asean india
PROGRESS & PROSPERITY

MINISTRY OF EXTERNAL AFFAIRS
Government of India

ORF OBSERVER RESEARCH FOUNDATION

SPECIAL REPORT

India-ASEAN Track 1.5 Dialogue on Cyber Issues

Contents

Introduction

THE past decade has witnessed the rapidly increasing 'cyberisation' of economic, social, and political relations, resulting in complex challenges as well as opportunities for the world. In this context, India and countries that are part of the Association of Southeast Asian Nations (ASEAN) share common interests in leveraging digital technologies for development, governance, national security objectives, and scripting equitable rules and norms for cyberspace.

To discuss new pathways of collaboration between India and ASEAN in the digital realm, Observer Research Foundation, in partnership with the Ministry of External Affairs of India (MEA), hosted the India-ASEAN Track 1.5 on Cyber Issues on 14 October 2019.

The Dialogue addressed issues under three pillars:

1. Data Governance: Models, Goals and Possibilities
2. Taking Stock of Cyber (In)security in Asia
3. Cyber Norms Processes: The Way Forward

Over the course of the one-day event, nearly 40 participants representing government, think tanks, start-ups, and industry experts from India and ASEAN delved into trends, state of play, and potential next steps under the three pillars.

Keynote Address

by **Ms. Vijay Thakur Singh**
Secretary (East) at the ASEAN-India Track 1.5 Dialogue on Cyber Issues

I warmly welcome the eminent cyber experts representing governments, think tanks, academia and industry — especially our guests from ASEAN. I thank the Observer Research Foundation for putting together this conference in partnership with the MEA, thereby helping us implement a longstanding commitment.

As experts on this subject, you are familiar with the challenge that policymakers and industry face in managing policy and social changes along with the exponential rate at which technology transforms our world. India is a case in point — internet-based services and digital technologies are transforming our society, economy, and nation in unprecedented ways. With 451 million internet users and internet penetration at only 36 percent, Indians are only at the dawn of the technological age. On one hand, this means enormous opportunities, as Indians move from no phones to mobile phones; from cellphones to smartphones. It also means a universe of possibilities, as our digital economy already generates around US$ 200 billion annually. Indeed, by 2025, India could create a digital economy of between US$ 800 billion to USD 1 trillion.

A similar story is unfolding in Southeast Asia, where I am told some 90 percent of your 300 million netizens access the Internet via smart phones. ASEAN's digital economy is already generating nearly US$ 150 billion in revenue every year, and I believe you too are looking at adding US$ 1 trillion in value through the digital economy in the coming decade.

These statistics tell us that digital technologies, applications, and the internet economy are becoming truly ubiquitous. We connect with each other, move money, shop, and pay for services online in unimaginable numbers. Governments today offer services ranging from birth to death, from licenses to tax payments, using the digital domain. This enormous consumption and generation of data, which drives data-based technologies and services, will power innovation in Artificial Intelligence (AI), Internet of Things (IoT) and Industry 4.0. Unforeseen and unimagined vistas lie before us, promising to improve the quality of human existence beyond anything we have ever imagined.

However, these achievements come at a cost, and they offer as many risks as rewards. The obverse of convenience and seamless 24x7 connectivity at blistering speeds includes challenges to privacy, cybercrime, and data theft. Policymakers face competing challenges: we citizens demand faster, better, freer, cheaper connectivity, and we also want stronger measures to protect our data and privacy. Security agencies have an entire universe of concerns too, as the borderless world of the internet equally empowers a range of bad actors.

Nation-states have not as yet been able to unify policy measures adequately to create a robust data governance regime that manages the balancing act of dealing with both privacy and security concerns. There are efforts, but these are disaggregated at the global level. These include the Master Plan on ASEAN Connectivity 2025, which calls to develop an ASEAN Framework on Digital Data Governance as a key priority. India is also drafting a Personal Data Protection Bill. Events such as this one help us bring various initiatives closer together, because we all have a lot to share with each other.

We need to cooperate — quite simply — because the challenge posed by malicious actors in cyberspace is borderless. It is, in fact, the newest arena for contestation between individuals, entities, and even States. No country today is immune from such attacks. Cyber-attacks not only cause loss of data — including sensitive state and personal information —they also compel states to invest heavily in protection and countermeasures. It is no surprise, therefore, that the World Economic Forum identified cybersecurity as the third most-feared threat after extreme weather events and natural disasters. In this context, a special word must be said about securing our youth from cybersecurity threats, especially as children today are digital natives. Recognising the convergence of risks and technologies in this regard, India will fund a 'Child Online Risks Awareness Campaign' through the Ministry of Posts and Telecommunications of Cambodia under a Quick Impact Project in 2020-2021. We would be happy to offer similar projects to other ASEAN partners as well.

At the intersection between cyberspace and politics, the most sensitive issue is that of cyber norms. India emphasises that the core values of liberty, freedom of expression, and rule of law apply to cyberspace as well. It is in our common interest to maintain a peaceful, secure, and resilient cyberspace. We want countries to find common ground on cyber norms, which encourage international cooperation toward security, while fostering equitable access to cyberspace.'

Themes of discussion

Data Governance Frameworks

DIALOGUE participants agreed that India and ASEAN, as leading generators of data, should collaborate and build a broader regional data-exchange framework. They should also learn from issues that technology companies in the US and Europe are currently facing — restrictive or standalone data regimes should not hinder cooperation between law enforcement regimes for investigating and prosecuting cybercrimes.

Participants highlighted four thematic goals with regard to data governance:

- Developing technical standards for effective data management
- Ensuring human rights and the rule of law, through adequate protection of personal data
- Building security in digital platforms and networks at the enterprise and consumer levels
- Promoting and harnessing the generation of local economic value from the proliferation of data in India and ASEAN

Several delegates emphasised the need for effective data-sharing regimes that respect sovereign concerns around the investigation and prosecution of cybercrimes. Many were concerned that criminals have access to digital infrastructure from across the world, but law enforcement agencies remain constrained by domestic laws that do not adequately reflect the transboundary nature of malicious activity in cyberspace.

Sovereignty and Data Localisation

Participants identified localisation as an animating theme in draft data governance rules in India and other jurisdictions. Localisation, it is believed, will generate economic value and enhance state capacity in the countries where it is implemented. The participants also discussed the potential benefits and drawbacks to the end user on account of such policy. Even with localisation, there is no guarantee that access to specific categories of data held by technology companies remains restricted. Second, the current move towards restricting data flows needs to be analysed — for instance, how will it affect the user's choice and freedom with respect to market choices and more secure platforms?

Three broad reasons were identified in favour of data localisation:

1. Making law enforcement's access to data easier;
2. Ending the economic exploitation of data of developing nations;
3. Usage and analytics of data by states that store such data.

The Indonesian government, it was observed, has taken a novel approach with regard to data governance. Indonesia's proposed framework will classify data into two categories — strategic or classified data, and "common" data. Data belonging to the second category will not be localised.

Development for All

Participants at the Dialogue concurred that there is a digital gap, even amongst the countries of ASEAN. On account of lack of adequate access to technology, Cambodia, for instance, has thus far been unable to capitalise fully upon its demographic dividend. The rapid economic growth of Cambodia in the past two decades has left policy following its tail. To bridge the digital gap, policymakers from across ASEAN countries must pay greater attention to the cyber domain, especially through efforts to promote public education in terms of technology and data.

Another point of intersection between data and development is the need for accurate identification and authentication. Malaysia, the Philippines, and Thailand are exploring the idea of a digital ID to provide a reliable authentication platform. Interestingly, financial institutions have been leading the drive for such platforms. At the same time, privacy concerns continue to clash with digital ID initiatives. In Indonesia, which has had a digital ID since 2006, private sector institutions have been gathering personal data from the government, under the guise of 'Know Your Customer' (KYC). Participants expressed the need for stronger and more secure digital ID frameworks.

Disinformation

Stakeholders at the Dialogue observed that an increase in internet penetration and mobile phone usage has corresponded with an increase in disinformation campaigns. Participants conceded that the problem of fake news was not new, but the use of messaging and social media platforms to spread disinformation has complicated policy responses. Social media has become the public's primary source of information and has thus become a fertile ground for the manipulation of truth and facts. The impact of disinformation includes:

- Its effect on private business;
- Influencing electoral processes; and
- Incitement of violence.

Malaysia introduced a law in April 2018 to cull fake news but has faced criticism on the grounds that the law restricts free speech. It was eventually abolished after public resistance. Disinformation is, therefore, a problem that needs to be addressed with sensitivity and after widespread consultation.

Cybersecurity

Cybersecurity is yet to become part of popular discourse in many emerging markets. A lack of awareness amongst the public has permitted governments to move slowly on

cybersecurity-related policy discussions. However, there are notable exceptions: in the Philippines, cybersecurity is currently at the forefront of public consciousness owing to major data breaches.

During the course of the dialogue, participants observed that ASEAN countries must be proactive in developing measures to identify and prosecute cyber-crime and sanction cyber criminals. In this regard, India is also in the process of setting up sectoral Computer Emergency Response Teams (CERTs), especially to aid the financial sector — where most attacks are concentrated. In this vein, the participants discussed how ASEAN and India could create an effective regime to share information in case of cyber incidents. A participant noted that Singapore had shared data with India in the aftermath of the SingPass data breach, which proved very helpful to the latter for forensic purposes.

In the Philippines, measures taken to protect against cyber-attacks in the financial sector are based on the value of the assets that they protect. A participant suggested that to ensure accountability, willful negligence by the data custodian should be punished. Another suggested that punitive measures should be weighed for malicious actors attempting to steal or corrupt data.

Participants emphasised the need for domestic implementation of international law to enhance efficacy. An example presented was the Budapest Convention on Cybercrime, passed by the Council of Europe. The Philippines, for instance, acceded to the convention and enacted the Cybercrime Prevention Act of 2012. Participants also cited the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules, which allow for the redressal of cross-border data violations by enabling the pursuit and investigation of crimes by a counterpart agency in the country of the offender's residence.

Finally, there are standards emerging in Asia for the IoT, smart cities, privacy of mobile devices, and other digital advancements that permeate every level of development and deployment of technologies. It was emphasised that technical standards that protect citizens' rights must be embedded in the hardware of the technologies themselves.

ASEAN delegates also emphasised the role of institutions in coordinating responses to cybersecurity threats. There are currently four major mechanisms within ASEAN for cybercrime: the ASEAN Ministerial Meeting on Transnational Crime; ASEAN Telecommunications and IT Ministers Meeting; the ASEAN Regional Forum, and the ASEAN Senior Officials Meeting on Transnational Crime. Supplementing these mechanisms, the ASEAN Ministerial Conference on Cybersecurity (AMCC) — during its 2019 meeting, which took place shortly before the Track 1.5 Dialogue — announced a new working-level committee that would deliberate pathways for ASEAN CERTs to coordinate responses to cyber threats; the protection of critical infrastructure; and mutual assistance to tackle cyber incidents.

Cyber Norms Processes

The Dialogue looked into the norms and processes that are currently underway and how India and ASEAN nations can promote value-based regional cooperation in cyberspace.

There are four major multilateral and multi-stakeholder approaches to norms-making that are in play at the international level.

1. International organisations: The United Nations Group of Governmental Experts (UNGGE) on Cyber made significant contributions to this space in its fourth iteration through the introduction of right to self-defence in cyberspace. The sixth iteration will submit a report in 2021, with each country positing the frameworks for cyberspace governance.
2. Private technology companies: Microsoft has helped curate and coordinate initiatives like the Digital Peace Campaign focused on protecting ordinary, civilian users. Siemens is another example, with the Siemens Charter of Trust, promoting greater cybersecurity, which was signed in Munich in 2018.
3. Government-private partnerships: The Paris Call for Trust and Security in Cyberspace by Microsoft and the Government of France.
4. Expert committees: The Global Commission on Stability in Cyberspace, which ended its term recently, will be drawing up its report soon.

ASEAN has built upon these efforts and established novel, multidisciplinary instruments to tackle the cybersecurity challenge. Under the aegis of ASEAN, Singapore hosted the first AMCC in 2016. In 2018, the fourth AMCC took another crucial step by officially endorsing the 11 norms on state behaviour in cyberspace proposed by the UNGGE in 2015.

Efforts underway in the realm of AI norms serve as both models and cautionary tales for cyber norms-making. In the past two-three years, there appears to be a growing synergy in statements made by governments, international bodies, and technology giants regarding AI principles. There has been an emphasis on fairness, equality, responsibility, and accountability. However, there is often considerable daylight between the core values that drive principles and how they are often implemented on the ground by different actors. For instance, China's Beijing AI Principles underscore the values stated above. However, under the umbrella of "social harmony", algorithms have been deployed to subdue minorities and curb speech. While norms are, by design, open to a certain degree of interpretation, the constant undermining of their core values by powerful norm leaders sets a dangerous precedent. Participants agreed that there is a need to establish certain red lines and moral-ethical principles, which are beyond vitiation.

Capacity-Building and Responsive Regulation

At present, existing conventional laws are applied in Cambodia, Laos, and Brunei — all of whom are also struggling with capacity-building. Singapore, Malaysia, and Indonesia meanwhile have specific laws related to data protection and cybersecurity. Consequently, harmonisation of laws for regulation of cyberspace remains a challenge. Cyber-regulatory lawmaking in ASEAN nations has not been geared toward a wider regional framework, hence several distinct models of multistakeholder participation exist. Issues other than cyber conflict among nations and information security — such as capacity-building and the role of NGOs — need to be deliberated further for greater participation of ASEAN nations in the UNGGE.

There are efforts in this vein that are underway in the region. In 2016, the AMCC announced two major initiatives: the ASEAN Cyber Capacity Program and the ASEAN Cyber Capacity Fund. Together, these initiatives seek to build technical and policy capacity among ASEAN members through multistakeholder workshops and conferences. In 2018, Singapore

announced that the ASEAN-Singapore Cybersecurity Centre of Excellence will spend over S$30 million over the next five years to help ASEAN member states develop their cybersecurity capabilities.

In terms of innovations in regulatory methods, the Government of Singapore formed the Cybersecurity Advisory Panel working under the office of the Prime Minister. The group comprises private sector representatives and independent researchers from around the world who advise the government on norms which have long-term viability and cater to the needs of emerging technological challenges. This instrument ensures that policy serves as a complement to advancement in technology, rather than being reactive.

Finally, as an example of the necessity of responsive, up-to-date, and technologically grounded policymaking on emerging technologies, a participant presented a brief on India's Drone Policy 1.0. India imposed a blanket ban on drones in 2014, and in 2018 the Directorate General of Civil Aviation (DGCA) released its first drone policy, which laid out a comprehensive set of rules to register and take permission for flying remotely piloted aircraft systems. However, the DGCA essentially supplanted present models for civil aviation training to the use of drones, resulting in a set of regulations that did not—in many cases—align well with the reality of this new technology.

Shared Policy Priorities in a Fragmented Technology World Order

INDIA and ASEAN have both committed to adding US$ 1 trillion in economic value to their GDPs through the digital economy by 2025. Central to this effort will be the onboarding of presently unconnected populations (over 50 percent for both regions) and the creation of a regulatory environment that enables new data-driven enterprises. The ASEAN is responding to these imperatives through the 'ASEAN Framework on Digital Data Governance' — an initiative that is intended to facilitate harmonisation of data regulations among ASEAN Member States. In India, a flurry of new policies relating to cross border investments, e-commerce, broadband access, and concessions for Micro, Small & Medium Enterprises under the banner of the 'Digital India' initiative have attempted to support this ambition.

As with infrastructure connectivity, however, "digital" connectivity has come to signify more than access to digital technologies. It captures the interdependence of multiple national technological systems in the global economy. As part of this effort, both India and the ASEAN will integrate their markets with digitally mature economies — like the US, Japan, China, and the EU member states — in search of investments and commercial opportunities. Home to young and rapidly digitising young populations, India and Southeast Asia's economies are the next battleground for information technology companies from around the world.

Both India and the ASEAN must acknowledge that this "digital connectivity" will take place amid new geopolitical alignments. Diffused transnational networks of multinational companies, state intelligence agencies, platforms, and service and infrastructure providers are competing for market share and state power. As the US-China 'tech cold war' demonstrates, emerging technologies are now causing friction in international trade.

As the Fourth Industrial Revolution continues to alter economic relations, pathways for development, and national security concerns, the India-ASEAN partnership is well placed to

lead efforts that prioritise national imperatives amid international uncertainty and contest. Navigating the new geopolitics of digital connectivity will require India and ASEAN to address five areas going forward:

Development outcomes: India and ASEAN are likely to become the largest sources of commercially useful data in the world. However, it remains unclear whether these economies will be able to capture the value of this data. Digital value chains do not necessarily offer reliable pathways for development to states in South and Southeast Asia. In fact, the onset of the Fourth Industrial Revolution, 3D Printing, and automation will allow capital-rich nations to "re-shore" supply chains — depriving developing states of reliable development pathways. These economies are considering measures like data localisation to address this deficit — and are facing pressure from American and European partners. This raises questions of whether such measures are the only available tools, and how India and ASEAN can ensure that the digitisation of the global economy creates local value.

Political Values and Sovereign Concerns: The business decisions of a small set of technology platforms often produce outsized political and social consequences in the markets in which they operate. The community guidelines or corporate practices that underpin these decisions are often at odds with established legal and political principals in host markets. India and countries in Southeast Asia have often lamented at the unresponsiveness of multinational platforms in addressing these concerns. India and ASEAN should enter into a political dialogue to create new frameworks for accountability and transparency from technology platforms.

Equitable market rules: Currently, the US and China account for 90 percent of the market capitalisation value of the world's 70 largest digital platforms — significantly altering the topography of the global economy as it digitises. The digital economy is expected to entrench new commercial hierarchies — economies of scale for data-driven networks privilege those actors with control over data. The ASEAN and India must coordinate approaches to measuring the value addition of the digital economy, and reform rules relating to investment, competition, and tax to ensure that their enterprises are globally competitive.

National Security: A new infrastructure will underpin modern digital economies—with 5G communications technology forming the foundation of this arrangement. 5G wireless technologies will also enable a new set of digital products, ranging from autonomous vehicles to IoT appliances, creating new surface area for cyberattacks. Domestic decisions pertaining to 5G have also increasingly come under international scrutiny, with India and the ASEAN facing immense diplomatic and economic pressure from both the US and China to accede to their respective technological regimes. India and ASEAN countries should coordinate efforts to secure their digital infrastructure from both technological and political vulnerabilities.

International Efforts: ASEAN nations, as established pioneers in norms-making in cyberspace, and India, a growing strategic power in emerging technologies, must endeavour to establish and participate cooperatively in norms-making processes for cyberspace governance. Within this realm, India and ASEAN share common interests. First, owing to cyber norms processes

being driven largely by the West, there has been an inordinate focus on securitisation. It is thus important that a diverse set of state-level values are integrated into global-level processes. Furthermore, while ASEAN and India have both participated in multilateral norms-setting processes, there is scope for their respective business communities to more actively engage in cyber-diplomacy as well. Confidence-building exercises, sharing of cyber infrastructure, and cybersecurity (common but differential goals) remain crucial.

Conclusion

AS India and ASEAN ponder policy responses and norms frameworks to tackle new digital realities, and embark on their respective growth stories, the Track 1.5 Dialogue organised by ORF and the MEA sought out points of synergy, both for bilateral cooperation and for broader engagement in global multilateral and multi-stakeholder forums. Each country represented at the forum has its own capacities and strengths — including demographic dividend, booming technology industries, a vibrant start-up sector, and novel approaches to policy challenges. Continued dialogue enables all stakeholders to learn from the experiences and experiments of others.

Participants

ASEAN

Government

Chhem Kieth Rethy, Advisor to the Supreme National Economic Council, Cambodia
Francis Maleon, Ambassador of the Philippines to Kenya
Jakkrapong Chavong, Executive Director, Office of the Permanent Secretary, Ministry of Digital Economy and Society, Thailand
Myo Myint Htike, Assistant Director, Informations Technology and Cyber Security Department Ministry of Transport and Communications, Myanmar
Norsalimi Shaleh, Assistant Director, National Cybersecurity Agency, National Security Council, Malaysia
Vu Chi Cao, Deputy Chief of Division, Cyber Crime Department, Ministry of Public Security, Vietnam

Non-Government

Aishwarya Natarajan, Research Associate, Rule of Law Programme Asia, Konrad-Adenauer-Stiftung, Singapore
Alex Emms, Head of Blockchain, Ever Medical Technologies, Thailand
Andre Kwok, Founder and CEO, Future City Summit
Chhem Siriwat William, Director of Centre for Inclusive Digital Economy, Asian Vision Institute
Dondi Mapa, Former Deputy Commissioner, National Privacy Commission, Philippines
Moonyati Yatid, Senior Analyst in the Technology, Innovation, Environment and Sustainability (TIES) Programme of ISIS Malaysia
Nguyen Minh Duc, CEO, CyRadar, Vietnam
Pengiran Alias bin Pg Dato Paduka Haji Hidup, Authority for Info-communications Technology Industry (AITI), Brunei Darussalam
Sheryl Foo, Director, Vertech Capital, Singapore
Spark Perreras, Co-Founder and CEO, Pearl Pay, Philippines

India

Government

Vijay Thakur Singh, Secretary (East), Ministry of External Affairs
Nikhilesh Giri, Director (Indo-Pacific), Ministry of External Affairs
BC Pradhan, Deputy Secretary (Indo-Pacific), Ministry of External Affairs

Non-Government

Arindrajit Basu, Senior Policy Officer, Centre for Internet and Society
Arun Sukumar, Head of the Technology and Media Initiative, Observer Research Foundation
Akhil Deo, Junior Fellow, Technology and Media Initiative, Observer Research Foundation
Gulshan Rai, Distinguished Fellow, Observer Research Foundation
Sailesh Sriram, Research Assistant, Observer Research Foundation
Samir Saran, President, Observer Research Foundation
Sarvjeet Singh, Executive Director, Centre for Communication Governance, National Law University
Trisha Jalan, Author, Medianama
Trisha Ray, Junior Fellow, Technology and Media Initiative, Observer Research Foundation
Vinay Kesari, General Counsel, Setu

20 Rouse Avenue, New Delhi-110002
Ph: +91-11-43520020. Fax: +91-11-43520021
www.orfonline.org
info@orfonline.org