cyber
ASEAN

Advancing Cyber Resiliency and Capacity in Southeast Asia

Mark Bryan Manantan, editor

PACIFIC FORUM
INTERNATIONAL

Based in Honolulu, Pacific Forum International (Pacific Forum) is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, Pacific Forum collaborates with a broad network of research institutes around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region. The Forum's programs encompass current and emerging political, security, economic, and technology policy issues, and work to help stimulate cooperative policies through rigorous research, analyses, and dialogue.

About the Editor

Mark Bryan Manantan is the Director of Cybersecurity and Critical Technologies at the Pacific Forum. At the Forum he leads the Cyber ASEAN capacity-building initiative and the US Technology and Security partnerships with Japan, Australia, South Korea, and Taiwan.

Acknowledgments

Pacific Forum is grateful to all stakeholders who shared their time and expertise during the country consultations and virtual expert meetings throughout this project.

Our sincere appreciation to Jesslyn Cheong, Jane Deita, Fitri Bintang Timur, Farlina Said, Genalyn Macalinao, Nguyễn Việt Lâm, Ph.D., Đỗ Hoàng, Adrian Glova, Mabda Haerunnisa Fajrilla Sidiq, Lesley Manantan, Elina Noor, Francesca Spidalieri, Koichiro Komiyama, Klée Aiken, Scott Flower, Ph.D., David Sandell, Aldrin Pelicano, Brooke Mizuno, Georgette Almeida, Megan Tanaka, Crystal Pryor, Ph.D., David Santoro, Ph.D., and Carl Baker.

We would also like to acknowledge Audrey Tey, Brandt Mabuni, Sach Nguyen, Shwe Yee Oo, Ginger Link, Hanah Park, Munique Tan, Chelsea Patrick, Jamie Lee,

Vanice Rodriguez, Regan Lee, Sholto Byrnes, Alex Fry, Rachel Hancock, Haris Amiel, Ana Costa, and Shanna Khayat for supporting the project's implementation and publication efforts.

Cyber ASEAN is supported by the Australian Government and implemented by the Pacific Forum International.

Australian Government

This publication has been funded by the Australian Government through the Department of Foreign Affairs and Trade. The views expressed in this publication are the author's alone and are not necessarily the views of the Australian Government.

Pacific Forum International

Web: www.cyberasean.pacforum.org
Facebook: Pacific Forum
Twitter: @PacificForum
Instagram: @pacforum
Podcast: Indo-Pacific Current
Email: pacificforum@pacforum.org

Foreword

Aloha!

With the rapidly evolving regional security environment and technological advancements of many countries in the Indo-Pacific, the Pacific Forum seeks to bring clarity to these emerging dynamics. As a testament to this, we launched the Cybersecurity and Critical Technologies program in 2022, led by its inaugural director, Mark Bryan Manantan.

Cyber ASEAN is a landmark initiative that seeks to elevate our engagement in the region as we move toward all things digital. It exemplifies the Pacific Forum's capacity for providing in-depth analysis of, and proposing solutions to, key strategic and security issues facing Southeast Asia specifically, and the Indo-Pacific more generally. Although cyber and critical tech may appear futuristic, Cyber ASEAN's foundation rests on the Forum's long history of engaging the region, especially Southeast Asia, in other domains such as maritime, nonproliferation, counterterrorism, and regional security architecture.

Not only do we feel that our geographic position in Hawaii affords a fantastic milieu, but also a unique vantage point to engage the region on new and cutting-edge issues. We sit at the intersection of East and West. The representation and participation of experts, practitioners, and other regional stakeholders illustrate the Pacific Forum's convening power and footprint in the region.

Kicking off the Cyber ASEAN project was not easy. Behind the scenes, Director Manantan encountered various challenges, including having to shift some project activities from virtual to hybrid. A lot of sweat also went into building a great team to make this project a success, and we are proud of the project's outcomes.

As the Cyber ASEAN project enters a new phase with the completion of the framework and the release of this publication, I commend Director Manantan, the expert advisors, and the country's scholars and researchers who helped ensure that the analysis and recommendations advance the region's cyber resiliency and capacity. More than just another cyber capacity-building project, the Cyber ASEAN

Framework adopts a collaborative and forward-leaning approach that embraces international best practices and is grounded in local perspectives, which makes it unique.

On behalf of the Pacific Forum, I invite you to immerse yourself in this publication to grasp Southeast Asia's first homegrown cyber-capacity assessment framework, which highlights the region's complex cybersecurity challenges, as well as its innovative, entrepreneurial, and inclusive approaches. We thank Australia's Department of Foreign Affairs and Trade for its support of this program.

Mahalo,

David Santoro, Ph.D.
President and CEO
Pacific Forum International

About the Authors

Mark Bryan Manantan is the Director of Cybersecurity and Critical Technologies at the Pacific Forum.

Mabda Haerunnisa Fajrilla Sidiq is a researcher at the Habibie Center in Jakarta, Indonesia.

Lesley Manantan is an independent data scientist and project manager.

Adrian Glova is an Assistant Professor at the School of Statistics, University of the Philippines.

Fitri Bintang Timur is the Cybersecurity Project Lead and Research Consultant at the Centre for Strategic and International Studies (CSIS) in Jakarta, Indonesia.

Farlina Said is a Senior Analyst in the Foreign Policy and Security Studies Program of the Institute of Strategic and International Studies (ISIS) Malaysia.

Genalyn Macalinao is the Lead of Critical Information Infrastructure Protection, CIECSD - Cybersecurity Bureau, Department of Information and Communications Technology, Philippines.

Nguyễn Việt Lâm, Ph.D. is a Visiting Lecturer at the Diplomatic Academy of Viet Nam.

Đỗ Hoàng is a research officer at the East Sea Institute, Diplomatic Academy of Viet Nam.

Contents

PART II_ APPLICATION OF CYBER ASEAN

CONCLUSION

Abbreviations

3C	Consultative, collaborative, and community-building
ACCP	ASEAN Cyber Capacity Programme
ADDM-Plus	ASEAN Defence Ministers' Meeting Plus
ADM	ASEAN Digital Masterplan
ADGMIN	ASEAN Digital Ministers Meeting
ADGSOM	ASEAN Digital Seniors Officials' Meeting
AFP-CERT	Armed Forces of the Philippines Computer Emergency Response Team
AI	Artificial Intelligence
AMCC	ASEAN Ministerial Conference on Cybersecurity
AMMTC	ASEAN Ministerial Meeting on Transnational Crime
AMS	ASEAN Member States
ANSAC	ASEAN Network Security Action Council
APAC	Asia Pacific
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ARF	ASEAN Regional Forum
ARMA	Autoregressive Moving Average
ASCCE	ASEAN-Singapore Cybersecurity Centre of Excellence
ASEAN	Association of Southeast Asian Nations
ASEAN CERT	ASEAN Regional Computer and Emergency Response Team
ASEAN CRISP	ASEAN Cybersecurity Resilience and Information Sharing Platform
ASEAN Cyber-CC	ASEAN Cybersecurity Coordinating Committee
ASEAN TELMIN	ASEAN Telecommunications and Information Technology Ministers Meeting
ASCN	ASEAN Smart Cities Network

ASTNET	ASEAN Science & Technology Network
ATRC	ASEAN Telecommunications Regulators' Council
BPO	Business Process Outsourcing
BSP	Bangko Sentral ng Pilipinas
BSSN	National Cyber and Crypto Agency
CBM	Confidence Building Measures
CCID	Commercial Crime Investigation Department
CERT	Computer Emergency Response Team
CERT-PH	The Philippine National Computer Emergency Response Team
COA	Commission on Audit
CII	Critical Information Infrastructures/Critical Infostructures
CIIP	Critical Information Infrastructure Protection
CIS	Cybersecurity Information Sharing
CISO	Chief Information Security Officer
CNII	Critical National Information Infrastructures
CREST	Council for Registered Ethical Security Testers
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DA	Department of Agriculture
DC	Department Circular
DFA	Department of Foreign Affairs
DICT	Department of Information and Communications Technology
DND	Department of National Defense
DPNS	Draft Philippine National Standard
ECM	Error Correction Mode
EU	European Union

FDIs	Foreign Direct Investments
FIRST	Forum of Incident Response and Security Teams
FPT	Financing and Promoting Technology
G2G	Government-to-Government
G2I	Government-to-Industry
GAD	Gender and Development
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
Gen AI	Generative Artificial Intelligence
GFCE	Global Forum on Cyber Expertise
GMV	Gross Merchandise Value
GVA	Gross Value Added
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IoT	The Internet of Things
IP	Internet Protocol
IRR	Implementing Rules and Regulations
ISM	Inter-Sessional Meeting
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
IT-ISAC	Information Technology-Information Sharing and Analysis Center
ITE	Informasi dan Transaksi Elektronik
ITU	International Telecommunication Union
JTC	Joint Technical Committee
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MC	Memorandum Circular

MCIT	Ministry of Communication and Information Technology
MCMC	Malaysia Communications and Multimedia Commission
MDEC	Malaysia Digital Economy Corporation
MIC	Ministry of Information and Communications
MOST	Ministry of Science and Technology
MOSTI	Malaysian Ministry of Science, Technology, and Innovation
MSMEs	Micro, Small, and Medium Enterprises
MyCERT	Malaysia's Computer Emergency Response Team
NACSA	National Cyber Security Agency
NC4	National Cyber Coordination and Command Centre
NCERT	Philippine National CERT
NCSP	National Cyber Security Policy
NISER	National ICT Security and Emergency Response Center
NIST	National Institute of Standards and Technology
NPC	National Privacy Commission
NSS	National Standardization Strategy
PACF	Partial Autocorrelation Function
PCED	Point of Contact Experts Directory
PDP	Personal Data Protection
PDPA	Philippines Data Privacy Act
PDPD	Personal Data Protection Department
PPP	Public-Private Partnership
PPPP	Public-Private-People Partnership
PNS	Philippine National Standard
SC	Sub-committees

SDO	Standards Development Organizations
SICW	Singapore International Cyber Week
SKKNI	Standar Kompetensi Kerja Nasional Indonesia
SME	Small and Medium Enterprises
SNI	Indonesian National Standard
SOMTCWG CC	Senior Officials Meeting on Transnational Crime Working Group on Cybercrime
STAMEQ	Directorate for Standards, Metrology and Quality
STEM	Science, Technology, Engineering, and Mathematics
TC	Technical Committee
TELMIN	ASEAN Telecommunications and Information Technology Ministers Meeting
TLP	Traffic Light Protocol
UN	United Nations
UN GA	United Nations General Assembly
UN GGE	United Nations Group of Government Experts
UN OEWG	United Nations Open-Ended Working Group
VNCERT	Viet Nam's Computer Emergency Response Team
WTO	World Trade Organization

Executive Summary

Southeast Asia's digital decade has begun. However, seizing its full potential in the emerging data-driven economy requires confronting head-on fundamental challenges in cybersecurity: Internet penetration is high, but digital inequity is growing; mobile connections are skyrocketing, yet digital literacy to combat cybercrime, disinformation, and misinformation is plummeting. Most importantly, cyberattacks are rising, but trust-building among key stakeholders remains stagnant, or worse, declining. If these issues are not fully addressed, the region's digital ambitions oriented around ASEAN's inclusive community-building agenda are likely to be aspirational rather than attainable.

To harmonize and elevate Southeast Asia's cyber resiliency and capacity, this project offers *Cyber ASEAN*, the region's proposed homegrown cyber-capacity assessment framework built around the key dimensions of the ASEAN Cybersecurity Cooperation Strategy 2021-2025. The Cyber ASEAN Framework is composed of four pillars: *international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion.* The framework's application aims to provide policy recommendations that are critical to the implementation of the current ASEAN Cybersecurity Cooperation Strategy and its future iterations.

The Cyber ASEAN Framework stands out among existing cyber-capacity assessment frameworks firstly because it is indigenously designed for Southeast Asia by Southeast Asians. Its purpose and significance are driven by three underlying principles: local context and ownership, agency and autonomy, and public-private-people partnerships. Put simply, Cyber ASEAN contends that if cyber capacity-building frameworks and initiatives are grounded, informed, and shaped by the local perspectives of the target stakeholders from the onset of its incubation all the way to operationalization, then Southeast Asia can adopt a more proactive, context-specific, and inclusive approach to raising cyber capacity and resiliency at the sectoral, national, and regional levels.

Secondly, it adopts a participatory-design approach called 3C—consultative, collaborative, and community-building. The Cyber ASEAN Framework is the outcome of four multisectoral consultations among its pilot countries in Southeast Asia: Indonesia, Malaysia, the Philippines, and Viet Nam. The four countries are illustrative test cases that can provide comprehensive insights regarding the framework's application, given their varying digital economic maturity, government systems, and demographics. The local consultations brought together cybersecurity experts, researchers, economists, policymakers, and technologists from the four countries. Three virtual regional meetings complemented the country consultations, serving as feedback mechanisms to ensure that the Cyber ASEAN Framework remains attuned to international best practices. Such iterative processes helped to develop and refine Cyber ASEAN's relevance and practical utility within the context of the intended users.

Finally, because of its 3C approach, the Cyber ASEAN Framework is tailored to the distinct contexts and priorities of the four countries, thereby ensuring a degree of local buy-in and ownership. This makes the framework a practical and easy-to-use policy and technical tool that can assist policymakers, industry practitioners, academic experts and researchers, and civil society advocates. Using the four pillars of the framework, stakeholders can better understand and operationalize pragmatic approaches to cybersecurity, and, in the process, advance and achieve the ASEAN community's vision for cybersecurity and resiliency.

Throughout Cyber ASEAN's conception and implementation, conducted from 2022 to 2023, several critical findings emerged:

1. ASEAN's Evolving Cybersecurity Approaches

Cybersecurity has become a cross-sectoral issue in Southeast Asia. Initially skewed toward the digital economy, cybersecurity now cuts across ASEAN's three community pillars: political-security, economic, and social-cultural. The release of various strategic frameworks and roadmaps like the ASEAN Cybersecurity Cooperation Strategy 2021-2025, alongside the establishment of new technical and policy working groups oriented around the digital economy, cyber defense, and security, attest to the region's evolving multidimensional approach to cybersecurity. Due to the increasing geopolitical competition between the two great powers,

Southeast Asia is increasingly under pressure to exercise greater agency to maintain its autonomy. The current strategic reordering, combined with the prevailing mood for decoupling or de-risking, are putting more pressure on Southeast Asia to outline its normative vision in the cyber realm supported by practical interventions. After the endorsement of the 11 UN cyber norms on responsible state behavior in cyberspace, the region is gradually moving toward more pragmatic approaches to minimize the risks and mitigate the impact of cyber incidents, particularly around the peaceful use of Information and Communications Technology. Notable progress can be observed in the adoption and promotion of international technical standards, as well as initiatives geared toward information-sharing and incident or threat management through the establishment of the ASEAN-Computer Emergency Response Team (ASEAN-CERT).

2. Harmonizing Standards

Collectively, ASEAN member states (AMS) still lack a coherent strategy in negotiating their position in relevant regional and international forums like the UN Group of Government Experts (UN GGE) and the Open-Ended Working Group (UN OEWG) processes, as well as Global Standards Development Organizations (SDOs). AMS should improve policy coordination to harmonize standards and frameworks to effectively advance the region's collective interest in such forums.

The ASEAN Cybersecurity Coordinating Community can help policymakers take stock of cybersecurity discussions across various sectoral bodies to improve coordination. However, such a top-down approach should be best complemented by track 1.5 or track 2 dialogues built around multistakeholder consensus and mustering public support to make the process more inclusive. If executed in this way, Southeast Asia can achieve a feasible, middle-path approach to cybersecurity standards: one that is aligned to international standards and best practices, yet context-specific. Along with each country's earnest efforts to pour more investments into digital infrastructure and human resources, the middle-path approach can pave the way for Southeast Asia to become a rule-maker rather than a rule-taker in standard settings, thereby improving its capacity to influence various technical and policy discussions.

3. Adopt then Localize

Across Indonesia, Malaysia, the Philippines, and Viet Nam, international technical standards like the ISO 27001 and ISO 27002 are well-recognized, especially among large companies, as critical benchmarks to promote best practices in cybersecurity. Small and medium enterprises (SMEs) prefer the US National Institute of Standards and Technology (NIST) cybersecurity framework due to its flexibility and cost-effectiveness. However, the multistakeholder consultations revealed that wholesale adoption of such internationally known standards and frameworks is not the preferred choice.

Depending on the size and resources available, most organizations opt for "adopt then localize." Standards-setting bodies in each country adhere to flexible and risk-based approaches in promoting the adoption of cybersecurity standards to accommodate domestic needs and priorities. Public consultations are widely employed to obtain feedback or comments to ensure that cybersecurity standards, policies, and frameworks are fit for purpose before their intended rollout.

Stakeholders emphasized that cybersecurity standards should be outcome rather than implementation-oriented to avoid being too prescriptive. Such an approach can help Southeast Asia strike a healthy balance in the adoption of international standards according to the domestic context. Conversely, experts also noted that the standards-setting processes should be agile and iterative due to the ever-changing nature of emerging and critical technologies. Adhering to highly rigid or inflexible processes could render standards obsolete in the long run.

4. Incentives and Transparency

Enhancing information-sharing remains an uphill climb in Southeast Asia. Issues like regulatory non-compliance, cost considerations, exposure or leakage of sensitive data or intellectual property, and reputational damage prevent the public and private sectors from sharing or disclosing information on cyber incidents in a timely fashion. Stakeholders also admitted that the failure to mitigate cyber incidents is often seen as shameful, which deters organizations from sharing more information publicly.

Across the board, ineffective information-sharing is driven by the prevailing trust deficit, which leads to weak enforcement of rules and regulations. Even though there is a strong appetite to collaborate on information-sharing and incident management—due to the borderless nature of cybersecurity risks, and the obvious interdependences among industries—the lack of government incentives for the private sector often undermines the effectiveness of public-private partnerships. Industry representatives agreed that partnerships must provide equal benefits to all parties involved, either through financial means or the reciprocal exchange of information. To be fair, government policymakers recognize the role of incentives, however, resource constraints and shifting political bandwidth at the government level largely undercut their ability to invest in positive inducements consistently.

5. Building Mutual Trust

Overcoming the trust deficit is considered critical to achieving effective information-sharing and incident response systems across Indonesia, Malaysia, the Philippines, and Viet Nam. To this end, the partnership-building dynamics within the community of Computer Emergency Response Teams (CERTs) or the Computer Security and Incident Response Teams (CSIRTs) is an interesting case study that offers hope in narrowing the trust gap. Despite existing political and diplomatic disagreements between their governments, CERTs/CSIRTs avoid politicizing cyberattacks and instead focus on the bigger picture of addressing cybersecurity risks and threats that have the potential to spiral into bigger crises. Installing trust among CERTs/CSIRTS relies on a combination of formal and informal channels that include conferences, training activities, partnerships, and social gatherings. What makes trust-building possible is the people-to-people ties that transcend professional and personal settings. In such collaborative and collegial environments, the CERTs/CSIRTs community has developed trust and reinforces it over time.

Stakeholders noted that the close people-to-people ties among CERT/CSIRT organizations are critical in activating anticipatory and remediation strategies and interventions. The mutual trust that is established facilitates timely information-sharing, especially during high-level cyber incidents. Because trust has been established, it becomes feasible among public and private CERTs/CSIRTs to move beyond incident management to threat management or hunting. The latter

is perceived to be more proactive than the former and is executed through joint interactive drills or routine tabletop exercises. Threat-hunting or management synthesizes information available from enterprises, service providers, regulators, and CERTs. The combined information produces a higher definition of the cyber-threat landscape that leads to early notifications of potential cyberattacks.

6. Emerging Trends and Threats

To combat the increasing rate, volume, and sophistication of cyber activities, cybersecurity professionals are employing artificial intelligence (AI), big data, and cryptography. As much as generative AI can be weaponized to conduct more sophisticated cyber campaigns, the same logic can be applied to fortifying cyber defenses. The integration of emerging technologies with existing cybersecurity platforms and tools has allowed governments, law enforcement agencies, the private sector, and academia to collaborate effectively in setting up early warning signs and sharing actionable information to combat and better detect and prosecute malicious activities like ransomware. However, on the flip side, AI-enabled technologies have paved the way for state surveillance that consequently perpetuates digital authoritarianism.

As most users rapidly shift to online platforms for financial transactions, cybercriminal groups are employing social engineering tactics and spear-phishing emails to acquire sensitive and personal information. The declining digital literacy in the region has also exposed women, girls, the elderly, and young people in particular to cyber-enabled crimes like online scams, financial fraud, and harassment. Disinformation and misinformation are also major concerns, particularly with the rise of deepfakes and bots that further inflame existing social tensions between groups. Malicious “fake news” has also incited violence and riots and damaged the credibility of electoral processes.

7. Inclusive Capacity-building: Public-Private-People-Partnership

Integrating the “people” aspect—such as including underrepresented communities

like women and girls, persons with disabilities, the elderly, and minority groups—in public-private partnerships can tangibly put inclusion front and center in cyber capacity-building initiatives. In adopting Public-Private-People-Partnerships, policymakers can avoid the common pitfalls of highlighting inclusion only as an afterthought in such arrangements.

Stakeholders across Indonesia, Malaysia, the Philippines, and Viet Nam do not consider inclusivity solely as a numbers game or a band-aid solution to providing digital public goods or undertaking reskilling or upskilling opportunities. While these interventions offer relief in the short-term, policymakers, industry leaders, and academic researchers stressed the importance of a forward-leaning approach to capacity-building given the evolving nature of technology. Learning opportunities and outcomes from basic to higher education that heavily emphasize Science, Technology, Engineering, and Mathematics should be tempered with core competencies from the Arts and Humanities. In doing so, academic institutions can produce well-rounded individuals capable of tackling complex tasks in the digital age.

8. Human-centric Approach to Cybersecurity

Shifting the focus away from technology back to humans and societies can revitalize cybersecurity policymaking. This will demand moving beyond the technocratic impulses of digital transformation agendas toward a more community-driven approach to technology policy. In practice, this approach demands a proactive process of iterative co-creation and consultation among stakeholders.

During the four country consultations, guiding principles like “accessibility-by-design” or “human dignity-by-design” were suggested to ensure that the knowledge of all possible users, especially underrepresented communities, is incorporated throughout the stage of policy or tech development. For instance, the formulation of educational or training curriculums or the design of software and hardware should involve the users at the very start of the process to make them as universally accessible and inclusive as possible.

Guide to this Publication

The Cyber ASEAN publication is divided into two interlinked sections: **Foundation** and **Application**. As a testament to the project's commitment to emphasizing Southeast Asia's local perspectives, this publication brought together the region's foremost cybersecurity experts, researchers, economists, policymakers, and technologists from Indonesia, Malaysia, the Philippines, and Viet Nam.

Foregrounding the publication, **Part I: Foundation** establishes the main impetuses of the Cyber ASEAN Framework as Southeast Asia's homegrown cyber assessment framework. Essentially, it tackles the "so what" of Cyber ASEAN, providing compelling arguments for why policymakers should use the framework as a fundamental toolkit for cyber policy and strategy formulation.

Setting the context for the entire publication, the introductory chapter explores the underlying assumptions of Cyber ASEAN, particularly the vital importance of reframing the conduct of cyber capacity-building in the region. It expounds on the origins of the Cyber ASEAN Framework's foundational pillars: *international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion*. To further highlight Cyber ASEAN's unique contribution and fulfill its inherent aim of persuasive cyber policymaking, three analytical chapters examine the *strategic* and *economic* imperatives of cybersecurity cooperation and capacity-building in the region.

In unpacking the strategic imperatives of cybersecurity, two chapters are presented. The first chapter maps Southeast Asia's evolving approach to cybersecurity from the purely economic to the more cross-sectoral. By tracing the regional development of cybersecurity cooperation, the chapter locates the tangible contribution of the Cyber ASEAN Framework in complementing and even remedying ASEAN's shortcomings, especially in the implementation of the ASEAN Cybersecurity Cooperation Strategy 2021-2025. The second chapter discusses the strategic dimensions of cybersecurity in Southeast Asia amid the region's changing geopolitical environment. It tackles the nuances in Southeast Asia's response to cyber incidents, as well as the implications of the prevailing trust deficit and lagging digital capacity to the region's cybersecurity posture.

Rounding up the foundational chapter is an analysis of the economic benefits of cybersecurity standards. Through a regional and cross-country comparison, the chapter applies economic regression analysis among Indonesia, Malaysia, Viet

Nam, and the Philippines to quantify the added value of adopting international technical standards and cybersecurity frameworks to gross domestic product and foreign direct investments.

Moving to **Part II: Application**, the four subsequent chapters operationalize the Cyber ASEAN Framework, particularly its four pillars across Indonesia, Malaysia, the Philippines, and Viet Nam. The main findings of the multistakeholder country consultations held in Jakarta, Kuala Lumpur, Manila, and Hanoi are discussed in detail in each chapter.

The concluding chapter summarizes the overall outcome of the project and reveals the feedback on Cyber ASEAN's pilot run among the key stakeholders across the four countries. It revisits and emphasizes the distinct contribution of the Cyber ASEAN Framework as well as prospects for future engagements.

PART I_

FOUNDATION OF CYBER ASEAN

Mark Bryan Manantan

Reimagining Cyber Capacity-Building in Southeast Asia: The Cyber ASEAN Framework

Southeast Asia is on the precipice of its digital decade. Emerging resilient from the pandemic, the region continues to weather macroeconomic headwinds, demonstrating a slow yet steady economic recovery. If the current trendlines persist, experts project that Southeast Asia could exceed US$300 billion in Gross Merchandise Value (GMV) by 2025, and hopefully hit US$1 trillion by 2030.[1] But Southeast Asia's digital outlook could be side-tracked because of mounting cybersecurity challenges.

Getting cybersecurity right has been a top priority for the Association of Southeast Asian Nations (ASEAN) following the release of key strategic documents like the

ASEAN Cybersecurity Cooperation Strategy 2021-2025 and the ASEAN Digital Masterplan (ADM) 2025. Initiatives to build capacity and resiliency across the region also abound. Among ASEAN Member States (AMS), Singapore is the obvious frontrunner following its establishment of the ASEAN-Singapore Centre for Cybersecurity Excellence. And of course, ASEAN dialogue partners are also chipping in: Australia, Japan, China, and the United States are engaged in various cyber-capacity engagements throughout the region.

Despite initial progress, practical outcomes remain incommensurate with the speedy evolution of cybersecurity risks and threats in terms of scale, and sophistication. With the increasing integration of artificial intelligence (AI) and cybersecurity tools and platforms, underpinned by the digital transformation agenda, the playing field has shifted. Add to this the persistent digital inequity that undermines the advancement of an inclusive development agenda. Therefore, the cybersecurity community finds itself at a crossroads to reflect and reassess current policy approaches.

The reality is that hackers will do what they need to do. Based on Cyber ASEAN's Cyber Threat Tracker—the project's online platform that catalogs cyber activities in Indonesia, Malaysia, the Philippines, and Viet Nam—advanced persistent threat actors continue to mix and match their tools to improve their tactics, techniques, and procedures for strategic and/or economic ends. The onus lies upon government policymakers to devise and reframe policy interventions that are adaptive to the ever-shifting tempo of the cyber threat landscape. Undeniably, cybersecurity is a team sport and should pursue a multistakeholder or whole-of-society approach. Solid cooperation among the private sector, academia, and civil society groups is vital to achieve lasting impact.

However, such goals are easier to state than achieve, particularly in Southeast Asia. Depending on the current government leadership and the relative digital maturity of the country, the political bandwidth and fiscal resources dedicated to cybersecurity vary. Public-private partnerships are vulnerable to competing interests over

national security and corporate profit among governments and the private sector, especially large tech companies. There is a patchwork of cybersecurity regulations, yet enforcement gaps remain deeply problematic due to the lack of trust. An emerging area of concern among civil society groups is the growing phenomenon of state surveillance, which could trump fundamental human rights in the digital age.

At the regional level, cybersecurity is becoming deeply entangled in the geopolitical power play between the US and China, leading to the bifurcation of normative standards in technological development. ASEAN itself is facing tremendous pressure to buttress regional stability and deliver on its promise of economic prosperity. Amid its current bureaucratic challenges, ASEAN is called to act with greater agency as the race to establish the normative foundations for critical technologies like AI is underway. Otherwise, it risks losing its autonomy to external powers—a scenario that would be detrimental to the region's digital prospects.

Positioning Southeast Asia as a proactive rather than a passive actor in the game of evolving cybersecurity risks and threats amid the geostrategic reordering is only the initial step. To win, let alone sustain, the long battle toward achieving cybersecurity and resilience will demand greater multistakeholder participation. Combining proactive, community-driven, and tailored approaches is thus integral to unlocking Southeast Asia's digital ambitions.

To harmonize and elevate Southeast Asia's cyber resiliency and capacity, this project offers the *Cyber ASEAN Framework*, the region's homegrown cyber-capacity assessment framework built around the key dimensions of the ASEAN Cybersecurity Cooperation Strategy 2021-2025. The framework is composed of four pillars: *international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion* to raise the resiliency of critical national infrastructures through inclusive cyber capacity.

Employing its participatory design approach—consultative, collaborative, and community-building—the Cyber ASEAN Framework is the outcome of the multisectoral consultations in its four pilot countries, Indonesia, Malaysia, the Philippines, and Viet Nam. To complement the local consultations, three virtual regional experts' meetings were also convened. The three-part online roundtables

served as feedback loops to ensure that the Cyber ASEAN Framework is synchronized with international best practices.

Together, the country consultations and virtual experts' meetings were iterative processes designed to improve the Cyber ASEAN Framework and gauge its relevance and practical utility. Both activities help ensure that the Cyber ASEAN Framework is tailored to the distinct context and priorities of the four countries, yet still aligned with international best practices.

This makes the Cyber ASEAN Framework a practical and easy-to-use tool that can assist policymakers, industry practitioners, academic researchers, and civil society advocates. Using the four pillars of the framework, stakeholders can better understand and operationalize pragmatic approaches to cybersecurity, and in the process, advance and achieve the ASEAN community's vision of cybersecurity and resiliency.

Mind the Gap in Cyber Capacity-Building

There is still no standard definition for cyber capacity-building. Viewing cyber capacity through practice rather than an academic lens, the Global Forum on Cyber Expertise (GFCE), a global and multistakeholder network of cybersecurity experts and practitioners on cyber capacity-building, defines it as "people from different countries helping each other through the sharing of skills, knowledge, and resources in a collaborative, global effort to make us all safer in a digital world." For this project, we define cyber capacity as the deployment of cybersecurity assessment frameworks, and/or the provision of technical training, infrastructure investments, and policy resources aimed at providing actionable policy recommendations, developing skills and know-how, and achieving cyber resiliency and capacity.

In 2021, the GFCE released a study, "Global Overview of Assessment Tools," which cataloged existing cyber-capacity assessment frameworks, models, and indices.[2] The report raised awareness of existing tools and approaches to address prevailing needs, offering a snapshot of the leading voices setting the tone in the current cyber-capacity landscape—the majority of which were originally from North America or Europe. This concentration of power in the hands of institutions mostly

from the Global North has profound implications in shaping the contours of cyber capacity around the world, including Southeast Asia. Of course, many emerging economies stand to benefit from the resources and expertise afforded by willing and technologically advanced countries. However, the reality is, who sets the agenda matters. Cyber-capacity initiatives can inadvertently or advertently impose donor interests among recipient states.[34]

Moving to the implementation of cybersecurity assessment models, several observations emerge. It is often the case that international cybersecurity experts, researchers, and practitioners collaborate with local partners to conduct cybersecurity assessments. However, most of the metrics embedded within the frameworks employed have very little or no prior inputs from the target audience before the assessment.[5] Researchers, consultants, and policymakers will often copy and paste such frameworks with very minor or no consideration at all for the intended users' distinct context.[6]

It is also worth noting that most cyber assessment frameworks are predisposed to ranking countries based on pre-identified variables. Such a tiering approach leads to unsurprising results in which most countries in the Global South lag against their peers in the Global North. One stakeholder interviewed during preliminary research for the project disclosed that less digitally mature countries like Myanmar, Laos, and Cambodia have often shied away from participating in questionnaires that "audit" their cyber capacity due in large part to the pressure they feel about submitting inadequate or zero responses at all. Because such an approach has become the dominant practice, it was observed that over time less digitally mature countries become reluctant, or worse, lose interest in participating.[7]

Finally, there is the question of sustainability. Research outcomes and findings from cyber assessment frameworks bring to the fore the practical question of how to integrate the results into domestic legal frameworks and policies. In some instances, government officials revealed that cybersecurity framework assessments carried out by international experts often become just another academic exercise with very little impact on policymaking due to the lack of ownership and affinity among the intended users.[8]

The Cyber ASEAN Framework

Responding to the major gaps outlined above in cyber policymaking and capacity-building in Southeast Asia, the fundamental purpose and significance of Cyber ASEAN are based on three underlying principles: *local context and ownership, agency and autonomy, and public-private-people partnerships*. Put simply, Cyber ASEAN contends that if cyber capacity-building frameworks and initiatives are grounded, informed, and shaped by the local stakeholder perspectives from incubation to operationalization, then Southeast Asia can adopt a more proactive, context-specific, and inclusive approach to raising cyber capacity and resiliency at the sectoral, national, and regional levels.

To be clear, the project has no intention to disregard and dismiss past and present efforts to raise cyber capacity in Southeast Asia. It recognizes the invaluable contributions of such initiatives to making the region more cyber secure. More so, the lessons and takeaways from such interventions even inspired the incubation of the Cyber ASEAN Framework. However, there is still room to reimagine how cyber-building capacity is conducted in Southeast Asia.

Local Context and Ownership

The project starts with the assumption that Southeast Asia can produce its indigenous cyber-capacity assessment framework tailored to its distinct context. Essentially, the project undertakes a more grounded, empirical, and inductive approach that considers the agency of the intended users *at the very onset*. Rather than importing "cyber maturity models," Cyber ASEAN builds on existing resources that are readily available in Southeast Asia's cyber capacity toolbox like the ASEAN Cybersecurity Cooperation Strategy 2021-2025. Since the strategy has gained wide endorsement among AMS, Cyber ASEAN can mobilize such momentum by supporting its operationalization. This becomes feasible through the Cyber ASEAN Framework's bottom-up approach: it emphasizes the interests and preferences of the intended end-users, which is complementary to the top-down provisions of the ASEAN Cybersecurity Cooperation Strategy 2021-2025. In fusing the region's top-level consensus-driven style with context-appropriate intervention, the Cyber ASEAN Framework inspires local accountability and, in the longer term, regional

adoption and/or adaptation.

To achieve its stated goals, Cyber ASEAN adopted a participatory design, conducting four multistakeholder consultations in Manila, Hanoi, Jakarta, and Kuala Lumpur. The four closed-door events served as feedback mechanisms to determine if the framework was relevant to the users' needs and priorities. The consultations' participatory nature gave the key stakeholders a more proactive role in the formulation of the Cyber ASEAN Framework.

The consultative process facilitated cross-cutting exchanges among local stakeholders and participants to share their perspectives on the distinct political, economic, technological development, and socio-cultural considerations from their respective sectors and/or countries. During the process, it was observed that the agency of the intended users and stakeholders among the four partner countries was activated and recognized, invoking a deeper sense of ownership of the Cyber ASEAN Framework and the project's overall outcomes.

Obtaining participants' feedback and inputs at the initial stages of the project before the formal completion of the framework was consequential to the project's aim of local ownership because it determined the viability and practical use of the Cyber ASEAN framework early on. As will be shown in the succeeding country reports, the local country consultations contributed to the iterative and flexible inception and the application of the four pillars (international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion), resulting in a positive appraisal of the Cyber ASEAN Framework.

Agency and Autonomy

At the heart of increasing cyber insecurity and technological disruptions is the imperative for Southeast Asia to steer clear of an increasingly bifurcated terrain in the emerging data-driven economy. As the US and China offer competing models of cyber governance and AI development, the question is whether Southeast Asia will remain as a passive rule-taker or follower or demonstrate its agency as a rule-maker in debates concerning norms and standards-setting.[9]

Fortunately, Southeast Asia is showing signs of proactiveness. AMS have subscribed in principle to the 11 voluntary UN norms of responsible state behavior,[10] while Singapore and Indonesia serve as participants and observers in the current ISO/IEC JTC 1/SC 42 standards committee on AI.[11] Although these developments offer optimism, it remains to be seen how the endorsement of norms or soft laws can produce concrete outcomes considering the stark realities of the region's cyber landscape, which require tangible solutions. Even though Southeast Asia is one of the world's leading big data generators,[12] a critical ingredient in AI development, it remains underrepresented in relevant discussions on AI standards-setting. As the US and China compete for dominance over critical technologies that will define the digital economy, AMS are expected to exercise more agency in crafting a regional approach. If not, Southeast Asian states might find themselves entangled in a bifurcated world—a scenario that would be inimical to their national interests and the welfare of their citizens.

Recognizing this challenge, the Cyber ASEAN Framework endeavors to harmonize Southeast Asia's approach to cybersecurity. Practically, the goal is to carve a middle path for Southeast Asia that adheres to internationally recognized norms and technical standards yet remains deeply rooted in each country's unique priorities and needs and respects the principles of national sovereignty and non-interference. Through its series of consultations, the Cyber ASEAN Framework goes beyond assessing progress in adopting international standards; it also examines the innovative and entrepreneurial mindset of each country in customizing their approaches to standards-setting.

Based on the project's research, most companies, as well as Micro, Small and Medium Enterprises (MSMEs), contribute to establishing sectoral and even national cybersecurity standards by drawing concepts and inspirations from the US National Institute of Standards and Technology (NIST) cybersecurity framework and the ISO 27001. But rather than a wholesale adoption, the approach is more "adopt then customize," whereby organizations, whether big or small, craft cybersecurity standards, guidelines, and policies tailored to their distinct organizational objectives and, of course, availability of resources.

In leveraging the best practices and lessons learned from the multistakeholder consultations in Indonesia, Malaysia, the

Philippines, and Viet Nam, the Cyber ASEAN Framework can bring to bear a fit-for-purpose and middle-ground approach for Southeast Asia—one that promotes and preserves its agency and autonomy amid the ongoing bifurcation of norms and standards.

Public-Private-People-Partnership

The cornerstone of the Cyber ASEAN Framework's sustainability rests on its ability to foster trust and mainstream inclusion, which emphasizes people-to-people connections. Public-private partnership (PPP) is the holy grail of implementing cyber policy and strategy, where the success of initiatives like information-sharing and incident response is predicated on the willingness of governments and the private sector to share valuable information and know-how to download an accurate picture of the cyber threat landscape and undertake effective mitigation solutions. Likewise, capacity-building is contingent on PPPs that leverage resources among governments, industry, and academia to grow cybersecurity talent.

While it appears promising, the true marker of PPPs' success depends on implementation. Tensions among parties may occur due to divergent motivations and expectations regarding accountability, transparency, and investments. In Southeast Asia, debates continue regarding the government's scope of responsibility in ensuring the cybersecurity of privately-owned and operated critical national infrastructure. Furthermore, governments and industry are still reluctant to share information or, in worst-case scenarios, withhold it due to varying perceptions of costs and benefits.[13]

Industries are concerned about sharing too much information, because it may expose their intellectual property, and that could benefit their competitors. Others see additional financial costs from information-sharing. Unfortunately, these short-sighted assessments only benefit malicious actors in carrying out cyberattacks while cultivating an environment riddled with mistrust. Capacity-building, reskilling, or upskilling opportunities under PPP arrangements are often considered mere

band-aid solutions to addressing the acute shortage of cybersecurity professionals. Often, they fall under corporate social responsibility and are sometimes ad hoc or one-off engagements, posing sustainability concerns over the long haul.

Cyber ASEAN dove into the undercurrents of PPP by installing the missing piece in such arrangements—the people. The people-centric approach to PPP will facilitate its execution in a strategic, coordinated, and inclusive fashion. The consultation workshops highlighted how personal relationships based on mutual trust foster a more collaborative environment. For instance, most Computer Emergency Response Teams (CERTs) would occasionally rely on their professional networks and contacts in the CERT community, especially during heightened or high-level cyber incidents.

With established trust among professionals built via formal or informal channels, it becomes feasible for CERT-to-CERT cooperation to share timely and actionable information to remediate cyberattacks. Because of the mutual trust grounded on strong people-to-people ties, CERTs from the public and private sectors can engage in threat-hunting, a more predictive approach than incident response. With agreed mechanisms for sharing sanitized information across government intelligence agencies, enterprises, internet service providers, regulators, and CERTs, threat-hunting makes it plausible to anticipate cyber incidents ahead of time, and consequently lessen the potential disruptive impact.[14]

Inclusion is also key to making sure that the people dimension in PPP is executed effectively and sustainably. Inclusion goes beyond tackling the digital divide; it considers the socio-economic and technological variables that cannot be addressed by the mere provision of digital public goods such as the installation of broadband internet or 5G. Inclusion is all-encompassing, aiming for equitable representation and access to opportunities that benefit women and girls, as well as minority groups. More than just an afterthought, Cyber ASEAN's emphasis on inclusion aims to promote equity that complements top-down policies with bottom-up and community-led approaches.

While achieving inclusion is quite an ambitious and challenging goal, given the cultural diversity present in Southeast Asia, the project managed to engage representatives from civil society groups to ensure that their perspectives were heard in the creation and testing of the Cyber ASEAN Framework. Challenging the

conventional technocratic approach to most cyber capacity-building initiatives, the project endeavored to expand multistakeholder participants by engaging grass-roots organizations representing women and girls, persons with disabilities, and ethnic minorities. In prioritizing inclusion, Cyber ASEAN strengthens public-private partnerships on cyber capacity-building anchored through human or people-centric development.

FIGURE 1

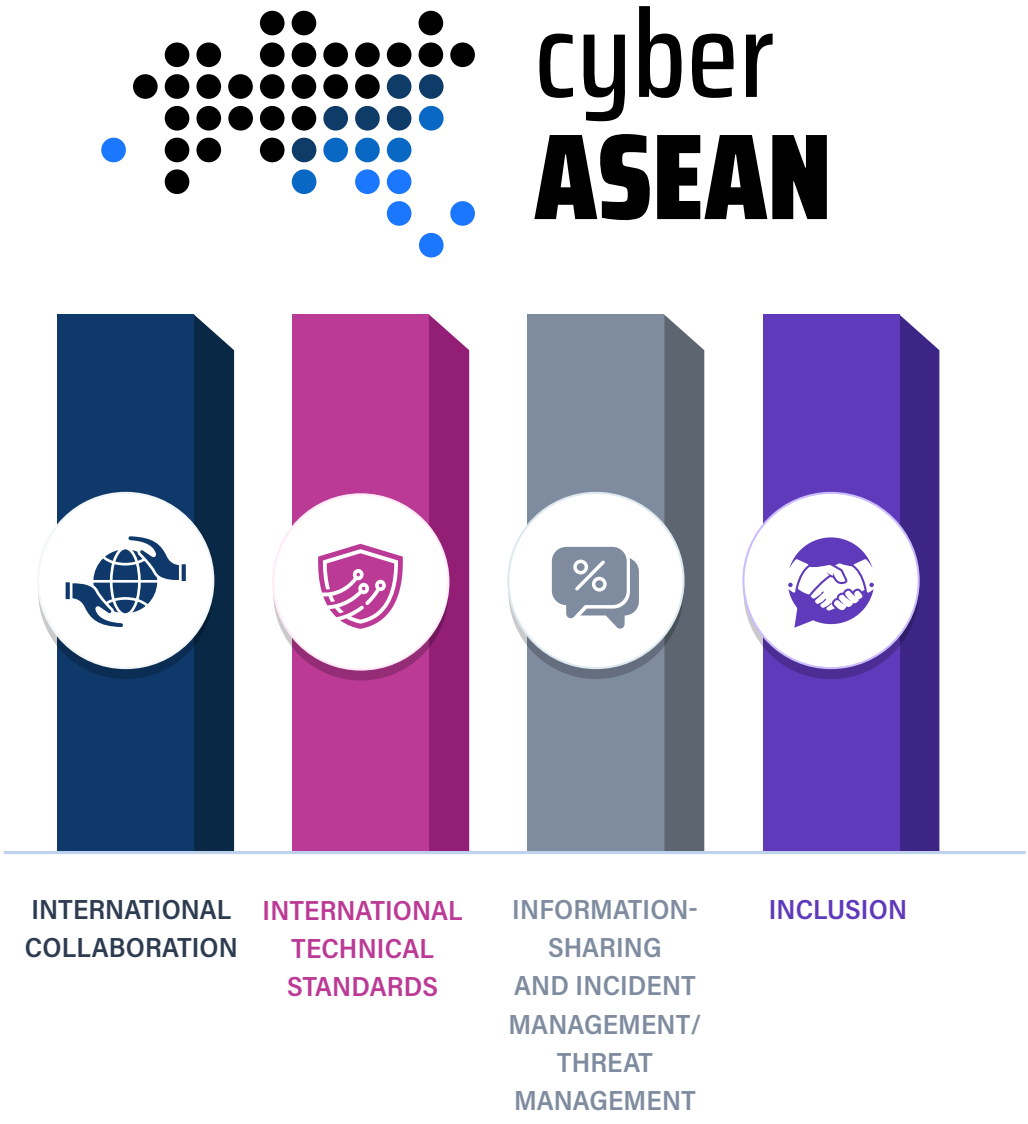
ASEAN Cybersecurity Cooperation Strategy 2021 – 2025

CYBERSECURITY IN SUPPORT OF ASEAN'S DIGITAL AMBITIONS	
ASEAN Smart Cities Network Improve the lives of ASEAN citizens using technology as an enabler	
ASEAN Declaration on Industrial Transformation to industry 4.0 A well-prepared ASEAN able to maximise the opportunities of Industry 4.0 to foster regional economic growth and maintain ASEAN centrality as a key player in global production networks	
ASEAN Digital Masterplan (ADM) 2025 ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies and ecosystem	
All digital activities undergirded by building secure and resilient cyberspace	
DIMENSION 1 **Advancing Cyber Readiness Cooperation**	▪ CERT Coordination—incidence response and threat information sharing ▪ Coordination on regional CII protection
DIMENSION 2 **Strengthening Regional Cyber Policy Coordination**	▪ Norms implementation ▪ Coordination on cybersecurity and related digital security issues
DIMENSION 3 **Enhancing Trust in Cyberspace**	▪ Promoting International Cybersecurity Standards ▪ Cyber hygiene and digital inclusion
DIMENSION 4 **Regional Capacity-Building**	▪ Multi-disciplinary, modular, measurable multistakeholder capacity-building programs
DIMENSION 5 **International Cooperation**	▪ Multilateral Engagement with Dialogue Partners

FIGURE 2

The Cyber ASEAN Framework

Built around the key dimensions of the ASEAN Cybersecurity Cooperation Strategy 2021-2025 (above) the Cyber ASEAN framework is composed of four pillars: *international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion*.



Approach and Limitations

From the period of May 2022 to January 2024, the Cyber ASEAN project team, led by the Chief Investigator and four country experts in Indonesia, Malaysia, the Philippines, and Viet Nam, embarked on a series of consultations. Likewise, three regional experts led the feedback sessions during the three-part virtual experts meeting. Across its policy engagements and research activities, the Cyber ASEAN team adopted its 3C approach: collaboration, consultation, and community-building.

Collaboration

As mentioned, intended users and recipients of the Cyber ASEAN Framework were involved in its establishment from the start. Through a multistakeholder and participatory-design approach, each country consultation sought feedback and paid close attention to the needs and priorities of key stakeholders. This led to an interactive and collaborative exercise in applying the foundational pillars of the Cyber ASEAN Framework in each country.

In tandem with the country consultations, three virtual experts' meetings were held. The virtual experts' meeting convened the country experts alongside expert advisors and other regional cybersecurity interlocutors and practitioners to further refine and develop the framework to be consistent with international best practices. Additionally, the online sessions further examined salient issues that emerged during the country consultations like building trust, fostering inclusion, and practical strategies to effectively engage and persuade policymakers in Southeast Asia regarding cyber resiliency and capacity. Such deliberations enriched the Cyber ASEAN Framework. Thus, the combined outcomes and inputs of the country consultations and the virtual experts' meeting demonstrate the iterative process that forms the micro-foundations of the Cyber ASEAN Framework.

Consultation

Guided by Cyber ASEAN's aim of breaking silos, the country consultations

and virtual experts' meetings involved industry, academic, and civil society representatives. Similarly, the local consultations engaged key stakeholders in Indonesia, Malaysia, the Philippines, and Viet Nam. The forum served as a track 1.5 platform to deeply understand each country's distinct contexts (digital maturity, cyber capacity, political-security, and economic resources). Using the Cyber ASEAN Framework as the main reference point, the deliberations engendered pragmatic perspectives to support the ASEAN Cybersecurity Cooperation Strategy 2021- 2025.

At the time of Cyber ASEAN's implementation, the government policymakers, and decision-makers among the four countries covered in this report are in the process of planning or developing legal regulations that are well-suited to maximize opportunities and minimize challenges in the ever-changing cybersecurity landscape. The four country consultations served as informal and neutral venues to supplement such policymaking efforts. The deliberations of Cyber ASEAN sought to provide critical insights for context-specific cyber policymaking, which can feed into the outcomes of the regulatory or legal frameworks of the four countries.

Community-building

Crucially, the formation and implementation of the Cyber ASEAN Framework not only provide useful insights into operationalizing the ASEAN Cybersecurity Cooperation Strategy 2021- 2025, but also reframe cybersecurity as a cross-cutting issue that transcends ASEAN's political-security, economic, and social-cultural community pillars. The concept of the multistakeholder is put into practice, linking the three ASEAN community pillars. Cybersecurity is viewed beyond the myopic lens of the digital economy.

Central to the project's community-building approach is the engagement of cybersecurity experts and practitioners from diverse backgrounds across its four pilot countries. Therefore, in harnessing Southeast Asia's reputable network of cybersecurity scholars, researchers, and practitioners, Cyber ASEAN has achieved two milestones: 1) gained cross-sectoral perspectives to achieve holistic and well-rounded insights on cyber policymaking, and 2) established a tight and reputable community of cybersecurity experts that may give rise to a dedicated Point of Cyber Expert Directory (PCED) in each country. Public and private sector entities can consult the PCED to seek strategic advice in formulating or implementing

effective cyber policies and strategies and capacity-building engagements.

Admittedly, Cyber ASEAN has only engaged Indonesia, Malaysia, the Philippines, and Viet Nam. While the four countries do not represent the entirety of Southeast Asia, they are important test cases for the Cyber ASEAN Framework inspired by the ASEAN Cybersecurity Cooperation Strategy 2021- 2025. Hopefully, the interesting takeaways and concrete outcomes of the Cyber ASEAN project—embodied through the framework and the relevant country reports in the succeeding chapters—catalyze the enthusiasm to adopt and adapt the Cyber ASEAN Framework among the remaining countries as the region's homegrown cyber assessment framework implemented in a multistakeholder and inclusive fashion.

Mabda Haerunnisa Fajrilla Sidiq

Tracing the Development of Cybersecurity Cooperation in ASEAN: Progress and Shortcomings

Introduction

Cybersecurity has become increasingly salient in dialogues within ASEAN to address common challenges. However, progress has remained incremental due to various reasons. First, ASEAN Member States (AMS) have differing views on cyber issues, extending to the different degrees of prioritization placed upon addressing challenges in cyberspace. AMS have different comprehensions about cyberspace

and the potential it holds for their societies and economies. This influences how AMS incorporate cyber threats into their policies to varying degrees.[1] Second, there are considerable gaps in the member states' cyber capacities, given their diverging levels of commitment to the issue. For instance, some AMS are ranked favorably in the International Telecommunication Union's (ITU) Global Cybersecurity Index (typically Singapore and Malaysia). In contrast, other member states achieved some of the lowest scores.[2]

Despite such disparities, recent developments demonstrate ASEAN's positive momentum in advancing impactful dialogues and achieving consensus on cybersecurity issues. This chapter provides an overview of ASEAN's evolving cybersecurity cooperation over the past decades. It maps out the development of ASEAN's cybersecurity policy, noting landmark initiatives that illustrate progress, but also reveal several shortcomings. Recognizing the prevailing gaps in ASEAN's collective approach to cybersecurity policy and capacity, this chapter helps to situate the distinct contribution of the Cyber ASEAN Framework in advancing the region's cyber resiliency through a participatory and multistakeholder-led initiative.

The Emergence and Development of Dialogues on Cybersecurity Issues in ASEAN

Cybersecurity cooperation in ASEAN emerged out of decades of collective efforts to address the rise of ICTs, harness the benefits of digitalization, and address transnational cyber threats. These efforts can be chronologically categorized into three phases, each marking attempts to specify the focus of cooperation.

Table 1 provides a comprehensive list of key efforts, based upon existing mechanisms and documents relevant to ICT and cyber issues. Dialogue platforms include the relevant avenues, primarily at the ministerial level, to facilitate routinized deliberations and decision-making. Key outcomes are found in consensus documents that stipulate decisions reached through deliberations within dialogue platforms or processes occurring in relevant sectoral cooperation. Lastly, coordination and implementation mechanisms refer to technical and policy platforms available for AMS to maintain constant engagement in their respective areas of concern.

TABLE 1

Phases of the development of cyber dialogues in ASEAN

DIALOGUE PLATFORMS	EMERGENCE OF COOPERATION ON ICTs 1989 - 2010	RISING RELEVANCE OF THE SECURITY LENS 2011 - 2016	HABITUATION OF CYBER DIALOGUES AND COOPERATION 2016 - PRESENT
	ASEAN Telecommunications Ministers Meeting (TELMIN) (2001-2018);	ASEAN Ministerial Meeting on Transnational Crime (AMMTC) (cybercrime discussed since 2011);	ASEAN Ministerial Conference on Cybersecurity (AMCC) (since 2016);
	ASEAN Regional Forum (ARF) (since 2001);	ASEAN Defence Ministerial Meeting Plus (ADMM-Plus) (since 2013);	ARF Inter-Sessional Meeting (ISM) on Security of and in the Use of Information and Communications Technology (since 2018);
	Virtual Forum of ASEAN Cyber-security (launched in 2003, information on its continuation is unclear);	ASEAN-Japan Cybercrime Dialogue (since 2014)	ASEAN-Australia Cyber Policy Dialogue (since 2018);
	ASEAN-Japan Information Security Policy Meeting (since 2009)		ASEAN Digital Ministers Meeting (ADGMIN) (previously TELMIN, renamed since 2019);
			ASEAN-US Cyber Policy Dialogue (since 2019);
			ASEAN-China Cyber Dialogue (since 2020)

DOCUMENTS

EMERGENCE OF COOPERATION ON ICTs
1989 - 2010

e-ASEAN Framework Agreement (2000)

RISING RELEVANCE OF THE SECURITY LENS
2011 - 2016

ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space (2006);

ASEAN ICT Masterplan 2015 (2011);

ASEAN Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security (2012);

ASEAN-Japan Critical Information Infrastructure Protection (CIIP) Guideline (2014, updated in 2015 and 2016);

ASEAN ICT Masterplan 2020 (2015)

HABITUATION OF CYBER DIALOGUES AND COOPERATION
2016 - PRESENT

ASEAN Framework on Personal Data Protection (2016);

ASEAN Cybersecurity Cooperation Strategy (2017-2020) (2017);

ASEAN Declaration to Prevent and Combat Cybercrime (2017);

ASEAN Framework on Digital Data Governance (2018);

ASEAN Leaders' Statement on Cybersecurity Cooperation (2018);

ASEAN Digital Integration Framework (2018);

ASEAN-US Leaders' Statement on Cybersecurity Cooperation (2018);

ASEAN-European Union (EU) Statement on Cybersecurity Cooperation (2019);

ASEAN Leaders' Statement on Advancing Digital Transformation in ASEAN (2021);

ASEAN Data Management Framework (2021);

ASEAN Cybersecurity Cooperation Strategy (2021-2025) (draft published in 2022)

COORDINATION AND IMPLEMENTATION MECHANISMS

EMERGENCE OF COOPERATION ON ICTs
1989 - 2010

ASEAN Science and Technology Network (ASTN) - Sub-Committee on Microelectronics and Information Technology (since 1989);

ASEAN Network Security Coordinating Council (established in 2002 under the 2002 Manila Declaration, information on its continuation is unclear);

ASEAN Computer Emergency Response Team (CERT) Incident Drill (since 2006)

RISING RELEVANCE OF THE SECURITY LENS
2011 - 2016

ASEAN Network Security Action Council (ANSAC) (established in 2011);

Senior Officials Meeting on Transnational Crime Working Group on Cybercrime (SOMTC WG on CC) (since 2013);

ADMM-Plus Experts Working Group on Cyber Security (since 2017)

HABITUATION OF CYBER DIALOGUES AND COOPERATION
2016 - PRESENT

ASEAN Cyber Capacity Programme (ACCP) (since 2016);

ASEAN-Japan Cybersecurity Capacity Building Centre (established in 2018);

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) (launched in 2019, operational since 2020);

ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) (established in 2020);

ASEAN Cybersecurity Resilience and Information-Sharing Platform (CRISP) (launched in 2019, operational in February 2021).

ADMM Cybersecurity and Information Centre of Excellence (launched in 2022)

As demonstrated in Table 1, dialogues on cyber issues resulted from a combination of relevant discussions and documents, initially under the economic pillar and gradually permeating to sectoral dialogues under the security pillar.

In the first phase, ICTs were primarily discussed as a trade issue, as aptly elaborated by the e-ASEAN Framework Agreement. Then, ASEAN started to refer to the idea of a regional information infrastructure. Significant progress was marked by the inauguration and, in subsequent years, routinization of ASEAN TELMIN, further institutionalizing the telecommunications sector as a focus area of cooperation. Having a dedicated ministerial meeting to discuss such issues ensured incremental progress was made on ICT initiatives. Consequently, some of the mechanisms resulting from dialogues within the telecommunications sector facilitated the development of capacity-building and coordination efforts for CERTs, after the establishment of the ASEAN Network Security Action Council (ANSAC).

It is worth emphasizing that most of the initiatives emerging from the first phase primarily situated cooperation in ICTs within the economic pillar, considering that most discussions on ICTs took place under the remit of TELMIN. Moreover, ASEAN's vigor in pushing for its community-building agenda translated into efforts to improve access to ICTs, improve regional connectivity, and enhance competitiveness in the ICT sector. These objectives are still present in the current e-ASEAN Framework Agreement.

The second phase marks an intensification of efforts to include cyber issues in dialogues under the security pillar. While the security dimension of cyber issues was first discussed under the ARF in 2001, ASEAN eventually appraised the transnational risks arising from cyberspace in 2011. In this respect, cybercrime became one of ASEAN's priority areas under transnational crime. Moreover, following relevant discussions on cybersecurity under the purview of the ADMM-Plus, AMS have started to engage in military-to-military exchanges to specifically discuss cybersecurity among themselves and with their dialogue partners. Such engagements have designated cybersecurity as a key area of practical cooperation among member states of the ADMM-Plus.

The third phase may be regarded as the most productive period, following the establishment of the ASEAN Ministerial Conference on Cybersecurity (AMCC) in 2016. The conference is designed as an informal meeting among ministers in charge of cybersecurity, signaling an elevated focus on the issue. Every iteration of the AMCC to date has been held under the broader agenda of the Singapore International Cyber Week (SICW), demonstrating Singapore's investment and leadership in cybersecurity, particularly through the ASEAN Cyber Capacity Programme (ACCP) and the establishment of the ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE). The decision to rename TELMIN to ADGMIN in 2019 was also notable, showcasing ASEAN's view of cybersecurity issues as cross-cutting. With such momentum, ASEAN further enhanced its coordination in cybersecurity by forming the ASEAN Cyber Coordinating Committee (Cyber-CC), which gathers representatives from ASEAN sectoral bodies to facilitate cross-sectoral coordination.

Another significant milestone was ASEAN's decision to "subscribe in principle" to the norms derived from the 2015 United Nations Group of Governmental Experts (UN GGE) Report, followed by the development of a regional plan of action to implement such norms. Lauded as the first of its kind, the endorsement of the 11 UN cyber norms exemplifies ASEAN's solid effort to establish standards for responsible state behavior in cyberspace.[3] The release of the ASEAN Cybersecurity Cooperation Strategies in 2017 and 2022 crystalized ASEAN's desire to streamline its cyber initiatives. The latest iteration of the strategy synthesizes various initiatives built around the political-security, economic, and socio-cultural pillars to support "ASEAN's digital ambitions" to become a "leading digital community and economic bloc.[4]"

Evaluating the Progress and Shortcomings of ASEAN's Cybersecurity Cooperation

The incremental development of cyber cooperation within ASEAN has resulted in significant progress toward a more cohesive approach to cybersecurity. First, after years of dialogues and activities, AMS have reached a sufficient level of understanding of what can reasonably be achieved under ASEAN to maintain sufficient progress in cyber cooperation. While others correctly point

out the ideational gaps in the member states' ways of conceiving cyberspace, tangible efforts to habituate cyber cooperation have generated modest results amid ASEAN's complex consensus-driven process known as the "ASEAN Way." Notwithstanding its acknowledgment of the transnational nature of cyberspace, ASEAN has maintained its staunch adherence to the non-interference principle.[5] Aside from developing a common approach to addressing cyber threats, there is equal emphasis on enhancing domestic cyber capacity and digital development, while encouraging coordination and confidence-building across the region. Such a balanced approach bodes well for meeting the interests of member states that put less priority on digitization.

Indeed, modest expectations about what can be collectively achieved under the purview of ASEAN can be regarded as an achievement in and of itself, considering various fundamental socio-political differences that shape how cyber technologies are utilized and cyber policies are formed among member states. Such an observation attests to ASEAN's key milestones in building trust and confidence among its member states, particularly concerning states' behavior in cyberspace and their ability to collectively address transnational challenges.

Second, by understanding what ASEAN can collectively agree on, the existing cybersecurity cooperation strategy is more realistic and creates flexibility regarding the minimum level of capacity that all member states can feasibly meet. Like the consensus documents listed in Table 1 that show ASEAN's flexibility and accommodation among member states toward regional integration,[6] expectations were also tempered over what constitutes a sufficient level of cyber capacity at the regional level. Such expectations are manifest in ASEAN's adaptive approach toward the establishment and development of a regional CERT among its member states. For instance, in TELMIN's early years, ASEAN put a strong emphasis on encouraging all member states to form CERTs within their jurisdictions. However, this expectation has slightly changed under the latest ASEAN Cybersecurity Cooperation Strategy, suggesting the establishment of the ASEAN CERT to better support coordination and various joint activities.

Third, it is also important to emphasize ASEAN's capability to streamline cybersecurity cooperation made possible by the cybersecurity cooperation strategy. As cybersecurity discussions become less ad hoc and more regularized instead, the strategy advanced progress in two areas. First, it systematically structured

previously sporadic initiatives and how pre-existing and upcoming initiatives can support ASEAN's objectives in the digital sector.[7] Second, the strategy adds more clarity to the intended objectives of cybersecurity initiatives collectively pursued by AMS. Every activity outlined in the strategy is mapped according to its relevance to ASEAN's broader digital efforts, with the ASEAN Digital Masterplan 2025 as the primary point of reference. This allows for the identification of objectives and outcomes expected from the activities undertaken.

Fourth, another important achievement is ASEAN's resourcefulness in supporting its cybersecurity initiatives. As a regional bloc with varying degrees of digital maturity, ASEAN has capitalized on its internal and external relationships to address the increasing demand for capacity-building and confidence-building measures. For instance, ASEAN has reached out and collaborated with its dialogue partners to make up for resource constraints. Japan and Australia serve as an important example, as they conceive ASEAN as a strategic beneficiary for much of their assistance in technical and normative capacity-building activities.[8]

Internally, Singapore's leadership has been integral in establishing the ACCP and ASCCE, which are geared toward cyber capacity-building programs and activities within the region. Thailand and Malaysia have also demonstrated the will to actively contribute to cyber initiatives. Thailand is instrumental in the development of the ASEAN Critical Information Infrastructure Protection Framework, while Malaysia, together with Singapore, were co-proponents in the formulation of the regional action plan to implement the UN GGE norms.[9] Malaysia also worked in tandem with Australia to initiate the ASEAN regional cyber points of contact that earned an in-principle endorsement from the ARF in 2019.

Although ASEAN's evolving approach has very much acknowledged the cross-pillar and -sectoral character necessitated by cyber cooperation, the reality is that cybersecurity cooperation is still considered primarily to be an economic objective. According to the current ASEAN cybersecurity cooperation strategy, cybersecurity is still largely conceived of as an "enabler" for ASEAN's ambitions in the digital realm under the economic pillar. While this does not impede progress, ASEAN should aspire to genuinely set a more comprehensive view of cybersecurity beyond the myopic lens of the digital economy. It cannot continue to apply its conventional approach to cybersecurity, given the evolving nature of such a domain. Rather than compartmentalizing cybersecurity issues as merely economic,

defense and security, or socio-cultural, ASEAN must seriously take a holistic stance that considers the growing prevalance of advanced persistent threat actors, disinformation campaigns, deep fakes, and ransomware.

It is also important to highlight that cybersecurity cooperation in ASEAN primarily hinges upon Singapore's leadership. Although interest among other AMS to contribute to cybersecurity issues and initiatives is there, tangible efforts to do so remain lacking or absent. In most cases, sustaining current efforts remains a challenge due to resource considerations. Once again, the varying levels of cyber capacity, as well as prioritization, impact the level of dedication, commitment, and contributions each AMS dedicates to cybersecurity cooperation.

Lastly, the implementation of the ASEAN Cybersecurity Cooperation Strategy 2021-2025 will demand mobilizing resources and support beyond government entities. While the strategy has attempted to consolidate all existing cyber-related initiatives, it will demand buy-in among key stakeholders in Southeast Asia. As pointed out, ASEAN remains resource-strapped, and the political bandwidth each member dedicates changes depending on the issues of the day. These observations thus raise the question of how the strategy will be implemented on the ground.

To this end, the Cyber ASEAN Framework seeks to support the ASEAN Cybersecurity Cooperation Strategy 2021-2025. Aspiring to become the region's homegrown cyber-capacity assessment tool, it adopts key elements of the strategy document and integrates them into its four pillars: international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion. Through its 3C approach—consultative, collaborative, and community-building—the Cyber ASEAN Framework complements the top-down nature of the strategy document, which brings to bear on the whole of the ASEAN community.

In pathfinding practical interventions, Cyber ASEAN narrows the gap within the ASEAN Cybersecurity Cooperation Strategy 2021-2025 toward achieving cross-pillar and multi-sectoral cybersecurity cooperation involving a wide range of stakeholders from governments, industry, academia, and civil society. Using the Cyber ASEAN Framework as the reference point, the conduct of country and region-wide consultations will reveal the underlying tensions among public and private stakeholders about implementing the strategy. It will probe deeper into

what conditions are necessary to ensure greater collaboration in cementing regional initiatives such as information-sharing and incident response, as in the case of ASEAN CERT. More importantly, the outcomes and findings derived from the application of the Cyber ASEAN Framework among Indonesia, Malaysia, the Philippines, and Viet Nam can provide practical recommendations for how individual countries should aim to apply the regional strategy in their domestic contexts.

Conclusion

Cyber cooperation in ASEAN has developed incrementally, starting from ad-hoc initiatives to address common issues about ICTs from an economic standpoint and then gradually expanding to mechanisms under the security pillar. However, in recent years, cyber cooperation has been increasingly viewed as a cross-pillar issue. Aside from conceptual and ideational shifts, ASEAN has paid more attention to cyber cooperation by institutionalizing and capitalizing on various cyber initiatives, further eliminating the sporadic nature of most of the cyber-related initiatives before 2006.

Although expectations have been largely modest due to ASEAN's longstanding norms and principles of non-interference as well as its consensus-driven approach, the region has been able to gradually intensify and enhance cyber cooperation. ASEAN has remained realistic about what it can achieve. It has adopted flexible standards on the minimum level of capacity. Recent documents such as the ASEAN Cybersecurity Cooperation Strategy 2021-2025 have also provided clarity on the interlinkages between various mechanisms and implementations in the cyber realm, further improving prospects for regional collaboration.

Still, doubts linger over whether ASEAN's consolidated approach to cybersecurity, embodied in the ASEAN Cybersecurity Cooperation Strategy 2021-2025, can yield concrete outcomes. The Cyber ASEAN Framework attempts to fill the gap. Synthesizing the strategy's key dimensions into its four pillars—international collaboration, international technical standards,

information-sharing and incident or threat management, and inclusion—Cyber ASEAN endeavors to rally support for the strategy document by making the process of cyber policymaking and capacity-building more inclusive and holistic. Drawing from the expertise of the region's cybersecurity community, it seeks to propel pragmatic recommendations that can feed into the realization of the strategy document, to sustain or even elevate the region's momentum toward cybersecurity cooperation.

Mark Bryan Manantan and Lesley Manantan

Buffering: Southeast Asia's Response to Cyber Insecurity

Introduction

The evolution of ASEAN's approach to cybersecurity as an intersectional policy issue has been marked by a gradual proliferation of dialogue platforms and implementation mechanisms. But perhaps an underemphasized aspect of Southeast Asia's goal to consolidate its cybersecurity cooperation is the uncomfortable reality that it can no longer shrug off its strategic dimensions. During Cyber ASEAN's country consultations, several experts and policymakers repeatedly emphasized that cybersecurity is not just an economic, technical, or development issue but is also increasingly geopolitical.[1] This chapter examines Southeast Asia's complex approaches toward the strategic dimensions of cybersecurity.

Recognizing the variances in cyber policy and capacity as well as the political sensitivities in addressing cyber insecurity, personal interviews were arranged among cybersecurity policymakers, experts, researchers, and industry practitioners in order to deeply understand the context, as well as the underlying motivations in Southeast Asia, in responding to cyber incidents.

The South China Sea dispute is the major driving force of cyber-espionage activities in the region.[2] Most state-sponsored cyber-threat actors are actively gathering geopolitical intelligence with immense scale and sophistication.[3] Indonesia, Malaysia, the Philippines, and Viet Nam have experienced high volume of cyber-espionage activities linked to advanced persistent threat (APT) groups that are based in China, Russia and North Korea.[4] The majority of the reported cyber incidents occurred during heightened tensions in the South China Sea, to which Malaysia, the Philippines, and Viet Nam are all claimant states.[5] Due to an increasingly contested geostrategic environment, cyber capabilities have become indispensable tools to obtain confidential information concerning the negotiations on the South China Sea Code of Conduct.[6]

The COVID-19 pandemic outbreak in 2020 also saw an increase in various cyber activities, ranging from cyber espionage to ransomware.[7] State-sponsored hackers were deployed to siphon sensitive information about countries' varying responses to the pandemic during a time of increasing geopolitical flashpoints. As most countries in the region grappled with intermittent lockdowns and border shutdowns, cyber criminals were also exploiting the rapid migration to digital platforms, as well as mounting social anxiety, to prey on their targets.

However, the motivations were not just geopolitical; other cyber-threat actors were also conducting intellectual property and financial theft, which impacted both the public and the private sector.[8] On top of governments and the military, cyber-threat actors have infiltrated the financial, technology, and infrastructure sectors, as well as academia and civil society groups.[9]

Responding to Risks and Vulnerabilities

Attribution and Quiet Diplomacy

Southeast Asia's response to cyber-espionage activities has been lukewarm at best, yet strategically logical. In contrast to the US and its allies, public attribution remains taboo in Southeast Asia, because most countries have very complex political and economic ties with active cyber powers like China and Russia. In addition to trade and investments, Chinese state-owned companies like Huawei are also deeply involved in various digital infrastructure developments in Indonesia, the Philippines, and Malaysia, while Russia still supplies weapons to several countries in the region, including Viet Nam and Indonesia.

Any attempts at conducting public attribution will be political and legal decisions, carrying an immense risk of possibly antagonizing key economic and strategic partners. But this does not mean that Southeast Asia ignores state-sponsored hackers or completely disregard attribution—the execution might be more veiled and behind the scenes.

In various consultations with key stakeholders, backdoor or quiet diplomacy was recognized as a potent tool in raising issues with actors who are alleged to be behind cyber-espionage campaigns.[10] Some Southeast Asian countries use quiet diplomacy to notify the alleged perpetrator(s) regarding suspected cyber incidents found in their networks or systems.[11] Stakeholders that deal with cyber incidents hold the view that such an approach is more pragmatic in addressing cybersecurity concerns. Of course, it can be debated if the use of backdoor or quiet diplomacy is effective, considering the potential implications of cyber incidents that could compromise the personal data of thousands or millions of Southeast Asians/or the possible disruptions if cyber incidents escalate due to miscalculations.[12]

Lack of Technical Capacity and Shame Behind Cyberattacks

Aside from political and legal hurdles, another major deterrent for Southeast Asian countries to assign attribution with the utmost confidence is their inadequate technical expertise. Attribution relies on sophisticated tools and methods of digital forensics to arrive at a definitive conclusion as to who did what and how. Yet, most Southeast Asian countries, and in particular their government departments and ministries, lack a dedicated pool of cybersecurity professionals.

Relatedly, another major impediment is the prevailing reluctance in the private sector to disclose or cooperate in the incident investigations. Some experts interviewed revealed that the private sector would often deal with cyber incidents on their own rather than report to the government, in large part to avoid regulatory sanction. However, other industry representatives believe that governments do not have adequate resources in the first place to implement their national cybersecurity strategies, let alone to fully mitigate the increasing rate of daily cyber incidents.[13]

Disclosure of cyberattacks also has reputational and/or social implications. More than a public relations crisis, most stakeholders, whether from government or industry, believe that publicly admitting or revealing cyberattacks is tantamount to a shameful admission—that an entity or organization failed to safeguard the data entrusted by its customers.[14]

Trust-building and Depoliticization of Cyber Incidents

Although most stakeholders agree that people, process, and technology remain the standard approach in optimizing cybersecurity processes and frameworks, personal trust is the glue that binds the three elements. Across the four country consultations, the Asia Pacific CERT (APCERT) community stands out as a near-perfect case study of trust-building. The APCERT community leverages its collaborative partnerships to achieve a common goal of addressing cybersecurity risks. Cybersecurity professionals point to the role that the tight-knit network in the CERTs community in the Asia Pacific plays in confidence-building measures, information-sharing, and incident management.

The unique ingredient to establishing and preserving the culture of trust within the APCERT community is their distinct approach to depoliticizing cyberattacks. Despite the existing political and diplomatic disagreements among some of its members, APCERT recognizes the urgency of prioritizing cybersecurity risks and threats over political issues that could lead to bigger crises. Such standard operating procedures at the working level have led to normative agreements among APCERT members that emerged from regular formal and informal technical activities that build and reinforce trust over time. With established trust, CERTs from the public and the private sector collaborate with one another to share timely and actionable information, especially during high-level cyber incidents.[15]

Harmonizing Cybersecurity Standards for Interoperability

Throughout the multistakeholder consultations, it became obvious that international technical standards serve as a common language that permits interoperability. Considering that cyberattacks are borderless, international technical standards act as a baseline in synergizing strategies to manage risks at the sectoral, national, and regional levels.[16] Harmonization of cybersecurity standards will be vital to fully operationalize a regional CERT that deals with vulnerability management, incident response, and information-sharing. Other experts also contend that AMS can use international technical standards to further strengthen their capabilities by raising specific cyber incidents linked to suspected cyber actors in a more systematic and sophisticated fashion.[17] Should ASEAN decide to produce a cyber-diplomacy toolbox, international technical standards could be an important component to support the region's backdoor diplomacy as the ebb and flow of geopolitical challenges move to and from the cyber domain.

From a digital economy standpoint, policymakers and practitioners are aware of the ongoing efforts to harmonize standards in ASEAN, driven by the intent to reduce technical barriers to trade and ease any restrictions that accelerate economic integration. For instance, attaining interoperability through the adoption of ISO 27001:2013 will help Southeast Asia streamline its electronic payment system, which will benefit its booming e-commerce market.[18]

Convergence of Cybersecurity and Critical Technologies

Throughout the consultations, experts highlighted the rapid digital transformation that has expanded the threat surface for malicious actors. The use of the Internet of Things and Cloud computing, and the breakthrough of AI-enabled technologies, specifically generative AI, have changed the playing field. Through Large Language Models, hackers can write more sophisticated malicious codes, produce stealthier spear-phishing emails and social engineering tactics, and create deep fakes to sow social discord.[19]

Fortunately, the same technologies are also being used to beef up cyber defenses. For instance, machine learning is employed for malware detection alerts. In Indonesia, cybersecurity experts are using post-quantum cryptography to manage the sheer volume of cyberattacks. Viet Nam has also established a platform that utilizes big data and AI to manage cybersecurity risks and threats and to issue early warning signs and alerts to subscribed stakeholders.[20]

Human-centric Approach to Cybersecurity

Even though the initial focus of the Cyber ASEAN Framework was on the protection of critical national infrastructure, a common thread across the four country consultations was the growing concern over malicious and harmful content, mainly peddled by disinformation and misinformation campaigns. On top of these, digital authoritarianism, particularly in Indonesia, is also becoming an emerging threat.

The growing salience of disinformation and misinformation, combined with discussions on digital authoritarianism, have raised a fundamental conceptual question as to whether information security, not cybersecurity, should be the apt terminology in Southeast Asia. The former is more encompassing, while the latter only emphasizes cyber-enabled activities involving critical national infrastructure, as well as defense and security. The conceptual debate is converging on Southeast

Asia's understanding and approach to cybercrime. Except for the Philippines, no AMS have acceded to the Budapest Convention—a non-binding international treaty on cybercrime—due to diverging definitions and concerns regarding national or digital sovereignty.[21] Aside from cybercrimes like malware or ransomware, Indonesia strongly considers content-related activities such as incitement to terrorism, disinformation, and hate speech as cybercrime.[22]

However, from the viewpoint of academic experts and civil society advocates, the core issue goes beyond the conceptual definition of cyber or information security. It demands a recentering of current debates toward human (cyber)security amid the rise of cyber mercenaries, hacking as a service, digital bot sweatshops, and state surveillance.[23] The argument stems from the observation that humans remain the weakest link in cybersecurity. Human cognitive aspects make them highly vulnerable, which may jeopardize the implementation of processes or deployment of technologies. In the age of digital authoritarianism and misinformation or disinformation backed by AI-powered technologies, humans are increasingly at risk of being the primary targets and/or subjects.[24]

In reframing cybersecurity through a human-security lens, inclusion becomes feasible, which puts the individual's digital rights at the core of cyber policies or frameworks. A human-centric cybersecurity approach that is more encompassing guarantees open internet access, the protection of freedom of expression online, and the enhancement of online security, including privacy and freedom from online violence and threats, that can bring positive benefits to underprivileged communities and minorities.[25]

Conclusion

State-sponsored hackers are not the only ones to blame regarding Southeast Asia's cyber insecurity. As observed in Indonesia, Malaysia, the Philippines, and Viet Nam, the sobering lack of trust and lagging technical and policy capacity are the two greatest vulnerabilities that beset the region. Without standard metrics and mechanisms to cultivate and sustain transparency and accountability among the public and the private sectors to genuinely share timely and valuable information, malicious actors will continue to have the advantage. Conversely, the talent shortage remains an obstacle to contending with the increasing capabilities

of cyber-threat actors. Despite the promises of AI and big data to augment the workforce gap, humans remain indispensable in providing the strategic context to enhance threat analysis. Viewing cybersecurity through a human-security lens will aid policymakers in striking the right balance between progress and parity in crafting regulatory frameworks and engaging in capacity-building.

Ultimately, the borderless nature of cyberattacks underscores the strategic imperatives of cybersecurity that further warrant a collective response. While there is no silver bullet, government policymakers, industry representatives, and academic experts will have to grapple with the prevailing trust deficit and talent shortage. Such a reality should prompt deeper reflections to build lasting partnerships in Southeast Asia that advance coordinated, but also inclusive, responses against cyber insecurities through more robust and trusted information-sharing and incident or threat-management strategies.

Adrian Glova and Mark Bryan Manantan

Assessing the Economic Benefits of Cybersecurity Standards in Southeast Asia

Introduction

This chapter outlines the economic imperatives of adopting international technical standards and frameworks on cybersecurity, referred to here as cybersecurity standards. Based on the outcomes of the Cyber ASEAN country consultations across Indonesia, Malaysia, the Philippines, and Viet Nam, there is a positive understanding of the utility of cybersecurity standards to ensure stability and security in the cyber realm. Participants consider it as the first line of defense that protects private information and prevents data breaches in critical sectors such as

banking and finance, information and communications technology, energy, water, transportation, and health.

But in addition to warding off potential cybersecurity threats, the protection of critical national infrastructure also comes with tremendous economic advantages.[1] The benefits of cybersecurity standards adoption on economic performance are well-documented in the extant literature, including but not limited to (i) facilitating trade and investment, (ii) spurring innovation and technology transfer, (iii) encouraging good management and conformity practices, and (iv) mitigating risks to operational disruptions (ISO, 2017[2]; ISO, 2021[3]; ISO, 2022)[45] . Existing studies found the potential benefits of cybersecurity standards[6] through case analysis of compliant firms/industries or with accounting approaches, i.e., examining the supply value chain and financial statement analysis. This chapter builds on the existing literature, offering a unique approach, and examines the correlation between cybersecurity standards adoption and value-added output through country-level time-series regression models. It aims to determine the estimated magnitude and direction of association between cybersecurity standards adoption and economic performance among Indonesia, Malaysia, the Philippines, and Viet Nam.

This chapter directly responds to the feedback and observations raised by key stakeholders during the country consultations to build a persuasive economic policy or business case for Cyber ASEAN. Although there is a slight improvement, elevating cybersecurity awareness as a top policy or business priority either in the political or business communities remains an uphill challenge in Southeast Asia. As noted in the proceeding country chapter reports, governments continue to underspend on cybersecurity, while the private sector often views it as an additional cost. The quantitative findings and results of this chapter will compel policymakers and business leaders among the four countries and the rest of Southeast Asia toward the sustained and increased adoption of international technical standards and cybersecurity frameworks—a key pillar in the Cyber ASEAN framework.

Modelling Framework and Data Description

As mentioned, this chapter models economic performance as a function of the independent variable cybersecurity adoption, as well as control variables that affect economic activity, such as (i) interest rates, (ii) gross capital formation, (iii) total exports, (iv) total imports, and (v) a COVID-19 dummy variable.[7] Interest rates reflect the cost of borrowing money and global economic conditions as proxied by the one-year Treasury bill rate. Gross capital formation captures the amount of expenditure that goes into investment as opposed to consumption, while total exports and imports account for the economic openness of countries. Mathematically, economic performance may be taken as a function of said variables such that:

Economy = f(cybersecurity, investments, exports, imports, interest rates)

Table 1 summarizes the data sources for the variables that capture economic conditions. Note that macroeconomic data were obtained from the respective national statistics offices of the four pilot countries for Cyber ASEAN, while financial market data on Treasury bill rates were collated from *Investing.com*. All four countries had publicly available data in quarterly intervals except for Viet Nam, whose national accounts were presented in annualized values. All data related to prices and values were obtained in constant terms (i.e. in real instead of nominal terms) so that figures are adjusted for inflation. With data quoted in the same base years, real changes in output may be observed rather than mere changes in prices. This is also the reason why the dataset was limited to the years 2010 up to 2022, since most of the countries have complete price-adjusted data in this time horizon.

TABLE 1

Control Variables for Economic Performance

Country	Variables Considered	Data Sources	Frequency
Philippines	- Gross Capital Formation - Exports - Imports - 365-day Treasury Bill Rates	Philippine Statistics Authority; Investing.com for interest rates	Quarterly
Indonesia		Badan Pusat Statistik Indonesia; Investing.com for interest rates	Quarterly
Malaysia		Kementerian Ekonomi; Investing.com for interest rates	Quarterly
Viet Nam		General Statistics Office of Viet Nam; Investing.com for interest rates	Annual

To capture adoption of cybersecurity standards, formal executive or legislative action mandating the implementation of cybersecurity standards was considered in the period 2010 to 2022, the relevant data set and study period. Table 2 summarizes the milestones used for each country:

TABLE 2

Basis for Cybersecurity Standards Adoption

Country	Standards Adoption Metric	Time Period
Philippines	Launch of National Cybersecurity Plan 2022; Memorandum Circular 005-2017; Memorandum Circular 006-2017; Memorandum Circular 007-2017[8]	Q1 2017
Indonesia	Implementation of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 standard for information security management systems that is adapted to Indonesia National Standard (SNI)[9]	Q1 2016

Country	Standards Adoption Metric	Time Period
Malaysia	Adoption of ISO/IEC 27001:2013 Information Technology, Security Techniques, and Information Security Management Systems Requirements[10]	Q1 2013
Viet Nam	Legislation of Cyber Security Law, numbered 24/2018/QH14	Q2 2018

In the language of statistical modelling, a dummy variable was generated whose value is equal to one for time periods succeeding cybersecurity standards adoption (and whose value is equal to zero for time periods preceding it). This was done for each country, and these dummy variables were incorporated into the time-series regression models to estimate the effect of cybersecurity adoption on economic performance.

Meanwhile, Gross Domestic Product (GDP) was used to proxy the overall economic performance of a country. GDP is the aggregate value of goods and services produced within the borders of a country. On the production side, it is the combined gross value-added (GVA) output of the major sectors in an economy, namely agriculture, industry, and services. GDP may also be treated as the total consumption in an economy, considering household consumption, investment (or gross capital formation), government spending, and net exports (exports minus imports). Again, GDP data and related indicators were extracted from the respective countries' national accounts.

At a sectoral level, the GVA of certain industries was utilized to measure economic performance coinciding with cybersecurity standards adoption. This way, the correlation between cybersecurity standards adoption and economic activity may be tested in the general (i.e. total economic output) and the particular (i.e. industry-level output) sense. Another advantage of using data from national accounts is that the accounting techniques and measurements are standardized and maintained by international organizations[11] which member states adhere to. This ensures data integrity, while allowing comparisons of regression results for the different countries. Table 3 summarizes the variables and data sources related to the economic performance of each country.

TABLE 3

Economic Performance Variables

Country	Variables Considered	Data Source	Frequency
Philippines	- GDP - GVA in Information and Communication - GVA in Financial and Insurance Activities - GVA in Human Health and Social Activities - GVA in Transportation and Storage - GVA in Electricity, Steam, and Waste Management - GVA in Manufacturing	Philippine Statistics Authority[12]	Quarterly
Indonesia		Badan Pusat Statistik Indonesia[13]	Quarterly
Malaysia		Kementerian Ekonomi[14]	Quarterly
Viet Nam		General Statistics Office of Viet Nam[15]	Annual

Empirical Methodology

Time-series regression models were estimated to obtain the statistical relationship between adoption of cybersecurity standards and economic performance. Time-series models take observations sequenced over time to draw relationships between variables. In this study, we regress economic performance against adoption of cybersecurity standards, along with control variables on economic conditions. A total of 28 time-series regression models were estimated (four countries with seven proxies for economic performance) with the specification:

$$\textit{Economic Performance}_t = \beta_0 + \beta_1 \textit{Cybersecurity Standards}_t + \beta_2 \textit{Investments}_t + \beta_3 \textit{Imports}_t + \beta_4 \textit{Exports}_t + \beta_5 \textit{Interest Rates}_t + \beta_6 \textit{COVID}_t + \varepsilon_t \quad (1)$$

where the error term follows an autoregressive moving average (ARMA) structure to account for dependencies over time such that:

$$\varphi(B)\varepsilon_t = \theta(B)a_t \text{ where random shocks } a_t \sim WN(0, \delta^2) \quad (2)$$

The statistical parameter β_1 captures the direction and magnitude of the correlation between cybersecurity standards adoption and economic performance. In running the time-series regression models, standard diagnostics and procedures were followed to ensure the reliability of results (i.e. stationarity, autocorrelation, and conditional heteroskedasticity were considered in the models). Construction of the time-series regression models with ARMA errors is summarized in Table 4.

TABLE 4

Time-Series Regression Modelling Approach

Step	Purpose	Diagnostics
Step 0: Data Preparation Stage	Ensure stationarity of dependent, independent, and control variables If variables are non-stationary, transformations are conducted (i.e. difference of logarithms)	- Historical Plot - Augmented Dickey-Fuller Test
Step 1: Identification	Choose candidate model with Autoregressive Moving Average (ARMA) errors	- Estimated Autocorrelation Function (ACF) - Estimated Partial Autocorrelation Function (PACF)
Step 2: Estimation and Hypothesis Testing	Estimate the parameters of the model at Stage 1	- T-tests - F-test - ARMA Roots Graph/Table

Step	Purpose	Diagnostics
Step 3: Diagnostic Checking	Check the adequacy of candidate model(s)	- Ljung-Box Autocorrelation Test - Jarque-Bera Residual Normality Test - Autoregressive Conditional Heteroskedasticity Test
Step 4: Model Selection	Select final model	Model R^2, Akaike Information Criterion, Log-likelihood

Furthermore, long-run relationships were examined among the variables for each country model. This is called a cointegrating regression. Cointegration means that although short-run developments can cause permanent changes in the individual time series, there is a long-run equilibrium relation tying the time series. If evidence for cointegration is found, then two models will be estimated to capture: (i) the long-run equilibrium relationship between variables or the cointegrating regression; and (ii) a correlation model in the first differences to estimate short-run dynamics or an error correction model. These are represented in equation form below:

Long-run model in the levels of the variable:

$$\textit{Economic Performance}_t = \beta_0 + \beta_1 \textit{Cybersecurity Standards}_t + \beta_2 \textit{Investments}_t + \beta_3 \textit{Imports}_t + \beta_4 \textit{Exports}_t + \beta_5 \textit{Interest Rates}_t + \beta_6 \textit{COVID}_t + \varepsilon t_t \quad (3)$$

Short-run Error Correction Model in the first differences of the variables where $\hat{\varepsilon}_{t-1}$ is the error correction term from the long-run model:

$$\Delta\textit{Economic Performance}_t = \beta_0 + \beta_1 CS_t + \beta_2 \Delta\textit{Investments}_t + \beta_3 \Delta\textit{Imports}_t + \beta_4 \Delta\textit{Exports}_t + \beta_5 \Delta\textit{Interest}_t + \gamma\hat{\varepsilon}_{t-1} + u_t \quad (4)$$

The steps for this long-run analysis are outlined in Table 5.

TABLE 5:

Cointegration Long-Run Equilibrium Approach

Step	Purpose	Diagnostics
Step 1: Checking for Long-Run Relationship	Check if the variables have a long-run equilibrium	- Engle-Granger Test
Step 2: Cointegrating Regression	If a long-run relation exists, fit a cointegrating regression. For the short-run, fit another model in their first differences with the error correction term	- T-tests - F-test
Step 3: Diagnostic Checking	Check the adequacy of candidate model(s)	- Ljung-Box Autocorrelation Test - Jarque-Bera Residual Normality Test - ARCH Test for Conditional Heteroskedasticity
Step 4: Model Selection	Select final model	Model R^2, Akaike Information Criterion, Log-likelihood

Results and Discussion

The charts below display the historical trend of GDP by country. Economic performance has been steadily increasing as measured by aggregate output, except in the time of COVID-19. The same observation can be made for sector specific GVA, though the graphs are omitted for brevity. For this reason, diagnostic checks for stationarity must be implemented to account for trends over time. This will prevent the scenario of arriving at spurious correlations (i.e. that economic output is positively related to cybersecurity standards adoption when economic activity is just trending upward over time). Likewise, the aforementioned control variables on economic activity have to be introduced to the models so we can adequately estimate the relationship between cybersecurity standards adoption and economic performance.

FIGURE 1

Philippine Quarterly GDP, 2010 to 2022

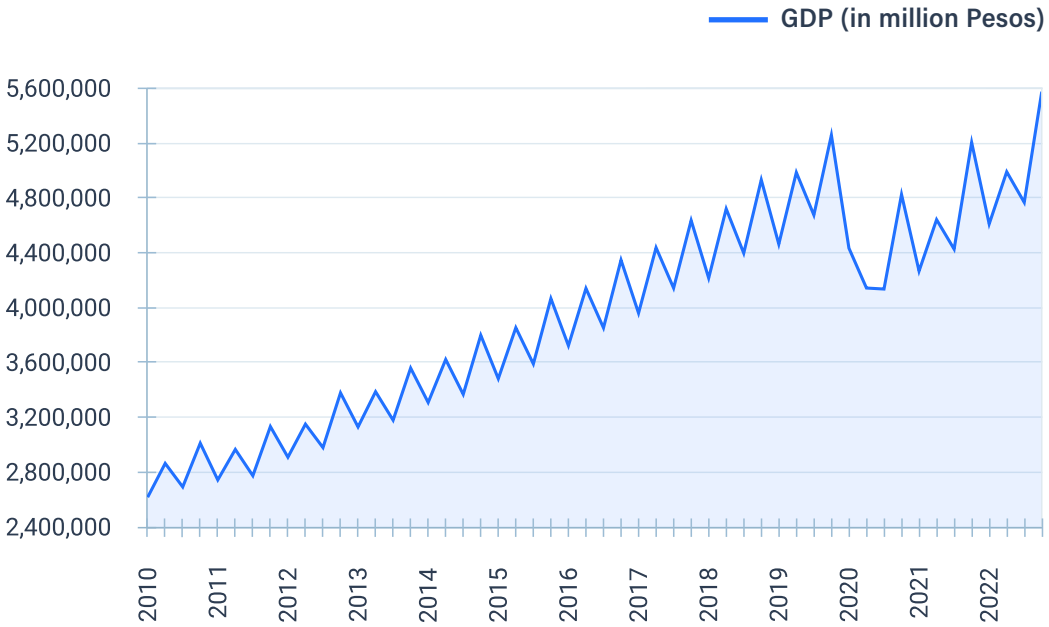


FIGURE 2

Indonesia Quarterly GDP, 2010 to 2022

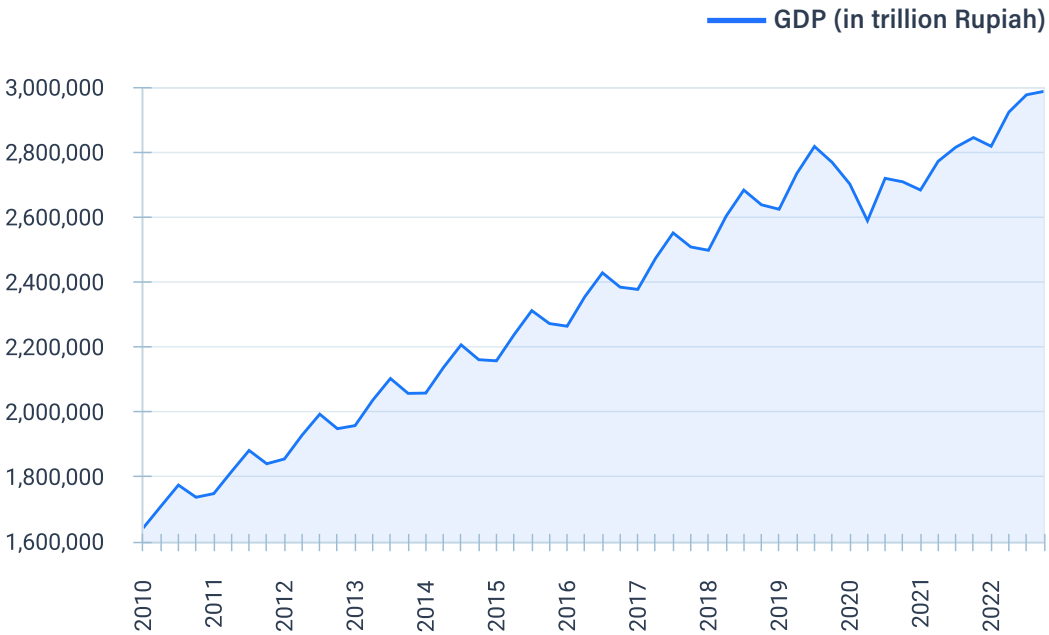


FIGURE 3

Malaysia Quarterly GDP, 2010 to 2022

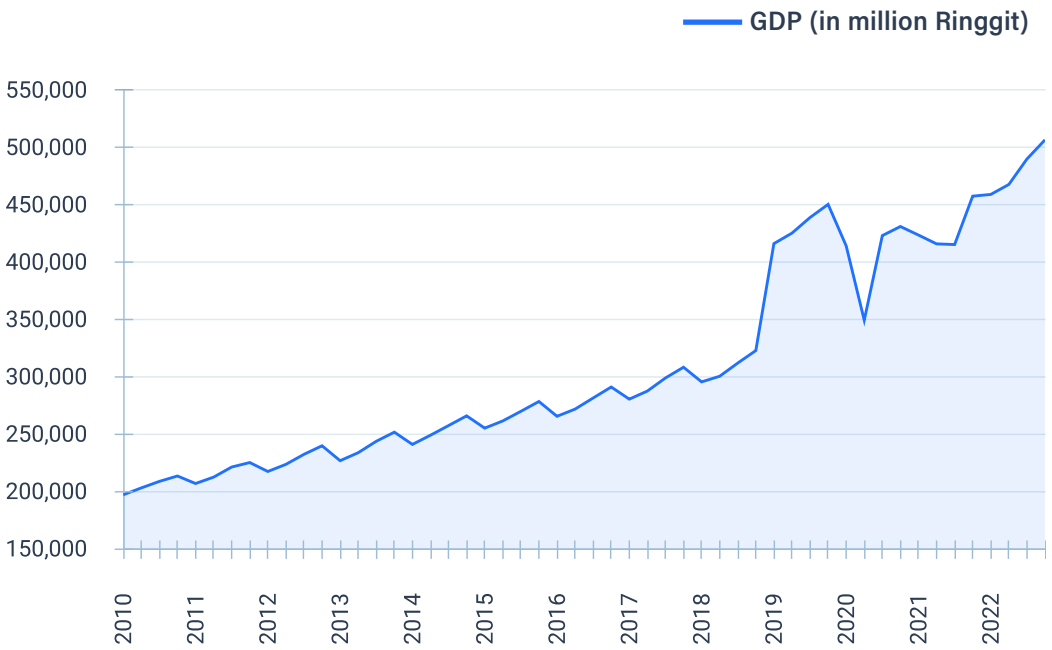
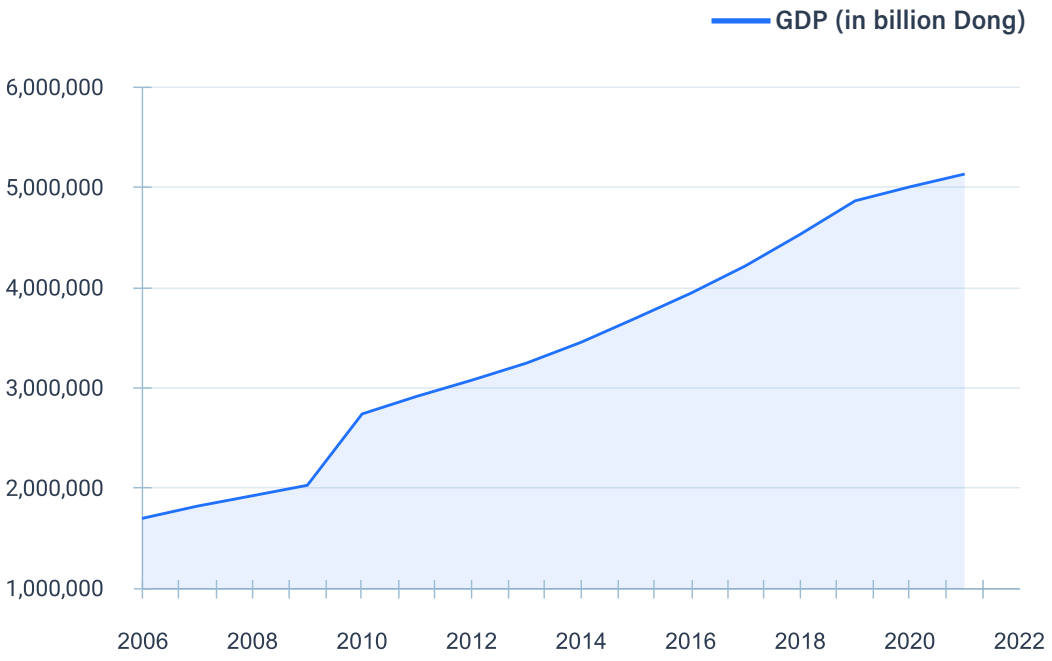


FIGURE 4

Viet Nam Annual GDP, 2010 to 2022



Tables 6 to 9 show the results of the estimated relationship between cybersecurity standards adoption and economic performance per country. The regression outputs for the relevant models for different indicators of economic performance may be found in the Annex (Tables A1 to D2).

A long-run relationship (i.e. cointegrating regression) was only found in the case of the Philippines. Likewise, for the regular time-series regression models, the interpretations are in terms of percent changes due to a requirement in statistical modelling.[16] Another qualification is that regression models obtain correlations such that two variables move in the same or opposite direction. This does not necessarily mean that changes in the dependent variable (i.e. economic performance) are solely attributable to the independent variable (i.e. cybersecurity standards adoption). In short, correlation is not causation.

The regression results for the Philippines may be found below. Through an Engle-Granger Cointegration Test, a long-run relationship was uncovered between cybersecurity standards adoption and economic performance (as proxied by GDP). In the long-run, the two variables are related such that quarterly GDP increased by PhP274 billion, on average, in the period after cybersecurity standards adoption was implemented. Again, while these results are not causal, they provide evidence that cybersecurity standards adoption contributed to greater economic output in the Philippines.

In the short-run through the error correction model (ECM), cybersecurity standards adoption was found to be correlated with a 0.0008 percentage points (ppt) increase in quarter-on-quarter GDP growth. Cointegration suggests that there might be deviations from the long-run equilibrium, as captured by the ECM, but the variables will converge to the long-run relationship over a longer time horizon (as represented by the cointegrating regression). Other proxies for economic performance suggest that cybersecurity standards adoption is associated with increased quarter-on-quarter GVA growth in Information and Communications Technology (+0.005 ppts). These results were found to be statistically significant at the 5% level. At the outset, these values may seem minimal, but consider that the quarterly GDP of the Philippines is at about US$72 billion and the sectoral output would also go into the tens of billions of dollars. In this sense, the impact is still significant.

DICT MC 005 requires the adoption of the Philippine National Standard (PNS) ISO/IEC 27000 Family of Standards and other relevant international standards for mandatory compliance. Specifically, it orders all government agencies to adopt the Code of Practice stipulated in the PNS ISO/IEC 27002 (Information Technology–Security Techniques–Code of Practice for Information Security Controls). Further, the PNS on Information Security Management System (ISMS) ISO/IEC 27001 is required to be implemented for mandatory compliance by all CII operators. Other sectors not classified as CIIs are advised to adopt the PNS ISO/IEC 27002 voluntarily.

TABLE 6

Cybersecurity Standards Adoption and Economic Performance of the Philippines

Type of Model	Proxy for Economic Performance	Estimated Effect of Cybersecurity Standards Adoption
Long-run Relationship (Cointegrating Regression)	GDP	Positively correlated (+PhP274 billion on average)
Short-run Relationship (Error Correction Model)	GDP	Positively correlated (+0.0008 ppts increase in QoQ GDP growth)
Time-Series Regression	GVA in Information and Communications Technology	Positively correlated (+0.005 ppts increase in QoQ GVA growth)

As for Indonesia, cybersecurity standards adoption was positively associated with growth in GVA in multiple sectors, namely: (i) Financial and Insurance Activities (+0.007 ppts), (ii) Electricity, Steam, and Waste Management (+0.029 ppts), (iii) Information and Communications Technology (+0.003 ppts), and (iv) Human Health and Social Activities (+0.004 pts). These findings are not surprising considering the implementation of Ministry of Communications and Information Technology (MCIT) Regulation No. 4 of 2016, which mandates the implementation of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 standard as an international reference for information security management systems that are adapted to the Indonesia National Standard (SNI). This covers all firms in the public and private sectors, thus affecting multiple industries.

The increase in GVA for Information and Communications Technology may also be due to Indonesia having the largest digital economy in ASEAN, accounting for around US$77 billion in 2022, about 40% of the market share in Southeast Asia.

TABLE 7

Cybersecurity Standards Adoption and Economic Performance of Indonesia

Type of Model	Proxy for Economic Performance	Estimated Effect of Cybersecurity Standards Adoption
Time-Series Regression	GVA in Financial and Insurance Activities	Positively correlated (+0.007 ppts increase in QoQ GVA growth)
Time-Series Regression	GVA in Electricity, Steam, and Waste Management	Positively correlated (+0.029 ppts increase in QoQ GVA growth)
Time-Series Regression	GVA in Information and Communications Technology	Positively correlated (+0.003 ppts increase in QoQ GVA growth)
Time-Series Regression	GVA in Human Health and Social Activities	Positively correlated (+0.004 ppts increase in QoQ GVA growth)

For Malaysia, cybersecurity standards adoption was positively associated with growth in GVA in multiple sectors, namely: (i) Information and Communications Technology (+0.003 ppts), and (ii) Human Health and Social Activities (+0.004 pts). On the aggregate, it was also related to a +0.0006 percentage points increase in quarterly GDP. While the increase in values might seem marginal, note that the quarterly GDP of Malaysia is at about US$90 billion, with the GVA output of its sectors also being valued at billions of dollars. The positive relationship between cybersecurity standards adoption and economic performance may be due to the fact that Malaysia had already laid the foundations on cybersecurity enforcement as early as 2006 through the Cyber Security Policy completed by its Ministry of Science, Technology and Innovation. This was only strengthened with the adoption of ISO/IEC 27001:2013 to strictly enforce standards on Information Technology, Security Techniques, and Information Security Management Systems.

TABLE 8

Cybersecurity Standards Adoption and Economic Performance of Malaysia

Type of Model	Proxy for Economic Performance	Estimated Effect of Cybersecurity Standards Adoption
Time-Series Regression	GDP	Positively correlated (+0.0006 ppts increase in QoQ GDP growth)
Time-Series Regression	GVA in Information and Communications Technology	Positively correlated (+0.004 ppts increase in QoQ GVA growth)
Time-Series Regression	GVA in Electricity, Steam, and Waste Management	Positively correlated (+0.006 ppts increase in QoQ GVA growth)

For Viet Nam, note that national accounts data were only available on an annualized basis. Cybersecurity standards adoption was shown to be positively related to quarter-on-quarter GVA growth in Financial and Insurance Activities (+0.01 ppts) and Electricity, Steam, and Waste Management (+0.06 ppts). This may be explained by the country acquiring ISO 27001 and 27002 certifications, which are related to information security, cybersecurity, and privacy protection.
Viet Nam's standardization system comprises 70 national standards, overseen by multiple government agencies (e.g. Ministry of Information and Communications, Ministry of Science and Technology).

TABLE 9

Cybersecurity Standards Adoption and Economic Performance of Viet Nam

Type of Model	Proxy for Economic Performance	Estimated Effect and Interpretation
Time-Series Regression	GVA in Financial and Insurance Activities	Positively correlated (+0.01 ppts increase in QoQ GVA growth)
Time-Series Regression	GVA in Human Health and Social Activities	Positively correlated (+0.03 ppts increase in QoQ GVA growth)

Overall, the results show that cybersecurity standards adoption is associated with improvements in total economic output for the Philippines and Malaysia. For a sectoral-specific analysis, cybersecurity standards adoption was found to be positively associated with GVA in Financial and Insurance Activities (Indonesia and Viet Nam), Information and Communications Technology (the Philippines, Indonesia, and Malaysia), Electricity, Steam, and Waste Management (Indonesia and Malaysia), and Human Health and Social Activities (Viet Nam). Many of the mechanisms through which cybersecurity standards adoption has improved economic performance, both in the total and sectoral sense, have been discussed in the individual country reports.

Conclusion

To further explore the research question and truly isolate the causal impact of cybersecurity standards adoption on economic performance, firm-level survey data may be obtained from the four pilot Cyber ASEAN countries. The advantage of a macroeconomic approach, which this chapter adopted, is that national accounts data are readily available (i.e. aggregate output through GDP, sectoral output through industrial GVA). However, many other factors mediate changes in macroeconomic indicators such as geopolitical conditions, global financial developments, and country-specific macro-fiscal policies.

Having disaggregated data on foreign direct investments (FDIs) would also provide another indicator for sectoral output aside from GVA. FDIs may better capture innovation and technology transfer, factors that are outside the purview of GVA as it purely investigates production. It's also worth collecting data on damage/disruptions to operations due to cyberattacks, perhaps through a firm-level survey, as this is another dependent variable that is worth modeling aside from economic performance.

Finally, panel regression models may be utilized to arrive at a regional interpretation of the impact of cybersecurity adoption on economic performance in the ASEAN region. The models in this paper are fitted *per country* as pooling data will result in small sample sizes. Having access to firm-level panel data across different countries would address this issue and provide richer insights. Nevertheless, the findings and results of this chapter build a strong case for the economic and strategic imperatives of cybersecurity. It can aid policymakers and decision-makers when conducting cost-benefit analyses, especially on the importance of raising more awareness, allocating funding resources, and providing incentives to fast-track the adoption of cybersecurity standards.

PART II_

APPLICATION OF CYBER ASEAN

Fitri Bintang Timur

Indonesia

Overview

Indonesia's digital economy is booming. As proof of such positive momentum, its digital industry value has increased from US$41 billion in 2019 to US$77 billion in 2022 and is expected to further rise to US$125 billion by 2025.[1] While digitalization plays an important role in advancing Indonesia's economy, the increasing interconnectivity in the country's critical national infrastructure also creates more cyber-threat vulnerabilities that could disrupt its current trajectory. Incidents that involved scams, data leaks and intelligence gatherings, intrusions through vulnerable outdated platforms and software, and the lack of digital literacy and skills have been reported on extensively.

With 212.9 million registered internet users in 2023, yet with the lowest cybersecurity resilience among the G20 countries, there is no doubt that malicious

cyber-threat actors have been preying on Indonesia.[23] In 2022, the National Cyber and Crypto Agency (BSSN) recorded approximately 976 million traffic anomalies. Although the figures show a decline from 1.6 billion anomalies in 2021, they are still a cause for concern given the rapid utilization of advanced technologies, including artificial intelligence.[4] In response, Indonesia issued Presidential Regulation No. 82 of 2022 on Protection for Vital Information Infrastructure,[5] which specifies the country's strategic sectors.[6] More recently, Indonesia also released Presidential Regulation No. 47 of 2023 on National Cybersecurity Strategy and Cyber Crisis Management.

Indonesia has established mechanisms to protect information and infrastructure from malicious activity through the promulgation and enforcement of laws and regulations. Yet, until the end of 2023, Indonesia had no law dedicated to cybersecurity and mainly relied on Law No. 11 of 2008 on Electronic Information and Transactions (*Informasi Transaksi Elektronik* – ITE Law).

The law regulates transactions and information transmitted through digital means and unauthorized remote access to computer systems, as well as the distribution, transmission, and/or production of electronic information that contains disinformation, insults, and/or defamation. The law was revised twice, in 2016 and early 2024. Due to increasing geopolitical tensions and the 2024 election, regulatory discussions of the second revision were held privately to minimize conflicting interests, which consequently raised concerns about the quality and effectiveness of the revised law.

The prevalence of data breaches concerning election information, national passport directories, and online shopping databases in recent years compelled Indonesia to issue the Personal Data Protection Law (PDP Law) in 2022, which regulates how personal information data is obtained, stored, and managed. The law is modelled on the European Union General Data Protection Regulation (EU GDPR) and is expected to improve Indonesia's standing from being one of the top three countries experiencing the highest number of data breaches in Q3 2022 after Russia and France.[7] The law makes Indonesia the fifth country in Southeast Asia to enact cybersecurity laws, following Singapore, Malaysia, Thailand, and the Philippines.[8]

After years of regulatory absence, the PDP law regulates the protection of content by cybersecurity, and covers some key features including data subjects, processing personal data, exemptions, and extraterritorial impact. It also mandates that organizations or corporations are subject to hefty fines of up to two percent of revenue for failure to notify the data subject and authority within 72 hours of a data breach.[9] This makes small and medium businesses wary of the cost of non-compliance. The law will be fully implemented in October 2024. Although many welcome such a positive development, the move can be regarded as coming quite late, especially for a country that often prides itself on being a leader of ASEAN.

International Collaboration

Indonesia considers itself to be a proactive cyber-diplomacy actor. In the regional and international spheres, it aspires to achieve "safe, peaceful, and open cyberspace, while increasing national cybersecurity capacity."[10] As an active member of ASEAN, Indonesia initiated the ASEAN political-security pillar and has supported ASEAN Member States (AMS) like Singapore in addressing transnational crime, including cybercrime. Through various ASEAN mechanisms, Indonesia has been working actively to bolster the development of ASEAN cybersecurity cooperation. Additionally, it also contributes to the ASEAN Regional Forum (ARF) discussions on cybersecurity, the ASEAN Defense Ministers' Meeting (ADMM)–Plus Experts' Working Group (EWG) on Cyber, including various training initiatives, and more recently, the development of a regional-level Computer Emergency Response Team known as ASEAN-CERT.

The 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation is considered as a key strategic document on cybersecurity cooperation in the region. In the document, the AMS acknowledged that both state sovereignty and international norms and principles apply to states' conduct in ICT-related activities and to their jurisdiction over ICT infrastructure within their territories. The document highlighted the significance of the concept of state sovereignty for AMS. States affirm their commitment to international norms and principles derived from that concept and apply them to any ICT-related activities.[11]

At the international level, Indonesia has been actively engaged in cybersecurity discussions. For instance, in 2020, Indonesia, along with Estonia, Belgium, Kenya,

and the Dominican Republic, co-sponsored an Arria-formula Meeting of the UN Security Council that stressed the importance of cyber stability and international cooperation against cyber threats, especially with the increasing digitalization during the COVID-19 pandemic. During the meeting, Indonesia highlighted the significant role of regional organizations in preventing cyber conflicts, especially through confidence-building measures (CBMs).

Indonesia also believes that the implementation of international law and cyber norms is necessary to complement the technical aspects of ICT. This is showcased in its active participation in the formulation of global cyber norms within the framework of the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies, which involved all members of the UN and was firstly mandated from 2019 to 2020 and subsequently renewed from 2021 to 2025. Additionally, Indonesia has shown its commitment and leadership in strengthening the formulation of cyber norms through its membership in the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the context of international security (Cyber GGE) from 2019 to 2021.[12] Despite its proactiveness in cyber diplomacy, Indonesia has yet to appoint a cyber ambassador, while its diplomats are still developing their knowledge on cyber diplomacy and negotiations. Indonesian diplomats attended cyber-diplomatic course held by the Netherlands[13] and Australia[14] as ways to build capacity and trust.

International Technical Standards

As it sets its ambitions on digitalization, Indonesia adopts and implements international technical standards to foster cybersecurity resilience. Having the highest digital transaction value in ASEAN, at 40 percent of the entire market of the ten-country association, Indonesia is projected to maintain such a position until at least 2025.[1516] But bundled with the digital economy's perceived benefits is the likelihood of increasing cybersecurity risks. To this end, the Indonesian government puts cybersecurity as one of its national priorities, including the adoption of international technical standards related to cybersecurity management, while also adapting and simplifying them to allow national uptake.[17]

The Ministry of Communications and Information Technology Regulation No. 4 of 2016 mandates the implementation of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 standard as an international reference for information-security management systems that are adapted to the Indonesia National Standard (SNI).[18] Aside from assessing technologies, the standard also assesses human capital such as leadership, planning, support, operation, performance, improvement, and protection of customer data.[19] In the early preparation stage for companies or organizations to adopt the ISO/IEC 27001, Indonesia has its information security index, Indeks Keamanan Informasi (Indeks Kami) introduced in 2007. By 2012 Indeks Kami has already been used by 123 government institutions.[20]

Table on the Comparison between ISO/IEC 27001 and Indeks Kami

International - ISO/IEC 27001	Indeks Keaman Informasi (Kami)
Information Security Policy	Governance
Organisation of Information Security	Risk Management
Asset Management	Asset Management
Human Resources Security	Working Framework
Physical and Environment Security	Technology and Information Security
Communication and Operation Management	
Access Control	
Information System Acquisition, Development and Maintenance	
Information Security Incident Management	
Business Management Continuity	
Compliance	

The ISO/IEC 27001 was iterated periodically, in 2005, 2009, 2013, and lastly in 2022. All versions of ISO/IEC 27001 adopted nationally received positive responses on their effectiveness and efficiency. The national standards adaptation gives

local organizations more flexibility to develop their own information-security management systems since the standard does not specify any specific approach or method.

In ensuring cybersecurity standards are being followed, all electronic systems providers operating in Indonesia must register themselves with the government and obtain standardization certification from National Cyber and Crypto Agency (BSSN) assessors using Indeks Kami.[21] The BSSN also manages a Professional Certification Agency through multistakeholder collaboration with public, private, and academic entities operating in Indonesia's territory, including with various government ministries, such as the Ministry of Manpower, the Ministry of Tourism, and the Ministry of Communications and Information Technology, to enforce standardization.[22] The BSSN also issues workforce expertise certifications for roles such as Chief of Information Security Officer (CISO), Cyber Risk Specialist, Cybersecurity Administrator, Cyber Forensic Specialist, Network Security Manager, and Information Security Auditor. All business entities are required to adopt the government-recommended national cybersecurity standards and industry-related guidance. Indonesia's Central Bank issues recommendations for the finance and banking industry, suggesting best practices for security systems and infrastructure that align with international ICT security standards.[23]

However, advancements in technology are not accompanied by a readiness and capacity to adopt international cybersecurity standards. Some challenges constrain the effective adoption of international standards, such as (1) different understanding and approaches toward cyber security, whereby many actors in cyberspace have contrasting perspectives, policy interests, and priorities in interpreting cybersecurity; (2) human resources capacity constraints caused by the digital divide and lack of human resources in the field of information security. In Indonesia, foreign workers dominate in the field of IT and cybersecurity since local expertise is still very low, and; (3) lack of collaboration, whereby private sector and civil society organizations only participate passively in multistakeholder engagements.[24]

Although the country has also bolstered its Critical Information Infrastructure Protection (CIIP), which covers the ICT, food, finance, defense, health, government, energy, mineral resources, and transportation sectors, it was noted during the Cyber

ASEAN consultation that not all electronic system providers can comply with the relevant standards. Some stakeholders argued that the need to implement new technologies is considered more pressing than ensuring compliance, and adopting standards also takes time.

During its G20 chairmanship in 2022, Indonesia endeavored to collaborate with international standards bodies like the International Electrotechnical Commission (IEC), International Organization for Standardization (ISO), and International Telecommunication Union (ITU), to urge world leaders to recognize and adopt international standards to meet the G20 goals defined under the theme of "Recover together, recover stronger." The International Standards Summit was convened by the National Standardization Agency of Indonesia (BSN) with the participation of the World Trade Organization (WTO) on October 2022.[25] Through the G20 discussions, the Indonesian government stressed the important role of international standards in fostering digital transformation, which has become essential since COVID-19.

The adoption of international cybersecurity standards has also been promoted at the regional level through ASEAN. The ASEAN Cybersecurity Cooperation Strategy (2021-2025) emphasizes the adoption and promotion of international cybersecurity standards to make sure the increased use of emerging technology is secure. In this sense, cyberspace should be interoperable and promote common security standards and frameworks, as well as sharing best practices.[26] The ASEAN Digital Senior Officials' Meeting and Ministers' Meeting (ADGSOM/ADGMIN) is the sectoral body tasked to lead the promotion of international cybersecurity standards, including emerging technologies such as 5G and the Internet of Things (IoT). Given that the proliferation of smart devices will expand attack surfaces, common standards could be promoted to collectively raise the security levels of consumer IoT devices. Therefore, the region aspires to harmonize technical standards with dialogue partners, such as Japan and Australia.

To secure emerging technologies through the adoption of international best practices and standards, ASEAN has jumpstarted several initiatives such as: (1) developing regional cybersecurity standards for IoT, led by the ASEAN Network Security Action Council (ANSAC); (2) establishing regional cybersecurity

procedures and guidelines for 5G and IoT implementation, led by ADGSOM/ADGMIN and the ASEAN Telecommunications Regulators' Council (ATRC); (3) initiating regional cybersecurity policies, procedures, and guidelines for SMART City implementation, led by the ASEAN Smart Cities Network (ASCN) in coordination with ANSAC; and (4) conducting capacity-building activities on digital infrastructure product as well as software security testing and certification, led by ANSAC.[27] Despite ASEAN having many discussion channels on cybersecurity, which takes time and resources, Cyber ASEAN's Indonesia consultation noted that there is an urgent need to consolidate Southeast Asian countries' views amid the competing models and visions of internet governance and standardization.[28]

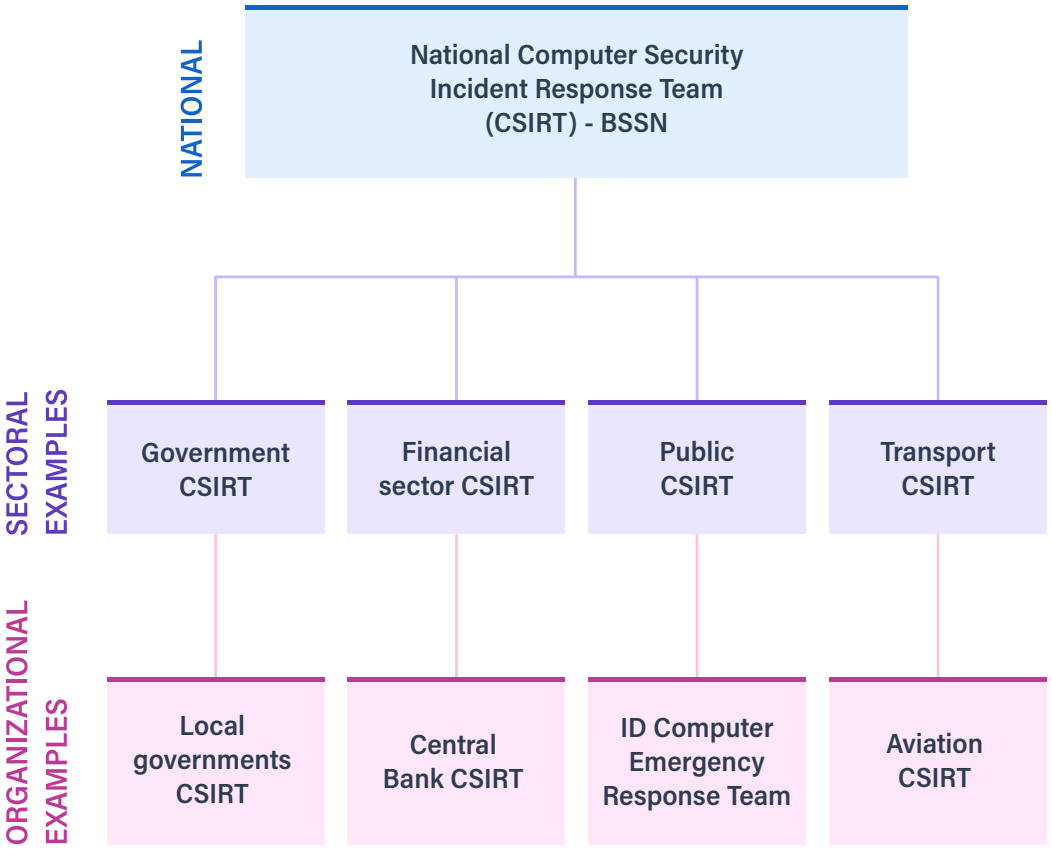
Information-Sharing and Incident Management

Indonesian stakeholders address risk and increase cybersecurity awareness through Cybersecurity Information Sharing (CIS) activities. Local and sectoral CIS forums have emerged as collaborative spaces for the private and public sectors to mitigate cyber risks, address incidents, and share best practices. Collaboration among cyber-related communities has been successful in building public awareness, helping identify potential risks, and preventing cyberattacks at an early stage in order to safeguard critical infrastructure.[29]

Presidential Regulation No. 133 of 2017, Article 2 has delegated the BSSN as the main organization tasked to run cybersecurity effectively and efficiently by utilizing, developing, and consolidating all elements.[30] Although the BSSN is in charge of the protection of critical-information infrastructure at the national level, and is responsible for sharing Cyber Threat Intelligence (CTI) information with local and sectoral forums, many of the existing CIS forums have been created ad hoc by the cybersecurity communities and industries, due to necessity. Ideally, the BSSN and the CIS forums should be complementary. The BSSN employs a dedicated automation mechanism for sharing information at both national and sectoral levels through CIS forums, which the latter in turn validate and enrich the shared information, encompassing tactical/technical, operational, or strategic aspects.

Under its national cybersecurity strategy, Indonesia has called for stronger regulations to facilitate public-private partnership collaboration between the government and industry in information-sharing and approval mechanisms in

dealing with cyber threats. So far, collaboration on regulations exists in the health and financial sectors to prevent cybercrime and terrorism funding. Formally, the MCIT established the Information Technology-Information Sharing and Analysis Center (IT-ISAC) in 2018 to support Critical Information Infrastructure Protection.[31] This enriches existing informal CIS forums such as Financial-CIS and the Association of State-Owned Banks.[32] While national-level CIS is carried out by BSSN, sectoral levels have established their own collaborative mechanisms, although still under BSSN. This is shown in the diagram below.



Based on Presidential Regulation No. 82 of 2022 on Protection for Vital Information Infrastructure, Indonesia has established a sectoral Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) that covers the sectors of government administration; energy and mineral resources; transportation; finance; health; information technology and communication; food; and defense sectors. Indonesia has incident-management frameworks that can be used as guidelines in the event of any cyber incident. Frameworks on cyber-incident management aim to quickly detect incidents; accurately diagnose the incident; appropriately manage incidents, defend from attacks, and minimize threats; recover the services to their original conditions; search for the major causes of incidents and; implement system development to avoid incidents from occurring.

Due to the absence of a nationally recognized cybersecurity law, when this paper was written in early 2024, the closest tool to address cyber emergencies was the recently issued Presidential Regulation No. 47 of 2023, which allows the President to legally declare a cyber crisis when it is deemed suitable. The regulation calls for the formulation of a National Cyber Security Action Plan on (1) governance; (2) risk management; (3) preparedness and resilience; (4) strengthening of national protection of vital information infrastructure; (5) national cryptography independence; (6) capability, capacity, and quality enhancement; (7) cyber security policy and; (8) international cooperation. The regulation assigns BSSN to execute cyber-crisis management and undertake preparatory measures, including developing a Cyber Crisis Contingency Plan and conducting simulation scenarios or exercises.

Cyber-crisis Management based on Presidential Regulation No. 47 of 2023			
Preparedness	**Before Crisis**	**Crisis Occurring**	**After Crisis**
Formulating contingency standard procedures	Cyber-incident response preparedness	Cyber-crisis countermeasure	Calculation of damage and losses
Simulation	Cyber-crisis early warning	Cyber-crisis recovery	Calculation of estimated recovery cost
	Cyber-crisis status deliberation	Reporting cyber-crisis handling until termination of crisis status	Evaluation of cyber-crisis handling

The regulation also details stages of addressing cyber crises in order to identify, protect, detect, respond, and recover. The difference between the BSSN cybersecurity framework and the ISO 27001 standard and Indeks Kami that were mentioned above, is that the framework serves as a tool for BSSN and other organizations in Indonesia to effectively manage and mitigate cybersecurity risks associated with their networks and data, while ISO 27001 and Indeks Kami work to enhance organizations' information-security management systems. But more than regulations, fostering a culture of information-sharing is necessary to overcome the prevailing notion of shame associated with the act of reporting or disclosing cyber vulnerability or incidents, because there is a fear of repercussions and reputational damage.[33]

Regarding international collaboration, Indonesia recognizes the importance of working together with key international partners in addressing cyber incidents. The Presidential Regulation No. 47 of 2023 notes explicitly that Indonesia puts international collaboration as one of its cybersecurity strategies and that it is executed through "practical cooperation, information-sharing, and best practices in dealing with crises." The country receives support from the Asia Pacific Computer Emergency Response Team (APCERT) and ASEAN CERT cooperation through periodic incident drills to build capacity and provide early warning mechanisms. As exemplified by the Wannacry 2017 incident, Indonesia's national CERT has immensely benefited from international information-sharing and successfully isolated the attack to only several hospitals.

Public-private partnerships are also key enablers in strengthening Indonesia's information-sharing ecosystem. For instance, Microsoft has played a role in supporting national capacity-building through its initiatives of the Digital Crime Unit and Cyber Threat Intelligence Program. This strategic partnership, formalized in 2022, allows BSSN to access Microsoft's cyber-threat intelligence that tracks malicious actors.[34] The Indonesian government also gained information on Microsoft malware and botnet takedown operations. Likewise, information-sharing is also becoming vital to Indonesia's efforts to establish smart cities. It enables the exchange of best practices to create and sustain cybersecurity infrastructure. For example, Indonesia is collaborating with Germany in developing the Jakarta Smart City and participates in the US-ASEAN Smart Sustainability Mobility program to address transportation challenges while ensuring data privacy.[35]

However, some challenges continue to limit information-sharing practices. Major shortcomings stem from the prevailing assumptions and difficulties in evaluating the necessity and purpose behind data requests and providing timely and accurate responses.[36] In addressing such challenges, Indonesia's ICT conglomerates like Telkom have installed a systematic approach to decision-making through assessment of data necessity, evaluation of data-sharing requests, and options for information-sharing. Unfortunately, fewer cyber-mature institutions have yet to establish standard procedures for conducting information-sharing due to resource constraints and mostly rely solely on personal connection. Informal channels built around the tight-knit community of cybersecurity professionals, most of whom are connected to CERTs and CSIRTs, have become instrumental in plugging such gaps in order to enhance information-sharing, especially during incidents of cyber crisis.[37]

Inclusion

Just like other countries, Indonesia suffers a shortage of cybersecurity talent and therefore makes efforts to facilitate workforce development. The MCIT has developed a standard for talents working in cyber and information security through the Indonesian National Work Competency Standards (*Standar Kompetensi Kerja Nasional Indonesia* - SKKNI). It sets the baseline of technical skills for those who perform information-security functions in organizations.[38] The ministry also conducts digital literacy education on big data analytics, AI, and cloud computing

for a targeted segment of the population and aims to reach 50 million people in 2024.[39]

In collaboration with the private sector, the Indonesian government also provides workforce training, with the example of MCIT partnering with Xynesis International, a cybersecurity company, that offered a youth boot camp in 2019, and the BSSN collaborating with the InfraDigital Foundation and Mastercard for Inclusive Growth that also implemented a cybersecurity course in 2022.[40] This cybersecurity public-private partnership model will be implemented in the Ministry of Defense, Ministry of Maritime Affairs, Ministry of National Education, Bank Indonesia, and state-linked financial institutions, collaborating with private partners in the automotive, telecommunications, banking, and critical information industries.

In addition to reskilling and upskilling, Indonesia also encourages more inclusion with the participation of women, girls, youth, elderly, minority groups, and persons with disability. Indonesia's inclusive approach acknowledges the systemic and individual barriers that need to be addressed. To effectively address inclusion, the government has outlined three types of strategies:

Short-term Strategies:

- Skill Mapping and Assessment: The initial step involves identifying skill gaps and assessing the cybersecurity landscape's needs, ensuring a targeted approach.
- Rapid Training Programs: Offer focused skill development within a short time frame, catering to the urgency of building a skilled workforce.
- Online Resources: Freely accessible online resources, such as webinars, tutorials, and open courseware, were proposed to help individuals quickly upskill and learn about cybersecurity, regardless of their background.
- Partnerships with Security Industries: Collaboration with the industry to provide practical training and exposure to align training with real-world demands.

Medium-term Strategies:

- Structured Training Programs: Expanding from rapid training, comprehensive and structured programs should be developed to cover a broader range of cybersecurity concepts and skills.

- Apprenticeships and Internships: Partnering with companies to offer internships and apprenticeships provides practical experience, connecting aspiring cybersecurity professionals with established experts.
- Certification Pathways: Creating clear pathways for recognized certifications enables professionals to deepen their expertise and commitment to cybersecurity.

Long-term Strategies:

- Educational Reform: Educational systems need to change to allow people with various backgrounds to be educated on digital literacy and cybersecurity. These skills should be taught from early to higher education.
- Research and Innovation: Investing in research and innovation is crucial to stay ahead of evolving cyber threats and technologies, fostering a skilled and adaptive workforce.
- Public-Private Cooperation: Indonesia encourages collaboration between governments, the private sector, academia, and civil society in order to collectively address the digital skills gap and ensure comprehensive skills development.
- Global Operations: International partnerships to share best practices and resources, fostering sustainable cybersecurity skills development on a global scale.

In enhancing women's participation in the field, Indonesia issued the Presidential Instruction on Gender Mainstreaming No.9 Year 2000 to reduce the gap between Indonesian women and men in accessing and obtaining development and increasing participation in and control over the development process.[41] To further accelerate the gender mainstreaming agenda, the BSSN initiated a Women in Cybersecurity network and annual summit to facilitate women working in the sector. The initiative seeks to create a new ecosystem where women will have the same knowledge and capability to participate in the cybersecurity field. Many industries have been joining this initiative such as the telecommunications, banking and education sectors.[42]

Technology and internet access are also a challenge for remote areas in Indonesia, where services available are often unaffordable and unreliable. Populations in far-flung areas have no broadband access and have suffered disproportionately

from the digital divide that further exacerbates the talent shortage in Indonesia.[43] Obviously, the digital divide is a direct result of disparities in access and quality that consequently widen the gap between talent availability and the industry's demand for ICT professionals. This adds layers of challenges to the knowledge gaps between formal education and industry; language barriers and limited access to education; outdated curriculum and learning methods; and availability of infrastructure that supports high-quality learning.[44]

People with disabilities are also neglected in discussions on cybersecurity policy and capacity-building. Konekin, an Indonesian organization that advocates for digital inclusion, has emphasized the vital importance of accessibility in software and hardware development to cater to differing needs. Konekin has found that there is limited screen-reading software and accessible websites and apps in Indonesia for blind individuals. Therefore, it is important for websites, apps, operating systems, and content to have "accessibility guidelines" and should also be "universally accessible" to support mobility and allow equitable access.[45] Indonesia needs to challenge the idea that disability is a personal, not a societal issue. In adopting more inclusive policies, Indonesia would most likely procure and develop accessible technology that will not only benefit people with disabilities but everyone.[46]

Perhaps an emerging yet worrying trend that may stifle inclusion in Indonesia is digital authoritarianism. Civil society organization SafeNet has raised concerns about governments imposing online controls that could impact freedom of expression and public opinion, especially in conflict-prone areas.[47] For instance, the Indonesian government imposed limitations on social media usage through "internet throttling" in Jakarta in May 2019 and Papua in August and September 2019, to prevent further riots after the election result announcement and anti-racism demonstrations that turned unruly. Similarly, in February 2022, the internet in Wadas, a village in Central Java, was cut after a demonstration to protest against a proposed andesite mine took place.[48] As such moves may inadvertently undermine fundamental digital rights, Indonesia is encouraged to take a balanced and more human-centric cybersecurity approach to social media or internet regulations, allowing open internet access and freedom of expression, while maintaining privacy and security.[49]

Conclusion

Reflecting on Indonesia's cyber landscape, it is obvious that the country has benefited significantly from its thriving digital economy and has therefore pushed for more technological adoption. However, to guarantee continuous growth, Indonesia's cybersecurity maturity needs to catch up. If not, Indonesia's critical information infrastructures—the backbone of its economy—will continue to face increasing vulnerabilities. Fortunately, the government has made efforts to improve national cyber capacity through several initiatives that are mainly led by the MCIT and the BSSN.

Such initiatives include setting cybersecurity standards, information-sharing, and capacity-building that involves the public and private sectors, academia, and civil society organizations, including professional/technical associations. Indonesia also actively participates in various regional and international forums to discuss strengthening cybersecurity, such as through ASEAN and the G20.

Despite all the efforts undertaken, Indonesia still needs to seriously confront its cyber vulnerabilities and ensure that it not only has all the necessary regulations in place but also the capacity and resources to implement them. Like other countries in Southeast Asia, Indonesia is a story of contradictions: increasing internet penetration but a growing digital divide, and high investments in digital literacy but flourishing cybercrime. This is where the Cyber ASEAN Framework provides a novel and thorough lens to analyze and address these challenges head-on. Cyber ASEAN is different from other international cybersecurity assessment frameworks because it explores the distinct context of cyber diplomacy, national technical standards, and domestic methods of information-sharing inherent in a specific country. In the case of Indonesia, the framework is relevant because it raises regional collaboration and promotes international norms and standards without undermining its sovereignty.

Policy Recommendations

As shown in the previous sections, the Cyber ASEAN Framework is useful in assessing Indonesia's progress using the framework's four pillars of *international*

collaboration; international technical standards; information-sharing and incident or threat management; and inclusion. Based on the insights gathered from the country consultations plus additional research and interviews, key recommendations are provided below:

1. **Raise Indonesia's profile in standards-setting bodies.** The Indonesian government should increase its participation and activity in international standards discussions in forums such as the IEC, ISO, and ITU beyond its G20 presidency or ASEAN chairmanship. Additionally, Indonesia should be more proactive in engaging in regional and global cybersecurity norm-making processes through the United Nations GGE and OEWG, as well as various groupings to which it belongs such as the Non-Aligned Movement.

2. **Streamline existing collaboration among government and non-governmental stakeholders on information-sharing and incident management.** Indonesia's multistakeholders need to establish a common understanding and shared responsibility for cyber vulnerabilities. The shortfall in coordination will result in the absence of a holistic and comprehensive approach. Without continuous coordination, efforts to addressing cybersecurity will continue to become fragmented. The Indonesian government should take precautionary measures to maximize the protection of cybersecurity for assets and infrastructure that are considered vital to Indonesia's economy. This will also reduce the risk of cyber threats to Indonesia's national security and interests in the cyber domain. Safeguard measures can be implemented by conducting periodic cybersecurity simulation exercises for the existing cybersecurity-related agencies and institutions in Indonesia. Additionally, with the borderless nature of cyberspace, it would also be wise for Indonesia to conduct capacity-building training and simulation exercises with other states in the region, as well as with like-minded countries.

3. **Embrace a pragmatic approach to multistakeholder collaboration.** It is important to include all relevant stakeholders in the process of cybersecurity policymaking and ensure continuous collaboration among government, business, academics/universities, and civil society/population. There is merit in intensifying dialogue between the public and private sectors in regulation formulation, developing a national cybersecurity framework, and simulation exercises for addressing the resources and capacity gap and further improving

legislation. Additionally, the government should also streamline the depth and scope of information to engage the wider public.

4. **Prioritize inclusive cyber policies to benefit marginalized and vulnerable groups and communities.** Indonesia should advocate for the development of global "accessibility guidelines" that businesses can refer to when developing their products. Too much emphasis on the digital economy may obfuscate the reality that Indonesia's rising digital inequity is untenable in the long run. Inclusion should be front and center to ensure the proper distribution of digital growth dividends across Indonesia's emerging data-driven society.

Farlina Said

Malaysia

Overview

Cybersecurity was initially regarded as a technical matter in Malaysia, thus it was approached strictly as an Information Technology (IT) rather than a state-security issue. This perception is rooted in Malaysia's governance structures, legal developments, and strategic postures. For instance, Malaysia's Computer Emergency Response Team (MyCERT) was established in 1997 under MIMOS Berhad, Malaysia's national applied-research and development center in the Ministry of Science, Technology, and Innovation (MOSTI).[1] At that time, MOSTI was not equipped with the legislative mandate or jurisdiction to regulate the private sector. Thus, the story of developing intra-governmental mechanisms for cybersecurity only began after the turn of the millennium.

FIGURE 1

Malaysia's cybersecurity governance in 2014 with separate components for crisis, content, and cybercrime management as well as cybersecurity coordination.[2]

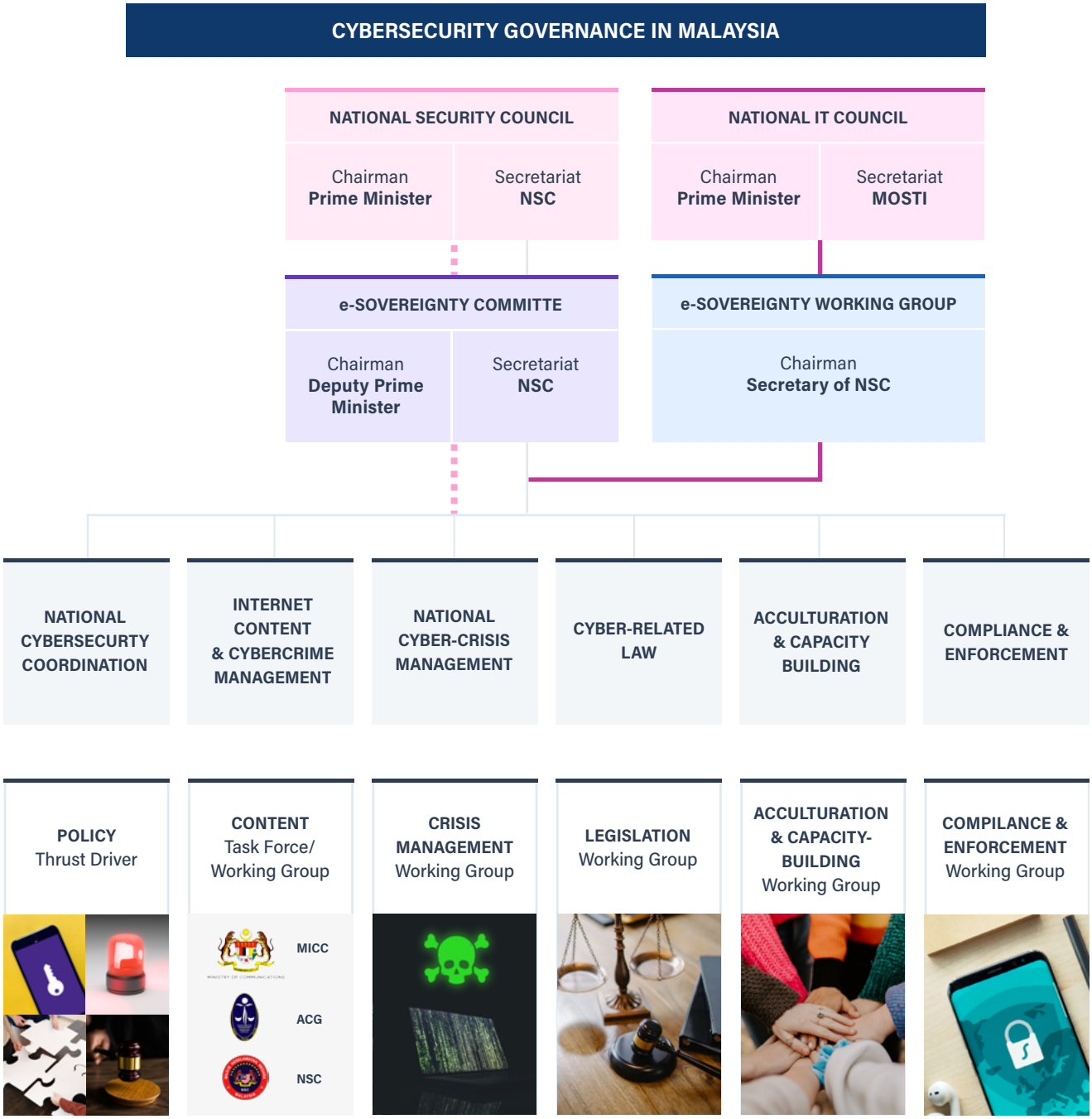
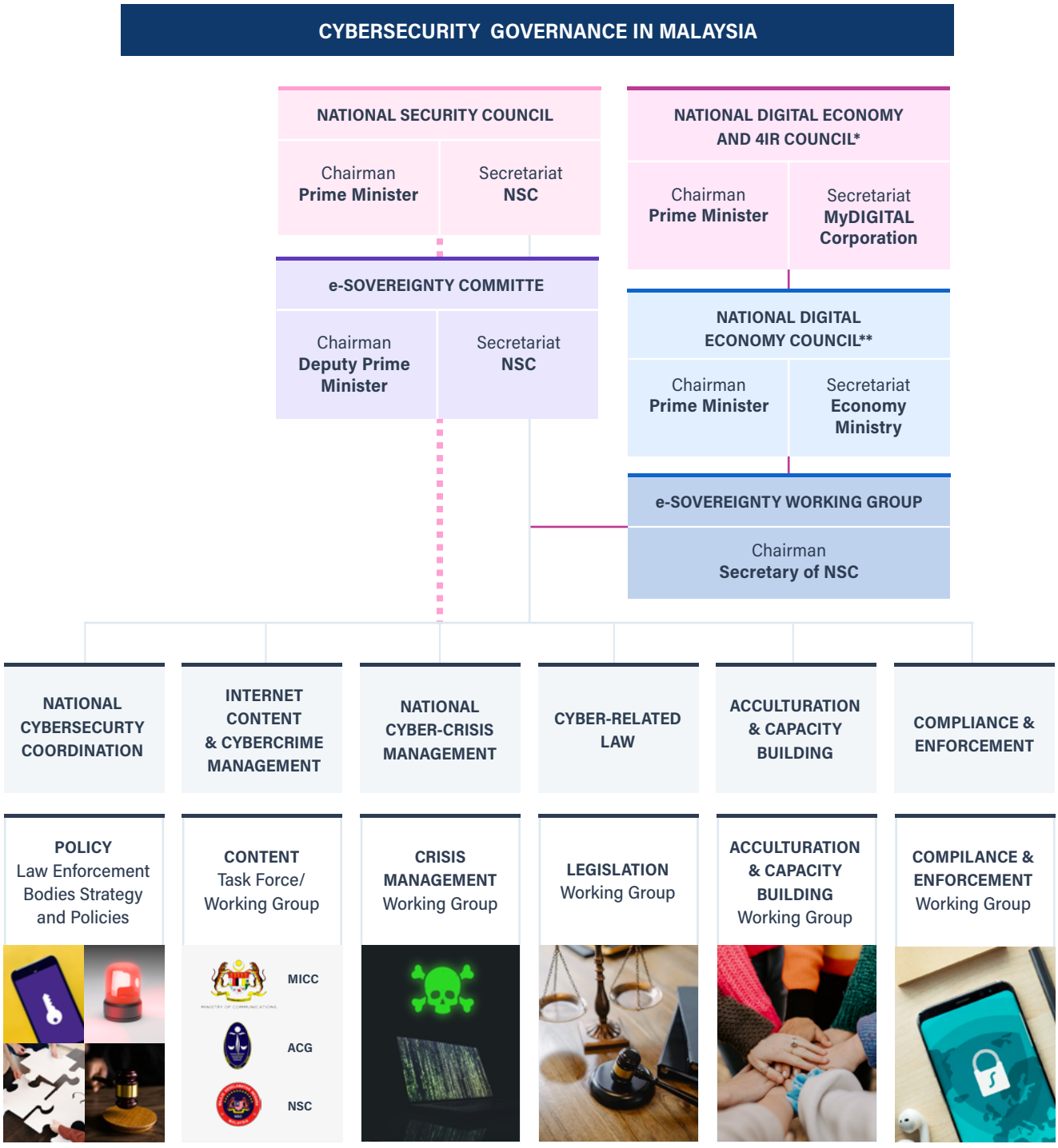


FIGURE 2:

Updated version of Malaysia's cybersecurity governance in 2014 with separate components for crisis, content, and cybercrime management as well as cybersecurity coordination.[3] *National Digital Economy and 4IR Council was announced in 2021 and is tied to the National 4IR Policy, as well as the MyDigital Initiative. **The National Digital Economy Council was announced in 2023



In 2006, Malaysia's first National Cyber Security Policy (NCSP) was completed by MOSTI, which laid down Malaysia's cyber governance utilizing a multistakeholder and multi-sectoral approach. The NCSP identified 10 critical national information infrastructures (CNII) which were National Defense and Security, Banking and Finance, Information and Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services, and Food and Agriculture. Under the updated Malaysia National Cyber Security Strategy 2020-2024, the sectors were updated to 11: (i) Government; (ii) National Defense and Security; (iii) Banking and Finance; (iv) Information and Communications; (v) Energy; (vi) Transportation; (vii) Emergency Services; (viii) Water; (ix) Health Services; (x) Agriculture and Plantation and; (xi) Trade, Industry, and Economy. As such, Malaysia's CNII is defined as those entities whose destruction would have a devastating impact on the (i) national economic strength, (ii) national image, (iii) national defense and security, (iv) government capabilities to function, and (v) public health and safety.[4]

Malaysia has several government bodies tasked to manage the cyber landscape. The National Cyber Security Agency (NACSA), as per the National Security Committee Order No. 26, has the jurisdiction of establishing regulatory compliance and safeguarding cyber assets, especially for the CNII. There are also governmental institutions such as the Malaysian Communications and Multimedia Commission (MCMC) to enforce communications and multimedia laws, while CyberSecurity Malaysia offers cybersecurity services, programs, and initiatives to improve Malaysia's self-reliance in cyberspace.[5] Malaysia views cybersecurity through the parameters of crime, data breaches, supply chain vulnerabilities, terrorism and violent extremism, and harmful online content. This means enforcement relies on several government bodies, including the Royal Malaysia Police and MCMC, as well as the Personal Data Protection Department (PDPD).

Furthermore, the cabinet reshuffle in December 2023 separated the Ministry of Communications and Digital into two ministries—the Ministry of Communications and Ministry of Digital,[6] which should have implications for agency jurisdiction in Malaysia's cybersecurity sphere. Additionally, Malaysia has sector leads corresponding to the CNII sectors. Examples are the Malaysian Administrative Modernisation and Management Planning Unit for the government sector, the Ministry of Defense and Ministry of Home Affairs for National Defense and Security, and the Ministry of Health for Health.

Legal regulations

One of the earliest government bodies on cybersecurity was MOSTI's National ICT Security & Emergency Response Centre (NISER) which acknowledged that "firewalls and technological solutions are not sufficient in tackling security threats."[8] Thus, between 1997 and after the launch of Malaysia's Cyber Security Strategy in 2020, several policies and laws were introduced to strengthen Malaysia's cybersecurity ecosystem: Malaysia's Computer Crimes Act was passed in 1997, meanwhile, the Communications and Multimedia Act regulating communications operators and improper use of network facilities was enacted in 1998,[9] the Electronic Commerce Act in 2006, and the Personal Data Protection Act in 2010. Malaysia's laws also cover specific cyber-enabled activities such as terrorism with the Security Offences (Special Measures) Act 2012, Prevention of Terrorism Act 2015, and Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. Other laws to protect children include the Child Act 2001 and the Sexual Offences Against Children Act 2017. These legal and policy documents are supported by non-binding guidelines and frameworks such as the guidelines for the management of information security through Cloud computing in the public sector[10] (relevant only to the public sector) or the technical codes issued by MCMC.

It is worth noting that Malaysia utilizes separate tools for the governance of the public sector and the private sector. An example is the Personal Data Protection Act 2010, which applies to the private sector but does not apply to government bodies. The government's data-management practices are determined by the Official Secrets Act 1972, the Public Sector Cyber Security Framework, and other relevant guidelines. Further, government bodies responsible for enforcement may differ. The public sector's security practices are under the purview of the Office of the Chief Government Security Officer (CGSO), while the private sector and general public are overseen by the Personal Data Protection Department PDPD.

Malaysia's Cyber Threat Landscape

Cybersecurity is an economic, security, and social issue. The growth of interconnected devices has widened surface vulnerabilities. Furthermore, the swift adoption of new technologies such as the Cloud during the pandemic did not

prepare businesses and governments for the necessary cybersecurity transitions. This means that users can be running unsupported software or outdated software on what are perceived as a low-risk devices.[11]

An analysis of advisories distributed by NACSA, the National Cyber Coordination and Command Centre (NC4), and MyCERT in 2022-2023 highlighted Malaysia's cybersecurity vulnerabilities from outdated platforms, scams, ransomware, espionage, and intelligence-gathering activities, as well as heightened alerts due to geopolitical circumstances. The latter were issued following developments such as the conflict in Palestine,[12] where concerns of reciprocating hacktivism activities[13] could threaten Malaysia's cyber systems. In addition, advisories on information gathering and espionage were also released in the context of platform vulnerabilities, updates from threat-hunting platforms such as Mandiant, or building awareness on phishing campaigns.

Data-gathering activities for criminal gain are also rampant. Several MyCERT advisories address such scams, in addition to other forms of cybercriminal and fraudulent activities. Furthermore, malicious programs or applications developed for other markets such as India, Pakistan, and China may proliferate and appeal to a Malaysian audience.

Private sector observations such as Microsoft's Digital Defense Reports corroborate these findings, especially on the rise in ransomware attacks. However, the reports also indicated an upward trend in state-sponsored attacks on critical infrastructure that is not explicitly mentioned in public documents. Vulnerabilities in sectors other than government such as universities and other educational institutions are not frequently addressed. Microsoft's information-sharing approach is formed from the analysis of activities across Cloud infrastructure in addition to information-gathering arrangements with Malaysia's CERTs.

Responding to Cyber Threats

Malayia's approach to analysing threats is based on incident reporting. According

to MyCERT's incident statistics, Malaysia has experienced incidences amounting to 10,722,[14] 10,790,[15] 10,016,[16] 7,292[17] and 5,480[18] annually from 2019 to November of 2023. However, studies by private security firms such as Palo Alto Networks stated that almost a third of Malaysian organisations encountered a staggering 50% or more increase in cybersecurity incidents from 2022 to 2023.[19] The International Data Corporation further reported a two-fold increase of ransomware in 2023 compared to the previous year,[20] despite official records showing a decline in malicious codes (from 1,023 to 472 between Jan 2022 and Nov 2023). This could indicate a trend of underreporting, where further analysis is needed to identify discrepancies and deep dive into the downward trend.

Malaysia is moving forward as a digitally-mature economy, with internet penetration at 97.4%, computer access at 80.2%,[21] and 70.2% of the nation with 5G coverage[22] (though adoption of 5G remains low).[23] However, due to barriers in institutional structures amid a rapidly changing threat landscape, governance challenges persist. There may be a need to strengthen cooperative mechanisms and improve information-sharing between parties to enhance Malaysia's effectiveness in cybersecurity defense and response. There may also be a need for Malaysia to build consistent security baselines across sectors.

International Collaboration

Malaysia is cognizant that cybersecurity challenges are not confined within the country. So, as challenges spill across borders, developments in policy and legislation must be harmonized at the national, regional, and international levels, thus raising the importance of cyber diplomacy. The term cyber diplomacy can be defined as "the use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace."[24] Therefore, in the interest of safeguarding Malaysia's national interests, engagements on the cyber diplomatic front can be categorized as those for confidence-building measures for times of crisis, the development of harmonized standards and processes to raise preparedness and national cyber resilience, and playing the role of mediator to ensure conversations in international forums stay on track and balanced.[25]

Malaysia actively engages in regional and international platforms and forums like ASEAN, the ASEAN Regional Forum (ARF), and the United Nations. In ASEAN,

Malaysia has co-chaired three ARF information security management systems (ISMs) discussions on ICT security and seven ARF Open-Ended Study Groups in cybersecurity workstreams.[26]

Malaysia is also developing the Matrix-ASEAN Plan of Action on the 2015 United Nations Group of Governmental Experts (UNGGE) 11 voluntary, non-binding norms of responsible state behavior in cyberspace under the ASEAN Cybersecurity Coordinating Committee. Malaysia also plays a larger role in cybersecurity for the defense sector with the establishment of the ASEAN Cyber Defense Network.

On CBMs, Malaysia collaborated with Australia to establish an ARF Directory of Cyber Points of Contacts, which aims to establish better interaction and coordination among countries in response to cyber incidents. Pursuing a practical approach, co-chairs Malaysia and Australia performed a table-top exercise at the ARF, highlighting the gaps in processes that could reduce understanding in times of crisis.[27] Among the recommendations was to improve communication among states, dedicate a point of contact in the event of a crisis, and establish effective communication policies from the technical side for cyber crisis management.

Unsurprisingly, the ARF findings emphasized the need to identify gaps in technical and human resources capacity, advocate responsible state behaviour, and identify roles for regional organizations that can contribute to discussions at multilateral stages. There is also a need to establish clear linkages with industry contacts and develop a regional framework for cyber-incidence response protocol. The success of Malaysia and Australia's joint-efforts in driving the ARF Directory of Cyber Points of Contacts is perhaps best attributed to opportunity and time. The tabletop exercise was held in 2015, before the intensification of major geopolitical rivalry. Undoubtedly, with the current mood of strategic competition, solid cooperation across all AMS and their dialogue partners might be too farfetched.

At the UN, Malaysia has engaged on various platforms on international security in cyberspace since the UN General Assembly (GA) Resolution 61/55 on the Role of Science and Technology in the context of international security and disarmament.

Malaysia supported the formation of the UN GGE and participated in their 2004-2005 and 2014-2015 iterations. Malaysia has maintained a balanced approach to engagements in the UN aimed at moving discussions forward.[28] For instance, in 2018 when competing resolutions were advanced for the continuation of the UN GGE process or the formation of an inclusive Open-Ended Working Group, Malaysia supported both proposals. Malaysia's international engagements aim for practical interventions where principles and agreements can be operationalized.[29] Also, where possible, Malaysia also participates in conversations on responsible state behavior on critical technologies. Malaysia supported the Call to Action on Responsible AI in the Military Domain at the Responsible AI in the Military (REAIM) Summit in 2023. The Call to Action was endorsed by 34 countries in attendance and fostered directions forward on safer AI use in conflict.[30]

Overall, Malaysia's participation and efforts to engage and shape international forums directly and indirectly impact the country's cybersecurity landscape. During the Cyber ASEAN consultation, participants emphasized that discussions could not be confined to Malaysia alone. As cybersecurity challenges stemming from the adoption of technologies spill across borders, Malaysia's policies and legislation must not only work at the national level, but also at regional and international levels.[31] However, today's geopolitical climate could delay the advancement of constructive conversations on international security, particularly in the cyber domain. Among them is the over-politicisation of policy discussions, given the current international dynamics. This may require Malaysia to engage meaningfully and locate commonalities in efforts to advance productive and meaningful discussions. To do so, Malaysia would have to invest and further develop cyber-diplomacy talent pipelines.[32]

Thus, there is a need to build cyber-diplomacy capacity, as Malaysia's roster of experts remain limited, which can affect the country's participation should its representatives be unavailable. Malaysia recognizes the significance of cyber diplomacy, especially for the development of CBMs in times of crisis, as well as harmonizing approaches and standards to facilitate trust.[33] Engagements should be underpinned by the idea that cyber policies must be guided by analysis and thorough review and not by political affiliations.[34]

International Technical Standards

Malaysia holds the view that in an interconnected cyber ecosystem, the harmonization of local and international standards is needed. There are three ways to streamline technical standards. The first is to opt for certification. A method most useful in business cases is hiring or mandating employees to undergo certification courses that could assure partners—local or international—that cybersecurity practices are similar, thus building trust in systems. The second is to ensure compliance of ICT policies to government-issued or mandated standards. This would require the government to place controls on standards and introduce mechanisms that ensure compliance and availability of cybersecurity services. An example is Singapore's cybersecurity licensing framework, which includes licensing for cybersecurity service providers[35] and mandatory cybersecurity audits for owners of Critical Information Infrastructure.[36] The approach raises cybersecurity standards while addressing the information gap between the cybersecurity service providers and consumers of cybersecurity services. The third is the adoption of international standards and the NIST framework on cybersecurity to identify, protect, detect, respond, and recover.[37] The framework includes recommendations and approaches to risk management, including data protection and cybersecurity processes.

Participants in the Cyber ASEAN consultation stated that international standards do not merely appease the international community but could also translate to having a secure and robust cybersecurity system across the nation. Private sector companies in Malaysia such as Microsoft and Axiata adopt and adapt international frameworks such as the US Department of Commerce-issued NIST to elevate cybersecurity levels. Axiata adopts ISO 27002 and 27004 while encouraging personnel to obtain certification from the Council for Registered Ethical Security Testers (CREST).

Further, there are ISO certifications for information-security management systems with the ISO 27000 series offering 60 standards on a range of information-security management sectors.[38] Participants shared that the scarcity of skills cannot be addressed through mere upskilling. They reflected that new breeds of talent with flexible skills are needed to tackle emerging technology challenges, which is why Axiata continues to invest in staff training to keep its employees abreast with

cybersecurity trends and to understand threats.

In Malaysia, the private sector plays a crucial role in cybersecurity by agreeing to adopt international standards, whether it is through certification, internal IT policies, or continuous training to promote cybersecurity awareness among their staff. The benefits are reaped by the country, as companies can minimize the risk of their infrastructure being targeted by malicious actors. Interestingly, participants also mentioned that adopting ISO standards is not mandatory in Malaysia. Generally, organizations perform a cost-benefit analysis for effective compliance.[39] While the NIST framework is readily available, the ISO certification process can be burdensome and costly. Thus, ISO certification is only recommended for large businesses providing highly complex services.[40] Axiata for instance, obtains ISO certification to bolster customer confidence.

Likewise, Critical National Infrastructure operators would need to ensure that their policies and practices comply with international standards. Thus, CNII embeds ISO and/or NIST guidelines to set their minimum baselines. Fortunately, the private sector is actively promoting international standards adoption. In Malaysia, large companies such as Axiata and Microsoft develop their internal operating guidelines and procedures to conduct threat analysis and develop talent. The companies also utilize certification from various bodies such as the CREST while keeping up-to-date against emerging threat vectors.[41]

Malaysian agencies such as CyberSecurity Malaysia have attended ISO meetings to improve engagements on standards-setting. Malaysia's upcoming Cybersecurity Bill aims to elevate baselines, which would include considerations and developments on international standards. A national-level baseline is important to address sectoral disparities.[42] The bill will identify where some sectors such as finance are more advanced in implementing cybersecurity measures compared to other sectors. Malaysia's regulatory challenge is in integrating regulation which works cross-sectorally, without it being overly burdensome.[43]

However, implementing and enforcing technical standards remains a debilitating challenge should the private sector or the government be short of the resources necessary for certification.[44] Additionally, it is difficult to adopt one-size-fits-all frameworks.[45] One recommendation to strengthen the protection of cybersecurity infrastructure is for the government to provide incentives to the private sector.[46]

But aside from incentives to fast-track the adoption of international standards, the private sector needs government support to facilitate the upskilling of the workforce while cultivating young talent to reduce the talent shortage of cybersecurity experts in the long term.[47] Partnerships with agencies, such as the Malaysia Digital Economy Corporation (MDEC), can offer useful insights into building a sustainable talent pipeline.

Information-Sharing and Incident Management

Malaysia's National Security Council Directive No. 24 states the policy and mechanism for the management of cyber crises. The directive is the backbone for the sectoral approach adopted by Malaysia's digital governance. It appoints sectoral leads for the CNII and escalates reports to the National Cyber Coordination and Command Centre (NC4), a body developed under NACSA, should a situation meet crisis proportions. NC4 is connected to other cyber operating centers and thus could manage the information from MCMC, CyberSecurity Malaysia, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), and sectoral players.[48]

In its current status, NC4 has roles for peacetime and times of crisis. During peacetime, the outfit monitors Malaysia's cybersecurity situation, measures the level of readiness, issues early warnings and advisories, and informs the national cyber-threat level to the national cyber-crisis management committee, and the national cyber-crisis management working group.[49] In times of crisis, NC4 will coordinate and manage, report to stakeholders on the situation, and provide technical expertise. Since 2008 Malaysia has been conducting the X-Maya drills to improve cross-sectoral responses in the event of a cyber crisis.

In addition to anticipating crises, there are various ways for communication and incident management to be facilitated daily. For data breaches, individuals can report to the Personal Data Protection Department and Cyber999, Malaysia's portal for incident management. Meanwhile, activities such as scams have received attention through the years and thus have dedicated government bodies like the National Scam Response Centre or the Royal Malaysia Police CCID Infoline and CCID Scam Response Centre.

Malaysia does not have data breach-notification requirements except for those in financial institutions where data breach incidents are reported to the Central Bank or the Securities Commission of Malaysia.[50] Unfortunately, the lack of incident notification across all sectors impacts Malaysia's ability to gather information and fully assess the threat landscape in Malaysia's ecosystem. Due to the absence of mandatory breach notification and information-sharing obligations, the flow of information-sharing can falter, leading to various agencies working in isolation.[51] With this reality, Malaysia is facing two challenges in the information-sharing sphere. The first is the current state of information-sharing between public and private sector parties and agencies within Malaysia. This could be examined further in the context of information-sharing mechanisms between government-to-government (G2G), government-to-industry (G2I), or multistakeholder platforms such as universities and civil society organizations. While CNII operators and the government may have experience with information-sharing and coordination, G2G, G2I, and multi-stakeholder bodies are still catching up.

Participants in the Cyber ASEAN consultation in Malaysia stated that information-sharing is required for cybersecurity management. Information-sharing should be done horizontally and vertically to improve a nation's cybersecurity maturity to assess threats. However, Malaysia has a persistent challenge in building intelligence-sharing platforms.[52] Malaysia adheres to a broader and high-level incident-reporting basis that may not provide enough data for a deep sensitive analysis. A participant recommended that diving into sensitive analysis may improve Malaysia's assessment of baseline threats, to enable the implementation of more proactive measures for cybersecurity.[53]

The upcoming Cybersecurity Bill is expected to facilitate coordination and enhance information-sharing. It should also elevate baselines and grant appropriate powers to the relevant enforcement agencies.[54] One participant noted that the upcoming Bill should focus on enhancing cybersecurity through national policy action, strengthening cooperation, addressing the growing cyber threats, advancing information-sharing, and protecting critical infrastructure through the implementation of consistent security measures.[55]

There is also an urgent need to improve information-sharing mechanisms with parties outside of Malaysia like the ASEAN Defence Ministers' Meeting and the ASEAN-Singapore Cybersecurity Centre for Excellence. Further, Malaysia

proposed the creation of a regional cyber-defense network center called the ASEAN Cyber Defence Network.[56] Malaysia also shares information with the Asia Pacific Computer Emergency Response Team (APCERT) and contributes to the development of the ASEAN Computer Emergency Response Team.

Despite some progress made, several issues are still hampering Malaysia's move toward smooth information sharing. The main issue is trust, especially in the business sector, where there is a tendency to withhold information out of fear that sharing it may empower their competitors.[57] Another major consideration is the type and depth of information shared. Public and private sector organizations may not be keen to share because the information may either be sensitive or personal.[58] As one participant noted, establishing or improving controls on what can be shared and what can't be shared may be a practical step to enhance information-sharing within Malaysia.[59]

But aside from legislative frameworks, formal protocols, and procedures, improving people-to-people ties could also lubricate trust among public and private organizations. As discussed during the consultation, certain government agencies have greater engagements with the private sector that do not directly concern information-sharing or incident management processes. For example, Malaysia's defense and military and CyberSecurity Malaysia engage with industry and academia on less sensitive issues such as raising opportunities for cybersecurity talents and public awareness. Therefore, the consultation revealed that perhaps what is needed is bolstering more outreach that could enhance people-to-people relations, especially for institutional communications and trust-building.[60]

Inclusion

Digital inclusion can be assessed by disparities in access to devices, availability of internet connection, or opportunities to harness a digital future. Malaysians' access to computers, mobile phones, and the internet is high at 80.2%, 97.4%, and 99.1%, respectively.[61] The gender divide is small at three percent: 98.8% of males have internet access in comparison with 95.9% of females. At least 98.1% of urban areas can access the internet compared to 89.1% of rural Malaysia.[62]

However, digital literacy and skills present a stark scenario. While social media and

e-commerce register high usage of the internet, Malaysia's Department of Statistics stated that only 23.5% of those surveyed could write computer programs using a specific language. There is also the imperative to rethink education spaces not only as mere places to study but also as vibrant environments that equip individuals with adaptive skill sets for the future. Inclusivity in opportunities should be based on the role of learning institutes, to open spaces for an individual's dynamic participation in a digital future.

Like other countries in the region, Malaysia faces a talent shortage in cybersecurity. Estimates suggest that it needs 27,000 cybersecurity knowledge workers by the end of 2025.[63] Currently, it has 15,248 on the payroll. In addressing the talent shortfall, Malaysia's National Cyber Security Strategy highlights the role of Malaysia Digital Economy Corporation (MDEC) and CyberSecurity Malaysia as the government bodies tasked with building the cadre of cybersecurity talent.[64] CyberSecurity Malaysia offers a certification scheme, a training program, and partnerships with higher-learning institutes.[65] Meanwhile, MDEC conducts a reskilling and upskilling program that allows individuals to reskill in digital technology.[66]

Additionally, there are also programs by non-governmental organizations such as the Asia Foundation that offer training opportunities under the APAC Cybersecurity Fund to equip local communities and students with cybersecurity capabilities via upskilling tools and cyber clinics.[67] Despite such positive developments, the Cyber ASEAN consultation revealed that Malaysia's talent shortage in cybersecurity is not only an ICT-related issue but cross-sectoral.[68] For instance, the dearth of cybersecurity experts in the Ministry of Foreign Affairs will challenge Malaysia's ability to sustain its engagement in technical and policy-oriented discussions at the regional and international spheres.[69]

Inclusivity in the digital environment may also require looking into a wider discourse in policymaking, data sharing, and learning environments. The policymaking apparatus would require participation from technologists, civil society organizations, and the private sector. Existing digital literacy programs often target the general population. However, there may be a need to engage leaders and gatekeepers at the executive level to truly transform organizational and cultural approaches to cybersecurity.[70] As most plans, procurement, and budgetary allocations are made by decision-makers in an organization, there is an urgent need for digital literacy to spread in a multilayered manner throughout

organizations.[71] Additionally, mechanisms that capture and promote disaggregated data will enable policymaking processes to better target specific sectors of societies. While achievements on gender and representation may be worthwhile, understanding diversity at a granular level could improve policy engagements.[72]

Data sharing and open-data mechanisms are the crux of digital development, thus harnessing technology to inform policy for greater inclusion would be most useful for the digital future. Malaysia may need to further explore means of data sharing that could benefit the whole of society, such as the Smart City program which provides input to ongoing city planning and management. Relatedly, gender disparities remain as obstacles to Malaysia's quest to promote inclusive learning environments. For example, at Sunway University the female intake in the ICT program is still 20%-25%.

While providing scholarships and/or conducting hackathons or promotional events to spark the youth's interest in cybersecurity or information technology are instrumental, such engagements should be complemented by other out-of-the-box ideas to keep the momentum going.[73] In this regard Malaysian educational institutions are exploring specialized or customized training and course engagement strategies to capture the imagination of different groups, genders, and communities. In this way, the learning environment caters to the specific and varying needs of students and therefore promotes long-term professional and personal interest in cybersecurity or other technology-related careers.

Conclusion

Although Malaysia has high internet penetration, meaningful usage of online platforms is still in the early stages of development. Its cybersecurity governance remains riddled with legacy issues, leading to uneven adoption of standards, varying levels of cybersecurity maturity, and differing perceptions toward regulations, especially between the public and the private sector, as exemplified

by the initial feedback on its data governance regime. To this end, Malaysia is attempting to modernize and establish a cybersecurity benchmark to improve government mechanisms, hence the introduction of the Cybersecurity Bill.

With the highly-anticipated formulation and implementation of the Cybersecurity Bill, the Cyber ASEAN consultation serendipitously afforded the Malaysian cybersecurity community a neutral space to examine the country's aspirations toward a forward-leaning approach to cyber policy and implementation. During the consultation, the positive prospects for the Cyber ASEAN Framework were raised by participants, especially for its relevance to Malaysia's evolving cybersecurity challenges. The four pillars of (i) international collaboration, (ii) international technical standards, (iii) information-sharing and incident or threat management, and (iv) inclusion were recognized as timely subjects requiring further consideration.

Across ASEAN, countries are moving to establish dedicated agencies for effective coordination. ASEAN's ongoing governance restructuring will enable proactive action to manage cybersecurity, rather than having knee-jerk reactions to cyber incidents. Malaysia will continue to participate in international forums to raise Malaysia's viewpoint on cyber governance and facilitate exchanges that benefit its cyber ecosystem. Building on such momentum, Malaysia would seek to engage in formal and informal platforms simultaneously and effectively.

International technical standards play an important role in shaping Malaysia's digital economy and its future. Malaysia's baselines, adapted from international standards, aim to increase technical capabilities and facilitate processes such as threat hunting and enforcement. In the realm of incident management and information-sharing, Malaysia could improve channels of intra-governmental responses daily in addition to heightened events or crises. There is also an urgent need to recalibrate information-sharing mechanisms horizontally and vertically to increase the nation's ability to assess threats.

On inclusion, participants mentioned that cybersecurity requires a whole-of-society approach to effectively address cybersecurity threats. This would mean building more awareness and competencies among various levels of society, from the general public to shaping leaders and decisionmakers in charge of cybersecurity management. Lastly, Malaysia could mainstream inclusion beyond just cultivating

diverse talent management strategies by exploring multi-perspective approaches and practices to policymaking.

In sum, efforts to implement frameworks that benchmark or rank ASEAN countries' cyber capacity in comparison with each other or their dialogue partners are not rare. Undoubtedly, adequate cybersecurity levels require technical aptitude, governance bodies, and threat assessments. However, assessing ASEAN countries can be challenging mainly because of variances in digital maturity rooted in the political, security, and socio-cultural diversity present in each country and the region itself. Thus, applying external frameworks may meet the purposes of benchmarking over the short term, but could have little effect in helping Southeast Asia reflect and design context-appropriate solutions to its mounting cyber insecurities in the long haul.

Constructing an adaptable framework where the process is as much as the outcome is a useful and practical exercise— thus, Cyber ASEAN offers two distinct advantages. First, the participant-led process allows the articulation of priorities and issues across technical, governance, and threat-assessment mechanisms that reflect the opportunities and challenges currently faced by the identified member states and their citizens. For instance, Malaysia's emphasis on baselining and shifting cybersecurity assessments to threat hunting builds on governance structures and mechanisms developed through time.

Despite such significant developments, new challenges continue to emerge, Malaysia is still plagued by various obstacles in technical capability, talent development, and intra-government coordination. In response to these challenges, the Cybersecurity Bill is envisioned as a possible catalyst for change that will address such priorities within the short and medium timeframe. As a complement, the Cyber ASEAN Framework provides policymakers with a flexible tool for formulating, implementing, and assessing current priorities, while possibly setting future directions.

Second, as platforms for G2G, G2I, or multistakeholder exchanges can be difficult to achieve due to bureaucratic inertia or resource constraints, Cyber ASEAN is quite agile and provides various touchpoints to facilitate dialogue and exchange between different players within and outside Malaysia.

Therefore, while the prevailing use of benchmarks and rankings in cybersecurity capacity-building may be relevant to capture the challenges of the current times, a consistent participant-led and adaptable framework would have more added value because it allows the intended users the chance to adopt and adapt the metrics to fit their local context with their available resources but still mindful of future implications.

Policy Recommendations

Based on the findings, analysis, and outcomes of the Cyber ASEAN Malaysia consultation, the following policy recommendations are outlined:

1. **Develop a dedicated talent pipeline for cyber diplomats.** While Malaysia has demonstrated its cyber diplomacy prowess, there is still ample room for growth. In addition to technical or policy know-how, participants have further stressed that cyber diplomats should possess the flexibility to converse with a wide range of audiences from various sectors and countries. Malaysia should conduct capacity-building to develop national experts who could participate in and contribute to cross-regional and cross-sectoral dialogues and collaborations in Tracks 1, 1.5, and 2 diplomacy.

2. **Revitalize trust and partnership-building in cybersecurity cooperation.** Malaysia should revisit ASEAN and ASEAN-led mechanisms to reflect the evolving opportunities and challenges of the cybersecurity environment. Such mechanisms are inclusive of ARF and the East Asia Summit, which both draw a wide international audience. It is also essential to explore trust-building exercises within Malaysia and the region to foster people-to-people relations. This will entail efforts for Malaysia to improve its information-sharing arrangements, especially among CERTs whether in exchanging best practices for classifying information or seeking the right information to share.

3. **Retrofit cybersecurity frameworks and legislations.** Malaysia is currently drafting the Cybersecurity Bill to enhance cybersecurity coordination and elevate baselines to evaluate performance. As Malaysia embarks on streamlining its governance approaches while increasing platforms for collaboration among key stakeholders in the private sector, it should also

amend related legislation such as the Computer Crimes Act to address the changing nature of cybersecurity threats in the physical and digital spheres.

4. **Improve current multistakeholder collaborations.** Malaysia could enhance the multistakeholder process by continuously engaging think tanks both locally and internationally. Harmonizing approaches is vital for cybersecurity, whether it is in the development of standards, increasing the permeation of norms, or sharing information and combating future threats. Through Track 2 diplomacy, think tanks help stir policy conversations, especially when a stalemate occurs in formal diplomatic channels. In this role, think tanks can ensure consistency in policy discussions while providing alternative perspectives. Furthermore, as human capital can be limited, think tanks can support and provide expertise and insights as needed.

Genalyn Macalinao

Philippines

Introduction

With its rapid digital economic transformation and growing strategic significance in major geopolitical flashpoints, stemming mainly from the South China Sea and Taiwan, the Philippines continues to be impacted by major cyber incidents. The Philippines National Computer Emergency Response Team (CERT-PH), under the Department of Information and Communications Technology (DICT) Cybersecurity, Bureau handled a total of 1,542 cyber incidents from 2022 to June 2023.[1] The most targeted sectors were Government (61%), Education (16%), and Telcos (8%).

CERT-PH data showed that the most common type of incident encountered was compromised websites and systems, which accounted for 31.7 % of the total number of incidents. Following closely behind were malware and malicious files (24.9%) and data infiltration/data leak (16.9%) incidents. As of June 2023, CERT-PH

has received and handled a total of 714 cybersecurity-related incidents. Based on the summarized statistical data, agencies under the government and emergency services sector have been the most popular target of cyberattacks with 55.6% of the total incidents handled.

Designated as the primary policy, planning, coordinating, implementing, and administrative entity of the executive branch of the government, the DICT plans, develops, and promotes the national ICT development agenda. Among the DICT's powers and functions are cybersecurity policy and program coordination. This covers the mandate to formulate a national cybersecurity plan consisting of robust and coherent strategies that would minimize national security risks to promote a peaceful, secure, open, and cooperative ICT environment. Further, it is tasked to provide proactive government countermeasures to address and anticipate all domestic and transnational incidents affecting the Philippines.

With such a mandate, the DICT, in collaboration with various stakeholders, issued the National Cybersecurity Plan (NCSP) 2022 in 2017 to serve as the roadmap for the country's cybersecurity efforts. Immediately following its publication, the DICT issued three Memorandum Circulars (MCs), namely: Memorandum Circular 005-2017 Prescribing the Policies, Rules, and Regulations on the Protection of Critical Infostructure or Critical Information Infrastructures (CII) Stipulated in the NCSP 2022;[2] Memorandum Circular 006-2017 Prescribing the Policies, Rules and Regulations on the Protection of Government Agencies Stipulated in the NCSP 2022;[3] and Memorandum Circular 007-2017 Prescribing the Policies, Rules and Regulations on the Protection of Individuals[4] which are stipulated in the NCSP 2022.

Given the growing salience of data privacy and security as well as cross-border data flow as digital policy issues, the Philippines has enacted various legal frameworks governing personal data protection. The Philippines Data Privacy Act (PDPA) of 2012 was signed into law on 15 August 2012 to govern

data privacy protection in the country. The National Privacy Commission (NPC) is the government agency primarily mandated under the law to oversee the administration and implementation of the act. The NPC promulgated the Implementing Rules and Regulations (IRR) of the PDPA on 24 August 2016.

The PDPA highly resembles the provisions of the EU's General Data Protection Regulation (GDPR) to facilitate effective compliance of Philippine businesses with the EU market. The PDPA was found to be vital to the continuing growth of the Philippines' business process outsourcing (BPO) sector, which generates close to US$30 billion in economic output annually. To put that into context, the Philippines accounts for 10% to 15% of the worldwide BPO business. It is estimated that 1.3 million Filipinos were employed by one thousand BPO firms in 2019, and that number is increasing by 8–10% annually. Thus, the PDPA is expected to further boost the Philippines competitive edge as the leading BPO services hub globally.

Similarly, the PDPA's enforcement will also bring positive net benefits to the Philippines' digital economy, which was valued at US$7.5 billion in 2020 and is projected to grow by 30% annually to US$28 billion by 2025. With those favorable digital prospects, the Philippines is actively participating in the Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group and the APEC Framework for Securing the Digital Economy. The APEC-led initiatives provide non-binding recommendations and practical advice to assist member economies in developing their respective legislative and regulatory frameworks in the emerging data-driven economy.[5]

International Collaboration

Recognizing the borderless nature of cybersecurity threats, the Philippines participates and collaborates in several regional and international platforms, primarily through ASEAN, as well as the United Nations.

In ASEAN, the Philippines fully supports practical cybersecurity initiatives such as information-sharing efforts, including the creation of an ASEAN CERT. In cases of cybersecurity incidents within the region, the defense attachés can serve as diplomatic channels to ensure a timely and efficient resolution. The Armed Forces of the Philippines CERT (AFP-CERT) handles cybersecurity incidents affecting the

military, which then relays the information to the Department of National Defense (DND). The DND then collaborates with the Department of Foreign Affairs (DFA) in utilizing diplomatic channels to resolve cross-border cyber incidents.

Likewise, the DFA also utilizes the ASEAN Regional Forum's Points of Contact Directory as a confidence-building mechanism to reinforce mutual trust and transparency among other nation-states in the region. More recently, the Philippines has been contributing to the ASEAN Cybersecurity Coordinating Committee (Cyber-CC), which held its inaugural meeting in 2021. Considering ASEAN's highly bureaucratized nature, the ASEAN Cyber-CC serves as a coordinating platform that takes stock of cybersecurity matters across different sectoral bodies. The Philippines participates in the ASEAN Cyber-CC through the DICT Cybersecurity Bureau and the DFA.

The Philippines also contributes to international forums that seek to maintain peace and stability in cyberspace, most notably through the UN GGE, and the UN OEWG. Aside from supporting the implementation of confidence-building measures, it also recognizes the application of the 11 cyber norms on responsible state behavior in cyberspace. Among the 10 AMS, the Philippines is the lone signatory to the international treaty on cybercrime, also referred to as the Budapest Convention which has been ratified by 68 countries.[6]

International Technical Standards

The Bureau of Philippine Standards of the Department of Trade and Industry – (DTI-BPS) is the National Standards Body of the Republic of the Philippines. It is mandated to develop Philippine National Standards (PNS) to protect consumers, facilitate dynamic local trade, and create access to the international market for globally competitive Philippine products and services. The Standards Development Division of the BPS is tasked to lead and facilitate standardization activities in the country. Through the expertise and knowledge of the stakeholders or the experts comprising its technical committees, sound and realistic standards are developed.

The BPS does not simply adopt international standards but also personalizes them to fit the local or sectoral context.[7] The DTI-BPS has developed and promulgated more than 10,000 PNS as of September 2020. This was made possible through

the standardization efforts of key stakeholders and through collaboration with the Department of Agriculture (DA), Department of Health (DOH), DICT and other partner agencies tasked with developing sector-specific standards. To ensure that the standards development process is effective and efficient, the DTI-BPS established the procedures of standards development through the BPS Directives, a document patterned to ISO/IEC directives. According to the BPS directives, standards are developed using two methods: the Technical Committee (TC) Method and the Fast Track Method. Both methods require the participation of various stakeholders as their positions and interests are vital in the standards development process.

The PNS is prepared by the BPS Technical Committees (BPS/TCs).[8] To achieve the purpose of sound and balanced standardization, the TCs are composed of representatives from the following sectors: academia, trade and industry, consumers or users, professional associations, research institutions, government agencies, and testing institutions. The diverse profiles of the participants demonstrate that the development of the standards must be balanced to reflect the needs of the various sectors.

The overall process should align with the principle of consensus that is industry-wide and voluntary. The sequence of project stages and process flow of standards development is as follows: (1) new project/review of existing PNS; (2) research; (3) deliberation by TC; (4) circulation of Draft Philippine National Standard (DPNS); (5) comments; (6) finalization; (7) approval and; (8) publication. TC 60 is the committee responsible for information technology. It has three sub-committees (SC): SC 1 – Information Security, Cybersecurity, and Privacy Protection, which is chaired by DICT; SC 2 – IT for Learning, Education, and Training, currently chaired by GlobalKnowledge Philippines Incorporated; and SC 3 – Software and System Engineering, IT Service Management, and IT Governance.

TC members have the responsibility of ensuring that their technical standpoint is established and reflects the interest of the sector they represent. The technical standpoint should be made clear at an early stage of the standards development. Consensus involves the resolution of substantial objections. A sufficient period is required before the approval stage for the discussion, negotiation, and resolution of significant technical disagreements. However, in cases that demand market-relevant standards promptly, the Fast Track Method is pursued. Under such a track,

Stage 3 on the Deliberation of the Technical Committee can be omitted. This is usually undertaken in response to an urgent market need for a particular standard.

The DTI-BPS is a participating member of the ISO/IEC JTC 1/SC 27. This committee develops standards, technical specifications and reports, best practices, and related documents in the field of information security, cybersecurity, and privacy protection. SC 27 standards take into account the rapid advances in technology and the challenges of cyber risks. Standards are designed to meet the expectations and requirements of organizations of all sizes and across all types of business sectors.

As a participating member, BPS has the responsibility to comment and vote on all standards to be circulated by the technical committee. The bureau can also nominate experts for the technical committees. Currently, there are expert members from the National Privacy Commission, DICT, Central Bank of the Philippines, and GlobalKnowledge Philippines. They are actively participating in the face-to-face or hybrid meetings of SC27 to put forward the national position of the Philippines in the development of standards, particularly for information security, cybersecurity, and privacy protection.

The DICT MC 005 requires the adoption of the Philippine National Standard (PNS) ISO/IEC 27000 Family of Standards and other relevant international standards for mandatory compliance. Specifically, it orders all government agencies to adopt the Code of Practice stipulated in the PNS ISO/IEC 27002 (Information Technology–Security Techniques–Code of Practice for Information Security Controls). Further, the PNS on Information Security Management System (ISMS) ISO/IEC 27001 is required to be implemented for mandatory compliance by all CII operators. Other sectors not classified as CIIs can adopt the PNS ISO/IEC 27002 voluntarily.

The MC also requires all CIIs to participate in risk and vulnerability assessment by the DICT at least once a year. This assessment includes the overall process of identification, analysis, and evaluation of weaknesses of an asset or control that can

be exploited by one or more threats based on ISO 27000 and ISO 31000. Further, the MC mandates all CII operators and owners to participate in a DICT security-assessment program at least once a year. This includes security evaluation of operational systems based on ISO/IEC TR 19791:2010. Another provision in the MC is the requirement for all CIIs to secure a Certificate of Cybersecurity Compliance from the DICT. The basis for compliance is, but not limited to, the criteria stipulated in the relevant edition of ISO/IEC 15408 (Information Technology–Security Techniques–Evaluation Criteria for IT Security) and ISO/IEC 18045 (Information Technology–Security Techniques–Methodology for IT Security Evaluation) as reference standards.

Standardization is of the utmost consideration, especially with the underlying digital infrastructure that supports the government's information systems. A DICT official stated during the Cyber ASEAN consultation that, "protecting cyberspace does not only entail the interconnectivity aspect, but also protecting the infrastructure that connects us to cyberspace." The DICT has discussed its aim of standardizing the Philippine government's adoption of the national digitalization agenda. Notable agenda items include the Commission on Audit's (COA) recognition of legitimate digital signatures, which the experts believe will help streamline government processes. COA Circular No. 2021-006 was issued on 06 September 2021 to "prescribe guidance on the use of electronic signatures for accountability purposes to resolve doubts over the reliability of information to be used as audit evidence." However, the consultation revealed that the differing levels of digitalization and cybersecurity maturity among government agencies remain a crucial challenge that the DICT will face in its goal of standardizing government ICT processes.

During Cyber ASEAN's consultation in Manila, participants emphasized the prevalence of multi-approaches to international standards adoption and formulation in the Philippines. For instance, the Bangko Sentral ng Pilipinas (BSP) stated that it adheres to a flexible and risk-based approach in issuing regulations for the country's banking sector, due to the various sizes and risk profiles of the 6000 financial institutions under its supervision.[9] Conversely, several private sector representatives noted the need for flexibility rather than being too prescriptive. Considering the additional costs that come with compliance, participants echoed the need for cybersecurity standards to be cost-effective and fit for purpose. Aside from the associated costs, MSMEs are not inclined to get ISO certifications because they might not be fully relevant to their organizational structure or business

operations. In such a case, they often opt for non-binding cybersecurity frameworks promoted by the DICT, such as the NIST Cybersecurity Framework.[10] For larger organizations, a business case has to be made for additional standards adoption. But overall the participants echoed that if available, incentives may facilitate greater compliance.

The consultation also shed light on the need to strike the right balance between regulation and innovation. While new laws are required to achieve more effective compliance with cybersecurity standards and risk-assessment management frameworks, participants noted that regulations should not hinder innovation and development. In aiming for a balanced approach, policymakers and regulators must address the evolving nature of cyber threats and maintain the ability to stay ahead of malicious actors through robust yet flexible regulatory measures. As of writing, the Philippine government is currently drafting a cybersecurity bill that seeks to fill the regulation-innovation gap.

Participants also stressed the importance of cross-sectoral collaboration to harness the expertise and resources of various stakeholders in order to create comprehensive and effective cybersecurity policies and initiatives. TC is a concrete example of the multistakeholder approach, although more can be done to make it less technocratic. Participants stressed that by being more inclusive, deliberations will result in a more cohesive and coordinated approach to regulations that bear in mind the varying perspectives while effectively addressing cyber threats at the national and sectoral levels.

At the regional level, adhering to globally recognized standards can facilitate communication and cooperation to tackle emerging cybersecurity challenges posed by critical and emerging technologies like AI, the Internet of Things, and Cloud computing. The Cyber ASEAN consultation resulted in a deeper understanding that international standards can serve as a common language or benchmark to further facilitate effective and practical cybersecurity collaboration among nation-states, especially in Southeast Asia.

Information-Sharing and Incident Management

The Philippine government encourages greater sharing of cyber-threat information among critical infostructures through Sectoral CERTs, both in acquiring threat information from other organizations and providing internally-generated threat analysis to other organizations. In the Cyber ASEAN consultation, the Armed Forces of the Philippines (AFP) Cyber Battalion stated that the Philippine Army is attacked more than 350 to 500 times every day on their networks alone. Due to resource constraints and the need for greater coordination with the private sector, the AFP has tapped several ICT companies for cyber-threat information-sharing and incident management.

Despite the positive momentum of cybersecurity public-private partnerships, the lack of adequate trust remains a major roadblock to sharing actionable threat intelligence across all relevant stakeholders to capture a near-accurate picture of the cyber-threat landscape.[11] Although CERT PH has provided rules and guidelines, information-sharing is voluntary.[12] A few participants during the country consultation highlighted that the majority of cyber incidents remain unreported due in large part to looming concerns about regulatory fines and reputational damage.[13] As a remedy, a few participants voiced the need to establish anchors of trust and set the minimum parameters for information-sharing.[14] In practice, this means establishing standard levels determining the sensitivity and veracity of the information to be shared. In the short-to-medium term, the categorization or definition of information shared can set the baseline to promote predictability, transparency, and confidentiality among the public and private sectors.[15]

As a starting point to improve information-sharing, the DICT MC 005-2017 on information-sharing may provide practical insights to foster trust. DICT advocates adherence to the Traffic Light Protocol (TLP) to ensure that information is shared only with the appropriate audience or recipient. TLP employs four colors to indicate expected sharing boundaries to be applied by the recipient(s) as defined according to the Forum of Incident Response and Security Teams (FIRST) Standard Definitions and Usage Guidance.

TABLE 1

Traffic Light Protocol per DICT MC 005-2017

Color	When should it be used?	How may it be shared?
TLP: RED Not for disclosure, restricted to participants only	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.
TLP: AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organizations, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP: GREEN Limited disclosure, restricted to the community	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

Color	When should it be used?	How may it be shared?
TLP: WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

On incident management, DICT Memorandum Circular (MC) 005-2017 states that all identified CIIs are mandated to create their own Computer Emergency Response Team (CERT). DICT is responsible for handling the Philippine National CERT (NCERT) which serves as the central authority for all sectoral and organization-level CERTs in the country. The MC also requires the establishment of sectoral CERTs for all CIIs and that an information-sharing platform shall be established among member organizations. Supplementing MC 005-2017 is DICT Department Circular (DC) 003-2020,[16] which establishes the Philippine NCERT Division of the Department of Information and Communications Technology. This division under the DICT Cybersecurity Bureau leads, manages, and oversees the various government, sectoral, and organizational CERTs. Further, the DC requires that all CII sectors be classified and supervised by their respective lead CERT as follows:

CII Sector	Lead CERT	
	Agency Code	Agency Name
Government and Emergency Services	DICT-MISS-CERT-PH	Department of Information and Communications Technology–Management Information Systems Service
Business Process Outsourcing	DTI-CERT-PH	Department of Trade and Industry
Healthcare	DOH-CERT-PH	Department of Health
Media	PCOO-CERT-PH	Presidential Communications Operations Office
Banking	BSP-CERT-PH	Bangko Sentral ng Pilipinas
Financial	DOF-CERT-PH	Department of Finance

CII Sector	Lead CERT	
	Agency Code	Agency Name
Power	DOE-CERT-PH	Department of Energy
Water	NWRB-CERT-PH	National Water Resources Board
Telecommunications	NTC-CERT-PH	National Telecommunications Commission
Transport and Logistics	DOTr-CERT-PH	Department of Transportation

All government agencies are mandated to establish their respective Government CERT named in the following manner/syntax: [Agency acronym-CERT-PH]. As standard protocol, all government CERTs are required to report to and be subject to the supervision of their respective lead CERT. All CERTs not falling into the category of sectoral and government CERTs are classified as organizational CERTs and shall report directly to CERT-PH.

While the DICT efforts mentioned above were promising, implementation is still a daunting challenge. Participants suggested that incentives are effective enablers of information-sharing and incident management among the sectors.[17] Providing incentives may fast-track more robust cooperation between government CERTs, law enforcement agencies, and the private sector to ensure timely and effective management of cybersecurity incidents. Ideally, incentives may lead to building trust over time. Others also raised the prospect of the government sharing more high-quality information, considering the depth and breadth of its intelligence sources on cyber risks and threats.[18]

Inclusion

Coping with the increasing complexity of cyber threats necessitates different skillsets to resolve and respond to cyberattacks. Similarly, a diverse representation among cybersecurity professionals can help ensure a comprehensive risk management strategy.[19]

In addressing the country's cybersecurity workforce gap, the government, industry and academia are embarking on public-private partnerships. In such arrangements, major ICT and cybersecurity companies are providing reskilling and upskilling opportunities to women and girls and underemployed youth. The training opportunities are currently filling in the talent deficit in the Philippines over the short-to-medium term. However, in the long term, defining career pathways for early graduates in cybersecurity should be a priority. Often, unrealistic job expectations and the required qualifications for graduates, even for entry-level positions, become barriers to entry. Some participants in the consultation suggested that the Philippine government and the ICT industry must agree on a realistic set of qualifications to match the credentials of the current pool of cybersecurity professionals, backed by continuous investments in training programs.[20]

As the Philippines puts its bet on its digital economy, its young and tech-savvy population will become critical drivers of consumption, productivity, and innovation. With this in mind, the government must revisit the continuing relevance and competitiveness of its educational system, going beyond the near-term solutions of reskilling or upskilling. The Cyber ASEAN consultation has revealed that the Philippine educational curriculum must be evaluated to support the country's growth prospects in decades to come.[21] The Philippines is lagging behind its peers in Southeast Asia as far as educational literacy is concerned. Such an alarming observation should urge government policymakers to ensure that young graduates are equipped with robust skills to be globally competitive.

Although programs in Science, Technology, Engineering, and Mathematics (STEM) are crucial in ensuring a strong talent pipeline of ICT graduates, equal emphasis on social sciences, arts, and humanities can help augment the talent deficit within and beyond cybersecurity. If done right, the next generation of Filipino graduates,

whether in cybersecurity or information technology at large, will acquire technical and non-technical prowess—a flexible skillset fit for the changing times.

On women and young girls, the Philippine government has a strong commitment to narrowing the gender gap through the lens of gender and development (GAD). However, to effectively design policies and programs that will address the cybersecurity capacity gap from a gendered perspective in the Philippines, policymakers must first improve the acquisition of comprehensive gender disaggregated data.

Policy recommendations

Building on the cross-cutting exchanges at the Cyber ASEAN consultation in Manila, several policy recommendations per pillar of the framework are enumerated below to raise the Philippines' cyber resiliency and capacity:

International Standards and Frameworks

1. **Safeguard critical national infrastructure in the Philippines through the adoption of policies on basic information security standards.**

   Based on the deliberations at the Cyber ASEAN Philippines consultation, international technical standards like ISO-27001 and the NIST Cybersecurity Framework can serve as a common language that will enable international cooperation and confidence-building measures in cybersecurity. To evaluate the gap and the impact of future cyberattacks on the Philippines, a baseline of the existing information-security systems per sector will be essential. Likewise, mapping the country's level of information-security risks and vulnerabilities, including response and remediation strategies based on specific threats and threat levels, is equally critical.

2. **Leverage established and internationally recognized security baselines and frameworks in developing cyber policies and strategies for the country's digital economy.**

With its expanding data-driven economy, the Philippines needs to explore existing best practices, including security baselines such as the APEC Framework for Securing the Digital Economy. In this regard, policymakers must be mindful of the following considerations when devising a holistic cybersecurity risk-management approach: (1) utilizing an iterative, open, and collaborative development approach; (2) increasing awareness of risk management both inside and among organizations and; (3) enhancing security by taking a risk-based and results-oriented approach.

Considering the wave of cyber incidents afflicting the healthcare and manufacturing industries in the country, renewed attention to their cybersecurity measures is warranted.[22] [23] Recent DICT data shows that the Philippine healthcare sector has been consistently targeted for the last three years, even during the post-pandemic era. Similarly, technological supply chains have become increasingly vulnerable, including software update procedures, as the country's digital economy gains further momentum. Thus, new security measures for the healthcare industry and supply-chain protections, notably software security, should be seriously considered.

For the protection and safety of critical infrastructure and critical information infrastructure, security baselines are a crucial component. One of the six pillars of the upcoming Philippines National Cybersecurity Plan 2023-2028 is "Secure and Protect Critical Information Infrastructures (CII)." Similarly, the Philippines should also leverage international cybersecurity standards on IoT devices by facilitating access to best practices and recommendations.

3. **The implementation gap in cybersecurity policy must be prioritized**

The DICT department circulars on information security are currently in place, but implementation has been difficult. The DICT is currently working on a cybersecurity bill that will address this need. However, crafting a stronger legal framework is only the first step. To achieve effective implementation, legal frameworks should be infused with win-win incentive mechanisms.

Of course, the win-win argument may currently be rather aspirational, given that government spending on cybersecurity remains stunted. Competing priorities

may restrict the allocation of additional funds to cybersecurity initiatives. The Philippine government often faces challenges in distributing resources among various sectors and may prioritize other pressing issues over cybersecurity. There is also the challenge of fluctuating political priorities. Political agendas can significantly influence budgetary decisions at any given period.

Add to this, the bureaucratic hurdles and red tape that can derail the smooth implementation of cybersecurity initiatives. Complex approval processes, delays in decision-making, and inefficient allocation of resources can therefore hinder effective cybersecurity measures. But perhaps the more critical issue ultimately is the lack of awareness of cybersecurity. If decision-makers within the government are not fully interested or aware of the evolving cybersecurity threats and the potential consequences, they may not be serious about allocating sufficient resources to address such issues. Solutions to addressing the above challenges require a multifaceted approach that demands consistent awareness-raising, advocacy, policy development, and collaboration with stakeholders.

Information-sharing and Incident Management

4. **Increase funding allocations for CERT in every CII organization to achieve more robust information-sharing and incident management.**

   The Manila consultation has reaffirmed the need for more proactive rather than reactive information-sharing and incident management, especially among CERTs in the public and private sectors. CERTs are considered as frontliners; against threats emanating from cyberspace. They are also the drivers of national and international cooperation on trust-building. But to fully accomplish their goals, CERTs should continuously receive funding support.

5. **Build a Points of Contact Directory among CERTs**

   Given the current challenges of CERT-PH in engaging public and private institutions in managing cyber incidents or monitoring threats regularly, creating a national list of Points of Contact (POC) would come in handy. Leveraging the person-to-person ties, the directory could be used to facilitate critical information-sharing, especially in devising crisis response.

As an initial step for the suggested POC, the DICT, along with the current sectoral CERTS, can leverage existing communication channels and platforms to exchange real-time information. For instance, in the government, there are inter-agency committees such as the National Cybersecurity Inter-Agency Committee (NCIAC), and the NCIAC Technical Working Group on CII sectors (banking, healthcare, etc). In the private sector, the Bankers Association of the Philippines is a prime example. For the BPO industry, there is the IT and Business Process Association of the Philippines (IBPAP).

Inclusion

6. **Maximize multistakeholder contribution in cyber capacity-building**

The multistakeholder community has always been a key driving force behind many cybersecurity capacity-building efforts. Each multistakeholder brings to bear distinct contributions in raising cyber resiliency. Aside from providing manpower and fiscal resources, the industry offers unique perspectives in managing cybersecurity, given their oversight of critical national infrastructure. Conversely, the invaluable contribution of research practitioners and advocates from academia, think tanks and civil society groups cannot be overstated. Together they contribute their policy-relevant experience and expertise to make up for the government's lack of resources and know-how. In understanding the unique expertise and perspectives of each stakeholder, openness between public and private sector entities can flourish.

Advance inclusive cyber capacity-building

Equally vital in accelerating the multistakeholder agenda is the inclusion of women, girls,[24] and minority groups like persons with disabilities and the elderly. Rather than being an afterthought, their perspectives should be integrated from the inception of capacity-building efforts. This will ensure that such activities are not one-off and ad hoc in nature. Because the activities are context-specific, they gain legitimate buy-in and sustainability from the intended recipients or target communities.

Admittedly, the Cyber ASEAN Manila consultation has prompted the cybersecurity community in the Philippines to further examine the intersection of inclusion and cybersecurity beyond prevailing notions of the digital divide or gender gap. In this regard, a paradigm shift toward digital equity and inclusion has been recognized and hopefully adopted in the longer term to ensure that policy issues and approaches are all-encompassing and cross-sectoral.

Conclusion

The Manila consultation has confirmed Cyber ASEAN's underlying assumptions about local collaboration and contextualization. The grounded approach of the Cyber ASEAN Framework, which prioritizes local sensitivities, sets it apart from other existing frameworks and tools. It diverges from the conventional baselining or ranking approach and instead dives deeply into the domestic context of its pilot countries. As some participants noted, the Cyber ASEAN Framework's four pillars—international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion—are flexible and iterative, capable of meeting present and future cybersecurity policy issues and priorities.

Therefore, using Cyber ASEAN as a cybersecurity framework or policy tool for the Philippines can enhance the country's cybersecurity posture by considering the unique domestic challenges faced by the country, while promoting regional and international collaboration, addressing emerging cyber threats, and ensuring inclusivity. Overall, it provides the rest of Southeast Asia with a pragmatic approach to pursuing a middle path that aligns with regional and international standards and best practices, yet emphasizes local insights and expertise. In adopting and adapting the Cyber ASEAN Framework, the Philippines can strengthen its national vision of cyber resiliency and contribute constructively to a secure and trusted digital environment within ASEAN and globally.

Nguyễn Việt Lâm, Ph.D. and Đỗ Hoàng

Viet Nam

Overview

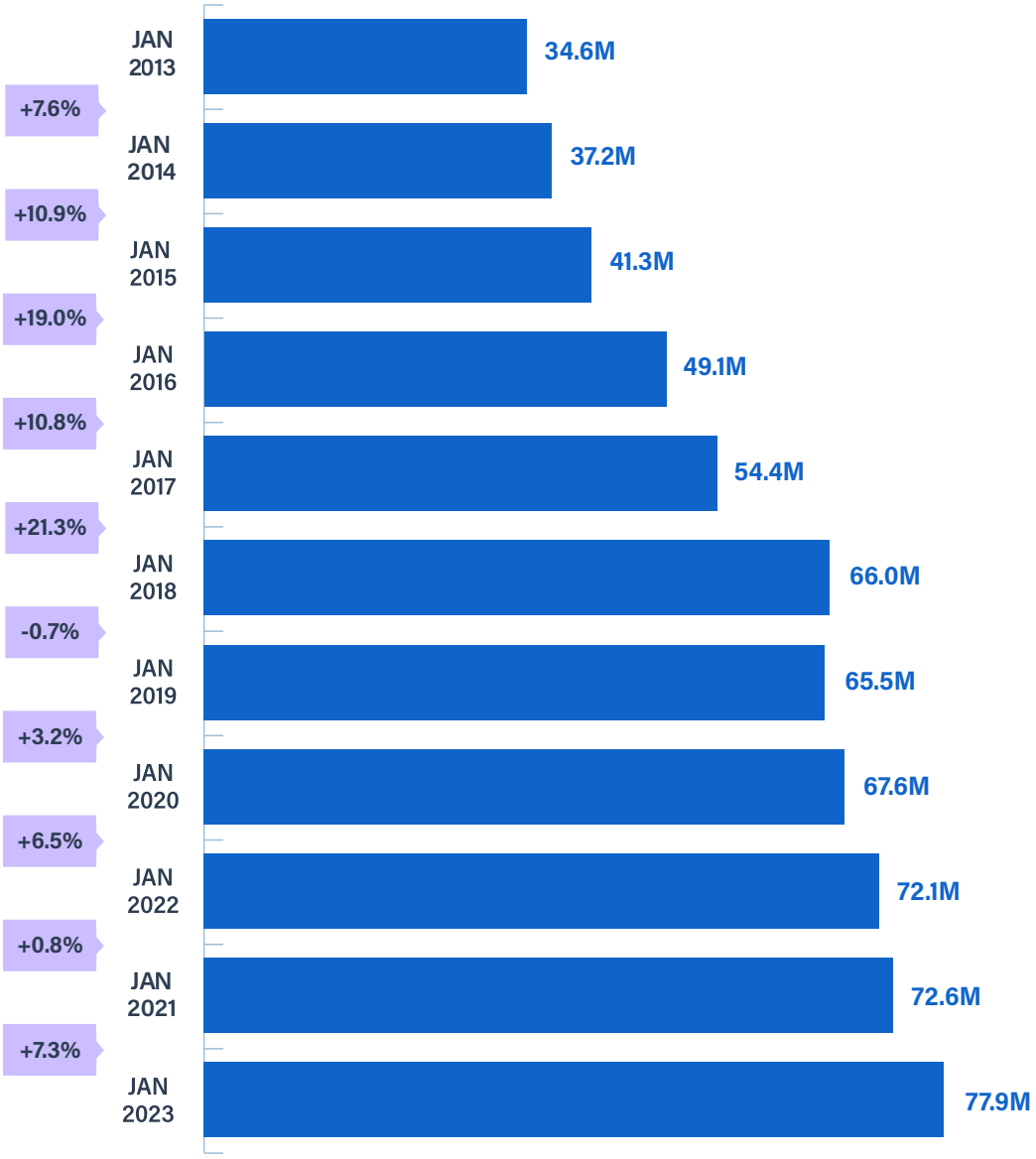
Despite only being introduced to the internet in the late 1990s—somewhat later than other ASEAN members—Viet Nam has quickly become a vibrant internet market, catching up with others in the region and the world in terms of usage. In 2022, it was estimated that Viet Nam had approximately 564,000 domain names ending ".vn", ranking second in ASEAN and among the top 10 in the Asia Pacific,[1] and with over 72 million users (almost 80% of the national population), the country ranks 13th globally.[2] According to experts,[3] the speed of internet penetration has been on the rise, with the total user numbers doubling in the 10 years up to 2023 (from 34.6 to 77.9 million, figures below).

Social media popularity is also growing fast: almost 90% of internet users above the age of 18 have at least one social media account;[4] streaming hours on average

have reached more than six hours per day.[5] The most used platforms are Facebook, Zalo, and Tik TikTok, used for multiple purposes, including staying in touch with acquaintances, looking up information, and entertainment.[6] In addition, Viet Nam's digital market has been increasingly expanding. The percentage of weekly online shoppers among internet users is quite upbeat (at over 60% in 2022, it is higher than the global average of 57.6%),[7] contributing to its growing digital economy, which has recently been predicted to hit US$49 billion in value in 2025 (more than 100% increase from 2022)[8] and considered ASEAN's fastest growing one.[9]

FIGURE 1

Viet Nam's internet users 2013-2023[10]



With such wide internet penetration, Viet Nam has been focusing on upgrading its digital infrastructure. Viet Nam is among the world's top 10 countries for IP version 6 (IPv6) transition. Mobile broadband infrastructure has covered 99.73% of villages across the country, and the fiber optic system has reached 100% of communes, wards, and townships, 91% of villages, and 100% of schools.[11] The number of undersea internet cables jumped in 2023 to a total of seven,[12] excluding FPT Telecom's US$300 million Asia Link Cable project.[13] Viet Nam's National Digital Transformation Program, with a vision toward 2030, establishes the goals of providing universal broadband access by 2025 and 5G coverage by 2030,[14] and focuses on "soft" infrastructure such as artificial intelligence (AI) technology and the Internet of Things (IoT). Innovation hubs, most notably the recently-inaugurated National Innovation Center, are considered the first step toward building a cyber ecosystem in Viet Nam.[15]

Security Challenges

However, Viet Nam's rapid digital developments come with a range of cybersecurity challenges. Viet Nam is not an outlier to the general trend of data breaches and cyber espionage witnessed worldwide. According to a Vietnamese expert,[16] cyberattacks have become more unpredictable globally and increasingly complicated. Perpetrators are better organized and even supported by governments, like the Stuxnet attack in 2010, the WannaCry virus spread in 2017, and the SolarWinds hack in 2020. Other experts shared similar assessments about the progressively complex nature of online data breaches, citing that 45% of data breaches are Cloud-computing related and 19% involve partners in the same supply chain of IT hardware, software, and applications. Even more worrisome, 67% of detected attacks in the Asia Pacific in 2022 were carried out by external partners or adversaries and attacks were largely unknown to the victims when they were being carried out.[17]

Viet Nam is also subject to multiple cyber crimes. In 2022, it was estimated that there were almost 13,000 cases of online fraud, with financial crimes making up more than 75% (500 of which were prosecuted in the second half of 2022 alone).[18] Around 31% of students in secondary and high schools are also subject to cyberbullying, according to a study done by Viet Nam's National University in 2019.[19]

Because of the alarming spike in cyber-enabled activities and crimes, some experts opined during the Cyber ASEAN consultation that Viet Nam's cybersecurity capacity can be characterized as being passive and of limited nature in the context of people, processes, and technology.[20] Many organizations lack qualified engineers and technology experts, especially in risk analysis, while some organizations' bureaucratic nature can prevent timely remediation measures. Others might not have a contingency plan for typical attack scenarios such as malware or phishing. In terms of technology, some organizations' are mostly defense-oriented but still many security systems do not work in line with their assigned purposes. Detection capability relies entirely on monitoring systems. Therefore, some agencies cannot detect flaws in their system and are unaware of attacks when the system has been infiltrated.

For instance, one organization can be penetrated from multiple directions, via a physical connection (such as a USB drive), phishing, end users, or supply chain. According to one speaker consulted, such risks could only be prevented in a limited time window. Cyber defenders must seize this window of opportunity when malicious actors are surveilling and collecting information before they launch an attack.

Legal Regulations

From a political and legal standpoint, Viet Nam's government has been paying attention to cybersecurity. Notably, Viet Nam has incrementally fortified its domestic legal framework to address cyber threats in the past decade via a comprehensive series of documents,[21] such as: the National Assembly's Criminal Code, numbered 100/2015/QH13 in 2015;[22] the government's Decree on the Prevention of Online Information Conflicts numbered 142/2016/ND-CP in 2016;[23] the Assembly's Cybersecurity Law, numbered 24/2018/QH14 in 2018[24] (marking the first time a legal document refers to the national cyberspace); the National Digital Transformation Program in 2020, aiming at national cybersecurity and safety from now to 2025, with direction to 2030 and;[25] the Prime Minister's Decree No.

53/2022/NĐ-CP on specific articles in the Cybersecurity Law in 2022.[26] In 2020, Viet Nam was ranked 25th in the International Telecommunication Union's Global Cybersecurity Index, which is an improvement in line with the government's direction embodied in Prime Minister's Decision No. 964 in 2022 aiming at national cybersecurity and safety by 2030.[27] Apart from such documents, Viet Nam's Steering Committee for Cyber Safety and Security made its debut in 2020 under the PM's supervision, to review past cybersecurity situations and work on subsequent five-year plans.[28]

International Collaboration

Various efforts have been made to strengthen Viet Nam's overall cybersecurity framework and cyber cooperation internationally. In the UN, Viet Nam has had a long history of engagement with cyber rules discourse.[29] It took part in the First Committee's resolution draft process (which first took place in 1998) and the dual-track working groups, the UN Governmental Group of Experts (GGE), and the Open-Ended Working Group (OEWG). Viet Nam is also a member of the UN's Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes.[30]

Within these UN forums, Viet Nam's position has always been clear and subscribed to three main pillars: (i) Viet Nam emphasizes the importance of both international and national law being applied in the cyber realm. A national space must be maintained to preserve the rights of countries, including sovereignty, self-determination, and non-intervention, among others; (ii) Viet Nam advocates for regional and international cooperation to establish a peaceful ICT environment backed by a stronger commitment among countries to achieve such goal; (iii) Viet Nam supports the development of cyber legal frameworks in multilateral platforms, particularly within the UN. While the European Union (EU), the United States (US), and France have proposed various alternative frameworks, Viet Nam always emphasizes that the UN is the only platform where decisions are made through consensus, transparency, and openness to all members. Regionally, Viet Nam has supported ASEAN's political and technical efforts to enhance mutual understanding and trust regarding cybersecurity, such as the formulation of ASEAN's Computer Emergency Response Team (ASEAN-CERT), the series of initiatives proposed by Singapore in 2018, as well as the ministerial meeting on cyber crime in 2022.

Still, there are limits to such cybersecurity efforts and initiatives. During the Cyber ASEAN consultation, experts noted the low official coordination among ASEAN members at the UN's GGE and OEWG processes. They also pointed out the lack of public-private cooperation in the UN process and the implications of ongoing geopolitical rivalry on global cyber governance. Some Vietnamese experts advised that ASEAN should pursue a region-wide framework for cybersecurity standards. This can be challenging, due to varying cyber infrastructure gaps, diverse concerns and operating procedures, and different interpretations of cybersecurity across Southeast Asia. Nevertheless, Vietnamese experts still consider a common cybersecurity framework feasible because ASEAN members share common principles and practices in ensuring cybersecurity,[31] mainly: (i) a focus on trust-building rather than the weaponization of cybersecurity among members; (ii) frequent informal exchanges at UN platforms; and (iii) the emphasis on international assistance and cooperation among developing countries.

International Standards, Information-Sharing, and Incident Management

Viet Nam's multisectoral cybersecurity efforts on the technical pillars of Cyber ASEAN can be analyzed via two case studies: (i) Viet Nam's subscription to international technical standardization; and (ii) Viet Nam's information-sharing and incident management via VNCERT (Viet Nam's Computer Emergency Response Team) and the establishment of Viettel's REPUTA system.

First, regarding standardization, Viet Nam soon realized the need for technical standards in cyber space, as indicated in the first part of its Cyber Law.[32] With that in mind, Viet Nam has: (i) established a National Standardization Strategy (NSS); (ii) adopted 70 international standards, overseen by the Ministry of Information and Communications (MIC), the Ministry of Science and Technology (MOST), and the National Agency of Cryptography and Information Security,[33] including those on cyber safety and security like ISO 27001 and 27002; and (iii) implemented the Digital Transformation in Standard, Metrology, and Quality project to "socialize" the standardization process, engaging with multiple governmental agencies as well as businesses and the public.

Apart from leading most of the activities above, the Directorate for Standards, Metrology, and Quality (STAMEQ) under the Ministry of Science and Technology of Viet Nam has also co-organized numerous Track 1.5-Track 2 events with international partners, such as the workshops in 2023 with Standards Australia[34] and the US-ASEAN Business Council[35] to develop best practices for cyber standards. As a result, within the private sector, enthusiasm for standardization has subsequently increased. For instance, only 14-40 Vietnamese enterprises adopted the ISO/IEC 27001 in 2013.[36] At present, the figure has jumped to 500.[37]

On information-sharing and incident management, speakers at the Cyber ASEAN consultation highlighted the role of MIC's VNCERT and Viettel's REPUTA system. According to one expert,[38] MIC established VNCERT in 2019[39] as the national coordinator in managing cyber incidents to perform three main functions: (i) developing and implementing regulations (including urging domestic entities to comply with the governmental directive on accelerating incident response, to develop and assess specialized CERTs in particular units, and to follow the handbooks for typical scenario responses, etc.); (ii) promoting professional technical tools to support incident response, including the deployment of the Network Information Security Incident Coordination Platform in December 2022, a digital support platform to perform centralized analysis of cyberattacks, and remote troubleshooting services, etc.; (iii) enhancing knowledge sharing about network attacks in collaboration with foreign CERTs. VNCERT was responsible for dealing with the WannaCry virus, such as sharing information about the attacks among all CERTs (there were about 80 incidents per day) and requesting international support upon identifying an overseas IP address. VNCERT has also focused extensively on its official and ad hoc networks with regional CERTS, including those in ASEAN.

Utilizing emerging technologies to combat cyber threats, Viettel established the REPUTA system, a platform that integrates AI and big data analysis to perform several cybersecurity functions. REPUTA can do so because of its notable features, including: (i) natural speech, sound, and image processing; (ii) monitoring data from multiple sources based on different criteria, such as social media trends; and (iii) analyzing certain topics, such as cyberbullying or scamming. The government and business communities have benefitted from REPUTA. It helps the government keep track of the flow of events and public opinion, enabling it to put out early warnings regarding cyber risks and to conduct research on the nature of and how to address cyber crimes. Aside from cyber safety services, the business sector

acquires timely market and customer analysis to improve its services' quality.

Despite the positive trajectory of Viet Nam's technical efforts to combat cyber risks and vulnerabilities, notable challenges and limitations persist. On standardization, there are some discrepancies among standard configurations between those developed locally and those accepted internationally. There have been cases where Viet Nam's products issued with the Viet Nam-developed timestamp SAVIS,[40] similar to that of ISO, were not allowed to enter the EU market because the EU followed another standard. Some ISO standards are also deemed too European or in favor of European partners.[41] Although Viet Nam adopted ISO/IEC 27001 in 2018 and integrated it with its own TCVN 11930:2017, more time is needed in setting up the required infrastructure to support its full implementation.[42] Several organizations in Viet Nam have adopted the NIST Cybersecurity Framework, but that is non-binding and can be costly to implement.[43] Several participants view the NIST framework as lacking clear guidance on certain cyber concerns, such as privacy by design[44] or shared responsibilities on Cloud computing,[45] as well as practical steps to achieving the desired outcomes.[46]

Another major challenge is the widening implementation gap. One expert reported weak regulatory compliance among businesses, while others contended that regulations need adequate time and resources to be fully operational. It was also observed in Viet Nam that several organizations have shied away from participating in the standards development process due to a lack of human talent. Other experts also emphasized that standards are always subject to becoming obsolete in the face of newly emerging developments.[47]

Incident management and information-sharing between public and private sectors are considered important, but remain very limited due to the lack of mutual trust or practical frameworks.[48] Again, the lack of human capacity is another issue, further impeding practical incident management measures, despite Viet Nam's efforts to train new experts. During the consultation, participants outlined several challenges that need to be overcome: (i) many local agencies are assembling a large number of response teams without a consistent focus on updating or deepening their skills; (ii) many end-users also lack awareness, which at times can cause incidents by accident; (iii) Viet Nam has inadequate human resources in a niche industry like blockchain that can help mitigate cybersecurity risks;[49] and (iv) international tech firms can also poach talents away from domestic businesses.[50]

Inclusion

Although Viet Nam is bullish on the ability of all things tech to prosper its digital economy, the sobering facts of digital inequity may impede progress. Women and girls are becoming increasingly vulnerable to cyber threats and risks. The prevailing digital inequity presents major roadblocks that could prevent the country from harnessing the potential of its younger population, especially in the face of a possible talent shortfall.

Injecting a gender-based approach to examine the impact of cybersecurity risk among women, one speaker[51] conducted a major study throughout 2021 with samples from Ha Noi, Quang Binh and An Giang (the representatives of the three main administration areas in Viet Nam). After surveying more than 700 women from diverse backgrounds, the study concluded that: (i) in general, women were more vulnerable than men to various cyber threats, including exposure to computer viruses or scams (50%), miscommunications (40%), sensitive information or identity theft (40%) and stalking (15%); (ii) women were less aware of the internet's benefits and were found to be more at risk online than their counterparts; (iii) males faced fewer risks, partially because of the female-male ratio of cybersecurity workers skewing dominantly towards males (1-4), and because females are often stereotyped as "gullible." These concerns are even more alarming considering that women in Viet Nam use the internet to undertake daily tasks more than males (with an average of 5.5 hours per day).

FIGURE 3

Comparisons between males & females regarding internet usage and risks[52]

	Male	Female
Social media	More for personal hobby, less likely to share photos	More friend connection, more family-oriented, more photo sharing
Online shopping behavior	Tech, expensive items	Household, family care products

	Male	Female
Vulnerability to threats	Less vulnerable	More susceptible to mental, verbal, and sexual harassment, defamation, catfish, manipulation, revenge porn, etc.
Typical response to threats	Calmer, even aggression toward the "culprit"	Silent, worries about retaliation or reputation harm

Because Viet Nam is still endowed with vibrant population growth,[53] it enjoys a rich reservoir of young talents. During the Cyber ASEAN consultation, one speaker discussed how the youth, especially in urban areas, have been equipped with cyber awareness and skills from Viet Nam's universal education and extracurricular activities. However, they are also susceptible to cyber threats, because (i) many lack specific technical knowledge on how to detect or respond to certain cyber threats like phishing emails, while some others are deemed overconfident in their skills; (ii) some tend to overshare personal information online, which could be stolen in the age of social media; and (iii) some youth members are overly emotional and lack common sense, and are therefore easily manipulated by fake news.

Policy Recommendations

Experts laid out several recommendations to address Vietnam's cybersecurity challenges while opening new avenues for academic research and policy formulation, all of which provide enforcement agencies with various practical resources. The policy recommendations outlined below synthesize the deliberations from the Hanoi consultation, and are presented using the Cyber ASEAN's "3Cs" approach, a participatory-led process based on (i) consultation to engage with all stakeholders, in both the private and public sectors and diverse in representation; (ii) collaboration to strengthen coordination in and outside Viet Nam and; (iii) community-building to bring solid and unified ASEAN-led cyber processes and initiatives.

Consultation

Viet Nam should ensure that cybersecurity is a whole-of-government goal, allowing multiple agencies to undertake specific roles. It should hold forums for continuous dialogue and collaboration between the cyber industry, academia, civil groups, and government entities. Proactive participation among public and private sector entities in Viet Nam's cybersecurity is essential. To achieve this goal, Viet Nam should: (i) encourage businesses and private organizations to be more proactive in the standards development process and incident information-sharing. Businesses like FPT and Viettel can better leverage technology, data, and human resources to improve capacity and procedures; develop a human-based approach to cybersecurity that considers the people as the priority; introduce legal provisions and policies to protect and elevate the voice of women, the youth, and vulnerable groups online; and urge businesses and associations to coordinate with the government to better inform and educate vulnerable groups on how to responsibly engage in cyberspace through conducting public awareness campaigns and/or offering cybersecurity courses.

In pursuing such programs, insights and learnings can be drawn from the Ministry of Public Security and Viet Nam Women's Union's Cyber Safety Campaign for Girls,[54] the Ministry of Industry and Trade's Guidebook for Cyber Safety for the Elderly in 2023,[55] and the Viet Nam Women's Union's frequent partnership with private companies to share social responsibility for businesses. At the international level, Viet Nam should continue supporting the active participation of Vietnamese female officials and diplomats in UN cybersecurity conferences.

During the consultation, speakers repeatedly emphasized the importance of the youth, due to their social media expertise and exposure. As a vital asset to the country's digital economy and society, the Vietnamese government should increase funding and assistance to upgrade the youth's role in cyberspace through continuous education, training, and skills development, including contests or seminars. The Ministry of Foreign Affairs can also explore exchange opportunities for enhanced cyber research between Vietnamese and international universities.

Collaboration

Viet Nam and its international partners, especially ASEAN Member states, should promote collaboration on all fronts via (i) the harmonization of binding international legal frameworks to address cybercrime, privacy, and data protection, especially via the UN, APEC, and ASEAN. In doing so, the overarching frameworks should respect each member's sovereignty, regardless of size, and support Viet Nam's global and regional cybersecurity partnerships on capacity-building, technical assistance, and knowledge sharing; (ii) create international incident response mechanisms to facilitate real-time information-sharing about cyber incidents and coordinate joint responses; and (iii) develop a global set of cybersecurity standards to avoid inconsistencies among different existing standardization systems while respecting local cultures.

To effectively engage in international cooperation, Viet Nam also needs a strong technical foundation domestically, especially in incident management. Solutions that Viet Nam can proceed with on its own to better manage online incidents include changing the current approach of incident management, from incident response to incident prevention and threat management.

Collectively, the cybersecurity community must make problem-solving a routine activity rather than an occasional duty. CERTs must reevaluate their human assets based on expertise and quality instead of just relying on quantity. They should continue to participate in reality-based simulation exercises or perform infiltration testing and source code evaluation regularly. In addition, CERTs must widen their safety net so that they can capture all possible attacks that are subject to further forensic investigation. Most importantly, CERTs should increase local expertise in information safety, given that human capacity is limited. Lastly, Viet Nam needs to invest routinely to improve technology and regulations. Software or applications need to be carefully evaluated before being introduced to the system to fully minimize the chances of cyber incidents.

Community-building

ASEAN countries must reinforce mutual trust in cyberspace by strengthening current efforts on (i) constant communication and stock-taking on cyber norms,

cyberattacks, and risks across sectors and stakeholders; (ii) implementing regional cyber training and certification program schemes to streamline workforce qualifications and increase the supply of talents for the whole ASEAN cyber market and; (iii) highlighting success stories of the cyber points of contact directory among AMS and dialogue partners.

The ASEAN Secretariat must also amplify coordination efforts to achieve a more unified ASEAN participation at the UN and APEC; (iv) increase the frequency of regional cybersecurity simulations on early warning systems and situational responses to evaluate the group's collective preparedness; (v) establish a common regional framework to promote and harmonize approaches to technical standards, information, sharing, and capacity-building and; (vi) increase aid among members to address the digital infrastructure gap. Viet Nam could also consider promoting Cyber ASEAN in consultation with ASEAN as the regional cyber framework to advance a common position at the UN on cybersecurity, as it is in line with ASEAN's principles of consensus-based decision-making while leaving room for flexibility.

Conclusion

Viet Nam's cyber landscape has been changing rapidly, characterized by speedy and widespread internet coverage in just over 25 years. This was made possible by relentless efforts to upgrade cyber infrastructure and strong political will to promote economic digitalization. In response to the lack of human resources and technology, Viet Nam has been building a comprehensive legal framework domestically. The goal is to reinforce the concept of cyber sovereignty and standardizations and strengthen technical cooperation among key stakeholders amid the increasing vulnerability of its population, including marginalized groups.

Many Vietnamese businesses such as Viettel and FPT have taken active measures to integrate new platforms like AI and establish a CERT ecosystem vital to their incident and threat management toolkits. Internationally, Vietnam has been proactive in ASEAN and UN-related platforms. However, such efforts have their limits. Against the backdrop of the changing regional order, and alongside Viet Nam's ongoing journey of constructing a cyber realm while protecting its interests,

the open, iterative, and inclusive approach in multi-stakeholder initiatives unique to the Cyber ASEAN Framework can be a helpful reference for Viet Nam to fill the gap.[56]

CONCLUSION

Mark Bryan Manantan

With its ambitious goal of assembling the region's homegrown cyber-capacity assessment framework, Cyber ASEAN has pushed the boundaries on what and/or how cyber capacity-building should be. In conducting consultations from one country to another, Cyber ASEAN was able to test its underlying assumptions.

The main findings and outcomes of the four country consultations in Indonesia, Malaysia, the Philippines, and Viet Nam plus the virtual experts' meetings have shown that the Cyber ASEAN Framework is highly applicable, locally accepted, and context appropriate.[1] The framework's 3C approach of collaboration, consultation, and community-building is widely appreciated among the stakeholders and has confirmed the underlying principles of local context and ownership, agency, and autonomy, and Public-Private-People-Partnerships.[2]

Cyber ASEAN's four pillars, international collaboration, international technical standards, information-sharing and incident or threat management, and inclusion are present at various levels and capacities among the four countries.[3] Because of Cyber ASEAN's string of local engagements, a dedicated network of cybersecurity communities has been established—forming a legion of advocates that may lead to the framework's potential adoption and adaptation. This makes it feasible for the

Cyber ASEAN Framework to become Southeast Asia's homegrown cybersecurity assessment tool that complements ASEAN's top-down cyber policymaking and capacity-building initiatives.

Cognizant of the need for a more persuasive approach to cyber policymaking in Southeast Asia, Cyber ASEAN has further strengthened its case as the region's cyber policy tool of choice by elaborating its strategic, economic, and inclusive imperatives. May the insights and outcomes encourage policymakers, practitioners, and experts to prioritize cybersecurity at the apex of national policymaking, backed by adequate resources and political will. In practice, this means narrowing the implementation gap through incentives and inducements where and when appropriate and constantly reinforcing partnership-building across a wide swath of stakeholders.

With its vicissitudes and challenges, there is no doubt that confidence in ASEAN's agency and autonomy is declining. However, in times of great crises, ASEAN looks to its greatest source of strength and resilience—its people. The project has made the process as dynamic, collaborative, and inclusive as possible. From incubation to operationalization, Cyber ASEAN has created a multistakeholder platform, drawing individuals and communities from different backgrounds. In emphasizing the often-missing perspectives, the framework installed the "people" aspect to cement a public-private-people-partnership. It has set the stage for future cyber capacity-building engagements through which local stakeholders, who lacked the opportunities to access regional and international discussions and forums in Tokyo, New York, Paris, or Geneva, are afforded a platform for their voices to be heard.

As we conclude the pilot run of Cyber ASEAN, I would argue that the greatest cybersecurity threat facing Southeast Asia is not the cyber threat actors or the looming implications of generative AI but the prevailing trust deficit. Across

Indonesia, Malaysia, the Philippines, and Viet Nam, the lack of trust is obvious, permeating all levels—from individuals, organizations, sectors and governments, to nation-states. Such a reality undercuts the successful implementation of any cybersecurity policy or regional strategy and initiatives. To this end, Cyber ASEAN has the bold aim of patching such vulnerability. Through its iterative and inclusive approaches that brought together key stakeholders, and created an open, safe, and neutral space specific concerns were raised, joint solutions were recommended, and ultimately trust was fostered and elevated.

In harnessing the distinct lens and expertise of the cybersecurity community within and beyond the four countries covered, Cyber ASEAN has catalyzed a significant step toward a pragmatic and regional approach to cyber resiliency and capacity—one that is built on mutual trust and sealed with local buy-in and ownership among Southeast Asians for Southeast Asia.

End Notes

Part I. Foundation of Cyber Asean

Reimagining Cyber Capacity-Building in Southeast Asia: The Cyber ASEAN Framework. *Mark Bryan Manantan*

1 Google, Temasek, Bain, "e-Conomy SEA 2022," *Temasek*, 2022, https://www.temasek.com.sg/content/dam/temasek-corporate/news-and-views/resources/reports/e_Conomy_SEA_2022_report.pdf.

2 Global Forum on Cyber Expertise, Working Group A – Task Force Strategy and Assessments, "Global Overview of Existing National Cyber Capacity Assessment Tools (GOAT)," *GFCE*, 2021, https://ocsc.com.au/wp-content/uploads/2021/12/Global-Overview-of-Assessment-Tools_CLEAN_17Aug.pdf.

3 Stakeholder consultation

4 *Ibid.*

5 *Ibid*.

6 *Ibid*.

7 *Ibid.*

8 *Ibid.*

9 Elina Noor and Mark Bryan Manantan, "Raising Standards: Data and Artificial Intelligence," *Asia Society Policy Institute*, July 2022, https://asiasociety.org/sites/default/files/inline-files/ASPI_RaisingStandards_report_fin_web_0.pdf.

10 "ASEAN Cybersecurity Cooperation Strategy, 2021-2025," *ASEAN*, accessed December 20, 2023, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_fi-

nal-23-0122.pdf.

11 Elina Noor and Mark Bryan Manantan, "Raising Standards: Data and Artificial Intelligence,"

12 "Harnessing the Potential of Big Data," *Asian Development Bank*, May 2022, https://www.adb.org/sites/default/files/publication/793596/potential-big-data-post-pandemic-southeast-asia.pdf.

13 Stakeholder consultation.

14 Stakeholder consultation.

Tracing the Development of Cyber Cooperation in ASEAN: Progress and Shortcomings. *Mabda Haerunnisa Fajrilla Sidiq*

1 Candice Tran Dai & Miguel Alberto Gomez, "Challenges and opportunities for cyber norms in ASEAN," *Journal of Cyber Policy* 3, Issue 2 (2018): 217-235, https://doi.org/10.1080/23738871.2018.1487987.

2 ITU, *Global Cybersecurity Index 2020* (Geneva, 2021), 25-27, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

3 S. Iswaran, "Opening Remarks by Mr S Iswaran, Minister for Communications and Information and Minister-in-Charge of Cybersecurity at SICW Press Conference," *Cyber Security Agency Singapore*, October 2, 2019, https://www.csa.gov.sg/news/speeches/sicw-2019press-conference.

4 ASEAN, *ASEAN Cybersecurity Cooperation Strategy (2021-2025)*, 2022, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

5 Eugene E.G. & Benjamin Ang, "ASEAN Ambiguity on International Law and Norms for Cyberspace," *Baltic Yearbook of International Law Online* 20, no. 1

(2022): 133-162, https://doi.org/10.1163/22115897_02001_008

6 Jayant Menon & Anna Cassandra Melendez, "Realizing an Asean Economic Community: Progress and Remaining Challenges," T*he Singapore Economic Review* 62, no. 3 (2017): 681-702, https://doi.org/10.1142/S0217590818400052.

7 Caitríona H. Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime," *Asia Policy*, no. 18, (July 2014): 131-160, https://www.jstor.org/stable/24905282.

8 Mark Bryan F. Manantan, "Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia," *Australian Journal of International Affairs 75*, Issue 4 (2021): 432-459, https://doi.org/10.1080/10357718.2021.1926423.

9 ASEAN, *ASEAN Cybersecurity Cooperation Strategy (2021-2025)*.

Buffering: Southeast Asia's Response to Cyber Insecurity. *Mark Bryan Manantan and Lesley Manantan*

1 Stakeholder consultations

2 Cyber Threat Tracker, Cyber ASEAN," accessed February 1, 2023, http: cybera-sean.pacforum.org.

3 *Ibid.*

4 *Ibid.*

5 *Ibid.*

6 Mark Bryan Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea," *Issues and Studies* 56, no. 3, (2020): https://doi.org/10.1142/S1013251120400135; Cyber Threat Tracker.

7 *Ibid.*

8 *Ibid.*

9 *Ibid.*

10 Stakeholder consultation

11 *Ibid.*

12 *Ibid.*

13 *Ibid.*

14 *Ibid.*.

15 *Ibid.*

16 *Ibid.*

17 *Ibid.*

18 *Ibid.*

19 *Ibid.*

20 *Ibid.*

21 *Ibid.*

22 Mark Bryan Manantan, "Cyber Diplomacy Cooperation on Cybercrime between Southeast Asia and Commonwealth Countries," *Commonwealth Cybercrime Journal*, 133 (2023), https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-03/D19156-CCJ-1-1-Cyber-Diplomacy-Cybercrime-SE-Asia-Commonwealth--Manantan.pdf.

23 Stakeholder consultation.

24 *Ibid.*

25 *Ibid.*

Assessing the Economic Benefits of Cybersecurity Standards in Southeast Asia. *Adrian Glova and Mark Bryan Manantan*

1 Knut Blind, Andre Jungmittag, and Alex Mangelsdorf, "The economic benefits of standardization," *DIN German Institute for Standardization*, 2011, https://www.din.de/resource/blob/89552/68849fab0eeeaafb56c5a3ffee9959c5/economic-benefits-of-standardization-en-data.pdf.

2 "Economic benefits of Standards," *International Organization for Standardization*, 2014, https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/ebs_case_studies_factsheets.pdf.

3 "Standards and Economic Growth: ISO members' research on the impact of standards on their national economies," *International Organization for Standardization*, 2021, https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100456.pdf.

4 "Economic Impact of Standards: Methodological Guidance," *International Organization for Standardization*," 2022, https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100465.pdf.

5 Gregory Tassey, "The Impacts of Technical Standards on Global Trade and Economic Efficiency," *East West Center*, 2015, https://www.eastwestcenter.org/sites/default/files/filemanager/pubs/pdfs/5-2Tassey.pdf.

6 Jorge Padilla, John Favies, and Aleksandra Boutin, "Economic Impact of Technology Standards," *Compass Lexecon*, 2017, https://www.compasslexecon.com/wp-content/uploads/2018/04/CL_Economic_Impact_of_Technology_

Standards_Report_FINAL.pdf.

7 This variable is equal to one in 2020 up to 2022 to capture the disruption caused by the pandemic.

8 The National Cybersecurity Plan (NCSP) was launched in 2017, serving as the roadmap for the country's cybersecurity efforts. In the same year, DICT issued three (3) Memorandum Circulars (MCs) namely: Memorandum Circular 005-2017 Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructure (CII); Memorandum Circular 006-2017 Prescribing the Policies, Rules and Regulations on the Protection of Government Agencies; and Memorandum Circular 007-2017 Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructure (CII).

9 This was formalized by the Ministry of Communications and Information Technology (MCIT) Regulation No. 4 of 2016 which mandates the implementation of such standards.

10 Malaysia has multiple government bodies regulating and managing its cybersecurity led by the National Cyber Security Agency, Malaysia, Ministry of Communications, Ministry of Digital, Malaysia Communications and Multimedia Commission, and Cybersecurity Malaysia.

11 These include the United States, International Monetary Fund, World Bank, Organization for Economic Co-operation and Development, and EuroStat.

12 National Accounts of the Philippines, "GDP Expands by 5.6 Percent in the Fourth Quarter of 2023: Brings the Full-Year 2023 GDP Growth Rate to 5.6 Percent," *PSA*, January 31, 2024, https://psa.gov.ph/statistics/national-accounts.

13 "Macroeconomic statistics," *BPS-Statistics Indonesia*, Accessed December 20, 2023,https://www.bps.go.id/en/statistics-table?subject=530.

14 "National Accounts," *Official Portal of Ministry of Economy*, Accessed December 20, 2023,https://www.ekonomi.gov.my/en/socio-economic-statistics/socio-economic/national-accounts.

15 "National Accounts," *General Statistics Office*, Accessed December 20, 2023, https://www.gso.gov.vn/en/national-accounts/.

16 In technical terms, variables tracked over time have to be "stationary" (that is, they should not display a trend over time) before regression analysis can be conducted. This is because spurious or unreliable correlations will be made if stationarity is not handled. Imagine regressing GDP against the age of a person over time, both of which are trending up over time. It would be faulty to conclude that GDP and his/her age are positively related, when both variables just share a common, upward trend. To handle this, variables are transformed (i.e. differenced) so that the changes in the levels of variables are inputted in correlation and regression analysis rather than the nominal values. The down-side is that estimated relationships are less interpretable as opposed to regular regression analysis, but this is a unique feature that must be accounted for in time-series regression.

Part II. Application of Cyber Asean

Indonesia. *Fitri Bintang Timur*

1 Siwage Dharma Negara and Astrid Meliasari-Sugiana, "The State of Indonesia's Digital Economy in 2022," *Fulcrum*, November 23, 2022, https://fulcrum.sg/the-state-of-indonesias-digital-economy-in-2022/.

2 Simon Kemp, "Digital 2023: Indonesia," *Datareportal.* , February 9, 2023, https://datareportal.com/reports/digital-2023-indonesia#:~:text=There%20were%20212.9%20million%20internet,percent%20of%20the%20total%20population.

3 MIT Technology Review, *The Cyber Defence Index* 2022/23, 2023, https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/.

4 Aditya Hadi, "Cybersecurity Threats in Indonesia Decreasing, with AI Deployed by Both Sides," *Jakarta Post*, August 31, 2023, https://www.thejakartapost.

com/business/2023/08/30/cybersecurity-threats-decreasing-with-ai-deployed-by-both-sides.html.

5 Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation, "President Jokowi Issues Presidential Regulation on Protection for Vital Information Infrastructure," *Setkab News*, June 15, 2022, https://setkab.go.id/en/president-jokowi-issues-presidential-regulation-on-protection-for-vital-information-infrastructure/.

6 *Ibid.*

7 Surfshark, "Data Breaches Rise Globally in Q3 of 2022," *Surfshark in Cybersecurity*, October 19, 2022, https://surfshark.com/blog/data-breach-statistics-2022-q3.

8 Ministry of Communications and Information Technology of the Republic of Indonesia, "Rapat Paripurna DPR Sahkan RUU PDP – Ditjen Aptika," *Aptika News*, September 29, 2022, https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu-pdp/.

9 PwC, "A Comparison of Cybersecurity Regulations: Indonesia," *PwC Publication*, 2023, https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations.html.

10 "Indonesia Presidential Regulation No. 47 of 2023 on National Cyber Security Strategy and Cyber Crisis Management," *President of the Republic of Indonesia*, 2023, https://peraturan.go.id/files2/perpres-no-47-tahun-2023_terjemah.pdf.

11 Citra Fatihah, "Indonesia's Approach on Cyberattack Attribution Through Its Foreign Policy," *Global Legal Review*, Vol. 22, No. 2, pp. 121-42. https://doi.org/10.19166/glr.v2i2.5140.

12 Ministry of Foreign Affairs of the Republic of Indonesia, "Indonesia Voices Cyber Stability in the UN," *Indonesian Way*, May 23, 2020, https://kemlu.go.id/portal/en/read/1327/berita/indonesia-voices-cyber-stability-in-the-un.

13 Gijs van Loon and Shannon Ayre, "First Ever Cyber Diplomacy Course in Indo-

nesia," *Clingendale News*, August 17, 2023, https://www.clingendael.org/news/first-ever-cyber-diplomacy-course-indonesia.

14 Department of Foreign Affairs and Trade of Australia, "Third Australia-Indonesia Cyber Policy Dialogue," *DFAT News*, September 2, 2020, https://www.dfat.gov.au/news/news/third-australia-indonesia-cyber-policy-dialogue.

15 Administrator, "Indonesia Accounts for 40% Digital Transaction Value in ASEAN," *Portal Informasi Indonesia*, July 11, 2023, https://indonesia.go.id/kategori/asean-2023-variety/7264/indonesia-accounts-for-40-digital-transaction-value-in-asean?lang=2#:~:text=Indonesia%20is%20a%20significant%20player,Authority%20(OJK)%20in%202022.

16 Ministry of Communications and Information Technology of the Republic Indonesia, "Dukung Akselerasi Pengembangan Ekonomi Digital, Keamanan Siber Jadi Prioritas Nasional," *Kominfo News*, July 7, 2023, https://www.kominfo.go.id/content/detail/50066/dukung-akselerasi-pengembangan-ekonomi-digital-keamanan-siber-jadi-prioritas-nasional/0/berita.

17 Barnaby Lewis, "G20 Indonesia: International Standards Summit 2022," *ISO News*, October 20, 2022, https://www.iso.org/contents/news/2022/10/int-standards-summit-2022.html.

18 Farisya Setiadi, Yudho G. Sucahyo, and Zainal A. Hasibuan, "An Overview of the Development National Cyber Security," *International Journal of Information Technology & Computer Science (IJITC)*, Vol. 6, November/December, 2012; Dwiyani, Permatasari, "Tantangan Cyber Security di Era Revolusi Industri 4.0," *Kemenkeu News*, August 31, 2021, https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-Era-Revolusi-Industri-40.html.

19 Janitra Haryanto and Anisa P. Mantovani, "ISO/IEC 27001: An Alternative for Indonesian Fintech Cybersecurity," *Center for Digital Society Case Studies Series*, April 2019, https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/01/48-CfDS-Case-Study-ISO-IEC-27001-An-Alfternative-for-Indonesian-Fintech-Cybersecurity.pdf.

20 Ministry of Communications and Information Technology of the Republic of Indonesia, "Indeks Keamanan Informasi", *Kominfo News*, October 2013, https://www.kominfo.go.id/index.php/content/detail/3326/Indeks+Keamanan+Informasi+%28KAMI%29/0/kemanan_informasi.

21 Ministry of Communications and Information Technology of the Republic of Indonesia, "PSE Eksisting Wajib Lakukan Pendaftaran Hingga Oktober 2020," *Kominfo News*, July 28, 2020, https://www.kominfo.go.id/content/detail/28202/pse-eksisting-wajib-lakukan-pendaftaran-hingga-oktober-2020/0/berita_satker.

22 I Nyoman Aji Suadhana, Dudi H. Rai, and Asep Kamaluddin, "The Role of Indonesia to Create Security and Resilience in Cyber Spaces," *Indonesia Parliament–Journal - Jurnal Politica*, Vol. 13, No. 1, 2022, https://jurnal.dpr.go.id/index.php/politica/article/view/2641.

23 Muhamad Rizal and Yanyan M. Yani. "Cybersecurity Policy and Its Implementation in Indonesia," *Journal of ASEAN Studies*, Vol. 4, No. 1, 2016, pp. 61-78, https://doi.org/10.21512/jas.v4i1.967.

24 Leonardus K. Nugraha and Dinita A. Putri, "Mapping the Cyber Policy Landscape: Indonesia," *Global Partners Digital*, November 2016, https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf.

25 Administrator, "G20 International Standard Summit," *Event Announcement*, October 20, 2022, https://www.worldstandardscooperation.org/g20/g20-2022/.

26 ASEAN Secretariat, A*SEAN Cybersecurity Cooperation Strategy*, February 2022, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

27 *Ibid*.

28 Stakeholder consultation.

29 Wanying Zhao and Gregory White, "A collaborative information sharing fra-

mework for community cyber security," *IEEE Conference on Technologies for Homeland Security*, November 2012, pp. 457–462, https://ieeexplore.ieee.org/document/6459892.

30 Indonesia Presidential Regulation No. 133 of 2017 on Amendment To Presidential Regulation Number 53 Of 2017 on National Cyber and Crypto Agency, Article 2, https://www.peraturan.go.id/files2/perpres-no-133-tahun-2017_terjemah.pdf.

31 Ministry of Communications and Information Technology of the Republic of Indonesia, "Perkuat Pertahanan Siber, Kominfo Bentuk CIIP ICT Sector," *Kominfo News*, September 19, 2018, https://www.kominfo.go.id/content/detail/14509/perkuat-pertahanansiber-kominfo-bentuk-ciip-ict-sector/0/berita_satker.

32 Farouq Aferudin and Kalamullah Ramli, "The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia," *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, Vol. 5, No, 3, 2022, https://doi.org/10.33258/birci.v5i3.6297.

33 Stakeholder consultation.

34 Stakeholder consultation.

35 *Ibid.*

36 *Ibid.*

37 Stakeholder consultation.

38 Nugraha and Putri, "Mapping the Cyber Policy Landscape".

39 Ministry of Communications and Information Technology of the Republic of Indonesia, "Atasi Kesenjangan Digital, Menkominfo Dorong Transformasi Digital Inklusif," *Press Release,* August 6, 2021, https://www.kominfo.go.id/content/detail/36185/siaran-pers-no-268hmkominfo082021-tentang-atasi-kesenjangan-digital-menkominfo-dorong-transformasi-digital-inklusif/0/siaran_pers.

40 Politeknik Siber dan Sandi Negara, "Menciptakan Insan Keamanan Siber yang Bertalenta, Poltek SSN melakukan penandatanganan kerjasama Cybersecurity Training dengan Infra Digital Foundation (IDF) dan Mastercard Center for Inclusive Growth," , February 2022, https://poltekssn.ac.id/artikel/menciptakan-insan-keamanan-siber-yang-bertalenta-poltek-ssn-melakukan-penandatanganan-kerjasama-cybersecurity-training-dengan-infra-digital-foundation-idf-dan-mastercard-center-for-inclusive-growth/.

41 World Bank, "Indonesia - Gender Equality: Gender Mainstreaming," *World Bank Document Database*, 2013, https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/746211468051553636/indonesia-gender-equality-gender-mainstreaming.

42 Audit Board of the Republic of Indonesia, "Peraturan Badan Siber dan Sandi Negara No. 5 Tahun 2020 tentang Rencana Strategis Badan SIber dan Sandi Negara Tahun 2020-2024," *Regulation Database*, 2024, https://peraturan.bpk.go.id/Details/174282/peraturan-bssn-no-5-tahun-2020.

43 Yoonee Jeong, "Asia Pacific Connections: Bridging the Digital Divide," *East Asia Forum Quarterly*, July 7, 2022, https://www.eastasiaforum.org/2022/07/07/bridging-the-digital-divide/.

44 Yayasan Anak Bangsa and Gojek, "Landscape of digital skills demand in Indonesia," *International Labor Organization Meeting Document Publication*, June 29, 2021, https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-jakarta/documents/meetingdocument/wcms_808837.pdf.

45 Stakeholder consultation.

46 *Ibid.*

47 *Ibid.*

48 Andreas Ulfen, "The Rise of Digital Repression in Indonesia under Joko Widodo," *Giga Focus Asia*, No. 1, January 2024, https://www.giga-hamburg.de/en/publications/giga-focus/the-rise-of-digital-repression-in-indonesia-under-joko-widodo.

49 Stakeholder consultation.

Malaysia. *Farlina Said*

1 "Milestones," *CyberSecurity Malaysia*, Accessed December 20, 2023, https://www.cybersecurity.my/en/about_us/milestones/main/detail/2325/index.html.

2 National Security Council, "ASEAN Regional Forum (ARF) Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects, National Cyber Security Management in Malaysia," *ASEAN Regional Forum*, 2013, https://aseanregionalforum.asean.org/wp-content/uploads/2019/10/Annex-IV-National-Cyber-Security-Management-in-Malaysia.pdf.

3 National Security Council, "ASEAN Regional Forum (ARF) Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects, National Cyber Security Management in Malaysia" .

4 Mohd Shamir Hashimm "Malaysia's National Cyber Security Policy: The country's cyber defence initiatives," *IEEE*, 2011, https://ieeexplore.ieee.org/document/5978782,

5 "Corporate Overview," *CyberSecurity Malaysia*, Accessed December 10, 2023, https://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html.

6 Bernama, "PM Anwar: Communications and Digital Ministry split to meet growing demands of portfolio," 2023, December 12, 2023, https://www.malaymail.com/news/malaysia/2023/12/1D2/pm-anwar-communications-and-digital-ministry-split-to-meet-growing-demands-of-portfolio/107116.

7 Arfa Yunus," Cybersecurity Bill on the cards, but sector needs more skilled workers," The Star, November 24, 2023, https://www.thestar.com.my/news/nation/2023/11/24/cybersecurity-bill-on-the-cards-but-sector-needs-more-skilled-workers.

8 "About Us," *NISER*, Accessed December 12, 2023, https://niser.org.my/about.html.

9 "Communications and Multimedia Act 1998," *MCMC*, December 11, 2023, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act588bi_3.pdf.

10 Malaysia Office of the Chief Government Security Officer, "Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam," *Department of Prime Minister*, December 10, 2023, https://www.cgso.gov.my/en/pengumuman/garis-panduan-pengurusan-keselamatan-maklumat-melalui-pengkomputeran-awan-cloud-computing-dalam-perkhidmatan-awam/

11 Stakeholder consultation.

12 "Heightened Alert for Cyber Activities on Domains and Infrastructures in Malaysia," *NACSA*, Accessed December 10, 2023, https://www.nacsa.gov.my/advisory10.php.

13 Aqil Hamzah, "Nearly 100 hacker groups take Israel-Hamas conflict into cyberspace by waging online proxy war," T*he Straits Times*, October 12, 2023, https://www.straitstimes.com/world/hackers-take-sides-in-israel-hamas-conflict-by-waging-proxy-war-in-cyberspace.

14 "Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2019," *MyCERT*, Accessed December 25, 2023, https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=0d39dd96-835b-44c7-b710-139e560f6ae0.

15 "Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2020," *MyCERT*, Accessed December 25, 2023, https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228.

16 "Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2021," *MyCERT*, Accessed December 25, 2023, https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-

66677d694932&id=77be547e-7a17-444b-9698-8c267427936c.

17 "Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2022," *MyCERT*, Accessed December 25, 2023, https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=4e056ced-6983-4487-a5d2-56c10879a24b

18 "Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2023," *MyCERT*, Accessed December 25, 2023, https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=f3f3ca31-1a85-4372-a321-a9b6cf097b0b.

19 "Palo Alto Networks Unveils 2023 ASEAN Cybersecurity Report: Malaysia's Alarming Disruptive Attack Surge and Budget Boost," *SME*, September 12, 2023, https://sme.asia/palo-alto-networks-unveils-2023-asean-cybersecurity-report-malaysias-alarming-disruptive-attack-surge-and-budget-boost/.

20 Dashveenjit Kaur, "Malaysia faces cyberthreat surge: phishing dominates, ransomware doubles," *Techwire Asia*, December 15, 2023, https://techwireasia.com/12/2023/what-is-behind-the-worsening-state-of-cybersecurity-in-malaysia/.

21 "ICT Use by Individual. *Ministry of Economy Department of Statistics*," Accessed December 15, 2023, https://www.dosm.gov.my/uploads/release-content/file_20230531124923.pdf.

22 "Fahmi: We have 70.2% of 5G coverage nationwide," *The Star*, October 10, 2023, https://www.thestar.com.my/news/nation/2023/10/10/fahmi-we-have-702-of-5g-coverage-nationwide.

23 Angelin Yeoh, "MCMC: Current 5G adoption rate remains low at 1.2 million subscribers," *The Star,* June 1 2023, https://www.thestar.com.my/tech/tech-news/2023/06/01/mcmc-current-5g-adoption-rate-remains-low-at-12-million-subscribers.

24 Mark Manantan. "Defining Cyber Diplomacy," *Australia Outlook*, November 10, 2021, https://www.internationalaffairs.org.au/australianoutlook/defining-cy-

ber-diplomacy/.

25 Stakeholder consultation.

26 "Security Outlook," ASEAN, 2021, https://asean.org/wp-content/uploads/2021/10/ASEAN-Security-Outlook-ASO-2021.pdf.

27 "Security Outlook," ASEAN, 2021.

28 Stakeholder consultation.

29 *Ibid.*

30 "Call to action on responsible use of AI in the military domain," G*overnment of Netherlands*, February 16, 2023, https://www.government.nl/latest/news/2023/02/16/reaim-2023-call-to-action.

31 Stakeholder consultation.

32 *Ibid.*

33 *Ibid.*

34 *Ibid.*

35 Mishell Arwan, "Singapore Cybersecurity Licensing," I*nternational Trade Administration*, November 8, 2022, https://www.trade.gov/market-intelligence/singapore-cybersecurity-licensing.

36 "Frequently asked questions: Cybersecurity Audit for CII," *CSA*, Accessed December 15, 2023. https://www.csa.gov.sg/faq/cybersecurity-audit-for-cii.

37 "Cybersecurity Framework Quick Start Guide," NIST, Accessed December 12, 2023, https://www.nist.gov/cyberframework/getting-started/quick-start-guide.

38 Paul Kirvan, "Top 12 IT security frameworks and standards explained," T*echTarget*, October 27, 2023. https://www.techtarget.com/searchsecurity/tip/IT-secu-

rity-frameworks-and-standards-Choosing-the-right-one.

39 Stakeholder consultation.

40 *Ibid.*

41 Stakeholder consultation.

42 *Ibid.*

43 *Ibid.*

44 *Ibid.*

45 *Ibid.*

46 *Ibid*.

47 *Ibid.*

48 "Optimising Resources," *MCMC*, 2016, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-AR2016-Eng.pdf

49 "About Us," *National Cyber Coordination and Command Centre*, Accessed December 12, 2023 https://www.nc4.gov.my/about-us.

50 Stakeholder consultation.

51 *Ibid.*

52 *Ibid.*

53 *Ibid.*

54 *Ibid.*

55 Stakeholder consultation.

56 Bernama, "15th ADMM: Malaysia calls for cyber defence network in ASEAN," *The New Straits Times*, June 15, 2021, https://www.nst.com.my/news/nation/2021/06/699104/15th-admm-malaysia-calls-cyber-defence-network-asean.

57 Stakeholder consultation.

58 *Ibid*.

59 *Ibid.*

60 Stakeholder consultation.

61 "ICT Use by Individual," *Ministry of Economy Department of Statistics*, Accessed December 11, 2023, https://www.dosm.gov.my/uploads/release-content/file_20230531124923.pdf.

62 "ICT Access by Household," *Ministry of Economy Department of Statistics*, Accessed December 11, 2023, https://www.dosm.gov.my/uploads/release-content/file_20230531124942.pdf.

63 "Malaysia needs 27,000 cybersecurity knowledge workers by end-2025," *FMT*. August 15, 2023, https://www.freemalaysiatoday.com/category/business/2023/08/15/malaysia-needs-27000-cybersecurity-knowledge-workers-by-end-2025/.

64 "Malaysia Cyber Security Strategy 2020-2024," *MKN*, 2020, https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf.

65 "Malaysia needs 27,000 cybersecurity knowledge workers by end-2025," *FMT*.

66 "Digital Up: Reskilling/Upskilling Incentive," *MDEC*, Accessed December 10, 2023, https://mdec.my/digitalup.

67 "Program Snapshot - APAC Cybersecurity Fund," *The Asia Foundation*, Accessed December 10, 2023,https://asiafoundation.org/2023/10/09/apac-cybersecurity-fund/.

68 Stakeholder consultation

69 *Ibid.*

70 Stakeholder consultation

71 *Ibid.*

72 *Ibid.*

73 *Ibid.*

Philippines. *Genalyn Macalinao*

1 Data obtained from interviews https://www.ncert.gov.ph

2 Rodolfo A. Salalima, "DICT Memorandum Circular 005-2017. Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructures (CII) as stipulated in the National Cybersecurity Plan (NCSP) 2022," *DICT*, August 1, 2017, https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-005.pdf.

3 Rodolfo A. Salalima, "DICT Memorandum Circular 006-2017. Prescribing the Policies, Rules and Regulations on the Protection of Government Agencies as stipulated in the National Cybersecurity Plan (NCSP) 2022," DICT, August 1, 2017, https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-006.pdf.

4 Rodolfo Salalima, "DICT Memorandum Circular 007-2017. Prescribing the Policies, Rules and Regulations on the Protection of Individuals as stipulated in the National Cybersecurity Plan (NCSP)," *DICT*, August 1, 2017 https://dict.gov.ph/

wp-content/uploads/2017/09/Memorandum-Circular-007.pdf.

5 Telecommunications and Information Working Group, "APEC framework for securing the digital economy," *Asia-Pacific Economic Cooperation*, November 2019, https://www.apec.org/publications/2019/11/apec-framework-for-securing-the-digital-economy,

6 "The Budapest Convention," *Council of Europe*, Accessed December 23, 2023, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

7 Stakeholder consultation.

8 "Bureau of Philippine Standards Technical Committees, *DTI*, Accessed December 10, 2023, https://www.bps.dti.gov.ph/images/SDD_Files/BPS_TC_Profile_-_First_Edition.pdf

9 "Regulations," *Bangko Sentral ng Pilipinas*, Accessed December 12, 2023, https://www.bsp.gov.ph/SitePages/Regulations/RegulationsList.aspx?TabId=1.

10 Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," *NIST Special Publication 800-53 Revision 5*, September 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

11 Stakeholder consultation.

12 *Ibid*.

13 *Ibid.*

14 Stakeholder consultation.

15 *Ibid.*

16 DICT, "Supplementing the DICT Memorandum Circular Nos. 005, 006 and 007, series of 2017, and Policies, Rules and Regulations on the Implementation of the National Cybersecurity Plan 2022," *DICT Department Circular 003-2020*, March 9, 2020, https://dict.gov.ph/wp-content/uploads/2020/03/Dept-Circu-

lar-No-003-3062020.pdf.

17 Stakeholder consultation.

18 *Ibid.*

19 "Cybersecurity Workforce Study 2022," *ISC*^{2}, Accessed December 10, 2023, https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

20 Stakeholder consultation.

21 *Ibid.*

22 "Procurement guidelines for cybersecurity in hospitals," *European Union Agency for Cybersecurity*, February 24, 2020, https://www.enisa.europa.eu/publications/good-practices-for-thesecurity-of-healthcare-services.

23 "Health Policies and Laws," *Department of Health*, Accessed December 11, 2023, https://dmas.doh.gov.ph:8083/Search.

24 "Women in Cybersecurity 2022 Report," *Cybersecurity Ventures*, 2022, https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf.

Viet Nam. *Nguyễn Việt Lâm, Ph.D. and Đỗ Hoàng*

1 "25 years of internet access marked in Vietnam", *MIC*, December 12, 2022, https://english.mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=156699.

2 "Viet Nam Has over 72 Million Internet Users," *MIC*, December 9, 2022, https://english.mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=156626.

3 Stakeholder consultation.

4 "Xu Hướng Phát Triển Internet Việt Nam 2023," *VNetwork*, January 16, 2023, https://www.vnetwork.vn/news/internet-viet-nam-2023-so-lieu-moi-nhat-va-xu-huong-phat-trien/.

5 *Ibid.*

6 *Ibid.*

7 "Internet Brings New Opportunities to Vietnam," *The Voice of Vietnam – VOV World*, November 23, 2023, https://vovworld.vn/en-US/news/internet-brings-new-opportunities-to-vietnam-1250023.vov.

8 "Vietnam's Internet Economy Predicted to Hit 49 Billion USD by 2025," *VietnamPlus*, November 23, 2023, https://en.vietnamplus.vn/vietnams-internet-economy-predicted-to-hit-49-billion-usd-by-2025/271674.vnp.

9 Google, Temasek and Bain & Company, "2022. e-Conomy SEA 2022", *Temasek*, July 18, 2022. https://www.temasek.com.sg/content/dam/temasek-corporate/news-and-views/resources/reports/e_Conomy_SEA_2022_report.pdf.

10 Simon Kemp, "Digital 2023: Vietnam - *Datareportal* – Global Digital Insights," DataReportal, February 13, 2023, https://datareportal.com/reports/digital-2023-vietnam.

11 VietNamNet, "Vietnam Changes Rapidly after 25 Years of Internet Connection," *VietNamNet News*, December 8, 2022, https://vietnamnet.vn/en/vietnam-changes-rapidly-after-25-years-of-internet-connection-2088999.html.

12 Đỗ Phong, "Sắp Có Thêm Tuyến Cáp Biển Mới Được Đưa Vào Vận Hành," *VNEconomy*, February 13, 2023, https://vneconomy.vn/sap-co-them-tuyen-cap-bien-moi-duoc-dua-vao-van-hanh.htm.

13 Trần Quang Huy, "Việt Nam Sắp Có Tuyến Cáp Quang Biển Mới Trị Giá 300 Triệu USD," *Thegioididong*, April 28, 2023, https://www.thegioididong.com/tin-tuc/viet-nam-sap-co-them-tuyen-cap-quang-moi-1527862.

14 "Vietnam Digital Transformation Agenda - *Open Development Vietnam*," *Open*

Development Vietnam, December 19, 2023, https://vietnam.opendevelopmentmekong.net/topics/vietnam-digital-transformation-agenda/#return-note-3850949-20.

15 "Inauguration Ceremony of National Innovation Center and Vietnam International Innovation Expo 2023," *MPI*, October 28, 2023, https://www.mpi.gov.vn/en/Pages/2023-10-31/Inauguration-ceremony-of-National-Innovation-Centet-zww8f.aspx.

16 Stakeholder consultation.

17 IBM Security, "Cost of a Data Breach 2022," *IBM*, August 3, 2022, https://community.ibm.com/community/user/security/events/event-description?CalendarEventKey=7097fd42-4875-4abe-9ff6-d556af01688b&CommunityKey=-96f617c5-4f90-4eb0-baec-2d0c4c22ab50&Home=%2Fcommunity%2Fuser%-2Fsecurity%2Fevents%2Fevent-description

18 "Năm 2022, Ghi Nhận Hơn 12.935 Trường Hợp Lừa Đảo Trực Tuyến," *Thanh tra Chính phủ*, January 9, 2023, https://thanhtra.com.vn/phap-luat/an-ninh-trat-tu/nam-2022-ghi-nhan-hon-12-935-truong-hop-lua-dao-truc-tuyen-206377.html.

19 "Gần 31% Học Sinh Là Nạn Nhân Của Bắt Nạt Trực Tuyến," *VTC News*, January 4, 2019, https://vtc.vn/gan-31-hoc-sinh-la-nan-nhan-cua-bat-nat-truc-tuyen-ar450372.html.

20 *Ibid.*

21 Authors' note: Apart from the ensurance of cyber safety, these documents also show that Viet Nam wants to seize the opportunities that the "Fourth Industrial Revolution" has promised by building up a nationwide information and communication technology (ICT) infrastructure for the overall national digital transformation.

22 "Law No. 101/2015/QH13 Criminal Procedure Code," *Vanbanphapluat*, November 27, 2015, https://vanbanphapluat.co/law-no-101-2015-qh13-criminal-procedure-code.

23 "Decree on the prevention of online information conflicts," *Thư viện pháp luật*, October 14, 2016, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Decree-142-2016-ND-CP-prevention-online-information-conflicts-331512.aspx.

24 "Law 24/2018/QH14 Cybersecurity," *Thư viện pháp luật*, June 12, 2018, https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Law-24-2018-QH14-Cybersecurity/388829/tieng-anh.aspx.

25 "Decision No. 749/QD-TTG 2020 National Digital Transformation Program through 2025," *LuatVietnam*, June 3, 2020, https://english.luatvietnam.vn/decision-no-749-qd-ttg-on-approving-the-national-digital-transformation-program-until-2025-with-a-vision-184241-doc1.html.

26 "Nghị Định 53/2022/NĐ-CP Hướng Dẫn Luật an Ninh Mạng Mới Nhất," *Thư viện pháp luật*, August 15, 2022, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-53-2022-ND-CP-huong-dan-Luat-An-ninh-mang-398695.aspx.

27 "Decision No. 964/QD-TTG Dated August 10, 2022 on Approving Strategy for National Cyber Safety and Security, Active Response to Challenges from Cyberspace until 2025 and Vision to 2030," *LawNet*, October 8, 2022, https://lawnet.vn/en/vb/Decision-964-QD-TTg-2022-Strategy-for-national-cyber-safety-and-security-until-2025-8B901.html.

28 "National Steering Committee for Cyber Safety and Security Makes Debut," *Báo Chính phủ*, November 24, 2020, https://en.baochinhphu.vn/national-steering-committee-for-cyber-safety-and-security-makes-debut-11139834.htm.

29 Stakeholder consultation.

30 "Vietnam Engages in Building of UN Convention Against Cybercrimes," *VietnamPlus*, January 23, 2023, https://en.vietnamplus.vn/vietnam-engages-in-building-of-un-convention-against-cybercrimes/247406.vnp.

31 Stakeholder consultation.

32 *Ibid.*

33 Author's note: Notable items include ISO/IEC No. 27000, 18028, 15408, 13888, 9797, 15443, 11770, 18033, among others.

34 "Phát Triển Các Tiêu Chuẩn Quốc Tế Trong Lĩnh Vực Công Nghệ Quan Trọng và Mới Nổi," *Ministry of Science and Technology*, March 22, 2023, https://www.most.gov.vn/vn/tin-tuc/22897/phat-trien-cac-tieu-chuan-quoc-te-trong-linh-vuc-cong-nghe-quan-trong-va-moi-noi.aspx.

35 "US-ASEAN Virtual Workshop on Cybersecurity Standards & Conformance to Support Digital Trade in ASEAN: US ABC," *US-ASEAN Business Council*, May 4, 2023, https://www.usasean.org/event/us-asean-virtual-workshop-cybersecurity-standards-conformance-support-digital-trade-asean.

36 Buu Dien, "Only 1% of Software Firms Meet ISO Standards in Information Security," *VietNamNet News*, March 15, 2013, https://vietnamnet.vn/en/only-1-of-software-firms-meet-iso-standards-in-information-security-E68768.html.

37 See Note 33.

38 See Note 18.

39 "Trung Tâm Ứng Cứu Khẩn Cấp Không Gian Mạng Việt Nam: Trung Tâm Vncert/CC," *VNCERT/CC*, accessed January 1, 2024, https://vncert.vn/.

40 "First-Ever Digital Timestamping Service Launched in Vietnam," *VietnamPlus*, April 1, 2021, https://en.vietnamplus.vn/firstever-digital-timestamping-service-launched-in-vietnam/199420.vnp.

41 Stakeholder consultation.

42 *Ibid.*

43 "An Assessment Model for Cyber Security of Vietnamese Organization," *VNU Journal of Science: Policy and Management Studies*, Vol. 33, No. 2 (2017): 97-103, https://js.vnu.edu.vn/PaM/article/view/4102.

44 "USA: An Overview of the NIST Cybersecurity Framework," *DataGuidance*, Sep-

tember 2021, https://www.dataguidance.com/opinion/usa-overview-nist-cybersecurity-framework.

45 Sam Bocetta, "3 Security Issues Overlooked by the NIST Framework," *Network Computing*, March 3, 2021, https://www.networkcomputing.com/network-security/3-security-issues-overlooked-nist-framework.

46 "Questions and Answers," *NIST*, January 2024, https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics.

47 "What Is the NIS 2 Directive and What Does It Mean for You?" *Risk Ledger*, November 16, 2022, https://riskledger.com/resources/new-nis-2-directive-explained.

48 "Tăng cường hợp tác và chia sẻ thông tin về an toàn, an ninh mạng giữa các cơ quan," *Tạp chí An toàn Thông tin*, August 7, 2023, https://antoanthongtin.vn/an-toan-thong-tin/tang-cuong-hop-tac-va-chia-se-thong-tin-ve-an-toan-an-ninh-mang-giua-co-quan-to-chuc-nha-nuoc-va-doa-109207.

49 "Blockchain Industry Faces Talent Shortage," *VietnamNews*, July 16, 2022, https://vietnamnews.vn/economy/1268984/blockchain-industry-faces-talent-shortage.html.

50 "In Vietnam, Technology Firms Struggle to Hunt for Talents," *VietNamNet News*, October 11, 2019, https://vietnamnet.vn/en/in-vietnam-technology-firms-struggle-to-hunt-for-talents-573110.html.

51 Stakeholder consultation.

52 *Ibid.*

53 Phuong Ha, "Vietnam's Younger Population Shrinking ," *VnExpress International*, October 24, 2023, https://e.vnexpress.net/news/news/vietnam-s-younger-population-shrinking-4668164.html.

54 "Bảo vệ Quyền Riêng Tư Cho Phụ Nữ và Trẻ Em Gái Trên Không Gian Mạng," *ANTV*, November 23, 2023, https://antv.gov.vn/xa-hoi-4/tang-cuong-an-ninh-

mang-va-bao-ve-quyen-rieng-tu-cho-phu-nu-va-tre-em-gai-tren-khong-gian-mang-83406E1D5.html

55 "Https://Hoilhpn.Org.vn/Web/Guest/Tin-Chi-Tiet/-/Chi-Tiet/Cam-Nang-034-an-Toan-Truc-Tuyen-034-Giup-Nguoi-Cao-Tuoi-Hieu-va-Phong-Chong-Thong-Tin-Xau-%C4%91oc-Tren-Khong-Gian-Mang-61352-7.Html ," *Hội Liên hiệp Phụ nữ*, December 19, 2023, https://hoilhpn.org.vn/web/guest/tin-chi-tiet/-/chi-tiet/cam-nang-034-an-toan-truc-tuyen-034-giup-nguoi-cao-tuoi-hieu-va-phong-chong-thong-tin-xau-%C4%91oc-tren-khong-gian-mang-61352-7.html.

56 Disclaimers: All views expressed are personal.

Conclusion

Mark Bryan Manantan

1 Cyber ASEAN post-consultation survey and feedback results.

2 Cyber ASEAN post-consultation survey.

3 *Ibid.*

Annex

TABLE A1

Regression Output for the Cointegrating Regression between GDP and Cybersecurity Standards Adoption (Philippines)

Dependent Variable: GDP

Method: Fully Modified Least Squares (FMOLS)

Date: 01/06/24 Time: 09:48

Sample: 2010Q1 2022Q4

Included observations: 52

Cointegrating equation deterministics: C

Long-run covariance estimate (Bartlett kernel, Newey-West fixed bandwidth = 4.0000)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
CS_FRAMEWORK	274116.6	129971.8	2.109047	0.0404
CAPITAL_FORMATION	0.928987	0.414450	2.241497	0.0299
IMPORTS	1.129075	0.589812	1.914298	0.0618
EXPORTS	-0.146819	0.576588	-0.254634	0.8001
TBILL_364	-122620.2	25072.81	-4.890564	0.0000
C	1897788.	196919.9	9.637357	0.0000

R-squared	0.928598	Mean dependent var	3932028.
Adjusted R-squared	0.920837	S.D. dependent var	773962.1
S.E. of regression	217761.0	Sum squared resid	2.18E+12
Long-run variance	4.22E+10		

TABLE A2

Regression Output for the Error Correction Model between GDP and Cybersecurity Standards Adoption (Philippines)

Dependent Variable: DLOG(GDP)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 00:20

Sample: 2012Q3 2022Q4

Included observations: 42

Convergence achieved after 48 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
CS_FRAMEWORK	0.004548	0.001773	2.564792	0.0152
DLOG(CAPITAL_FORMATION)	0.148741	0.059235	2.511025	0.0173
DLOG(IMPORTS)	0.095525	0.122088	0.782430	0.4397
DLOG(EXPORTS)	0.150826	0.119460	1.262562	0.2159
D(TBILL_364)	-0.001512	0.005198	-0.290983	0.7729
ECM_RESID(-1)	-1.66E-08	1.15E-08	-1.447678	0.1574
AR(1)	-0.896924	0.198637	-4.515393	0.0001
AR(2)	-0.838771	0.185015	-4.533535	0.0001
AR(3)	-0.922072	0.076296	-12.08545	0.0000
SIGMASQ	0.000393	0.000119	3.311391	0.0023

R-squared	0.961239	Mean dependent var	0.013592
Adjusted R-squared	0.950338	S.D. dependent var	0.101909
S.E. of regression	0.022710	Akaike info criterion	-4.370898
Sum squared resid	0.016504	Schwarz criterion	-3.957167
Log likelihood	101.7889	Hannan-Quinn criter.	-4.219249
Durbin-Watson stat	1.199935		

Inverted AR Roots	.05-.96i	.05+.96i	-.99

TABLE A3

Regression Output for the Time-Series Regression between GVA in Information and Communications Technology and Cybersecurity Standards Adoption (Philippines)

Dependent Variable: DLOG(GVA_ICT)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 00:14

Sample: 2010Q1 2022Q4

Included observations: 52

Convergence achieved after 20 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.011659	0.001670	6.979449	0.0000
CS_FRAMEWORK	0.005417	0.002248	2.410168	0.0205
COVID	-0.002966	0.009381	-0.316149	0.7535
DLOG(CAPITAL_FORMATION)	-0.043115	0.043478	-0.991660	0.3272
DLOG(IMPORTS)	0.289727	0.116478	2.487408	0.0170
DLOG(EXPORTS)	-0.224121	0.096205	-2.329612	0.0248
D(TBILL_364)	-0.002171	0.004756	-0.456501	0.6504
AR(1)	-0.954605	0.047833	-19.95697	0.0000
AR(2)	-0.919979	0.058034	-15.85240	0.0000
AR(3)	-0.962079	0.033040	-29.11901	0.0000
SIGMASQ	0.000412	0.000103	4.018439	0.0002

R-squared	0.987100	Mean dependent var	0.015200
Adjusted R-squared	0.983953	S.D. dependent var	0.180435
S.E. of regression	0.022857	Akaike info criterion	-4.348937
Sum squared resid	0.021419	Schwarz criterion	-3.936174
Log likelihood	124.0724	Hannan-Quinn criter.	-4.190694
F-statistic	313.7228	Durbin-Watson stat	2.094657
Prob(F-statistic)	0.000000		

Inverted AR Roots	.02-.98i	02+.98i	-1.00

TABLE B1

Regression Output for the Time-Series Regression between GVA in Financial and Insurance Activities and Cybersecurity Standards Adoption (Indonesia)

Dependent Variable: DLOG(GVA_FINANCE)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 04:48

Sample: 2010Q1 2022Q4

Included observations: 52

Convergence achieved after 35 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.008337	0.011487	-0.725786	0.4723
CS_FRAMEWORK	0.007236	0.012117	0.597227	0.5538
COVID	-0.008124	0.016992	-0.478110	0.6352
DLOG(CAPITAL_FORMATION)	1.963794	0.120684	16.27215	0.0000
DLOG(IMPORTS)	-0.412342	0.157194	-2.623150	0.0124
DLOG(EXPORTS)	0.097960	0.170158	0.575700	0.5681
D(TBILL_364)	-0.000945	0.009066	-0.104238	0.9175
AR(1)	-0.400296	0.155128	-2.580429	0.0137
AR(2)	-0.163362	0.162367	-1.006127	0.3206
AR(4)	0.743549	0.135493	5.487712	0.0000
AR(5)	0.375613	0.176456	2.128645	0.0397
MA(7)	-0.268383	0.324066	-0.828175	0.4126
SIGMASQ	0.001141	0.000226	5.056283	0.0000

R-squared	0.949494	Mean dependent var	-0.006961
Adjusted R-squared	0.933953	S.D. dependent var	0.151760
S.E. of regression	0.039002	Akaike info criterion	-3.344851
Sum squared resid	0.059324	Schwarz criterion	-2.857040
Log likelihood	99.96611	Hannan-Quinn criter.	-3.157835
F-statistic	61.09830	Durbin-Watson stat	2.109542
Prob(F-statistic)	0.000000		

Inverted AR Roots	.92	.00+.98i	.00-.98i	-.57
	-.76			
Inverted MA Roots	.83	.52+.65i	52-.65i	-.18+.81i
	-.18-.81i	-.75-.36i	-.75+.36i	

TABLE B2

Regression Output for the Time-Series Regression between GVA in Electricity, Steam, and Waste Management and Cybersecurity Standards Adoption (Indonesia)

Dependent Variable: DLOG(GVA_UTILITIES)

Method: Least Squares

Date: 01/15/24 Time: 04:51

Sample: 2010Q1 2022Q4

Included observations: 52

Convergence achieved after 26 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.030201	0.011122	-2.715456	0.0096
CS_FRAMEWORK	0.029436	0.015974	1.842773	0.0726
COVID	-0.025403	0.039963	-0.635660	0.5285
DLOG(CAPITAL_FORMATION)	2.425004	0.112278	21.59818	0.0000
DLOG(IMPORTS)	-0.345836	0.149787	-2.308857	0.0261
DLOG(EXPORTS)	0.184498	0.154969	1.190551	0.2407
D(TBILL_364)	0.001866	0.008405	0.222056	0.8254
AR(1)	-0.004751	0.091123	-0.052144	0.9587
AR(4)	0.548206	0.116333	4.712364	0.0000
AR(10)	-0.402770	0.125348	-3.213220	0.0026
SIGMASQ	0.001360	0.000409	3.323280	0.0019

R-squared	0.969328	Mean dependent var	-0.017828
Adjusted R-squared	0.961847	S.D. dependent var	0.212629
S.E. of regression	0.041532	Akaike info criterion	-3.225465
Sum squared resid	0.070722	Schwarz criterion	-2.812702
Log likelihood	94.86208	Hannan-Quinn criter.	-3.067221
F-statistic	129.5739	Durbin-Watson stat	2.417273
Prob(F-statistic)	0.000000		

TABLE B3

Regression Output for the Time-Series Regression between GVA in Information and Communications Technology and Cybersecurity Standards Adoption (Indonesia)

Dependent Variable: DLOG(GVA_ICT)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 04:54

Sample: 2010Q1 2022Q4

Included observations: 52

Convergence achieved after 22 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.014410	0.003279	4.394379	0.0001
CS_FRAMEWORK	0.003385	0.005768	0.586974	0.5604
COVID	0.001601	0.009611	0.166523	0.8686
DLOG(CAPITAL_FORMATION)	0.703976	0.050997	13.80440	0.0000
DLOG(IMPORTS)	-0.239754	0.077417	-3.096925	0.0035
DLOG(EXPORTS)	0.000798	0.073494	0.010857	0.9914
D(TBILL_364)	-0.001538	0.004565	-0.336850	0.7379
AR(1)	-0.333608	0.187641	-1.777900	0.0828
AR(2)	-0.454447	0.244008	-1.862429	0.0697
MA(4)	0.564308	0.216792	2.602986	0.0128
SIGMASQ	0.000232	5.79E-05	4.002062	0.0003

R-squared	0.925960	Mean dependent var	0.015351
Adjusted R-squared	0.907902	S.D. dependent var	0.056469
S.E. of regression	0.017137	Akaike info criterion	-5.065293
Sum squared resid	0.012041	Schwarz criterion	-4.652529
Log likelihood	142.6976	Hannan-Quinn criter.	-4.907049
F-statistic	51.27572	Durbin-Watson stat	2.162731
Prob(F-statistic)	0.000000		

Inverted AR Roots	-.17+.65i	-.17-.65i		
Inverted MA Roots	.61+.61i	.61+.61i	-.61-.61i	-.61-.61i

TABLE B4

Regression Output for the Time-Series Regression between GVA in Human Health and Social Activities and Cybersecurity Standards Adoption (Indonesia)

Dependent Variable: DLOG(GVA_HEALTH)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 04:57

Sample: 2010Q1 2022Q4

Included observations: 52

Convergence achieved after 17 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.005692	0.004663	-1.220669	0.2292
CS_FRAMEWORK	0.004332	0.008040	0.538735	0.5930
COVID	0.018153	0.009006	2.015579	0.0504
DLOG(CAPITAL_FORMATION)	1.736741	0.097800	17.75802	0.0000
DLOG(IMPORTS)	-0.577462	0.154108	-3.747123	0.0006
DLOG(EXPORTS)	0.307885	0.174342	1.765978	0.0848
D(TBILL_364)	-0.011703	0.009929	-1.178633	0.2453
AR(1)	-0.550299	0.148046	-3.717091	0.0006
AR(2)	-0.493094	0.142508	-3.460111	0.0013
AR(3)	-0.518033	0.115990	-4.466188	0.0001
SIGMASQ	0.001474	0.000306	4.818656	0.0000

R-squared	0.940112	Mean dependent var	0.000395
Adjusted R-squared	0.925505	S.D. dependent var	0.158422
S.E. of regression	0.043239	Akaike info criterion	-3.235464
Sum squared resid	0.076655	Schwarz criterion	-2.822701
Log likelihood	95.12206	Hannan-Quinn criter.	-3.077220
F-statistic	64.36057	Durbin-Watson stat	1.759676
Prob(F-statistic)	0.000000		

Inverted AR Roots	.11-.81i	.11+.81i	-.78

TABLE C1

Regression Output for the Time-Series Regression between GDP and Cybersecurity Standards Adoption (Malaysia)

Dependent Variable: DLOG(GDP)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 05:26

Sample: 2010Q2 2022Q4

Included observations: 51

Convergence achieved after 18 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.008312	0.007407	1.122208	0.2683
CS_FRAMEWORK	0.000621	0.008793	0.070577	0.9441
COVID	-0.021437	0.006431	-3.333368	0.0018
DLOG(CAPITAL_FORMATION)	0.164405	0.082555	1.991460	0.0531
DLOG(IMPORTS)	-0.068075	0.225817	-0.301459	0.7646
DLOG(EXPORTS)	0.827793	0.216922	3.816089	0.0004
D(TBILL_364)	0.013410	0.033866	0.395962	0.6942
AR(1)	-0.057468	0.266574	-0.215581	0.8304
AR(2)	-0.269175	0.196063	-1.372902	0.1772
SIGMASQ	0.000528	0.000120	4.380961	0.0001

R-squared	0.847761	Mean dependent var	0.018526
Adjusted R-squared	0.814343	S.D. dependent var	0.059454
S.E. of regression	0.025618	Akaike info criterion	-4.314175
Sum squared resid	0.026907	Schwarz criterion	-3.935386
Log likelihood	120.0115	Hannan-Quinn criter.	-4.169428
F-statistic	25.36820	Durbin-Watson stat	1.945380
Prob(F-statistic)	0.000000		

Inverted AR Roots	-.03-.52i	-.03+.52i

TABLE C2

Regression Output for the Time-Series Regression between GVA in Information and Communications Technology and Cybersecurity Standards Adoption (Malaysia)

Dependent Variable: DLOG(GVA_ICT)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 05:16

Sample: 2010Q2 2022Q4

Included observations: 51

Convergence achieved after 19 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.018553	0.014596	1.271119	0.2109
CS_FRAMEWORK	0.003930	0.004109	0.956532	0.3444
COVID	-0.001475	0.005696	-0.258936	0.7970
DLOG(CAPITAL_FORMATION)	-0.005305	0.036643	-0.144773	0.8856
DLOG(IMPORTS)	0.184514	0.045160	4.085775	0.0002
DLOG(EXPORTS)	-0.072928	0.043079	-1.692896	0.0981
D(TBILL_364)	-0.007471	0.006914	-1.080481	0.2862
AR(1)	-0.007569	0.047011	-0.161009	0.8729
AR(2)	0.934754	0.054243	17.23267	0.0000
SIGMASQ	7.16E-05	1.91E-05	3.755290	0.0005

R-squared	0.892405	Mean dependent var	0.023471
Adjusted R-squared	0.868787	S.D. dependent var	0.026052
S.E. of regression	0.009437	Akaike info criterion	-6.151934
Sum squared resid	0.003651	Schwarz criterion	-5.773144
Log likelihood	166.8743	Hannan-Quinn criter.	-6.007187
F-statistic	37.78443	Durbin-Watson stat	1.963666
Prob(F-statistic)	0.000000		

Inverted AR Roots	98	-.00+.98i	-.00-.98i	-.99

TABLE C3

Regression Output for the Time-Series Regression between GVA in Electricity, Steam and Waste Management and Cybersecurity Standards Adoption (Malaysia)

Dependent Variable: DLOG(GVA_UTILITIES)

Method: ARMA Maximum Likelihood (OPG - BHHH)

Date: 01/15/24 Time: 05:21

Sample: 2010Q2 2022Q4

Included observations: 51

Convergence achieved after 33 iterations

Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.007237	0.004162	1.738571	0.0896
CS_FRAMEWORK	0.005831	0.004950	1.178104	0.2455
COVID	-0.011291	0.004742	-2.380971	0.0220
DLOG(CAPITAL_FORMATION)	0.353465	0.063517	5.564910	0.0000
DLOG(IMPORTS)	-0.213799	0.133331	-1.603514	0.1165
DLOG(EXPORTS)	0.388215	0.128084	3.030938	0.0042
D(TBILL_364)	-0.008163	0.015174	-0.537964	0.5935
AR(1)	-0.509765	0.195385	-2.609032	0.0126
AR(2)	-0.419212	0.127982	-3.275566	0.0021
SIGMASQ	0.000345	8.04E-05	4.284978	0.0001

R-squared	0.767662	Mean dependent var	0.017196
Adjusted R-squared	0.716661	S.D. dependent var	0.038897
S.E. of regression	0.020705	Akaike info criterion	-4.732740
Sum squared resid	0.017576	Schwarz criterion	-4.353951
Log likelihood	130.6849	Hannan-Quinn criter.	-4.587993
F-statistic	15.05189	Durbin-Watson stat	2.190010
Prob(F-statistic)	0.000000		

Inverted AR Roots	-.25+.60i	-.25-.60i

TABLE D1

Regression Output for the Time-Series Regression between GVA in Financial and Insurance Activities and Cybersecurity Standards Adoption (Viet Nam)

Dependent Variable: DLOG(GVA_FINANCE)

Method: Least Squares

Date: 01/14/24 Time: 15:34

Sample (adjusted): 2006 2022

Included observations: 17 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.064277	0.006340	10.13834	0.0000
CS_FRAMEWORK	0.010948	0.005849	1.871751	0.0858
DLOG(CAPITAL_FORMATION)	0.079949	0.030825	2.593618	0.0235
TRADE_BAL	-4.54E-08	4.07E-08	-1.116853	0.2859
D(TBILL_364)	0.002474	0.001151	2.149560	0.0527

R-squared	0.637522	Mean dependent var	0.079680
Adjusted R-squared	0.516695	S.D. dependent var	0.015295
S.E. of regression	0.010633	Akaike info criterion	-6.009801
Sum squared resid	0.001357	Schwarz criterion	-5.764739
Log likelihood	56.08331	Hannan-Quinn criter.	-5.985442
F-statistic	5.276354	Durbin-Watson stat	1.458168
Prob(F-statistic)	0.010945		

TABLE D2

Regression Output for the Time-Series Regression between GVA in Human Health and Social Activities and Cybersecurity Standards Adoption (Viet Nam)

Dependent Variable: DLOG(GVA_HEALTH)

Method: Least Squares

Date: 01/06/24 Time: 09:56

Sample (adjusted): 2006 2022

Included observations: 17 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.001190	0.052926	0.022483	0.9824
CS_FRAMEWORK	0.032420	0.048827	0.663982	0.5193
DLOG(CAPITAL_FORMATION)	0.305439	0.257330	1.186955	0.2582
TRADE_BAL	-4.11E-07	3.40E-07	-1.210884	0.2492
D(TBILL_364)	-0.007829	0.009608	-0.814834	0.4310

R-squared	0.234457	Mean dependent var	0.089613
Adjusted R-squared	-0.020723	S.D. dependent var	0.087858
S.E. of regression	0.088764	Akaike info criterion	-1.765752
Sum squared resid	0.094548	Schwarz criterion	-1.520689
Log likelihood	20.00889	Hannan-Quinn criter.	-1.741392
F-statistic	0.918789	Durbin-Watson stat	2.152099
Prob(F-statistic)	0.484447		

For more content on Cyber ASEAN, visit **cyberasean.pacforum.org**