EVENT REPORTS

Report of the Second India-ASEAN Track 1.5 Dialogue on cyber issues

SPECIAL REPORT

INDIA-ASEAN TRACK 1.5 DIALOGUE ON CYBER ISSUES

2021
Jun
IO

INDIA-ASEAN INDONESIA

Introduction

India and the countries of ASEAN will go into the third decade of the 21st century with similar aspirations and challenges. India is home to world's second-largest base of internet users, numbering at 624 million; in ASEAN, nearly 400 million people are online with continued growth in the double digits. Added to this milieu are two challenges, on acute and the other chronic. The first is COVID-19, which demonstrated more than ever before the need for multilateral and regional solutions to crises. The second is the need to balance the imperatives of growth and security with the new paradigm of "geotech", the enmeshing of geopolitics and technology.

The First ASEAN-India Track 1.5 Dialogue on cyber issues was held in New Delhi on October 14, 2019. The Dialogue hosted 35 participants from 12 countries, including entrepreneurs, startups, MNCs, academia, and representatives from the ministries of external affairs and/or IT of the respective countries. Discussions focused on data governance, cyber norms, and trends in cybersecurity in the region.

37 experts from India and the countries of ASEAN convened virtually for the Second ASEAN-India Track 1.5 was held virtually on October 12, 2020, co-hosted by ORF and the Ministry of External Affairs. Participants delved into three specific policy response areas building on discussions in the 2019 edition:

1. Zero Days: Toward a Cross-Sectoral Approach to CybersecurityBoth India and the countries of ASEAN have set ambitious targets for becoming leaders in the 4IR, with strategies for 5G, Internet of Things (IoT), Artificial Intelligence (AI) and quantum computing. Robust cybersecurity underpins a connected world and will need to be a collaborative effort between businesses, governments, and civil society. How can the tw regions work together on areas like cybersecurity policy development, knowledge sharing, and capacity building so that experiences from each benefit efforts in the othe What measures can countries take to foster cyber resilience?

2. Going Viral: Regional Responses to Malicious Actors in CyberspaceCyberspace is host to range of malicious actors, state and non-state, which cost business and governments millions in damages each year. Even as incidences of cybercrime continue to rise exponentially. COVID-19 has seen incidences of cybercrime rise exponentially, targeting not just businesses and states but also citizens through sophisticated disinformation campaigns resulting in a parallel ‘infodemic’. What are the current bottlenecks faced by Indian and ASEAN authorities in investigating and prosecuting cross-border cybercrimes Can special exemptions be envisaged for extraordinary cases, where procedural delays i obtaining cross-border assistance?In what other ways can the modalities of resolving cross-border cybercrimes be eased without compromising state sovereignty?

3. The Socio-Economic Imperative in the Fourth Industrial RevolutionAutomation, digitalisation and artificial intelligence will create new opportunities for developing nations to leapfrog and together promise to boost global GDP growth by nearly 15 percent. Concurrently, policymakers must help prepare citizens for indelible changes in society and patterns of work the 4IR will bring. What kinds of technology solutions are both geographies adopting? Are there opportunities for B2B and G2G cooperation in th development of such technologies?

Opening Address by Ambassador Sidharto Suryodipuro, Ambassador of Indonesia to India

It is a pleasure to share my views at the opening of the Second ASEAN India Track 1.5 Dialogue on Cyber Issues. This is important not only for India and ASEAN today, but I thi it will become even more important into the future. This 1.5 Track Dialogue will form pa of the effort to discuss critical issues related to India-ASEAN digital cooperation and recommendations made in this dialogue could prove valuable to address the myriad of cyber issues faced by our region.

The importance of this issue has been further underscored with the advent of COVID-19 the lockdowns throughout the world, and accelerating digitalisation to connect various human activities and interests. I would like to congratulate ORF, MEA, and ASEAN exper for their foresight when they held the first Track 1.5 dialogue last year. The report provides an important roadmap for our thoughts and actions.

Unfolding international political events have also added further urgency for both India and ASEAN to strengthen cooperation on cyber issues. With a combined population of nearly 2 billion people, nearly a quarter of humanity, as well as significant economic hef and geopolitical standing, India and ASEAN are not only neighbors with flourishing physical, digital, regulatory and people-to-people and connectivity. We also share many similar and overlapping political, economic, social, cultural interests. We share similar interests in cyber security, cyber norms, capacity-building, and developing productive ar secure digital platforms for the population to further their livelihood and well-being. Or of the most important challenges that our countries would have to face in the midst of COVID-19 is how to revive our economies. The significant and growing role of the digita economy is obvious. We see this in India: I definitely see this living in New Delhi, we see this in ASEAN, and throughout the world.

COVID-19 has significantly accelerated India's digital economy. Likewise, in Indonesia, its young growing and digitally-savvy population, with some of the world's highest social media and mobile usage growth rates is powering e-commerce adoption, Indonesia's internet economy is valued at US $40 billion in 2019. It aims to reach US $130 billion by 2025. However, these are all projections made prior to COVID-19. How COVID will accelerate digital growth is yet to be seen; it may be too early for accurate projections.

At the regional level, ASEAN is on track to becoming one of the world's top five digital economies by 2025. It is currently the fastest growing internet market in the world with 125,000 new users coming on the internet every day. The World Economic Forum predicted that the ASEAN digital economy will grow significantly, adding an estimated l $1 trillion to regional GDP between now and 2030. Again, these are projections made prior to COVID-19.

All of these developments—growing in interregional trade, business, linkages, connectivity, and digital transformation—will and have exposed the region to cyber attacks, cyber threats, privacy breaches, amongst others. On our part, ASEAN is working to ensure that the region's response to cyber security challenges is comprehensive and forward looking, engaging an array of stakeholders to deal with the threat. This is an are for the ASEAN-India partnership framework to address as well.

The development of common norms between India and ASEAN is important to ensure a safe, open, peaceful, and accessible cyberspace for all stakeholders. Therefore, in our view, ASEAN-India partnership could expand into such areas as protection of critical information infrastructures and capacity building measures between national agencies i cyber security and cyber issues through experience sharing.

My final point for the participants and organisers: On October 16, 2020 India and ASEAN inaugurate[d] the ASEAN PhD Fellowship Program. This is a program for 1000 ASEAN citizens to do their PhDs at prestigious Indian institutes of technology. You will recall th this initiative was announced by Prime Minister Modi at the 25th anniversary of ASEAN-India dialogue relations in 2018, and launched by Honorable Ministers of External Affair and of Education. This is an excellent initiative to fill the void in education cooperation between India and ASEAN. It will be India's contribution to the education and upskilling ASEAN cyber capacity and to the closer collaboration between India and ASEAN and to our common digital transformation in the Fourth Industrial Revolution.

Opening Address by Ms. Riva Ganguly Das, Secretary (East), Ministry of External Affairs, India

I take this opportunity to welcome the eminent cyber experts representing government think-tanks, academia and industry from ASEAN Member States and India. I also thank ORF for putting together this dialogue in partnership with MEA.

The second ASEAN-India Track 1.5 Dialogue on cyber issues builds upon the success of it first edition held last year and aims to take forward the ASEAN-India cooperation on digital and cyber domain.

'Digital Technology' is a great enabler. When the world is facing travel restrictions and social distancing measures are in place, digital technology has brought all of us togethe to exchange views, hold discussions, and come up with solutions.

The COVID19 pandemic has accelerated the 'digitisation' and 'cyberisation' of our engagements—work from home has become a new norm. Dependence on virtual platforms has risen steeply. There is a greater dependence on digital payment platform due to reduced cash handling. Greater data sharing is happening online. Presence on social media has also increased. Digital technologies are playing a key role in keeping th supply chains open for an accelerated and sustainable economic recovery in the region.

With our increasing dependence on digital technologies and ever-increasing footprint ir cyberspace, there is an enhanced need to formulate and implement measures for securing our cyber domain from malicious actors. A recent assessment report of the COVID-19 cybercrime impact on Asia and the South Pacific region by INTERPOL shows that the major cyber security trends include COVID-19-related frauds, phishing campaig and online sale of fake medical supplies and PPEs. INTERPOL warns that the cyber criminals are taking advantage of the economic downturn and people's anxiety and hav enhanced their social engineering tactics by using COVID-19 as the basis for their attack The anxiety has been further fueled by the scourge of "fake news", "wrong information' and in some cases "targeted disinformation". This 'infodemic' of information has interfered with our abilities to craft proper public health and economic responses to the COVID crisis. According to a World Economic Forum report, one of the biggest concerns during the pandemic is the increase in cyber attacks and data fraud. With the increased online presence due to lockdowns and work from home, radical elements are using soci media platforms to disseminate misinformation through hate speech, fake news, and doctored videos. They seek to particularly target vulnerable individuals.

Increased dependence on digital technologies has created both pressures and opportunities for creative policy solutions and regional collaboration to foster a secure,

resilient, and equitable cyberspace.

As experts on this subject, you are all well aware about the challenge that policy makers and industry face, in managing policy and social changes, along with the exponential rat at which technology transforms our world. India is a case in point—India has already become the second largest internet user base in the world. Internet penetration has crossed the mark of 50 percent with about 700 million internet users and the number is poised to reach 1 billion by 2025. According to the India Cellular and Electronics Association report, the number of smartphone users are expected to reach 820 million 2022. This means huge possibilities; our digital economy already generates around US $200 billion annually which may reach between US $800 billion to US $1 trillion by 2025 However, this also puts daunting challenges for our policy makers. The number of cybercrimes have witnessed a 500 percent increase in the last five years.

With more than half of its 643 million people below the age of 30, ASEAN is passing through a similar digital growth trajectory. According to the World Economic Forum, ASEAN is the fastest growing internet market in the world. With 125,000 new users coming into the internet every day, the ASEAN digital economy which already generates around US $150 billion every year, is projected to add an estimated US $1 trillion to regional GDP in the coming decade. However, as expected, ASEAN is also witnessing increased incidences of cybercrimes.

Large percentage of young populations, huge potential to enhance economic ties, cultural, and civilizational affinity and already robust ASEAN-India Strategic Partnership provide adequate reason and incentive for strengthening ASEAN-India Cyber and Digita cooperation. The rapidly increasing threats to safe and secure cyberspace in the COVID and post-COVID era, make ASEAN-India Cyber Cooperation imminent.

There is a huge scope for us to learn from each other and synchronise our efforts:

India’s efforts to transform itself into a digitally empowered society and knowledge economy are exemplified by the flagship Digital India programme. India is home to the world’s largest digital literacy programme—Pradhan Mantri Grameen Digital Shaksharta Abhiyan (Prime Minister’s Rural Digital Literacy Campaign) which aims to train 60 millior rural adults. More than 300 government apps aim to bridge the digital divide in India. To

tackle the growing incidents of cybercrime and to ensure a safe, secure, trusted, resilier and vibrant cyberspace, Government of India is formulating the National Cyber Security Strategy 2020 for the next five years. The strategy will supersede the previous Cyber Security Strategy of 2013 and is likely to be launched by the end of this month. ASEAN, on its part, is also focusing on enhancing the region's cyber resilience. Important policy measures and frameworks to this end, include e-ASEAN Framework Agreement, ASEAN Economic Community 2025, and Master Plan of ASEAN Connectivity (MPAC 2025). MPA 2025 envisages to develop an ASEAN Framework on Digital Data Governance. In 2018, under the chairmanship of Singapore, ASEAN adopted the ASEAN Cybersecurity Cooperation Strategy. ASEAN-Singapore Cybersecurity Centre of Excellence, launched i October 2019, is doing a commendable job.

Clearly, there is a need to align and synergise these individual efforts. India's Centres of Excellence in Software Development and Training (CESDTs) being established in Cambodia, Lao PDR, Myanmar and Vietnam aim to enhance our digital cooperation. Indi is also funding 'Child Online Risks Awareness Campaign' and 'Building Capacity on Digita Public Services Implementation and Cyber Security for Government Agencies' as Quick Impact Projects in Cambodia in 2020. We would be happy to offer similar projects to other ASEAN partners as well.

In this context, the interaction of cyber experts representing governments, think tanks, academia, and industry from ASEAN and India, such as this, aims to help us in crystallisin the ideas for future cooperation into actions.

Cyberspace is border less and, therefore, our efforts to harness this shared space shoul also be unfettered by national boundaries and be based on regional and global cooperation. India emphasises that the core values of liberty, freedom of expression an rule of law, apply to cyberspace as well. It is in our common interest to maintain peacefu secure and resilient cyber space. We want countries to find common ground on cyber norms, which encourage international cooperation toward security, while fostering equitable access to cyberspace.

In closing, I hope that the technical sessions that follow this inaugural event will facilitat an active exchange of ideas and experiences. We look forward to your recommendation

to enhance cooperation on all aspects of cyber cooperation.

Themes of discussion

Networked problems

Dialogue participants noted trends in the geopoliticisation of cyberspace, including the US-China decoupling and the attendant opportunities for deepening technology ties between India and ASEAN. 2020 in particular witnessed a new wave of digital decouplin efforts not just amongst the two giants in the east and the west but by the European Union, Australia, Japan, and India, amongst others. Policy measures in the 5G space have been emblematic of this trend, and there is also mounting scrutiny of technology supply chains writ large. Participants also noted the significance of industry actors being increasingly supportive of decoupling efforts as well as allied actions and policies to secure digital ecosystems against hostile actors—both state and non-state.

Yet networked problems need networked solutions. The diffuse nature of cyber threats and the lack of hard borders in cyberspace mean that effective action requires collaboration, and all participants welcomed dialogue and cooperation between India ar ASEAN to address these shared challenges.

Mapping capabilities

Several participants noted that there is considerable variation between countries on cyber capabilities, and for any form of regional rapid response system for cyber incident these uneven capabilities must be accounted for. The first step for collaboration, therefore, would be to map existing capabilities, identify gaps and engage in capacity-building measures. An example of such a mapping exercise is India's TechSagar, an initiative supported by the National Cyber Security Coordinator, which maps India's current capabilities and competencies relating to technology areas that contribute to cyber, including startups, research and development, patents and products.

Trust through harmonised regulation

Robust regulation was viewed by participants as core to building trust, both amongst internal constituencies—citizens, start-ups, industry, civil society, local governments—as well as external constituencies. In this vein, participants also noted the need for

interoperable standards for data sharing for the seamless and timely prosecution of cybercrimes.

ASEAN participants stated that harmonisation of cybercrime laws and data protection regulations will need to be undertaken on three fronts: Sub-national, intra-ASEAN, bilateral processes with India. For instance, while some countries in ASEAN—Singapore, Vietnam, Thailand, Lao PDR, Indonesia, Malaysia, Brunei, and the Philippines—have enacted some form of cybercrime legislation, Cambodia and Myanmar are still in the draft legislation stage. On a global level, extradition often requires double criminality however there is considerable inconsistency in what acts countries define as a cybercrime. Finally, at a national and subnational level, one participant noted that in mo countries, investigation and prosecution of cybercrimes is not the domain of a single ministry or entity and that the interface between countries on cybercrime would need t account for all relevant entities.

Openness vs. security

There was some daylight between participants who felt unfettered access to online spaces is not tenable in the long-term and those who argued that individual rights and connectedness should always be at the centre of regulations in cyberspace.

“Anonymity”, one official noted, “is weaponised by cyber criminals.” The widespread use of virtual private networks (VPNs) and network protocols like onion routing, particularly in the dark web, are barriers to effective identification of culprits, and by extension, to the use of cybercrime laws. Others, however, cautioned against viewing anonymity and prosecution of cybercrime as a binary. Anonymity is one of the few forms of protection persecuted communities and minorities have under certain regimes. A secure cyberspac cannot be built upon backdoors that can lend themselves to misuse by malicious actors.

Rights-preserving access and human-centric digital revolution

The policy conversation on cybercrime, participants pointed out, are heavily concentrate around questions of state access to data, with individual rights and privacy positioned ir direct opposition to effective cybercrime investigation. Platforms that engage in a

meaningful and sustained way on matters of the digital rights of the individual are scarc and state engagement on these issues is particularly lacking.

Some speakers also cautioned against over-regulating. In the area of data governance, f instance, restrictive measures and a glut of regulatory bodies could hurt the creation of global data governance norms and interoperable data regimes.

Finally, the aim of digital regulations, whether they be on payments, or data, or cybercrime, must always keep the aim of an inclusive and sustainable digital revolution a their core. Emerging technology regimes should not disempower communities, marginalise stakeholders, and disproportionately harm vulnerable communities.

Next Steps

ASEAN-India Convention on cybercrime

Cybercrimes can occur at a rapid pace, affecting thousands of users and evidence can vanish in a matter of hours if not minutes. For effective cross-border investigation and prosecution, ASEAN and India should work toward a regional convention on cybercrime. The ASEAN-India Convention on Cybercrime will outline shared definitions of cybercrim identify nodal authorities, and provide a baseline for capacities that individual signatorie would need to build to fully participate in the convention. If bilateral agreements exist, there would also need to be clarity on how they interact with the convention. The ASEA India Convention on Cybercrime can, in later stages, extend to other regional powers, through forums like the East Asia Summit.

Shared tools to simplify existing MLAT processes

Many participants noted the difficulties of the Mutual Legal Assistance Treaty (MLAT) process to tackle cybercrime, including identifying the relevant nodal authorities and paperwork required to process requests. Some progress has been made in this respect: India, for instance, the Ministry of Home Affairs has recently identified the Indian Cybercrime Coordination Centre (I4C) as the nodal authority on cybercrime, including coordinating MLAT requests. ASEAN and India should, in tandem with efforts toward a cybercrime convention, build a shared portal that provides guidance on nodal authoritie

forms, regulatory requirements, and processing times to avoid delays due to bureaucrat hurdles.

Complementarity in ASEAN and India's engagement in global forums

ASEAN and India should agree upon a common approach and shared principles at globa multilateral and multistakeholder processes for securing cyberspace. Spaces like the UN Open-Ended Working Group (OEWG) on developments in the field of ICTs in the context of international security, The UN Group of Governmental Experts (UNGGE) on advancing responsible state behaviour in cyberspace in the context of international security, the U Secretary General's High-Level Panel on digital cooperation, the Paris Peace Forum and the Internet Governance Forum are all forums that India and ASEAN could productively engage with. Other issue-specific bodies that could also serve as important touch points include the Global Privacy Assembly, of which the Philippines is a member, and in which India and Malaysia had observer status till April 2021. Global forums provide pathways f industry-to-industry collaboration between India and ASEAN as well. Technology companies from the two geographies could, for instance, join industry bodies like the Charter of Trust and the Cybersecurity Tech Accord.[1]

Participants

ASEAN

Alastair Loh	Desk Officer, ASEAN Directorate, Ministry of Foreign Affairs Singapore
Captain Nguyen Huu Cuong	Officer of Hi-Tech Crime Prevention & Suppression Department, Vietnam
Cezar O. Mancao II	Executive Director V, Cybercrime Investigation and Coordinating Center, Philippines
Chheang Vannarith	President, Asian Vision Institute, Cambodia
Chitsanuphong Thanutong	Computer Technical Officer, Ministry of Digital Economy and Society, Thailand
Chong Zheng Ying	Senior Manager, Cyber Security Agency of Singapore
Daw Yi Mon Kyaw	Information Technology & Cyber Security Department, National Cyber Security Center, Ministry of Transport & Communications, Myanmar
Dondi Mapa	Regional Chief Privacy Officer, APAC, Citi
Dongwoo Kim	Program Manager, Asia Pacific Foundation of Canada
Intan Safinas	Senior Manager, Cyber Security Agency of Singapore
John Boitte Santos	Second Secretary, Embassy of the Philippines

Jose Carlos P. Reyes	Director IV, Cybersecurity Bureau, Department of Information and Communications Technology, Philippines
Karthik Nachiappan	Research Fellow, ISEAS, National University of Singapore
OU Phannarith	Director, Department of ICTs Security, Ministry of Post and Telecommunication of Cambodia
Ruthanne Soh	Desk Officer, ASEAN Directorate, Ministry of Foreign Affairs Singapore
Sandra Therese Christine Guiang	Third Secretary, Embassy of the Phillippines
Sheryl Foo	Director, Vertech Capital, Singapore
Sidharto Surydipuro	Ambassador of Indonesia to India
Spark Perreras	Co-Founder and CEO, Pearl Pay, Philippines
Tracy Ly	Graduate Researcher, Asia Pacific Foundation of Canada
Vongvilai INTHASANH	Deputy Director of Incident Response, LaoCERT
Wahyudi Djafar	Researcher at Institute for Policy Research and Advocacy [ELSAM], Indonesia

India

Akshay Mathur	Director, Observer Research Foundation Mumbai
Astha Kapoor	Co-Founder, Aapti
Kanchan Gupta	Distinguished Fellow, Observer Research Foundation
Amb. Latha Reddy	Co-Chair, Global Commission on the Stability of Cyberspace and Distinguishe Fellow, Observer Research Foundation
Lt. Col. Nishant Singh	OSD, EG&IT, Ministry of External Affairs
Nikhil Pahwa	Founder, Medianama
Rama Vedashree	CEO, Data Security Council of India
Riva Ganguly Das	Secretary (East), Ministry of External Affairs, India
S. Janakiraman	JS, Cyberdiplomacy, Ministry of External Affairs, India
Sadhana Relia	Advisor/Scientist G, Ministry of Science and Technology, India
Sangeet Jain	Junior Fellow, Observer Research Foundation
Sarvjeet Singh	Former Executive Director, Centre for Communication Governance, NLU Delhi
Trisha Ray	Associate Fellow, Observer Research Foundation
Vineet Kumar	US, Cyberdiplomacy, Ministry of External Affairs, India

---

[1] Charter of Trust

Cybersecurity Tech Accord

This report was written by Trisha Ray, Associate Fellow, ORF

ORF research and analyses now available on Telegram! Click here to access our curated content — blogs, longform and interviews.

Economics and Finance

Energy

Gender

Healthcare

International Affairs

Media and Internet

Content Type

Videos

Series

Books and Monographs

Commentaries

Event Reports

GP-ORF Series

Issue Briefs and Special Reports

Monitors

Occasional Papers

Primer

Surveys & Polls

Young Voices

Archives

Programmes and Centres

Centre for New Economic Diplomacy

Centre for Security, Strategy and Technology

Economy and Growth

Energy and Climate Change

Political Economy

Strategic Studies

Sustainable Development

Tech and Media

Initiatives

Cybersecurity and Internet Governance

Education and Skilling

Energy and Resources

Eurasian Studies

Future of Work

International Trade and Finance

Maritime Studies

Media Studies

Neighbourhood Studies

Nuclear and Space Studies

Political Reform and Governance

Public Health

Urban Policy

Geographies

Africa

Americas

China

European Union

India

Neighbourhood

Russia and Eurasia

south Asia

The Pacific, East and Southeast Asia

USA and Canada

West Asia

Who We Are

Work With Us

Write For Us

Media Release

Partners

Subscribe To ORF

Contact Us