Evolution of ASEAN's Policy on Cyber Security

by

Timuçin Tüner

Term Project Submitted in Partial Fulfillment of the Requirements

for the Asian Studies Degree

02/09/2023

Evolution of ASEAN’s Policy on Cyber Security

Abstract

This research investigates the evolutionary trajectory of ASEAN's cyber security policy, spanning from its historical roots to its future prospects. This research has identified three fundamental patterns of evolution: the growing regionalization through innocuous diffusion, an expanding holistic approach to cybersecurity, and a deepening people-centered focus. Within the frameworks of the ASEAN Way and diffusion, this study aims to provide a comprehensive explanation of the evolution of ASEAN's cyber security policy.

Keywords

ASEAN Way, Diffusion, Cyber Security

Introduction

The primary objective of this research paper is to provide a comprehensive analysis of the evolution of ASEAN's cyber security policies over time. Notably, there exists a significant gap in existing research concerning the specific mechanisms and processes that have driven this policy evolution in ASEAN’s cyber security policies, and this study seeks to address this knowledge gap. To achieve this, the research contextualizes ASEAN's cybersecurity policies within the framework of the ASEAN Way, a guiding principle that has played a pivotal role in the organization's development.

While some scholarly discourse has criticized the effectiveness of the ASEAN Way (*Beyond the Coup in Myanmar*, 2021), it is essential to recognize that this framework has successfully fulfilled its foundational objective. The essence of this objective is articulated in the opening sentence of the Treaty of Amity and Cooperation (TAC), a foundational document for

ASEAN. The TAC explicitly states its purpose as the establishment of perpetual peace within the region (ASEAN, 1976).

Innocuous diffusion fosters cooperation and engagement among member nations without inciting discontent or hostility. This approach has facilitated continuous communication and strengthened bonds among member states. Moreover, an increasingly people-centric approach in ASEAN's policy evolution suggests a potential transformation from a community of nation-states to a community of people. This shift underscores a growing emphasis on the well-being and participation of individuals within the ASEAN region.

Furthermore, the evolution toward a more holistic approach reflects ASEAN's aspiration to make a tangible difference in addressing not just specific issues but broader regional challenges. The organization's goals extend beyond mere problem-solving; they aim to create a lasting impact on the region's cyber security landscape.

Theoretical Framework

The evolution of ASEAN policies on cyber security can be viewed through the lenses of diffusion and the ASEAN way. Diffusion can be defined as the interconnected decision-making process that occurs when one actor's policies, institutions, and norms influence another actor's choices (Jetschke, 2017). Laura Allison-Reumann's work on norm diffusion in the context of ASEAN stands as one of the valuable contributions to this area. In their paper, (Allison-Reumann, 2017, p. 8 cited Finnemore and Sikkink 1998) ASEAN is described as predominantly a prescriptive norm diffuser, which means that ASEAN's goal revolves around determining what constitutes "appropriate" or "proper" behavior. However, the authors themselves also present an alternative perspective, which they term "innocuous diffusion."(Allison-Reumann, 2017, pp. 19–25). This concept suggests that diffusion occurs primarily in areas that do not threaten national sensitivities.

It can be argued that ASEAN's reluctance to establish a legal framework for addressing transnational cyber crime aligns with the authors' argument regarding innocuous diffusion. This is because judicial systems, particularly in matters involving actions from foreign countries, can be perceived as sensitive and unwelcome, potentially explaining why ASEAN has hesitated to create such a framework.

Alan Collins' study on ASEAN's adoption of global HIV norms illuminates the process of norm diffusion through a similar yet different theoretical framework. Collins uses a combination of localization, subsidiary, and mimicking to investigate ASEAN norm diffusing which is based on the works of Acharya and Katsumata. Despite the differences in subject matter and theoretical underpinnings, Collins adeptly illustrates the norm diffusion dynamics between the United Nations Programme on HIV/AIDS (UNAIDS) and ASEAN. This study serves as a valuable case study, showcasing norm diffusion occurring within the region and between international actors (Collins, 2013).

The cyber security and political security policies of the ASEAN organization should also be assessed within the context of the ASEAN Way framework. The ASEAN Way encompasses the established norms that govern how ASEAN member countries engage with one another and the broader international community (Yukawa, 2018). Meanwhile, it is also important to note that, it is also difficult to outline what exactly constitutes norms that are considered to be part of the ASEAN Way.

Cyber diplomacy is a specialized form of diplomacy where the primary focus and rationale for diplomatic activities and negotiations revolve around issues and challenges related to the cyber domain. In other words, if the central motivation and core reason for engaging in diplomatic efforts are primarily driven by cyber-related concerns, such as cybersecurity, cyberattacks, or cyber

norms, then it falls under the category of cyber diplomacy (Attatfa et al., 2020). Cyber diplomacy is becoming progressively more evident in ASEAN's committee meetings and cooperation frameworks. Previously, cyber security issues were often categorized under transborder crimes, and they were only briefly mentioned, not seen as a distinct element of cyber diplomacy. However, over time, there has been a shift in perception, and now, cyber security concerns are recognized as a separate and distinct category, rather than merely a subcategory of transnational crimes. To illustrate this within the context of ASEAN, we can consider the ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services as an example of cyber diplomacy. This program primarily addresses cybersecurity issues in the cyber space realm. On the other hand, APSC 2015 can be categorized as traditional diplomacy, as its main focus is on political security, with only a brief mention of cyber security.

Main Policy Documents

To comprehensively investigate the evolution of cyber security policies, a thorough analysis of various policy documents becomes imperative. The cyber security policies within the ASEAN region do not exist within a single consolidated document published by ASEAN itself; instead, they are distributed across several sectors. The primary documents central to this research encompass the ICT Masterplan (which was subsequently rebranded as the Digital Masterplan), the ASEAN Cyber Security Cooperation Strategy papers, the APSC Blueprints, Framework Agreements, and the Telmin (later renamed to ADGMIN) papers.

What Is Cyber Security?

The realm of cyber security is experiencing exponential growth, with an increasing number of conversations revolving around its significance. However, despite its undeniable importance, there remains a notable level of unawareness. Instances arise where even senior leaders, such as

those within the US Department of Defense, refer to cyber security as simply "all this cyber stuff (Singer, 2014, pp. 1–4). In light of such instances, it becomes important to provide precise meanings and implications of these terminologies.

Within the literature, a universally precise definition of cyber security is notably absent. As indicated by Schatz et al's paper on cyber security definitions (Schatz et al. 2017, citing Falessi et al. 2012), even within the EU, an entity often perceived as having more robust organizational influence than the ASEAN, a distinct and universally accepted definition of cyber security among its member states remains non-existent. Meanwhile, delving into academic discourses on different definitions of cyber security is interesting, it is also important to have one working definition. To fulfill this objective, this paper will adopt the definition provided by IBM, which is as follows: "Cyber security is the practice of protecting critical systems and sensitive information from digital attacks"(*What Is Cyber security?*, 2023). While this definition may not encompass all aspects, it does offer a clear framework for addressing the issues at hand.

Understanding the Importance of Cyber Security in ASEAN

The significance of cyber security within ASEAN is growing steadily due to the expanding digital economy and the increasing interconnectedness of people in the region. As a direct consequence of these trends, a larger volume of data is being stored online, consequently heightening the vulnerabilities associated with both national security and the protection of private information. Historically ASEAN nations have noted weaknesses in the cyber security realm with perhaps the exception of Singapore (Ang, 2021), According to the Interpol ASEN cyber-threat assessment report this weakness resulted in numerous and wide-range of attacks which include Business E-mail Compromise (BEC), Phishing, Cyber fraud, Ransomware, E-commerce data

interception and Crimeware-as-a-Service (CaaS). These attacks target many users ranging from individuals to institutions like banks and businesses (Interpol, 2021).

In the realm of cybersecurity, it is widely acknowledged that the most vulnerable component is often the human element (Jeong et al., 2019). Addressing this intricate challenge necessitates a comprehensive and multifaceted approach. This paradigm is exemplified in the ASEAN Cybersecurity Cooperation Strategy (2021-2025) document, where one of its primary objectives centers on the elevation of cyber hygiene standards (ASEAN, 2022). Cyber hygiene, in this context, encompasses a comprehensive set of rules and practices that individuals and organizations are strongly encouraged to adopt to enhance their cybersecurity resilience. It encompasses a wide spectrum of proactive measures aimed at bolstering digital security, spanning from robust password management to regular software updates and employee training.

Why ASEAN's Policies on Cyber Security Matters

The contemporary digital landscape is characterized by profound interconnectivity that extends beyond geographical confines. Cyber threats, fueled by this borderless nature, possess the ability to traverse and infiltrate any ASEAN country from diverse origins. The absence of a robust regional and international cyber security infrastructure diminishes the effectiveness of deterrence mechanisms. Given the intricate and cross-border nature of these threats, an imperative for a collective and transnational response emerges. This requires recognizing the important role that ASEAN's cyber security policy plays, especially in situations where its influence is vital for dealing with complex cross-national operations and legal issues.

A historical perspective underscores the formidable challenges of addressing cross-national crimes, especially in a domain as complex and rapidly evolving as cyberspace. This complexity is exacerbated by the fundamental structure of the internet itself - a web of interconnected servers

and networks that transcends national borders. As an example, a malevolent actor in Germany could use a server in Russia to orchestrate an assault on a computer system in Indonesia. In such scenarios, the involvement of multiple nations creates difficult-to-navigate situations. Notably, these nations might have varied understandings of what constitutes a "cyber crime," further exacerbating the situation. Additionally, the willingness to collaborate across borders could be marred by diplomatic and political considerations.

In this intricate landscape, ASEAN's policy on cyber security assumes profound importance. ASEAN's capacity to exert influence becomes paramount in mitigating the challenges stemming from cross-national operations and the ensuing legal battles. One of ASEAN's primary assets in this equation is its capacity to foster the creation of norms and joint frameworks. ASEAN can facilitate the development of shared norms that guide responsible conduct in cyberspace. These norms act as common ground among member states, promoting a consistent understanding and interpretation of cyber threats. Moreover, these shared norms serve as a foundation for cyber diplomacy, potentially mitigating the escalation of conflicts arising from cyber incidents.

Global Landscape of Cyber Security Policies

ASEAN, EU, and the African Union (AU) have all taken steps to develop regional cyber security policies. These three organizations are at different stages of regional institution building. However, it's important to note that while the EU has made significant progress, the AU lags behind, primarily due to limited regional policy development, with the exception of the "African Union Convention on Cyber Security and Personal Data Protection," which hasn't been ratified by a majority of AU member states (CCDCOE, n.d.).

In contrast, ASEAN has made notable advancements by establishing frameworks like the ICT Masterplans and the ASEAN Political-Security Community (APSC). These initiatives over

time are materialized into regional psychical institutions, exemplified by the establishment of the ASEAN Cert in Singapore.

The EU, on the other hand, has progressed towards a more centralized federal structure in terms of cyber security. It has established a joint cyber security agency that promotes data sharing and judicial cooperation among member states, including adherence to international agreements like the Budapest Convention (Council of Europe, n.d.). In summary, while all three regional organizations are engaged in cyber security efforts, the EU has already established regional institutions, while ASEAN has established a framework for joint collaboration and currently focusing on the creation of regional institutions, and the AU is still in the early stages of policy development, consensus building and framework building.

The Ideology Behind ASEAN Policy on Cyber Security

The formulation of policies inherently relies on the specific organizational environment in which they are crafted. This principle extends to the development of cyber security policies within the ASEAN framework. Within the realm of ASEAN cyber security policymaking, this process can be understood within the context of three core principles outlined in the political security community blueprint which are community based on shared norms and values, the goal of a stable and secure region with comprehensive security responsibilities, and the vision of an outward-looking ASEAN within a globally integrated context. Although the primary emphasis of this document does not revolve around cyber security, its principles align with ASEAN's cyber security policies.

The cyber security and political security policies of the ASEAN organization should be assessed within the context of the ASEAN Way framework. The ASEAN Way encompasses the established norms that govern how ASEAN member countries engage with one another and the

broader international community (Yukawa, T. (2017)). This framework is characterized by the principles of non-interference and consensus-based decision-making. Yet, the ASEAN way, being a collection of norms, presents a unique challenge in terms of precise definition.

A concrete illustration of the ASEAN's difference compared to other organizations can be found in a comparative analysis of the coups in Niger and Myanmar. Coup in Niger, prompted the potential intervention of the Economic Community of West African States (ECOWAS) military forces (AL JAZEERA, 2023). In stark contrast, ASEAN's response to the coup in Myanmar was notably different. True to its foundational principle of non-interference, ASEAN has refrained from engaging in military interventions, opting instead for a consensus-based approach that emphasizes the importance of dialogue and communication. ASEAN reacted to the situation by establishing a special envoy to Myanmar and reaching a common consensus at ASEAN Summit, however, the fear of disrupting consensus prompted ASEAN to express concerns regarding political prisoners through statements, rather than including it in the official consensus (Desker, 2021). Critics have argued that ASEAN's approach in response to the Myanmar coup represents a failure (Kurlantzick, 2022), but it can be simply understood as a continuation of the fundamental principles of the ASEAN Way.

A comparable analogy can be drawn between the European Union and ASEAN. EU can be understood through the concept of federation meanwhile ASEAN can be viewed as a confederation (Ramadhan, 2020). The EU, as an entity, possesses both formal and informal mechanisms to exert its influence over member states. A recent illustration of this is the introduction of the "Proposal for a Directive of the European Parliament and of the Council on the definition of criminal offenses and penalties for the violation of Union restrictive measures" by the Council of the European Union. This proposal, currently in the draft phase, received substantial support with 36 votes in

favor, 2 against, and 2 abstentions (European Parliament, 2023). If enacted, this proposal would empower EU bureaucrats to enforce uniform compliance with EU sanctions across member states by establishing a shared definition of sanctions and the authority to impose monetary penalties on non-compliant states (Council of the EU, 2023). Previously, this paper highlighted the significance of definitions in regional policymaking. In this regard, the EU has taken significant steps, although, in the realm of cyber security, they still lack common regional definitions (Schatz et al 2017, citing Falessi et al. 2012). In contrast to both the EU and ECOWAS, ASEAN does not have the inclination to intervene in the internal affairs of its member countries via monetary penalties or engage in direct military interventions as punitive measures. Furthermore, ASEAN lacks the capacity for a monetary penalty system like the EU.

The capacity to enforce EU laws on its member states has led to not only dissatisfaction among states but also among citizens. This discontent has, in turn, contributed to phenomena such as Brexit and the rise of anti-EU political movements (Agnew, 2020, pp. 7–10). However, a parallel example cannot be found within ASEAN. This is because every policy implementation in ASEAN is carried out through consensus, devoid of any monetary penalty system or the threat of military intervention. Moreover, in the European Union, most decisions do not necessitate unanimous votes. Instead, they can be reached through qualified majority voting, which constitutes the support of 55% of member states, representing at least 65% of the total EU population (Council of the European Union, 2023). Additionally, simple majority voting, where 14 member states cast affirmative votes, is also considered sufficient in some cases. In contrast, ASEAN declarations demand unanimous confirmation, a requirement evident in the texts of ministerial statements published by ASEAN. In summary, both the EU and ASEAN systems possess distinct advantages and disadvantages within their organizational frameworks. EU policies, while enforceable, can

foster discontent, whereas ASEAN lacks any formal mechanism to exert pressure on member states to implement necessary reforms but remains a non-controversial organization between states.

Regarding the cyber security policies of ASEAN, it can be said that they are aligned with the tenets of the ASEAN Way. For instance, the establishment of cyber security agencies and National Certs originated in Singapore. Over the course of two years, through diffusion, several ASEAN member countries embraced similar policies. Importantly, there isn't any mechanism in place to coerce or financially penalize member states for the adoption of these institutions.

Evolution of ASEAN's Policy on Cyber Security

General Patterns of Evolution

Upon examination of ASEAN policies and their evolution over time, several persistent and overarching themes can be found. The first of these general patterns of evolution would be regionalization through innocuous diffusion. The best example of this process would be Regional CERT's and Cyber Security Agencies. Meanwhile creation of regional cyber security agencies can threaten the national sensitives of member countries, regional CERTs don't have a similar threating position. As such, we can understand that ASEAN regionalization efforts avoid sectors and topics that can be considered threatening. Meanwhile, the EU system can be considered more hierarchical, the same can't be applied to ASEAN. Regional CERT project is spearheaded by Singapore but it also enjoys collaborative support from other ASEAN members.

The second general pattern is the growing adoption of a people-centric approach in addressing issues within ASEAN. This shift is evident in both APSC and ICT papers. In APSC, there's a noticeable movement towards emphasizing training, awareness, and education, while in ICT papers, there's a gradually increased attention to inclusivity, empowered citizens, and

vulnerable communities. This evolution contrasts with earlier versions of both APSC and ICT documents, which primarily centered on resolving national problems, highlighting a more recent focus on the people-focused approach of ASEAN.

The third general pattern is an increasingly holistic approach to cyber security concerns in ASEAN. Both ICT 2015 and APSC 2015 Blueprints focus on more rudimentary aspects of cyber security such as law enforcement and infrastructure. However, these initial concerns have evolved to encompass increasingly intricate issues including the digital divide, privacy, consumer data protection, harmful online content, and trust in cyberspace. This growing holistic approach can be theorized as a natural response to the rising use of ICT by both ASEAN citizens and governments.

CERT

A Computer Emergency Response Team (CERT) comprises a team of information security specialists tasked with safeguarding against, detecting, and responding to cyber security incidents within an organization. CERTs can operate at various levels, including private, national, and international. The very first CERT was established in the USA (Goodman, n.d.). It took more than a decade for ASEAN countries to establish their own CERT counterparts. Singapore has led CERT's by founding its national CERT in 1997 (*SingCERT*, n.d.), followed by Thailand in 1999 and other ASEAN nations. Recently Singapore spearheaded an effort to create regional CERT in collaboration with ASEAN nations (Yu, 2022). The establishment of national CERTs by ASEAN countries, following the example set by Singapore, can be viewed as a clear indication of diffusion. Conversely, the creation of a regional CERT can be seen as compelling evidence of the deepening regionalization of cyber security efforts.

Cyber Security Agencies

The first cyber security agency established in the region was in Singapore in 2015 (CSA, 2023), followed by Malaysia (NACSA, n.d.) and Indonesia in 2017 (Kelleher, 2017). Singapore, known as the pioneer, has taken the lead in the field of cyber security within the region, setting the norm for others. These agencies' establishment signifies more than just bureaucratic or performance-driven actions; it clearly demonstrates governments' commitment to conveying their serious approach to addressing cyber security concerns, especially in a region that is among the most susceptible to cyber security threats worldwide. This vision to establish digital trust can also be seen in the 2021-2025 ASEAN cyber security cooperation paper, as it outlines one of the ambitions of ASEAN's Digital goals as enhancing trust in cyber space, the creation of individual agencies, as opposed to existing under other agencies, can be interpreted as a step toward achieving this goal. Similar to CERTs, we can observe diffusion as Singapore extends its cyber security institutions to other ASEAN members. However, unlike regional CERTs, there is no mention of a regional cyber security agency akin to the EU's cyber security agency. Meanwhile, while ASEAN has adopted a similar system to the EU with regional CERTs, the same cannot be said for a regional cyber security agency. This can be attributed to the innocuous diffusion, as the hierarchical nature of a regional agency could potentially challenge national sensitivities regarding the independence of law enforcement institutions.

Framework Agreements

In the ASEAN digital sector, there are currently five framework agreements in effect. However, the term 'framework' used to describe these agreements does not accurately convey their document's nature. Each of these agreements explicitly states that the framework imposes no obligations on individual member states, which aligns with ASEAN's typical policy-making

approach. Furthermore, the suggestions and guidelines outlined in these agreements generally remain at a superficial level, with the noteworthy exception of the ASEAN Data Management Framework.

Regardless of the superficial nature of agreements, an increasingly holistic evolution pattern in these documents can be observed. As an example, the ASEAN Framework on Personal Data Protection (2016), conveys a strict and deliberate focus on the domain of data protection. In contrast, the Framework for Promoting the Growth of Digital Startups (2023) encompasses a wide array of issues, spanning talent cultivation, educational aspects, infrastructure development, funding mechanisms, and intricate legal considerations.

World and ASEAN

EU and ASEAN

ASEAN has implemented numerous initiatives aimed at fostering greater collaboration and interaction with international entities and fellow regional organizations. Among the most partners important partners in this context is the EU. Both the EU and ASEAN share a keen interest in bolstering cooperation between their respective regional bodies through joint declarations and committees (EEAS, 2023). One notable joint endeavor is the Plan of Action to Implement the ASEAN-EU Strategic Partnership. To date, two iterations of this plan have been released, covering the periods 2018-2022 and 2023-2027, respectively. Both documents are based on the ASEAN institutional framework, rooted in the three pillars of ASEAN, which encompass the ASEAN Political-Security Community (APSC), the ASEAN Economic Community (AEC), and the ASEAN Socio-Cultural Community (ASCC). Notably, there is a noticeable pattern of evolution between the two versions. In the first version, the ASEAN institutional framework is implied, while in the next version, the role of ASEAN is articulated more explicitly. This shift is evident in phrases

such as "recognizing the EU's commitment to adhere to all pertinent ASEAN-led security mechanisms" and "strengthening the EU's engagement with the region through ASEAN-led processes and platforms."(ASEAN, 2022). This transition also aligns with one of the evolutionary trends observed in this research, which is innocuous diffusion. ASEAN aims to mitigate potential conflicts arising from the adoption of the EU framework, which is notably more centralized and hierarchical. Therefore, it has advocated not only for the utilization of the ASEAN framework but also the incorporation of assurances for future plans of action. Allison Reumann presents an alternative perspective on this issue, as her research indicates that ASEAN actively endeavors to establish itself as the central institution in the Southeast Asian region. ASEAN's goal of becoming a central institution has garnered favorable responses from both the United States and the European Union, as evidenced by their joint summits and the appointment of ASEAN ambassadors (Allison-Reumann, 2017, pp. 13–15).

A potential hurdle for ASEAN and EU collaboration lies in the EU's dependence on the General Data Protection Regulation (GDPR), renowned for its rigorous measures designed to protect personal data. This stark contrast with ASEAN's absence of an equivalent framework may pose a challenge to the prospects of increased inter-regional cooperation in the field of cybersecurity (Manantan, 2023).

Interpol

ASEAN collaborates with various organizations, including the ASEAN Cybercrime Operations Desk under Interpol, established with support from Japan and Singapore. The United States also contributes to a similar initiative through Interpol, known as the Cyber Capabilities & Capacity Development Project, with a primary focus on enhancing overall capacity (Interpol, n.d.). Interpol's involvement in ASEAN goes beyond mere framework building and dialogue institutions;

they actively lead operations. Two publicly disclosed examples of their successful cooperation with ASEAN are Operation Night Fury and Operation Goldfish Alpha (ASEAN, n.d.). These occurrences underscore the efficacy of ASEAN's collaboration with Interpol, highlighting the institutional value that ASEAN offers to its member states. This is particularly advantageous for smaller member nations that might encounter challenges in organizing joint programs with countries like Japan or the USA.

Japan

Japan holds the distinction of being ASEAN's oldest international partner, having been the first to appoint an ambassador to the organization (ASEAN, 2023). Over the years, Japan and ASEAN have cooperated across various domains, encompassing security, economics, and, notably, cybersecurity. One of the earliest engagements in the realm of information technology was the yearly ASEAN-Japan Information Security Policy Meeting. In its early stages, cooperation emphasized the intersection of business interests and government leadership in the field of ICT. Between 2009 and 2011, these policy meetings continued, focusing on similar topics (*National Center of Incident Readiness and Strategy for Cybersecurity*, n.d.). However, recent years have witnessed a shift in accordance with the theory proposed in this paper, towards a more people-centric and comprehensive approach.

Two illustrative examples of this shift are the establishment of the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in 2018 and the ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services in 2023. Both initiatives concentrate on the people centric aspect of cybersecurity, specifically on the training of specialists and experts (*Signing of Record of Discussions on Technical Cooperation Project with ASEAN*, n.d.). The 2023 program delves deeper by incorporating the principles of Sustainable Development

Goals (SDGs). These initiatives are in line with the three evolution patterns introduced in this paper. They exemplify a transition from business-centric to people-centric, particularly in terms of specialist training. Moreover, these programs also prioritize a holistic approach by incorporating SDGs. Finally, they also demonstrate regionalization through innocuous diffusion, as their primary emphasis is on training which does not threaten sensitivities while effectively diffusing knowledge and expertise from Japan to ASEAN.

Australia

Australia's engagement with ASEAN has historically been somewhat limited, primarily involving the exchange of joint statements, diplomatic meetings, or collaborative endeavors driven by other regional actors, such as Japan and Singapore's regional CERT programs (Australian Government, 2018). This dynamic, however, sparks an intriguing conversation about the nature of cyber diplomacy, which constitutes the institutional aspect of diplomatic engagements in the digital realm. Previously, this paper delved into the significance of dedicated cyber agencies in addressing cybersecurity issues comprehensively. A similar discourse can be extended to the field of cyber diplomacy. An illustrative case in point is the Indonesia-Australia Cyber Cooperation, examined in the work of Priyono et al. In this context, Indonesia conducts its cyber diplomacy through the Ministry of Foreign Affairs and the National Cyber and Crypto Agency (BSSN), while Australia employs a cyber ambassador model, where a high-level coordinator assumes the role of leading their cyber diplomacy initiatives. The authors of this study argue that having a single individual vested with both the authority and training to navigate the complexities of cyber space concerns and diplomacy offers substantial advantages over the Indonesian model of cyber diplomacy, which is distributed across multiple agencies and individuals. Such an approach could potentially enhance

the effectiveness and agility of cyber diplomacy efforts in the modern digital landscape (Priyono et al., 2023).

APSC Blueprint

ASEAN has published two APSC Blueprints which are called APSC 2015 and APSC 2025. These papers provide a future road map for ASEAN members and the organization itself. This document is one of the primary sources that exemplify the evolution of ASEAN's approach to cybersecurity. In APSC 2015, the only reference to any cyber security concern was a single sentence that suggested nations develop laws against cyber security crimes but didn't mention harmonization of laws between ASEAN nations (APSC, n.d.). However significant shift can be observed in the APSC 2025 Blueprint where cyber security policies have their own dedicated section. APSC 2025 paper puts more emphasis on training, education, public-private cooperation, and awareness. This shift aligns with people people-centered approach of APSC (APSC, n.d.). Meanwhile, both papers strongly suggest collaboration of law enforcement, but they don't offer any framework. The transformation of cyber security policies within APSC illustrates an evolution from law enforcement towards more people-centered policy, which is in line with the overarching objectives of APSC. Furthermore, the heightened prominence of cyber security within the 2025 blueprint reflects the growing significance of cyber security issues in the realm of political security concerns.

ICT Masterplans and Digital

ICT (Information and Communications Technology) is a broad term that encompasses technologies, devices, and methods used in the manipulation and transfer of information. ICT encompasses a wide array of sub-categories such as internet, cyber security, and data management (Eurostat, n.d.). ASEAN published two ICT master plans and one Digital Master Plan which can

be considered a continuation of the ICT master plan. While all three editions acknowledge the digital divide as a critical problem to address, they notably lack any promotion or discussion of strategies to enhance women's participation to mitigate this divide. While the precise motivations behind this decision remain unclear, it can be theorized that ASEAN nations might be avoiding contentious topics like gender due to their potential to be viewed as political issues in certain ASEAN countries. A similar problem doesn't apply to children as they are in all three documents their training and introduction to ICT are supported.

ICT 2015 Masterplan

ICT 2015 Masterplan lays out several policy goals however their goals can be considered ambitious as several of them have not been accomplished even in 2023. One of these goals, for instance, harmonization of ICT regulations which can be considered the weakest part of ASEAN's policy on cyber security. The suggestion to promote two-factor authentication is laudable but the purpose for this authentication is meant primarily based on financial transactions not necessary for privacy concerns. In later editions of masterplan papers, a transition into more personal data protection concerns rather than a singular focus on financial concerns can be seen.

ICT 2020 Masterplan

ICT 2020 Masterplan just like its predecessor has similar focuses. However, there is increased attention given to information privacy and sustainability. Notably, unlike the ICT 2015 Masterplan, the ICT 2020 Masterplan also prioritizes the promotion of public-private partnerships for bolstering cyber security protection.

Digital Masterplan 2025

The length of Digital Masterplan 2025 is almost five times greater than its previous version, indicating a heightened emphasis on cyber security and information technologies. This updated

version also places a stronger focus on fostering trust in the digital space. It incorporates data indicating that approximately 35% of ASEAN citizens who have access to digital services choose not to use them due to a lack of trust in the digital realm (*ASEAN DIGITAL MASTERPLAN*, 2021). While both ICT papers and the ASEAN Cyber security Cooperation Strategy paper address concerns related to trust in cyberspace, Digital Masterplan 2025 stands out as the only document that substantiates these concerns with real-life data. This shift toward a more data-driven approach is evident in various other topics within Digital Masterplan 2025.

Overlap of resource allocation and responsibilities

The increased emphasis on addressing cyber security concerns has inadvertently led to a complex web of overlapping organizations, resulting in a negative evolution of cyber security policies. This intricate landscape is further complicated by the frequent rebranding of initiatives, exemplified by the transition from the ICT Masterplan to the Digital Masterplan and from the ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) to the ASEAN Digital Ministers' Meeting (ADGMIN).

Entities like ADGMIN, the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), and the ASEAN Regional Forum (ARF) each produce their own reports on cyber security. These reports often exhibit substantial overlap in their content, indicating inefficiencies in information and policy coordination.

Moreover, the ASEAN Political-Security Community (APSC) has issued its own comprehensive blueprints, which encompass cyber security policies, thereby adding another layer to the intricate cyber security framework. Beyond the aforementioned organizations, several sectoral committees and bodies, such as the East Asia Summit (EAS), the ASEAN Defence

Ministers' Meeting (ADMM)-Plus, and the ASEAN Ministerial Meeting on Social Welfare and Development (AMMSWD), contribute to this evolving landscape.

Furthermore, some of these organizations give rise to sub-entities dedicated to specific cyber security aspects. For instance, the SOMTC Working Group on Cybercrime (WG on CC) and the Inter-Sessional Meeting on Security of and in the Use of ICTs are created in response to specific cyber security concerns.

Legal framework

Previously this paper discussed potential problems with definitions of cyber security and the transnational nature of cybercrimes, these problems are also deeply connected with the ASEAN cyber security framework. Regionally, the only framework available for transborder crime investigations is the Treaty on Mutual Legal Assistance in Criminal Matters (MLAT) created in 2004, which is accepted by all ASEAN members (ASEAN, n.d.-b). Budapest convention which can be an alternative framework is only accepted by the Philippines (Council of Europe, n.d.). Not only MLAT is an outdated framework for today's modern cyber security investigations but the lack of harmonization of legal systems makes it difficult to apply. Furthermore, in comparison to the Budapest Convention, MLAT lacks provisions for expedited preservation and disclosure of computer data, mutual assistance in accessing stored data, transborder data access with consent or public availability, and real-time traffic data collection (Benincasa, 2021). Based on the fact that there hasn't been any meaningful change in the legal framework of ASEAN since the signature of MLAT it can be said that ASEAN's legal framework for Cyber-crime prevention has not only failed but also has not evolved at all.

The ASEAN nations each have distinct national legal frameworks for addressing cybercrime, and these frameworks differ from one another in their formulation. The cyber

lexicon and legal terminology used to refer to cyber crimes are not harmonized. In this context, harmonization does not necessarily imply that all ASEAN countries should adopt identical systems. Instead, it signifies the facilitation of effective collaboration among individual legal and government institutions within the region (Smith, 2023). One of the most concrete examples of this definition of cyber emergency response structure. For instance, Malaysia employs a five-tiered response system to assess the severity of threats based on their critical impact on infrastructure, while Vietnam utilizes a single-tier system that activates in response to attacks on critical state assets or large-scale incidents, meanwhile, Cambodia and Indonesia notably lack any comparable emergency response structures (Tay, 2023, p. 13). A real-world scenario might involve cybercriminals launching an attack from Cambodia against Malaysia. In this situation, Malaysian authorities would have limited response options available, potentially requiring them to submit an MLAT petition. However, this process could prove challenging for both sides, as the Malaysian authorities would need to structure their petition based on their tiered response system, which lacks a corresponding framework in Cambodia, creating potential complexities in cross-border cooperation and coordination.

Conclusion

The evolution of ASEAN's cyber security policy is a testament to the organization's responsiveness to the changing digital landscape and its commitment to safeguarding the interests of its member states in an increasingly interconnected world. This research paper has explored various dimensions of this evolution, shedding light on the general patterns, framework agreements, international collaborations, and the roles of specific countries in shaping ASEAN's cyber security policies. As we conclude, it is evident that ASEAN has made significant strides in addressing cyber security challenges, but there are key takeaways and challenges to consider.

The emphasis on regionalization through innocuous diffusion reflects ASEAN's pragmatic approach to fostering collaboration without imposing hierarchical structures that could challenge member states' sovereignty. Moreover, the shift towards a people-centric approach demonstrates ASEAN's recognition of the importance of citizens and communities in the digital realm. The organization has evolved from focusing on business or state-based concerns to people-centric concerns such as privacy and cyber hygiene. This shift aligns with ASEAN's broader objectives of promoting people-centric institutionalism.

The adoption of a holistic approach to cyber security challenges is another noteworthy aspect of ASEAN's evolution. As the use of ICTs has become more pervasive, ASEAN has expanded its agenda to encompass a wider range of issues, including the digital divide, privacy, data protection, online content regulation, and trust in cyberspace.

ASEAN's engagement with international entities and regional partners has played a pivotal role in shaping its cyber security policies. ASEAN has actively collaborated with various regional organizations, international entities, and individual states. The collaboration with the EU is a prime example of ASEAN's commitment to building global partnerships. The Plan of Action to Implement the ASEAN-EU Strategic Partnership reflects the organization's willingness to align with international frameworks while preserving its unique regional identity. An overview of ASEAN agreements with international actors shows ASEAN's desire to be a central institute in the region for collaboration and diplomacy. The Interpol-based ASEAN Cybercrime Operations Desk and the United States' contribution to capacity development through Interpol highlight the practical benefits of such partnerships. ASEAN's interactions with Japan have also been instrumental in enhancing its cyber security landscape, particularly in areas of specialist training and SDGs integration into the cyber security field. These collaborations are also examples of innocuous

diffusion as these countries funnel resources and knowledge into the region without challenging national sensitivities.

However, challenges remain, particularly concerning the EU's stringent General Data Protection Regulation (GDPR), which stands in contrast to ASEAN's lack of an equivalent framework. Bridging this gap in data protection regulations will be crucial for deepening inter-regional cooperation with the EU in cyber security.

ASEAN's commitment to the ASEAN Way and its unique approach to regionalization set it apart from other regional organizations. The principle of regionalization through innocuous diffusion, as observed in the establishment of CERTs, Cyber Security Agencies, ICT masterplans, and joint programs with foreign organizations underscores ASEAN's commitment to collaboration without challenging national sensitivities. While regional CERTs serve as a collaborative effort to address cyber threats collectively, the absence of a regional cyber security agency aligns with the organization's avoidance of hierarchical approaches that could threaten member states' sovereignty.

As ASEAN continues to evolve its cyber security policies, several challenges and opportunities lie ahead. One of the key challenges is the complex web of overlapping organizations and responsibilities within the region. The presence of numerous entities, such as ADGMIN, AMMTC, ARF, and various sectoral committees, can lead to inefficiencies in information and policy coordination. Streamlining these responsibilities will be essential for enhancing ASEAN's cyber security capabilities. Another critical challenge is the lack of harmonization in the legal framework for cybercrime prevention among ASEAN member states. While MLAT is accepted by all member states, it is outdated and lacks provisions for modern cybercrime investigations. ASEAN's commitment to facilitating effective collaboration among individual legal and

government institutions is vital to addressing this challenge and ensuring efficient cross-border cooperation in cybercrime cases.

In conclusion, this research has uncovered three distinct patterns of evolution in ASEAN's cybersecurity policies. These patterns are evident across a wide range of documents and agreements, including ICT Masterplans, ASEAN-Japan agreements, ASEAN-EU agreements, APSC Blueprints, TAC, and numerous ASEAN framework agreements. This study has identified the following general evolution patterns: increased regionalization through innocuous diffusion within the realm of cybersecurity, an expanding holistic approach to cybersecurity concerns, and an increasing emphasis on adopting a people-centered approach to cybersecurity. It is important to highlight that this paper's investigation into these patterns is based framework of the ASEAN Way, emphasizing the significance of employing regional frameworks to address regional concerns effectively.

Bibliography

Agnew, J. (2020). Taking back control? The myth of territorial sovereignty and the Brexit fiasco. *Territory, Politics, Governance*, *8*(2), 259–272. https://doi.org/10.1080/21622671.2019.1687327

AL JAZEERA. (2023, August 18). *ECOWAS defence chiefs agree 'D-day' for Niger military intervention*. https://www.aljazeera.com/news/2023/8/18/ecowas-defence-chiefs-agree-d-day-for-niger-military-intervention

Allison-Reumann, L. (2017). The Norm-Diffusion Capacity of ASEAN: Evidence and Challenges: Norm-Diffusion Capacity of ASEAN. *Pacific Focus*, *32*(1), 5–29. https://doi.org/10.1111/pafo.12089

Ang, B. (2021). Singapore: A leading actor in ASEAN cybersecurity. In *Routledge Companion to Global Cyber-Security Strategy*. Routledge.

APSC. (n.d.). *ASEAN Political Security Community*. ASEAN Main Portal. Retrieved August 30, 2023, from https://asean.org/our-communities/asean-political-security-community/

ASEAN. (n.d.-a). *ASEAN Cybercrime Operations Desk*. Retrieved September 1, 2023, from https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk

ASEAN. (n.d.-b). *Treaty on Mutual Legal Assistance in Criminal Matters*. ASEAN Main Portal. Retrieved August 24, 2023, from https://asean.org/our-communities/asean-political-security-community/rules-based-people-oriented-people-centred/treaty-on-mutual-legal-assistance-in-criminal-matters/

ASEAN. (1976). *The Treaty of Amity and Cooperation in Southeast Asia*. https://asean.org/wp-content/uploads/2021/01/20131230235433.pdf

ASEAN. (2022a). *ASEAN CYBERSECURITY COOPERATION STRATEGY*.

ASEAN. (2023). *Overview of ASEAN-Japan Dialogue Relations*.

ASEAN. (2022b, August 4). *Plan of Action to Implement the ASEAN-EU Strategic Partnership (2023-2027)*. ASEAN Main Portal. https://asean.org/plan-of-action-to-implement-the-asean-eu-strategic-partnership-2023-2027/

ASEAN DIGITAL MASTERPLAN 2025. (2021). ASEAN.

Attatfa, A., Renaud, K., & Paoli, S. D. (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*, *176*, 60–69. https://doi.org/10.1016/j.procs.2020.08.007

Australian Government. (2018, September 1). *ASEAN-Australia Cyber Policy Dialogue – Joint Chairs' Statement | Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/node/89

Benincasa, E. (2021, March 4). *Cybercrime Laws: Members of ASEAN Must Align on Standards*. Vision of Humanity. https://www.visionofhumanity.org/asean-needs-to-enhance-cross-border-cooperation-on-cybercrime/

Beyond the Coup in Myanmar: The ASEAN Way Must Change. (2021, May 17). International Human Rights Clinic. https://humanrightsclinic.law.harvard.edu/beyond-the-coup-in-myanmar-the-asean-way-must-change/

CCDCOE. (n.d.). Retrieved August 24, 2023, from https://ccdcoe.org/organisations/au/

Collins, A. (2013). Norm diffusion and ASEAN's adoption and adaption of global HIV/AIDS norms. *International Relations of the Asia-Pacific*, *13*(3), 369–397. https://doi.org/10.1093/irap/lct012

Council of Europe. (n.d.). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY - Cybercrime—Www.coe.int*. Cybercrime. Retrieved August 24, 2023, from https://www.coe.int/en/web/cybercrime/parties-observers

Council of the EU. (2023). *EU sanctions: Council finalises position on law that aligns penalties for violations*. https://www.consilium.europa.eu/en/press/press-releases/2023/06/09/eu-sanctions-council-finalises-position-on-law-that-aligns-penalties-for-violations/

Council of the European Union. (2023, February 2). *Voting system*. https://www.consilium.europa.eu/en/council-eu/voting-system/

CSA. (2023). *Who We Are*. Default. https://www.csa.gov.sg/Explore/who-we-are

Desker, B. (2021, May 23). *ASEAN's Myanmar dilemma*. East Asia Forum. https://www.eastasiaforum.org/2021/05/23/aseans-myanmar-dilemma/

EEAS. (2023, February 24). *ASEAN: 30th Joint Cooperation Committee Meeting with the European Union convenes in Jakarta | EEAS*. https://www.eeas.europa.eu/eeas/asean-30th-joint-cooperation-committee-meeting-european-union-convenes-jakarta_en?s=172

European Parliament. (2023, June 7). *EU sanctions: New law to crack down on violations | News | European Parliament*. https://www.europarl.europa.eu/news/en/press-room/20230703IPR01909/eu-sanctions-new-law-to-crack-down-on-violations

Eurostat. (n.d.). *Glossary:Information and communication technology (ICT)*. Retrieved August 24, 2023, from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT)

Goodman, P. S. (n.d.). *Computer Emergency Response Team (CERT)*. http://dli.library.cmu.edu/paulgoodman/computer-emergency-response-team-cert

Interpol. (n.d.). *Cyber Capabilities & Capacity Development Project*. Retrieved September 1, 2023, from https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cyber-Capabilities-Capacity-Development-Project

Interpol. (2021). *ASEAN CYBERTHREAT ASSESSMENT 2021*.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, 338–345. https://doi.org/10.1109/CIC48465.2019.00047

Jetschke, A. (2017). What Drives Institutional Reforms in Regional Organisations? Diffusion, Contextual Conditions, and the Modular Design of ASEAN. *TRaNS: Trans -Regional and -National Studies of Southeast Asia*, *5*(1), 173–196. https://doi.org/10.1017/trn.2016.30

Kelleher, J. (2017, October 27). *Indonesia launches Cyber Security Agency—OpenGov Asia*. https://opengovasia.com/indonesia-launches-cyber-security-agency/

Kurlantzick, J. (2022, August 29). *ASEAN's Complete Failure on Myanmar: A Short Overview*. Council on Foreign Relations. https://www.cfr.org/blog/aseans-complete-failure-myanmar-short-overview

Manantan, R. C., Mark. (2023). *EU-ASEAN Cooperation on Cybersecurity and Emerging Technologies - Reimagining EU-ASEAN Relations: Challenges and Opportunities*. Carnegie Europe. https://carnegieeurope.eu/2023/07/04/eu-asean-cooperation-on-cybersecurity-and-emerging-technologies-pub-90082

NACSA. (n.d.). *NACSA | About Us*. Retrieved August 24, 2023, from https://www.nacsa.gov.my/about-us.php

National center of Incident readiness and Strategy for Cybersecurity. (n.d.). Retrieved September 2, 2023, from https://www.nisc.go.jp/eng/fw_top.html

Priyono, U., Swastanto, Y., & Pramono, B. (2023). Cyber Diplomacy (A Perspective From Indonesia—Australia Cyber Cooperation). *International Journal Of Humanities Education and Social Sciences (IJHESS)*, *2*(4). https://doi.org/10.55227/ijhess.v2i4.371

Ramadhan, I. (2020). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). *Journal of Social and Political Sciences*, *3*(4). https://doi.org/10.31014/aior.1991.03.04.230

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Signing of Record of Discussions on Technical Cooperation Project with ASEAN. (n.d.). Retrieved September 2, 2023, from https://www.jica.go.jp/Resource/english/news/press/2022/20230228_41.html

SingCERT. (n.d.). Default. Retrieved August 30, 2023, from https://www.csa.gov.sg/faq/singcert

Singer, P. W. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Smith, R. (2023). Harmonisation of Laws in ASEAN: The Issue of Language. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4323491

What is Cybersecurity? | IBM. (n.d.). Retrieved August 23, 2023, from https://www.ibm.com/topics/cybersecurity

Yu, E. (2022, October 20). *Singapore champions Asean CERT as region's cyber armour*. ZDNET. https://www.zdnet.com/article/singapore-champions-asean-cert-as-regions-cyber-armour/

Yukawa, T. (2018). The ASEAN Way as a symbol: An analysis of discourses on the ASEAN Norms. *The Pacific Review*, *31*(3), 298–314. https://doi.org/10.1080/09512748.2017.1371211