ORF

AN ASEAN-INDIA CYBERSECURITY PARTNERSHIP FOR PEACE, PROGRESS, AND PROSPERITY

Report of the Third ASEAN-India Track 1.5 Dialogue on Cyber Issues

Trisha Ray

Attribution: Trisha Ray, *An ASEAN-India Cybersecurity Partnership for Peace, Progress, and Prosperity: Report of the Third ASEAN-India Track 1.5 Dialogue on Cyber Issues,* April 2022, Observer Research Foundation.

Observer Research Foundation
20 Rouse Avenue, Institutional Area
New Delhi 110002
India
contactus@orfonline.org
www.orfonline.org

The Observer Research Foundation (ORF) provides non-partisan, independent analyses and inputs on matters of security, strategy, economy, development, energy and global governance to diverse decision-makers (governments, business communities, academia, and civil society). ORF's mandate is to conduct in-depth research, provide inclusive platforms, and invest in tomorrow's thought leaders today.

Design & Layout: Rahil Miya Shaikh

CONTENTS

INTRODUCTION

In 2020, an estimated 4.6 billion people in the world were online; India was home to 795 million of them, and 440 million users were in the countries of the ASEAN (Association of South East Asian Nations).[1] The same year also saw a rapid increase in internet use, with the COVID-19 pandemic push bringing people online at an unprecedented scale amidst lockdowns and restrictions on movement. A surge in use of internet services has, however, exacerbated the already-intractable issue of the safety of data, people, livelihoods, and enterprises online.

Across geographies, the volume of cyber-attacks increased in 2020 and in 2021, but in the past year the Asia-Pacific (APAC) witnessed the highest number of these incidents. The pandemic period of 2020-21 also saw a global uptick in ransomware attacks.[2] An IBM report noted that ransomware accounted for nearly one-fourth of the volume of global cyber-attacks in 2020, and a fifth of attacks in 2021.[3] The threat landscape is shifting in the APAC region as well: data theft and leaks were the most prevalent type of attack in 2020; and in 2021, unauthorised server access and ransomware. APAC also leads globally on cyber-attacks on government, financial institutions, transportation, and manufacturing. Cyber-attacks not only result in lost revenue for companies and disruption of essential services but can also damage the trust users and consumers have in digital services. Cybersecurity is thus a policy issue that cuts across sectors and stakeholders.

The ASEAN members and India are not only neighbours but share similar goals for a sustainable, inclusive, and trusted digital transformation of their governments, societies, and economies. This shared vision was highlighted in the Plan of Action to Implement the ASEAN-India Partnership for Peace, Progress and Shared Prosperity (2021-2025), and its commitment to future-proofing institutions, workforces, and ICT infrastructure.[4] Key is securing the digital highways—be it data flows, communication networks, or critical information infrastructure—that enable the citizens, businesses, and governments of both geographies to grow and prosper. This is required to unlock both India's "trillion-dollar opportunity" as well as the *ASEAN Digital Masterplan 2025.*

At the inaugural ASEAN-India Track 1.5 on Cyber Issues in 2019, then Secretary (East) Vijay Thakur Singh outlined India's interests in a peaceful and inclusive cyberspace: "We want countries to find common ground on cyber norms, which encourage international cooperation toward security, while fostering equitable access to cyberspace."[5] In the backdrop of the COVID-19 pandemic, the imperative of secure and equitable access has only become more urgent: as the *ASEAN Comprehensive Recovery Framework* emphasises, there is a need to focus efforts on inclusion as well as resilience.

This report builds on the ASEAN-India Track 1.5 Dialogue on Cyber Issues, co-hosted by the Ministry of External Affairs, Government of India, and the Observer Research Foundation. The third edition of the dialogue was held virtually on 20 October 2022 (see Annex). The report starts with a high-level overview of cybersecurity policies in India and the ASEAN countries, and cybersecurity cooperation between them. It then delves into the intertwined issues of encryption and securing critical infrastructure, and concludes with three actionable recommendations.

VISION 2025: POLICIES AND PRIORITIES

Cybersecurity is an issue that cuts across several policy priority areas for the governments of India and the ASEAN countries alike, including digital-led economic transformation strategies, existing offline threats to regional security, and national security as well as sovereign control. The colour-coded Table 1 provides a glimpse of government strategies and policies in the region. Beyond the documents mentioned in this table, governments have also enacted sector-specific policies such as those for data, cybercrime, and electronic transactions.

Table 1: Data, Cybersecurity, and Digital Economy Policies in ASEAN and India

Relevant Strategy or Policy Enacted

Draft or section of broader legislation

No relevant law/policy exists

Country	Cybersecurity Strategy/Policy	Privacy and Data Protection Legislation/ Framework[a]	National Digital Transformation Strategy
India	National Cybersecurity Policy 2013; 2020 (Draft)	Information Technology Act 2000 Personal Data Protection Bill (Draft)	Digital India
ASEAN	ASEAN Cybersecurity Cooperation Strategy (2021-2025)	ASEAN Framework on Personal Data Protection	ASEAN Digital Masterplan 2025
Brunei	N/A	Draft Personal Data Protection Order	Digital Economy Masterplan 2025
Cambodia	N/A	Article 32 of the Law on Electronic Commerce (2019)	Cambodia Digital Economy and Society Policy Framework 2021-2035 Cambodian ICT Masterplan 2020

a Privacy and data protection legislation, as defined by the UN Conference on Trade and Development. This table does not include laws pertaining to specific sectors, such as digital transactions.

Indonesia	National Cyber Security Strategy 2020 (Draft)	Law of the Republic of Indonesia Number 11/ 2008 Concerning Electronic Information and Transactions (2008)	Making Indonesia 4.0 Draft Indonesia Digital Roadmap 2021-24
Lao PDR	National Cybersecurity Strategy (Proposed)	Law on Electronic Data Protection (2017)	N/A
Malaysia	Malaysia Cyber Security Strategy 2020-2024 (MCSS)	Personal Data Protection Act (2010)	Malaysia Digital Economy Blueprint
Myanmar	Draft Cyber Security Law (2021)	Law Protecting the Privacy and Security of Citizens (2017, Amended 2021) Draft Cyber Security Law (2021)	Myanmar Digital Economy Roadmap 2018-25
Philippines	National Cybersecurity Plan 2022	Data Privacy Act (2012)	The Philippine Digital Strategy Transformation 2.0: Digitally Empowered Nation
Singapore	The Singapore Cybersecurity Strategy 2021 Singapore's Safer Cyberspace Master Plan 2020	The Personal Data Protection Act (2012, took effect in 2021)	Smart Nation Strategy
Thailand	National Cybersecurity Strategy 2017-2021	Personal Data Protection Act, B. E. 2562 (2019)	Thailand 4.0
Vietnam	Cyber Information Security 2016-2020; 898/QD-TTg	Law on Information Technology No. 67/2006/QH11 (2006) Draft Decree on Personal Data Protection (2021)	National Digital Transformation Roadmap 2025 and Vision Toward 2030

At a regional level, ASEAN adopted the *ASEAN Digital Masterplan 2025*, for economic growth "powered by secure and transformative digital services, technologies and ecosystem."[6] Similarly, ASEAN member states have adopted their own digital strategies and roadmaps to 'future-proof' their economies and workforces: these include, for example, *Thailand 4.0,* and Vietnam's *National Digital Transformation Roadmap 2025 and Vision Toward 2030.* Similarly, *Digital India* consolidated the country's numerous digital economy initiatives under one broad strategy to transform India into an empowered digital economy. With a few exceptions, digital economy strategies view cybersecurity as key to building a trusted online environment for individuals and businesses.

> *To ensure adoption of digital services, particularly in areas like health and finance, consumers need to trust these services. This is also true of new and emerging technologies. A key part of this is ensuring that cybersecurity and digital data governance best practices are adopted as widely as possible, both to mitigate the direct impact of a breach on business and consumers and to build trust.*
>
> *- ASEAN Digital Masterplan 2025*

Some strategy documents also see trust as essential to squaring the trade-off between national security, economic growth, and individual privacy. For instance, Malaysia's *Digital Economy Blueprint* notes trust as a key principle to "ensure the growth of the digital economy, without compromising privacy and cyber security."[7]

While the digital priorities of ASEAN and India have grown increasingly aligned, the cybersecurity element of the partnership is relatively new. India's initial outreach to ASEAN was part of its successive 'Look East' and 'Act East' policies, which emphasised greater economic and security linkages. The two established a Strategic Partnership in 2012.[8]

> *Relations with ASEAN have become multi-faceted to encompass security, connectivity, strategic, political, space technology, counter terrorism and insurgency operations, anti-radicalisation, trade and investment, maritime security and defence collaboration, in addition to economic ties.*
>
> *- Lok Sabha Reference Note, 2018*[9]

ASEAN and India have in the past decade broadened and deepened engagement on cybersecurity issues. As a dialogue partner, India has been part of deliberations on cybercrime, ICT security, and emerging technologies at both the ASEAN Digital Ministers' Meeting (ADGMIN) and the ASEAN Defence Ministers' Meeting (ADMM). India has also undertaken campaigns with ASEAN member states, focused on online safety and cyber security capacity. It established Centres of Excellence in Software Development and Training in Myanmar, Vietnam, Lao PDR, and Cambodia.[10] In recent years, India has also initiated a number of 'quick impact projects' (QIPs) which are smaller yet high-impact projects under the Mekong Ganga Cooperation framework. These QIPs have a quick turnaround, with a budget of less than USD 50,000 and are focused primarily on capacity-building, empowerment, and development in the CLMV countries.[b,11] Such projects include "Building Capacity on Digital Public Services Implementation and Cyber Security for Government Agencies" and the "Child Online risks Awareness Campaign" in Cambodia. More recently, the *India-ASEAN Digital Work Plan 2022* listed as part of its agenda, cooperation through capacity building and knowledge-sharing in emerging technologies and applications such as Internet of Things (IoT), 5G, advanced satellite communication, and cyber forensics.[12]

The cybersecurity agencies of India and many ASEAN members also have a presence in a number of regional and international cybersecurity bodies

---

[b] CLMV includes Cambodia, Lao PDR, Myanmar, and Vietnam.

and frameworks. These include the Asia-Pacific CERT (APCERT); expert processes under the Council for Security Cooperation in the Asia Pacific (CSCAP); the UN's Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security; and its sister process in the Group of Governmental Experts (GGE) format. Outside of formal institutions, there are documents like the *Tallinn Manual*, which is the product of expert discussions hosted by Estonia in the aftermath of a massive Russian cyber campaign in 2017 that took banks, media outlets, and the government offline.[13] While the first edition of the manual, published in 2013, dealt with cyber operations only in the context of armed conflict, the second one, released in 2017, also addresses cyber operations below the threshold of armed conflict. Finally, multistakeholder initiatives like the Global Commission on the Stability of Cyberspace (GCSC) and the Paris Call for Trust and Security in Cyberspace—backed by governments, think tanks, tech giants and other stakeholders—have laid out common principles for protecting the "public core" of the internet.[14] The first ASEAN-India Track 1.5 on Cyber Issues in 2019 pointed to the need to identify "certain red lines and moral-ethical principles, which are beyond vitiation" and the 2020 dialogue identified cyber norms-making spaces where ASEAN and India must work toward defining complementary, if not common, principles and approaches.[15]

ENCRYPTION: NATIONAL SECURITY, INDIVIDUAL RIGHTS, GROWTH

As mentioned in the previous section, cyber policy in India and ASEAN is a balancing act between national security, economic growth, and individual privacy. This was seen at the Track 1.5 Dialogue, where civil society, industry, and government stakeholders often had highly different understandings of how such a "balance" could be found.

These seemingly competing imperatives are apparent in country approaches to encryption. Encryption is ubiquitous in ICT: it is used to secure the transit of information over networks and can be built into devices. The past decade has also seen the surge in popularity of virtual private networks (VPNs). A VPN is an encrypted private network "built over public and/or private network resources, used to support controlled and secure communications within a group of users."[16] As such, encryption is an issue that cuts across sectors and issues, including finance, telecommunications, digital public goods, online platforms, law enforcement, and inclusive digital development.

In India, for instance, Section 69 of the Information Technology Act 2000 (amended in 2008) gives the central and state governments the authority to intercept, monitor or decrypt messages/content transmitted through any computer resources for national security, law enforcement, and public safety.[17] Further, the Intermediary Guidelines (2021) state:

> *A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under Section 69 of the Act by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form.*

In Malaysia, the Strategic Trade Act (2010), the Computer Crimes Act, the Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007, and certain sections of the Criminal Procedure Code, among others, together outline a range of cases where service providers must assist authorities, including by providing encryption/decryption codes.

The 2021 Track 1.5 dialogue reflected this web of issues. Entrepreneurs from Southeast Asia cited the important role of encryption in improving their ability to provide secure, accessible services, especially to the swell of late adopters that started using these services during the outbreak of the COVID-19 pandemic. Indian representatives pointed to the "double-edged sword" that is encryption. They acknowledged benefits in terms of privacy and data security, but weighed these against pressing public safety issues like the spread of disinformation, radicalisation, and criminal activity online. Some government representatives from Indonesia similarly underlined how encryption policy must enhance both national security and people's digital rights, and urged ASEAN and India to work together to make positive policy contributions that could serve as a model for other countries.

What makes regional cooperation on encryption policy complicated is the milieu of sectoral regulators within each country that have set their own guidelines—on fintech, social media platforms, ISPs, and e-governance platforms.

The policy responses of different governments in the region fall across a wide spectrum. To be sure, the system of government, social and political histories, legal systems, and the relationship of governments with internet platforms play a role as well. As Eugene Tan, professor of law at the Singapore Management University has observed:

> *The legal systems of the ASEAN member states also differ greatly, ranging from common law as in the case of Singapore to civil law systems such as that in Indonesia, and hybrids of both, such as in Thailand, which makes it difficult to build a community law. ASEAN member states have also been reluctant to encourage the formation of a binding uniform legal system, stemming from a fear of impinging on ASEAN's long-held principles of non-interference and consensus.*[19]

It is necessary to understand these granularities to further the call for harmonised encryption regulations in both geographies. Many industry participants at the 2021 ASEAN-India Track 1.5 Dialogue called for an overarching encryption strategy at a national level, guided by a regional Indo-Pacific framework.[20]

TRUSTED AND RESILIENT CRITICAL INFRASTRUCTURE

The protection of domestic critical infrastructure has come under the radar of governments in ASEAN and India in light of several prominent cyber-attacks in recent years. In Singapore, for example, attackers exfiltrated the personal information of 1.5 million patients, for almost a year between 2017 and 2018, from SingHealth's database; the patients included the prime minister.[21] In 2020, a cybersecurity startup reported data dumps on the dark web that included payment card details of 300,000 cards belonging to the biggest banks in Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam.[22] In 2020-21, during the fallout from border skirmishes in Galwan, India's transportation sector and its electricity grid were targeted by threat actors with links to Beijing.[23]

The threat landscape is varied. It is populated by black hat hackers,[c] as well as state-sponsored threat actors, armed with an ever-evolving arsenal of tools and methods. In the case of the latter group, they may lie undetected in a system for months, if not years, before they are either detected, or they carry out a cyber-attack.[d]

---

[c] A black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons. See: "What Does Black Hat Hacker Mean?", Techopedia, https://www.techopedia.com/definition/26342/black-hat-hacker

[d] This type of threat is called an advanced persistent threat (APT). Threat actors may simply remain in the system for the purpose of cyberespionage, or they may engage in disruptive attacks.

National 5G rollouts are a current national policy priority, where the issues of critical infrastructure protection, national security and economic growth collide. Estimates of the economic value generated by 5G produce varied but impressive economic outlooks. PwC estimates that 5G mobile technology will add USD 1.3 trillion to global GDP by 2030,[24] IHS Markit pegs the economic value generated by 5G at USD 13.2 trillion by 2035,[25] and Nokia's research arm predicts a USD 8-trillion boost to global GDP.[26]

For India and most of ASEAN, a speedy, low-cost, efficient 5G rollout is paramount, and both geographies are concurrently in the process of increasing the coverage of (and, in some cases, rolling out) 4G networks.[27] Security measures specific to 5G encompass a range of policy actions and incentives, including export controls, imposing security obligations on telecom service providers (TSPs) and equipment providers, public procurement requirements, and international partnerships.[28] India's Department of Telecommunications (DoT), for instance, regularly notifies security requirements for TSPs and internet service providers (ISPs).[29] In March 2021, the DoT mandated that public procurement gives preference to "Make in India" cybersecurity products. In the same month, it mandated that licensed TSPs use only "Trusted Products" made by "Trusted Sources", as designated by the National Cyber Security Coordinator.[30] In Malaysia, CyberSecurity Malaysia, Celcom Axiata Bhd and Huawei Technologies collaborated to set up a 5G Cyber Security Test Lab, which will also – in its first phase – evaluate 4G equipment and networks.[31] However, the security of 5G networks also relies on the broader cybersecurity ecosystem, including data protection practices, encryption standards, and institutional capacity to monitor and respond to network intrusions — including sectoral computer emergency response teams (CERTs).

Finally, the case of 5G demonstrates the importance of the private sector in the protection of critical infrastructure. As an official at the 2021 ASEAN-India Track 1.5 Dialogue on Cyber Issues noted, "One observation when we talk about critical information infrastructure is that, over time, a lot of it has migrated to the private sector." This in turn calls for close

cooperation, whether in the form of public-private partnerships (PPPs), or regulations and safeguards set by the government, or a talent pipeline from the private sector to government to improve the government's own capacity and understanding of cybersecurity challenges. This cooperative relationship also requires a balance between punitive measures and those that build resilience. For instance, harsh penalties for cybersecurity breaches could lead to reluctance, especially but not exclusively among smaller enterprises, to report these incidents. Singapore, Indonesia, the Philippines, and Thailand all have mandatory data breach notification rules; India's draft data protection legislation includes such a provision as well.[e] In this context, one enabling measure would be a sectoral Information Sharing and Analysis Center (ISAC), that could serve as a central repository for cyber threats as well as a platform for information sharing between the private sector and government entities. In India, the National Critical Information Infrastructure Protection Center (NCIIPC) has supported the creation of an ISAC for telecommunications.[32]

[e] In many cases, however, disclosure is only mandated if the breach is likely to cause harm to users/consumers.

RECOMMENDATIONS

Capacity building and shared resources were two recurrent themes at the ASEAN-India Track 1.5 Dialogues on Cyber Issues in 2019, 2020 and 2021. Building on the expert inputs shared at the 2021 dialogues, this report offers three actionable recommendations, to be discussed in turn in the following paragraphs.

1. Build a Regional Malware Repository and Create an ASEAN-India Cybersecurity Threat Exchange Portal

Trusted PPPs are a cornerstone of cyber resilience and capacity building. The timely and secure exchange of information on cyber threats as they arise is crucial for a quick and coordinated response to cyber-attacks, especially on critical infrastructure. The most recent instantiation of this is the Log4j vulnerability, first identified by Chen Zhaojun, a security engineer with the Alibaba Cloud team.[33] Chen reported the vulnerability to Apache Software Foundation, a massive repository of open-source software projects maintained by a group of volunteer programmers. Alibaba Cloud faced backlash from Chinese regulators for reporting the vulnerability to Apache first, instead of the Chinese Ministry of Industry and Information Technology (MIIT).[34] MIIT suspended its information sharing partnership with Alibaba Cloud, citing the latter's failure to report the vulnerability directly to the former.

Malware repositories are collections of live malware samples that cybersecurity professionals can use to conduct analyses and practice cyber defence techniques. Such repositories exist, for instance, on platforms like GitHub,[35] as well as databases maintained by universities. Malware attacks do not respect national borders, and with ransomware attacks in APAC growing at double-digit rates, a common malware repository accessible by regional CERTs, ISACs and other authorised entities would be useful for conducting predictive analyses of ransomware families, as well as for cybersecurity professionals to use for practice. India has already built a national malware repository that could serve as a model for other countries to emulate.[36]

In a similar vein, an ASEAN-India Threat Exchange Portal can be a useful shared resource. White hat hackers and cybersecurity researchers can anonymously post threats and vulnerabilities likely to have widespread regional or global impact. The portal could be housed within the ASEAN-Singapore Cybersecurity Centre of Excellence.

2. Establish a Dialogue on a Regional Encryption Standard

With the current trajectory of cyber incidents, it is imperative to establish security protocols for data storage and transfer, especially in the form of strong encryption. According to many of the dialogue participants, the challenge lies in the patchwork of sector-specific regulations, superimposed upon uneven standards in the region. At the same time, the technical feasibility of decryption requirements imposed by new or draft regulations needs to be explored, in the context of not only the present threat landscape but also the coming challenges. While not explored during the dialogue, the issue of post quantum cryptography—making cryptographic methods resilient to the threats arising from advances in quantum computing—is one such challenge.

A multistakeholder dialogue on encryption would be a logical extension of the issue areas mentioned within the 2022 ASEAN-India Digital Work Plan. While arriving upon regional standards may be difficult given the need, first, to harmonise approaches at the national level, the dialogue could provide space for sharing knowledge and engaging in strategic foresight.

3. Establish Annual ASEAN-India Joint Cyber Drills

Cyber drills are a simulation of malware attacks, data breaches, and other cyber incidents that help test an organisation's cyber response and identify best practices and areas for further capacity-building. The ITU has run cyber drills with more than 120 countries, and the APCERT has facilitated APAC-level as well as narrower region-focused drills.[37] At the ASEAN level, there exists the annual ASEAN CERT Incident Drill (ACID). Each year's ACID focuses on a specific theme and strengthens cooperation between the CERTs of ASEAN member states, as well as those of dialogue partners.[38] India's CERT (CERT-In) has participated in these drills as a dialogue partner.

While these multilateral channels have helped build a level of operational familiarity between the CERTs of ASEAN members and India, an annual India-ASEAN cyber drill will further help establish best practices in cyber threat response between the two geographies. This can herald closer bilateral cooperation with ASEAN members as well.

ANNEXURE

A. Overview of the Dialogue

On 20 October 2021, the Observer Research Foundation, in partnership with the Ministry of External Affairs of the Government of India, hosted in a virtual format the third annual ASEAN-India Dialogue on Cyber Issues. The Dialogue hosted 55 participants from India and ASEAN, with representatives from national CERTs, national security councils, telecommunications ministries, and cybersecurity agencies, as well as think tanks, VCs, startups, and industry.

The third edition of the Dialogue centred around three themes:

1. The Road Ahead for Encryption

Encryption globally is caught in the friction between security and privacy, with a wide range of debates interwoven into policy. Encryption is a complex issue, and intersects with disinformation, the security of public digital infrastructure, law enforcement, and platform regulation. Stakeholders have suggested alternatives to breaking encryption, including client-side scanning, hashing constants and other measures that facilitate traceability.

What is the feasibility of privacy-preserving alternatives? Can India, ASEAN and the broader global community agree upon a set of baseline encryption standards?

2. Trusted and Resilient 5G Infrastructure

5G is the backbone of much of the world's bids to secure their space in the Fourth Industrial Revolution, a fact that is reflected in nationwide strategies for 5G rollouts. The debate over 5G has underlined the need for complete supply chain security of our communications networks. What are possible pathways of cooperation between the countries of ASEAN and India on creating a secure 5G ecosystem? Can the two geographies agree on specific parameters and definitions of "trustworthy" suppliers and vendors? Could the two foster competitive homegrown alternatives?

3. Securing Critical Infrastructure

A spate of prominent ransomware attacks on critical infrastructure in 2020-21, including healthcare providers, pipelines, and electricity grids points to a dangerous new normal. In this vein, the UN GGE on Cyber recently proposed additional norms on obligations of states viz damage to critical infrastructure and responding to requests for assistance in investigating such attacks, accounting for due regard to sovereignty. How can India and ASEAN help strengthen norms around "bright red lines" relating to critical infrastructure? Can the two engage in capacity building exercises for critical sectors like power and health?

B. Remarks by Smt. Riva Ganguly, Secretary (East)

Excellencies, Friends and Colleagues, Ladies and Gentlemen,

I am delighted to join you all today at the 3rd Edition of the ASEAN-India 1.5 Track Dialogue on Cyber Issues. I warmly welcome eminent cyber experts representing Governments, Think Tanks, Academia, and Industry and especially our guests from ASEAN.

I commend the efforts of ORF to take forward the engagement of ASEAN and India on this contemporary issue of relevance to our economies and societies, especially in these times. In recent times, the increasing use of cyber and information communication technologies has supported greater economic development, improved service delivery to citizens, generated greater social awareness and placed information and knowledge in the hands of individuals. The COVID pandemic is beyond doubt a health catastrophe that has delivered an enormous economic and social jolt, fundamentally changing the way we imagined societies, workplaces, and governance. The restrictions and disruptions posed by the ongoing COVID-19 pandemic have been mitigated to some extent by the advancements in digital technology that have enabled us to exchange views, continue discussions and cooperate effectively.

Most activities in this cyber-age - political, social, economic, humanitarian, and developmental – are now conducted in or connected to cyberspace. This has not only expedited the pace of growth but also brought forth a new set of challenges for which no pre-set solutions exist. Multiplicity of actors in the cyberspace as well as the growing dependency on critical infrastructure such as ports, airports, electricity grids, e-governance systems, and businesses, on the cyber platform imposes the responsibility to address concerns related to protection of the critical infrastructure from a cyber security perspective. Therefore, in the Cyber-age, though the meaning of peace has remained constant, the nature of threat and the tools to address them have transformed radically.

Some States are leveraging their expertise in cyberspace to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism. At the same time, non-state actors and terrorists around the world are using cyber space to broaden their appeal, spread virulent propaganda, incite hatred and violence, recruit youth and raise funds. There are widespread concerns that with the advent of new technologies like 5G - vulnerabilities and harmful hidden functions are being introduced, including through backdoor channels, into ICT networks and products.

Since cybercrime often has a transnational dimension, there is a crucial need for international cooperation to exchange experiences and share best practices for protection of information infrastructures. India lays huge emphasis on bilateral and international cooperation on cyber security. The need for cooperation between India and ASEAN member countries in this field is, therefore, self-evident. ASEAN, as we know, has been proactive in the region's efforts to tackle cyber security challenges and has undertaken various cyber confidence building measures.

This emphasis of ASEAN on Cyber Security and Cyber connectivity in accordance with international laws resonates deeply with India's approach towards Cyber space. India has also been working domestically to address the cyber security challenges through platforms capable of supporting and sustaining the efforts in securing the cyber space as well as through the adoption of comprehensive policies such as the New National Cyber Security Policy, which would provide an overview of what it takes to effectively protect information, information systems and networks.

Equitable access to the Cyberspace and its benefits is the other important area that India-ASEAN engagement on Cyber issues needs to focus on. We have witnessed the critical role played by Digital technologies during the Covid-19 waves, in keeping the supply chains open for an accelerated and sustainable economic recovery in the region and therefore, it becomes all the more important that the digital inequalities are addressed. Digital inclusion is at the heart of the Digital India Programme which envisions

transforming India into a digitally empowered society and knowledge economy with various programmes like BharatNet, Digital Village, Aspirational Districts, MyGov and Kranthi. This gradual Digital Inclusion has proven to be of immense value to us in these uncertain times. We must cooperate to bridge this digital divide through capacity building to create globally secure cyberspace.

India is committed to an open, secure, free, accessible, and stable cyberspace environment, which will become an engine for innovation, economic growth, sustainable development, ensure free flow of information and respect cultural and linguistic diversity. With our transformative technology initiatives in recent years such as IndiaStack, Aadhar and UPI, we have successfully leveraged the tremendous potential of cyber technologies in implementing the SDG agenda and improving governance. As part of its COVID vaccination drive, one of the largest such drives in.

The world has developed Co-WIN – a scalable, inclusive, and open technological platform. The Co-WIN platform can be customised and scaled up for health interventions across the globe. We are working on sharing this platform with partner countries in the interest of health cooperation and their preparedness to meet challenges to health of countries across the world.

Our overarching objective is to harness cyberspace for the growth and empowerment of people, not just of our own country, but for all humanity. Moving forward, India is keen to exchange its experiences with ASEAN toward a safer and more secure global cyberspace for our peoples.

I am glad to note that the agenda for today's meeting comprises some very important issues related to Cyber security including encryption, protecting critical infrastructure, and building resilient connectivity infrastructure. I wish all participants the very best and hope that some insightful suggestions for policymakers from India and ASEAN would be generated through this Dialogue.

C. Remarks of Shri Jayant Khobragade, Indian Ambassador to ASEAN

Good morning and Good Afternoon from Jakarta!

Since the event is taking place on the auspicious day of Eid, let me wish all participants Eid Mubarak.

Let me thank the Observer Research Foundation for organising the Third ASEAN-India Track 1.5 Dialogue on Cyber Issues and for giving me the opportunity to share a perspective from the Indian Mission to ASEAN in Jakarta.

Before assuming the charge of India's Ambassador to ASEAN, I was heading the Passport Seva Programme Division in the Ministry of External Affairs. The programme is one of the best examples of Digital India. I may mention that there have been more than 5000 attempted attacks on the Programme infrastructure every day, of course, not even one of them met with any success. According to India's Computer Emergency Response Team, which is known as CERT-In, in the year 2020 alone there had been 11 lakh, 58 thousand incidents of cybercrime (almost 100,000 incidents per month) which included website intrusion, malware propagation, Malicious code, Phishing, distributed denial of service attacks, website defacements, unauthorised network scanning/probing activities, ransomware attacks, data breach and vulnerable services. India is not an exception; this is happening globally.

The digital sector has been growing at a fast pace even before Covid-19 pandemic hit us, but this pandemic added new dynamism as it gave a boost to virtual communications, data flow, virtual meetings, like today's, and to the increased e-commerce. The economies after becoming digital have been advancing to a higher level of technologies through the use of Artificial intelligence, block chains, Fintech, Internet of Things, cloud computing etc. To continue this momentum uninterrupted, the role of 5G infrastructure, encryption and securing the infrastructure has

become more critical. In this context I must compliment the organisers for rightly choosing to focus on these topics of Encryption, 5G Infrastructure and Securing Critical Infrastructure, as these aspects are relevant in health, education, agriculture, finance, logistics, e-commerce, Science and technology, tourism and a range of other sectors and touch everyone's life as an individual, institutions, industry, and governments.

Let me now try to put this discussion in the framework of ASEAN-India context.

Together, ASEAN and India have more than a billion internet users and are among the world's fastest-growing digital economies. As we get digitally more and more connected, these challenges cannot be addressed by a country alone.

ASEAN has already done a lot of thinking, which is reflected in various statements, documents, and initiatives: If we look at the ASEAN LEADERS' STATEMENT ON CYBERSECURITY COOPERATION issued in 2018, two aspects get distinctly highlighted:

(i) Importance of sharing approaches.
(ii) Cooperation in Capacity building:

In general, the capacity building has both the aspects of technological upgradations and enhancing human skills including through creating awareness.

When we look at cooperating with ASEAN within the ASEAN structure, we may note the following three structures:

(i) For the Microelectronics & Information Technology sector, the priority areas of cooperation are artificial intelligence, block chain, cloud and edge computing, the Internet of Things, big data processing and analytics, cyber security, embedded systems and sensors, robotics and automation, telecommunications, and microelectronics.

(ii) Cyber security issues related to defence and military establishments fall under the purview of the ASEAN defence leadership. Priority areas of cooperation under this sector aim to: (i) enhance awareness on cyber security challenges; (ii) leverage capabilities among ASEAN Member States and its external partners; (iii) develop cooperative mechanisms and solutions in a coordinated manner.

(i) Under the oversight of the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the Senior Officials Meeting on Transnational Crime (SOMTC) covers the issue of cybercrime cooperation in the SOMTC Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime. The Work Programme focuses on several areas, such as exchange of information and knowledge, including on relevant laws and regulations of the ASEAN Member States; public awareness building; capacity building activities for law enforcement officials, particularly on cybercrime forensic capabilities; and promotion of cooperation with external partners.

ASEAN has already done work in fostering greater regional cybersecurity cooperation and capacity building, including law enforcement training on cybersecurity and cybercrimes through efforts such as the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), AMCC, ASEAN Cyber Capacity Programme, ASEAN Regional Forum (ARF) Inter-Sessional Meeting on ICT Security and the ADMM-Plus Experts' Working Group Meeting on Cyber Security. ASEAN also cooperates with their Dialogue Partners including India through these ASEAN led structures.

When we look at the ASEAN India cooperation, I must mention that the Plan of Action 2021-25 approved by the Foreign Ministers of ASEAN and India and noted by the leaders identifies cooperation in the IT Sector as one of the areas:

Information and Communication Technology (ICT) 41. Promote further ICT cooperation through relevant mechanisms, including capacity building and knowledge sharing, in areas such as e-commerce, Artificial Intelligence, Fourth Industrial Revolution, Internet of Things (IoT) & 5G, ICT in Disaster Management, Creating smart societies through ICT, Cyber Forensics, Next Generation Transmission Technologies, Future Trends in Mobile Communication, Advanced Satellite Communication and Regulatory and Policy issues; Strengthen cooperation, capacity building, and policy coordination on cybersecurity, including in personal data protection and support the implementation of the ASEAN Cybersecurity Cooperation Strategy by engaging relevant ASEAN mechanisms and institutions; Promote sustainable and inclusive economic growth and prosperity through increasing digital trade, entrepreneurship, preparing MSMEs for digital transformation and developing a digital-ready workforce equipped for the Fourth Industrial Revolution

While India is involved in cooperation in the field of cyber security through the ASEAN Defence Ministers Meeting and ASEAN Regional Forum processes; we are also working on these areas under the Transnational Crime Framework and Telecommunication and IT Ministers' Meeting.

ASEAN and India, we already have a structural mechanism for Digital cooperation with ASEAN at the Working Group level, Senior Official Level and Minister Level. The Department of Telecom, Ministry of Electronics and Information Technology is the coordinating agency from India. Currently, we also have annual action plans which are approved by ASEAN-India Digital Ministers Meeting. ASEAN-INDIA ICT WORK PLAN 2021 is under progress. Under ASEAN-India Fund, we have taken up several projects for cooperation in this sector. Currently, Department of Telecom and ASEAN Secretariat have been working on to develop project proposals for a few training courses including on 'Cyber Forensics' and '5G and its Potential Use Cases' among others.

While this is happening within the ASEAN-India structural framework, there are huge opportunities with the individual ASEAN Member States within the bilateral framework. Without going into the details, I would like to add that there is a substantial presence of Indian IT companies in the region. I am quite sure that these companies are actively involved in cyber-security cooperation.

Physical and digital connectivity between India and ASEAN is the priority of the Government of India. The Hon'ble Prime Minister of India has announced a Line of Credit worth USD 1 billion for enhancing both physical and digital connectivity.

To sum up, I would urge the panellists to inter alia focus on:

(i) How can we share our approaches in the areas of Encryption, Trusted and Resilient 5 G Infrastructure, securing Critical Infrastructure through regular interactions, seminars and conferences;

(ii) Identifying capacity building programmes in these areas.

The above two could be done through the institutional set-up of MEITY and under ASEAN-India Fund as mentioned above.

(iii) To identify commercial projects on building secured infrastructure by utilising the Line of Credit offered by Government of India.

I wish the forum a success.

Thank you very much.

D. List of Participants

Akshay Mathur, *former Director of ORF Mumbai, Head of the Geoeconomics Studies Programme, Observer Research Foundation*

Alastair Loh, *Desk Officer, Ministry of Foreign Affairs, Singapore*

Amalina Anuar, *Senior Analyst, Centre for Multilateralism Studies, RSIS*

Anjaneya Gupta, *ADET -2 (Security & East), DGT HQ, Department of Telecommunications, India*

Athena Foo, *Senior Manager (International Cyber Policy), Cyber Security Agency of Singapore*

Avinash Agrawal, *Director (IT), TEC, India*

Azman Iskandar Ariffin, *CIO, Cyber Security Brunei*

Chansambath Bong, *Deputy Director of Centre for Inclusive Digital Economy (CIDE), Asian Vision Institute*

Shashi Jayakumar, *Head of Centre of Excellence for National Security; Executive Coordinator of Future Issues and Technology, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) Singapore*

Farlina Said, *Analyst, Institute of Strategic and International Studies (ISIS) Malaysia*

Gen Macalinao, *Planning Officer III, Cybersecurity Bureau, DICT*

Gunjan Chawla, *Programme Manager, Technology and National Security, Centre for Communication Governance at National Law University Delhi*

Hajar Roslan, *Majlis Keselamatan Negara (National Security Council), Malaysia*

Ida Frida Abu, BruCERT, Brunei

Intan Safinas, *Assistant Director (International Cyber Policy), Cyber Security Agency of Singapore*

Irma Fitriani, *Junior Analyst, Indonesia National Cyber and Crypto Agency (BSSN)*

Izuana Ayob, *Awareness Officer, Cyber Security Brunei*

Shri Jayant Khobragade, *Ambassador of India to ASEAN*

Jhalak Kakkar, *Executive Director, Centre for Communication Governance at National Law University Delhi*

Josey George, *General Manager - Strategy, M&A - Cybersecurity & Risk Services, Wipro*

Jitendtra Joshi, *Director (T-Cert), Department of Telecommunications*

Kanika Gambhir, *ADET(SA), Department of Telecommunications*

Keolaka Soisaya, *Director of External Relations Division, ASEAN Department, Ministry of Foreign Affairs*

KHIM Socheat, *Assistant to Minister, Ministry of Posts and Telecommunication*

Kim Ann, *Deputy Director of Department of ICT Security, Ministry of Post and Telecommunications (MPTC)*

Lim May-Ann, *Director, Fair Tech Institute, Access Partnership*

Lisa Brown, *Department of Foreign Affairs and Trade, Australia*

Lwin Aung, *Junior Engineer 1, Ministry of Transports and Communication, Myanmar*

Mardonia Bani, *Assistant Director, National Cyber Security Agency, Malaysia*

Mark Crister Binag, *Department of Information and Communications Technology*

Napoleon Catilo, Co-founder, Chief Innovation & InfoSec Officer, Pearl Pay

Shri Narendra Nath G, *Joint Secretary, National Security Council Secretariat, India*

Nomi Hafiz Zakiah Hj Pawi, *Security Analyst, Cyber Security Brunei*

Norsalimi Shaleh, *Malaysia*

OU Phannarith, *Director of ICT Security, Ministry of Post and Telecommunications (MPTC)*

Pg Mohd Farid Zulhusni Pg Aziz, *Lead Trainer, Cyber Security Brunei*

Prachi Mishra, *Young Leaders in Technology Policy Fellow, Observer Research Foundation*

Pick Am, *Deputy Director of National Infrastructure and Videoconference Department, Ministry of Posts and Telecommunication*

R. Shakya, *DDG (IR), Department of Telecommunications, India*

Samyak Rai Leekha, *Junior Fellow, Observer Research Foundation*

Satinder Kumar Bhalla, *DDG (Telecom Security & Policy Research), NTIPRIT*

Shamsul Bahri Kamis, *Interim Commissioner, Cyber Security Brunei*

Siriwat Chhem, *Director of Centre of Inclusive Digital Economy, Asian Vision Institute*

Siti Khadijah Binti Hj Ismail, *Security Analyst, Information Technology Protective Security Services (ITPSS Sdn Bhd)*

Sokoudom Ung, Advisor, *Ministry of Post and Telecommunications*

Spark Perreras, *Co-founder & CEO, PearlPay*

Subrata Kumar Mitra, *Vice President - Head of Government & Industry Relations, Ericsson*

Thienxay BOLIBOUN, *Director of Division, Ministry of Technology and Communications, Lao PDR*

Tomy Prihananto, Senior Analyst, Indonesia National Cyber and Crypto Agency (BSSN)

Trisha Ray, *Associate Fellow, Observer Research Foundation*

Wahyudi Djafar, *Executive Director, Institute for Policy Research and Advocacy (ELSAM)*

Win Nyo, *Technician, NCSC, Myanmar*

Yanitha Meena Louis, *Researcher, ISIS Malaysia*

Yoga Mahardika, *Ministry of Foreign Affairs, Indonesia*

Zheng Ying Chong, *Senior Manager (International Cyber Policy), Cyber Security Agency of Singapore*

Endonotes

1 "Statistics", International Telecommunications Union, accessed January 18, 2022, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
"Indian Telecom Services Performance Indicator Report" for the Quarter ending October - December 2020", Telecom Regulatory Authority of India, April 27, 2021, https://www.trai.gov.in%2Fsites%2Fdefault%2Ffiles%2FPR_No.26of2021.pdf.
Google, Temasek Holdings, Bain & Company, "e-Conomy SEA 2019: Swipe up and to the Right: Southeast Asia's $100 Billion Internet Economy" (2019), https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf.

2 "X-Force Threat Intelligence Index 2021", IBM Security.
"X-Force Threat Intelligence Index 2022", IBM Security.

3 "X-Force Threat Intelligence Index 2021", IBM Security (2021), https://www.ibm.com/downloads/cas/M1X3B7QG
"X-Force Threat Intelligence Index 2022", IBM Security (2022), https://www.ibm.com/downloads/cas/ADLMYLAZ

4 "Plan of Action to Implement The ASEAN-India Partnership for Peace, Progress and Shared Prosperity (2021-2025)", ASEAN, March 11, 2021, https://asean.org/asean2020/wp-content/uploads/2021/03/11.-ASEAN-India-POA-2021-2025-Final.pdf.

5 "India-ASEAN Track 1.5 Dialogue on Cyber Issues", *ORF Special Report*, Observer Research Foundation, November 8, 2019, https://www.orfonline.org/wp-content/uploads/2019/11/ASEAN_Report.pdf.

6 *ASEAN Digital Masterplan 2025,* ASEAN (2021), https://asean.org/book/asean-digital-masterplan-2025/.

7 "Malaysia Digital Economy Blueprint", Economic Planning Unit, Prime Minister's Department, Malaysia, https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

8 "India and ASEAN", Lok Sabha Secretariat, No.5/RN/Ref./March/2018, http://164.100.47.193/Refinput/New_Reference_Notes/English/India_and_ASEAN.pdf

9 "India and ASEAN", Lok Sabha Secretariat.

10 "The 1st ASEAN Digital Ministers' Meeting and Related Meetings", ASEAN Secretariat, January 22, 2021, https://asean.org/wp-content/uploads/16-ADOPTED_Joint_Media_Statement_of_the_1st_ADGMIN_cleraed.pdf.

11 "Quick Impact Projects", Mekong Ganga Cooperation, https://mgc.gov.in/qip

[12] "India-ASEAN Digital Work Plan 2022 approved at 2nd ASEAN Digital Ministers (ADGMIN) meeting", Press Information Bureau, Jan 26, 2022, https://pib.gov.in/newsite/PrintRelease.aspx?relid=231114

[13] Damien McGuinness, "How a cyber-attack transformed Estonia", *BBC*, April 27, 2017, https://www.bbc.com/news/39655415

[14] The GCSC defines the public core to include packet routing and forwarding, naming, and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media.
"Global Commission Proposes Definition of the Public Core of the Internet", Global Commission on the Stability of Cyberspace, July 5, 2018, https://cyberstability.org/news/global-commission-proposes-definition-of-the-public-core-of-the-internet/

[15] "India-ASEAN Track 1.5 Dialogue on Cyber Issues", Observer Research Foundation, November 8, 2019.

[16] ITU-T, "Requirements and framework for the support of VPN services in NGN, including the mobile environment", *Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks,* Next Generation Networks – Service aspects: Service capabilities and service architecture, June 2009, https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-Y.2215-200906-I!!PDF-E&type=items

[17] "Section 69 in The Information Technology Act, 2000", Indian Kanoon, https://indiankanoon.org/doc/1439440/.

[18] "Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021", Ministry of Electronics and Information Technology, http://egazette.nic.in/WriteReadData/2021/225464.pdf.

[19] Eugene Tan, "Cyber Norms and International Law in ASEAN" in Gisela Elsner and Aishwarya Natarajan eds, *Regulating the Cyberspace Perspectives from Asia* (Konrad-Adenauer-Stiftung Singapore: 2020).

[20] Trisha Ray, "Report of the Second India-ASEAN Track 1.5 Dialogue on cyber issues".

[21] "PUBLIC REPORT OF THE COMMITTEE OF INQUIRY INTO THE CYBER ATTACK ON SINGAPORE HEALTH SERVICES PRIVATE LIMITED'S PATIENT DATABASE ON OR AROUND 27 JUNE 2018", Singapore Ministry of Communications and Information, January 10, 2019,
https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

[22] "310000 Cards from 1136 BINS of South East Asian Banks actively available for sale in Darkweb", Technisanct, February 18, 2020, https://www.technisanct.com/press-release.php

[23] "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions", Recorded Future, February 28, 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector/.

Press Trust of India, "Highways Ministry asks NHAI, automakers to tighten IT security after cyber attack threats", *Tribune India,* March 21, 2021, https://www.tribuneindia.com/news/nation/highways-ministry-asks-nhai-automakers-to-tighten-it-security-after-cyber-attack-threats-228534.

[24] "The Global Economic Impact of 5G", PwC, 2021, https://www.pwc.com/gx/en/tmt/5g/global-economic-impact-5g.pdf.

[25] "The 5G Economy: How 5G will contribute to the global economy", IHS Markit, November 2019, https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf.

[26] The Big Inversion: How 5G+ technologies will create new values for industry in a post-COVID world", Bell Labs Consulting, January 2021, https://d1p0gxnqcu0lvz.cloudfront.net/documents/Big_Inversion_whitepaper_Bell_Labs_Consulting_2021.pdf.

[27] Nikhila Natarajan, Trisha Ray, Michael Depp, "Indo-Pacific 5G Survey: Connections and Conflict", ORF Special Report, April 14, 2021, https://www.orfonline.org/wp-content/uploads/2021/04/Indo-Pacific-Survey.pdf.

[28] Andreas Kuehn and Trisha Ray, *This Connection is Secure: A 5G Risk and Resilience Framework for the Quad* (National Security College, ANU: September 2021), https://nsc.crawford.anu.edu.au/publication/19370/connection-secure-5g-risk-and-resilience-framework-quad?

[29] "Circulars: Security", *Department of Telecommunications*. https://dot.gov.in/circular-and-notifications/2688.

[30] File No. 20-1236/2021-AS-1, Ministry of Communication, Department of Telecommunications, Access Services Wing, March 30, 2021, https://dot.gov.in/sites/default/files/2021%2003%2031%20UL%20Proc%20AS-I.pdf?download=1.

[31] "CyberSecurity Malaysia, Celcom and Huawei kickstarts installation of 5G test lab", The Malaysian Reserve, October 18, 2021, https://themalaysianreserve.com/2021/10/18/cybersecurity-malaysia-celcom-and-huawei-kickstarts-installation-of-5g-test-lab/.

[32] Comments at the Third ASEAN-India Track 1.5 on Cyber Issues, October 20, 2021.

"Information Sharing and Analysis Center", https://www.isacindia.org

[33] "Inside the Race to Fix a Potentially Disastrous Software Flaw", Bloomberg, December 14, 2021, https://www.bloomberg.com/news/articles/2021-12-13/how-apache-raced-to-fix-a-potentially-disastrous-software-flaw

[34] Jonathan Greig, "Chinese regulators suspend Alibaba Cloud over failure to report Log4j vulnerability", ZDNet, December 22, 2021, https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/

[35] "APT & CyberCriminal Campaign Collection", GitHub, https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections

[36] "Central body accountable for nation's cyber security missing", Economic Times, October 26, 2021, https://economictimes.indiatimes.com/news/defence/central-body-accountable-for-nations-cyber-security-missing-ncsc-pant/articleshow/87285059.cms

[37] "CyberDrills", ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx.

APCERT Annual Report, 2020, https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf

[38] "16th Iteration Of ASEAN CERT Incident Drill Tests CERTs' Responsiveness Towards Supply Chain Attacks", Cyber Security Agency of Singapore, October 11, 2021, https://www.csa.gov.sg/News/News-Articles/csa-hosts-16th-iteration-of-asean-cert-incident-drill.

ABOUT THE AUTHOR

Trisha Ray is an Associate Fellow at ORF's Centre for Security, Strategy and Technology.

Ideas • Forums • Leadership • Impact

Observer Research Foundation
20, Rouse Avenue Institutional Area
New Delhi - 110 002, INDIA
+91-11-35332000 Fax: +91-11-35332005
contactus@orfonline.org
www.orfonline.org