ASEAN, this Conference has helped create a higher degree of awareness on cybersecurity and provided a good platform for sharing ideas and coming up with recommendations amongst various stakeholders.

- The next steps are to implement quick-win, low-hanging fruits, ideas based on the recommendations by panelists, i.e. to examine existing international laws and norms relevant to cybersecurity, identify specific topics for deeper dialogues and to strengthen coordination between public and private sectors.

- Panelists expressed the view that Vietnam, as the next ASEAN Chair, should consider hosting the 2nd international conference on cybersecurity: Implications on Peace and Security in the ASEAN Region.

Recommendations made during the Conference

- Panelists agreed that the following important ingredients are essential:

  - **Cybersecurity Awareness:** There should be increased efforts to enhance cybersecurity awareness within all ASEAN Member States, at all levels and across all spectrums of the society, since it would be the first step toward greater understanding and continuous learning about cybersecurity. The lack of awareness would lead to complacency and might cause immeasurable damages.

  - **Human Resources Development/Capacity-Building in a holistic and concerted approach:** ASEAN Member States need to fill the capability gap within the region through capacity-building. This effort would not only help the region to effectively defend itself against cyber attacks, but would also help the Member States and their citizens to reap the full benefit of the digital transformation that would eventually transform the ASEAN Community in all aspects.

  - **Information-Sharing:** Information should be shared both within and amongst ASEAN Member States and with its partners, in order to expand the available pool of knowledge and experience and enhance each State's cyber preparedness. This will eventually raise the bar of collective security on cyberspace, as the chain is only as strong as its weakest link.

- **Increased Coordination and Collaboration:** ASEAN Member States should be made aware of the cascading effects that a cyber incident in any Member State could potentially have on the entire digital eco-system of the region. Policy makers should also change their mindsets with regard to technology, to weigh in more on common benefits rather than pursuing national interest in isolation.

- **Enhanced Public-Private Partnership:** Since the private sector possesses technology and technical expertise, they are the driving force that the public sector should engage more with in the form of consultations, cooperation and collaboration, especially when it comes to preparing legislations and regulations on cybersecurity. The same can be said for efforts to create regional and international legal and normative frameworks for cybersecurity.

- **ASEAN should focus on more action, not more talk, to promote cybersecurity. Recommendations include:**

  - Start with quick measures, such as reviewing and assessing the needs of countries when it comes to cybersecurity, including what needs to be put in place, what knowledge or understanding need to be provided to the general public and what to do if people violate the prescribed measures or what have been put in place by the government.

  - Come up with a directory of international/regional points of contact of personnel on cybersecurity, in order to facilitate information-sharing and building confidence amongst ASEAN Member States. (This can take reference from the ARF Points of Contact Directory on Security in the Use of ICTs.)

  - ASEAN Member States should individually or collectively announce commitment to at least some (4 or 5) of the 11 international norms recommended by the 2015 UNGGE Report, taking into account the fact that ASEAN ICT Ministers have already agreed, in principle, to subscribe to such norms.

  - Increase information-sharing, including post-mortem examination of cyber incidents, to disseminate best practices and lessons-learned from previous attacks.

  - Setting up of an ASEAN Computer Emergency Response Team (CERT), and expand partnership with CERTs in each ASEAN Member States and in other parts of the world.

- Prepare training and handbooks in cybersecurity. Carry out regular exercises and drills against cyber threats, at the local, national and regional levels.

- Create an eco-system that is conducive to the implementation of protective measures, through practical and effective legal/regulatory frameworks at the national level, which be further developed into regional legal/regulatory and normative frameworks.

- Create a culture of security, by providing knowledge, understanding and know-how on cybersecurity. Built on both the hardware and software of cybersecurity, with special emphasis on the software or people level.

- Consider creating an international or regional (ASEAN) technical/ management certification system on cybersecurity. The focus can be on technical competence at the working level, rather than on university degrees.

- Participants agreed on the usefulness of the Conference which, for the first time, brought policy makers, business operators, academics and the interested public, together to discuss the important subject of cybersecurity. Participants expressed the view that efforts such as this should be continued.

Closing Session

- Ms. Usana Bherananda, Deputy Director-General of the Department of ASEAN Affairs, Ministry of Foreign Affairs of Thailand delivered closing remarks. She expressed appreciation for the insightful contributions from all the panelists and for the attention and active participation by more than 250 participants of the Conference. On behalf of the Ministry of Foreign Affairs of Thailand, she also expressed her sincere thanks to the sponsors of the Conference for their kind support and assistance. She echoed the message from the panelists that cybersecurity is a critical element to help ensure sustainable security, economic growth and social well-being within the ASEAN region.

- She suggested that information sharing and the strengthening of capacities of stakeholders are essential to promote awareness and increase the preparedness of States in countering cyber threats which are an integral part of the process of digital transformation. She highlighted the need to tailor awareness raising programmes for different target groups to ensure that all would benefit from the effort, and no one is left behind. She stressed the importance of maintaining continuity in discussions and consultations and expressed hope that Vietnam, as the next ASEAN Chair, would consider convening the "2nd International Conference on Cybersecurity: Implications on Peace and Security in the ASEAN Region" in 2020.

****

Summary Report Prepared by:
International Security Unit
Office of the Permanent Secretary for Foreign Affairs
Ministry of Foreign Affairs of Thailand

Mr. Phasit Chudabuddhi, Team Leader
Mr. Pichaya Lapasthamrong
Mr. Nontasit Kaewhanam
Mr. Tharind Lertsukekasem

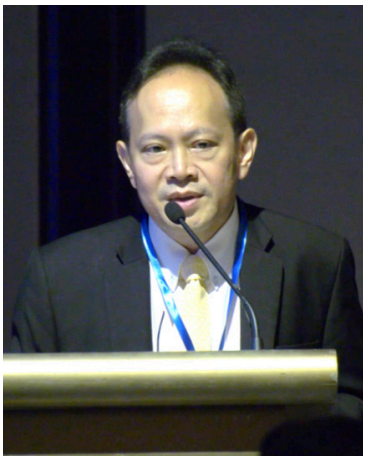
ASEAN
THAILAND 2019
ADVANCING PARTNERSHIP
FOR SUSTAINABILITY

PHOTO GALLERY

PHOTO GALLERY

Conference Participants

Opening Session

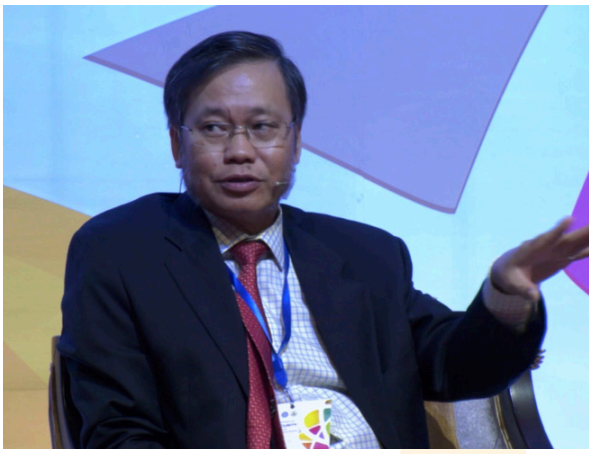


Session 1

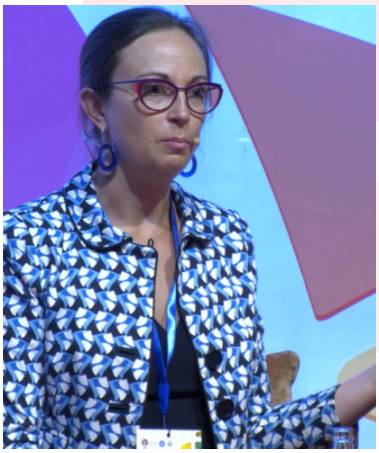

IN THE ASEAN REGION
10-11 MAY 2019 ,BANGKOK, THAILAND
Microsoft
paloalto
Symantec

Session 2

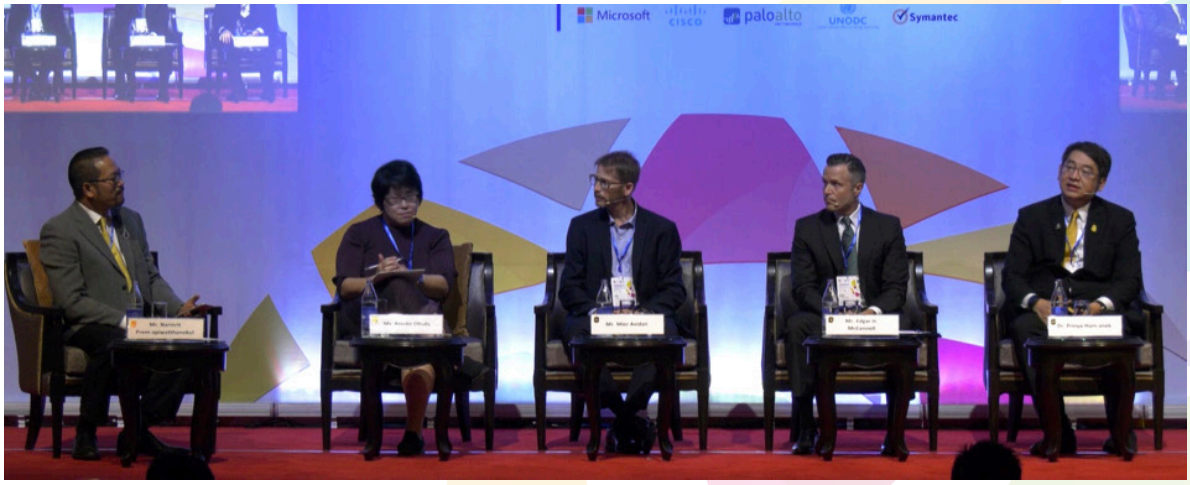
Session 3




IN THE ASEAN REGION
10-11 MAY 2019 ,BANGKOK, THAILAND
Microsoft
cisco
paloalto
UNODC
Symantec



Session 4

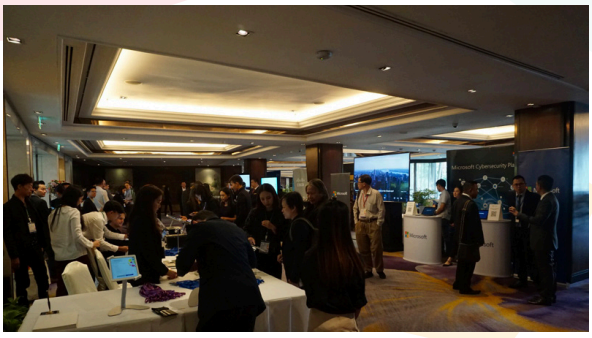


Session 5


ASEAN
THAILAND 2019
IN THE ASEAN REGION
10-11 MAY 2019 ,BANGKOK, THAILAND
Microsoft
cisco
paloalto
UNODC
Symantec

Closing Session

Exhibitions



Conference Organisers

ASEAN THAILAND 2019
ADVANCING PARTNERSHIP FOR SUSTAINABILITY

Conference Sponsers

Microsoft

cisco

paloalto NETWORKS

UNODC
United Nations Office on Drugs and Crime

Symantec

Download Final Report
http://www.mfa.go.th/asean/th/information/109335-Cybersecurity:-Implications-on-Peace-&-Security-in.html