The wild, wild web: explaining variation in ASEAN member-state cyber policy

by

Justin Yau

B.A. (Hons.), The University of British Columbia, 2021

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(POLITICAL SCIENCE)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2022

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, a thesis entitled:

The wild, wild web: explaining variation in ASEAN member-state cyber policy

submitted by **Justin Yau** in partial fulfillment of the requirements for

the degree of **Master of Arts**

in **Political Science**

Examining Committee:

Xiaojun Li, Professor, Department of Political Science, UBC
Supervisor

Yves Tiberghien, Professor, Department of Political Science, UBC
Supervisory Committee Member

Abstract

Cyberspace, as a global commons not under the jurisdiction of one actor alone, requires regional or global coordination in its governance. With respect to the former, regional organisations comprising multiple state actors have been active in taking a leadership role in governance. However, compliance is not always observed, for various reasons. As such, why might some states comply with the regional organisation's policy strategy while others do not? This paper focuses on this question by means of examining the Association of Southeast Asian Nations (ASEAN), which has been active in prescribing policy recommendations that its member-states ought to follow. Indeed, there exists a variation in member-state compliance with these policies, and this paper seeks to elaborate on two distinct explanations at separate levels of analysis on why this is the case. The first explanation approaches the question from a state-level perspective, and posits that external leverage exerted by a state actor in China is responsible for creating fluctuations in compliance. The second takes an organisational-level approach and hypothesises that it is ASEAN's own foundational principles of (1) non-interference in sovereign affairs, and (2) consensus-based decision-making which cause the variation observed. Using qualitative methods of process tracing in examining state documents and case studies of ASEAN's history in regional governance, this paper concludes that the linkage between external leverage and variation in compliance is weakly seen, and cannot be conclusively verified. On the other hand, through the case study of ASEAN's governance of regional pollution, it can be seen that variation in compliance can be traced to ASEAN's inability to do more in regional governance than recommend best policies and use moral suasion to convince its member-states to comply.

Lay Summary

This thesis illuminates the disconnect between efforts to govern cyberspace at a regional or global level, while the primary units involved in governing cyberspace are still states that possess the ability to decide how to govern territory within their own borders. By using ASEAN as the primary case study, this thesis aims to contribute to existing literature on cyberspace and international relations by linking this field to other areas of global governance requiring coordination and cooperation, such as Earth's oceans, outer space, and the environment. By identifying how inter-state relations, power politics, and organisational dynamics correlate, the key contribution is in identifying what future difficulties in cyberspace governance between state actors and regional or international organisations will ultimately look like.

Preface

This thesis is original and independent work by the author, Justin Yau. However, aspects of the causal mechanism of this thesis's primary hypothesis (H1) in Section 3 arise from a previous publication's exploratory work, "Defragmentation: Cyber Sovereignty in the Asia-Pacific and ASEAN's Normative Role," by myself, Justin Yau (2022). This earlier work was written and sent for publication by the Defence and Security Foresight Group's Asia-Pacific Team at the University of Waterloo.

Table of Contents

Abstract iii
Lay Summary iv
Preface v
Table of Contents vi
List of Tables vii
List of Abbreviations viii
Acknowledgements ix
Dedication x
Section 1: Introduction 1
1.1. Opening and research question 1
Section 2: Literature review, theories, and hypotheses 5
2.1. A background on ASEAN 5
2.2. Cyberspace governance and ASEAN's policy recommendations 6
2.3. Explaining comparative variation in compliance with ASEAN 10
Section 3: External leverage as an explanatory variable (H1) 16
3.1. Measuring member-state compliance with ASEAN policies 16
3.2. Testing H1 20
3.2.1. Malaysia 21
3.2.2. The Philippines 26
3.2.3. Singapore 30
3.2.4. Concluding remarks on H1 32
Section 4: ASEAN and non-interference in regional policy as an explanatory variable (H2) 34
4.1. Testing H2 34
4.2. Transboundary haze and ASEAN 35
4.3. Concluding remarks on H2 37
Section 5: Conclusions 40
References 45
Appendix: Constructing Table 1 52

List of Tables

Table 1. ASEAN member-states' compliance with ASEAN cyberspace regulation recommendations and quantitative scores on given issue-areas..... 18

List of Abbreviations

ARPANET – Advanced Research Projects Agency Network;

ASEAN – Association of Southeast Asian Nations;

BRI – Belt and Road Initiative;

CBM – Confidence Building Measures;

DICT – Department of Information and Communications Technology;

EEZ – Exclusive Economic Zone;

EU – European Union;

ICT – Information and communications technology;

NCSP 2022 – (The Philippines's) National Cybersecurity Plan 2022;

OCP – One China Policy;

TAC – Treaty of Amity and Cooperation (in Southeast Asia);

UN GGE – United Nations Group of Governmental Experts;

WTO – World Trade Organisation.

Acknowledgements

I would like to extend my deep gratitude to my supervisor, Xiaojun Li, for providing his constant support during the writing of this thesis and for his encouragement in this field of research. His guidance and advice allowed me to successfully navigate past the moments where parts of the thesis-writing process initially seemed most unclear. Moreover, I extend my gratitude to the following members of the Department of Political Science at UBC, who have all been a significant inspiration to me in completing this M.A. at UBC by specialising in the field of international relations: Yves Tiberghien, who also served as the second reader and examiner for this thesis, Robert Crawford, and Katia Coleman.

I would also like to thank my family for providing the bedrock of support during my time at UBC. First, my brother, Dr. Clement Yau, has been the individual whom I have looked up to most when I first began my journey at UBC five years ago. His own work and dedication during his studies have greatly inspired me during my own time in academia. Second, to my mother Susanna Li, her unwavering support of me and my academic journey since the beginning, but especially during the previous two years of this pandemic, has made the completion of this thesis and the M.A. programme all the more worth it.

Dedication

Dedicated to Susanna Li and Dr. Clement Yau.

Section 1: Introduction

1.1. Opening and research question

Cyberspace has historically received attention in international politics as another global arena not solely confined to a singular state actor's sovereign jurisdiction, as demonstrated by the Indonesian Ministry of Defence's white paper from 2015 concluding that cyberspace was to be a "battlefield" for national security, in addition to the prominent arenas of "sea, air, and space."[1] However, one key difference between cyberspace and Earth's oceans, air, and outer space remains that the former is a *constructed* global commons, with its early roots linked to national security purposes such as the U.S. Department of Defence's Advanced Research Projects Agency Network (ARPANET), an experimental network in the 1960s linking computers and allowing them to communicate with one another.

Since its infancy, cyberspace has grown at an exponential pace, prominently seen through the creation of the Internet, which allows for significantly higher rates of information flow and transactions between individuals as well as entire communities across borders. Yet, for all of its benefits, this exponential growth has been substantially marred by its lack of comprehensive regional or global regulation. In a manner similar to the other global commons on or around Earth, because this digital realm is not bound to one actor's central authority, questions surrounding who, if anyone, ought to govern it and in what manner ought it be governed obtain a higher priority in state-based discourse. While attempts have been made at both a regional and a global level to address these questions in turn, their respective successes have stalled due to the

[1] Defence Ministry of the Republic of Indonesia, "Defence White Paper" (2015), 16

ever-present necessity of a state to have unimpeded sovereignty restricting the scope of such coordinated, cooperative efforts. Therefore, a cleavage exists between models arguing for a regional or even global governance approach to regulating cyberspace and a resolutely state-centric approach bounded by the territorial demesnes of each country.

That such a cleavage exists also factors into a state's willingness to comply with a regional or a global approach to regulating cyberspace. For instance, some states may be more willing to abide by an organisation's policies, while others are staunchly against suffering any loss to their national sovereignty and policy autonomy. In that case, this thesis seeks to ask the following research question: *Why might some states comply with a regional organisation's strategies on cyberspace regulation while other states do not?*

Explaining the variation seen in state-level compliance with a particular regional organisation's strategies on cyberspace regulation will depend on multiple factors, such as the number and disposition of states involved with the organisation, the strength and cohesiveness of the organisation, or perhaps the amount of influence in this process exerted by external actors. This thesis will be situated in the Southeast Asian corridor, where the cleavage between regional or global forms of cyber governance and state-centric policies can be further analysed through viewing the historical attempts of the Association of Southeast Asian Nations (ASEAN) to promote recommendations and norms for responsible, regional behaviour in cyberspace. The overall theme of this thesis tackles ASEAN's own role as a regional organisation setting regulatory standards in cyberspace, as well as the careful distinction between traditional notions of maintaining state sovereignty and monitoring compliance to an organisation's policies and recommendations.

Choosing to situate this research in Southeast Asia, through examining ASEAN, is due to its unique position in contemporary international politics. First, unlike other regional organisations such as the European Union (EU), ASEAN features no overt efforts of political integration from its member-states. In fact, the 1976 Treaty of Amity and Cooperation (TAC) in Southeast Asia enshrines "mutual respect for the independence, sovereignty, equality, territorial integrity and national identity of all nations" part of ASEAN.[2] As such, this makes ASEAN an excellent case study for viewing the effects of this dichotomy between regional governance and respect for sovereignty. Furthermore, ASEAN as a regional organisation will be expected to play a crucial role in the politics of the Indo-Pacific[3] where major state actors like China and the U.S. will continue focusing on vital strategic areas of national interest, such as Taiwan, East Asia, and the South China Sea. ASEAN will thus find itself with an opportunity to shape policy in the Indo-Pacific as well, and studying its positions on cyberspace should provide insight as to how they plan to navigate the foreseeable future around such actors in this issue-area.

In addition to selecting ASEAN as the primary regional organisation of interest, this thesis will also focus on a particular subset of policies proposed or recommended by ASEAN with respect to regulating cyberspace. Defining a nebulous term such as 'cyber governance' requires precision, and this paper will explore ASEAN's recommendations on cyber governance to pertain to the following fields: personal data protection, integrity and provisioning of data, data security, and cross-border data flows. One reason for which these four aspects were selected

---

[2] ASEAN, "Treaty of Amity and Cooperation in Southeast Asia" (1976), 2

[3] While Asia-Pacific is still used in parts of relevant literature, ASEAN has referred to the geopolitical region as the Indo-Pacific as of their June 2019 summit where they published their "ASEAN Outlook on the Indo-Pacific." This thesis will therefore remain consistent with ASEAN's wording and also use Indo-Pacific instead of Asia-Pacific.

is that there are an exhaustive number of subfields in cyber governance which could feasibly be covered, which means that this paper will only select a representative sample to cover. However, on a practical level, ASEAN's documentation on cyber governance is also limited in scope, and the recommendations pushed in these four areas were noted to be the ones with the most observations with which to conduct analysis.

By centering this thesis in Southeast Asia, this paper will contribute to existing literature on ASEAN's own internal political dynamics, which includes literature on its consensus-based style of decision-making, its enshrining of sovereignty as a core tenet, and the ways in which ASEAN has needed to cautiously navigate their relations with actors in their geographical region. It will also contribute to the growing literature on cyberspace in international relations, from both an organisational and a member-states' standpoint. In doing so, this research will add to the gap seen in cyberspace governance as a field of study in international relations, specifically from the perspective of regional organisations. This will assist in illuminating ASEAN's path moving forward not only as an organisation active in shaping cyberspace policy, but as a regional organisation in contemporary international politics, as well demonstrating the difficulties inherent in all forms of coordinating digital governance policies.

Having laid the foundations for this study's scope, the next section will elaborate on the theories and causal mechanisms proceeding the research question, supported by a review of literature relevant to ASEAN as an organisation involved with cyberspace governance. Then, it will formally introduce the two main hypotheses to be tested.

Section 2: Literature review, theories, and hypotheses

2.1. A background on ASEAN

Prior to understanding why the comparative variation seen in ASEAN member-states on cyberspace policy is important in the context of the organisation, it is first necessary to briefly go over the impetus for ASEAN to form in the first place. The creation of ASEAN in 1967 principally reflected a desire to introduce regional political cohesion in Southeast Asia among non-communist states. Acharya (2003) discusses that through a desire to find "regional solutions to regional problems," this would eventually culminate in ASEAN being formed by Indonesia, Malaysia, the Philippines, Singapore, and Thailand.[4] The core goals of this organisation was not only to hasten economic, social, and cultural development in Southeast Asia, but to also encourage more stability in the region, especially during the events of the Cold War. While each founding member had their own particular reasons for wanting ASEAN to succeed from its inception, their shared vision for this organisation was the "creation of a set of norms for governing relations" between each member-state.[5]

These norms, argue Narine (2008), encompass the idea of ASEAN as an organisation that finds its greatest success in rallying its member-states around common interests but not a common identity.[6] In addition to the enshrinement of mutual respect for independence and sovereignty mentioned previously, the 1976 TAC also decrees that each member-state has a right to lead policy autonomy "free from external interference, subversion, or coercion," which

---

[4] Acharya, Amitav, *The Making of Southeast Asia: International Relations of a Region* (Ithaca: Cornell University Press, 2003), 154
[5] Ibid, 158
[6] Narine, Shaun, "Forty years of ASEAN: a historical review," *The Pacific Review* 21, no. 4 (2008), 412

extends to non-interference in all internal affairs, the settlement of disputes peacefully, and the renunciation of the use of force.[7] For ASEAN, these principles therefore provide its member-states with a guiding code of conduct, but these can also act as significant constraints. According to Stubbs (2014), it is true that these norms aid ASEAN in creating institutional infrastructure such as working groups, committees, and sub-committees within the organisation, as well as enhance their leadership capabilities in regional decision-making.[8] However, at a security level, Jones and Jenne (2016) argue that ASEAN suffers from the very same principle of maintaining non-interference insofar as this norm limits intra-ASEAN integration, citing regional disagreements such as the Thailand-Cambodia conflict and the ongoing South China Sea disputes as examples of where ASEAN cannot overcome their own principle of maintaining non-interference in a member-state's internal, sovereign affairs.[9]

2.2. Cyberspace governance and ASEAN's policy recommendations

While this may be the case for disputes regarding regional security, less clear is how ASEAN uses these fundamental norms with regards to cyberspace regulation as an issue-area of international politics. To unpack ASEAN's own policies and recommendations for cyberspace, it is first important to briefly elaborate on how cyberspace governance is conceived at a theoretical as well as a practical level, and finally contextualise this within international relations literature. Cyberspace can be understood as a geopolitical region chiefly concerned with a principal question: how open should access to the Internet be? Such a vague question engenders further

---

[7] ASEAN (1976), 2
[8] Stubbs, Richard, "ASEAN's leadership in East Asian region-building: strength in weakness," *The Pacific Review* 27, no. 4 (2014), 531
[9] Jones, David Martin, and Nicole Jenne, "Weak states' regionalism: ASEAN and the limits of security cooperation in Pacific Asia," *International Relations of the Asia-Pacific* 16 (2016), 234

questions on what openness ought to be defined as, and how boundaries around openness should be set. For the purposes of solely considering data as the main unit affected by the degree of open cyberspace, Liu (2021) considers data as a resource with economic and strategic value, where it is not always possible to "exclude nonpaying individuals from having access" to it, thus determining that data is a "quasi-public good" and that cyberspace must be open to a certain extent.[10] In a domestic political sense, data also faces a commitment problem where firms may or may not be forced to disclose user data to a national government, representing another facet of openness in cyberspace.

To discuss the question of how to consider forms of governance in cyberspace, each with their own conceptions of openness, O'Hara and Hall (2018) lay the foundations for other models (Aaronson (2019); Glen (2014); Mueller (2020); Ciuriak and Ptashkina (2020); Hufbauer and Lu (2019)) on how cyberspace can, and has, been seen in international relations. O'Hara and Hall consider four main possible versions of cyberspace: (1) an open Internet without restraints as was originally envisioned, (2) a legally-minded Internet focused on aggressive regulation on privacy and copyright laws, (3) an authoritarian Internet committed to surveillance and state control, and (4) a commercial Internet rejecting net neutrality and allowing for consumerism.[11]

These various models may also be viewed in the sense that they also prescribe how much national control should be given to cyberspace regulation, or conversely, how much global governance ought to shape cyberspace. Recent literature such as Hufbauer and Lu (2019) has made frequent mention of the fact that attempts at global governance through international

---

[10] Liu, Lizhi, "The Rise of Data Politics: Digital China and the World," *Studies in Comparative International Development* 56 (2021), 47

[11] O'Hara, Kieron, and Wendy Hall, "Four Internets: The Geopolitics of Digital Governance," *Centre for International Governance Innovation* (2018), 6-11

organisational negotiations, such as the WTO in 2019, have largely failed to reach any meaningful resolution on contentious digital commerce issues, which include data flows, data localisation, privacy, Internet taxes, and open Internet access.[12] As a result of international inertia, this allows states to put into motion their own plans for what each believe to be their own compatible version of cyberspace with their national government. For instance, traditional conceptions of economic protectionism may also apply to digital cross-border data flows,[13] and states may actively engage in pushing for O'Hara and Hall's conception of an authoritarian cyberspace, where each state is allowed to govern digital affairs with impunity so long as the action or the data lies within their physical state borders.

Within this global-national debate, ASEAN has historically adopted a moderate tone. As a regional organisation committed primarily to the economic, social, and cultural development of its member-states, measures on cyberspace regulation and governance coming from the ASEAN Community since 2015 have initially mostly focused on these areas as part of their Confidence Building Measures (CBMs).[14] This includes the desire to strengthen cooperation against the rise of cybercrime, projected to run parallel to cyber development, as well as the development of more robust infrastructure for mobile networks.[15] More recently, ASEAN has still continued these objectives through initiatives such as the ASEAN ICT Masterplan 2020 and the ASEAN

---

[12] Hufbauer, Gary Clyde, and Zhiyao Lu, "Global E-Commerce Talks Stumble on Data Issues, Privacy, and More," *Peterson Institute of International Economics* (2019), 2

[13] Aaronson, Susan Ariel, "What Are We Talking about When We Talk about Digital Protectionism?," *World Trade Review* 18, no. 4 (2019)

[14] ASEAN, "ASEAN Cybersecurity Cooperation Strategy (2021-2025)," January 23rd, 2022, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf, 2

[15] Heinl, Caitríona, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime," *Asia Policy* 18 (July 2014), 148

Smart Cities Network, which aims to enhance the region's cyberspace capabilities and in doing so, "assert its regional identity, unity, and centrality in engaging with the rest of the world."[16]

Beyond developing basic cyberspace infrastructure across the region, however, ASEAN's policy recommendations in cyberspace also involve key areas of critical interest, although it is here that one may witness ASEAN's moderate push towards regional, homogeneous policies being constrained by their own policies on non-interference in sovereign affairs. Firstly, ASEAN's Framework on Personal Data Protection in 2016 advises that individuals' personal data should not be collected, used, or disclosed, without notifying the individual or where it would not be deemed reasonable.[17] Yet, this is also paired with the limitation that breaching these conditions would be accepted if "authorised or required under domestic laws and regulations," effectively granting ASEAN member-states *carte blanche* to disregard the above policies when needed.[18]

Adding to this, ASEAN's policies on data integrity, security, and provisioning also note that the use and processing of data must contain accountability mechanisms that are transparent in nature. However, this is diluted once more by the addendum clarifying that these recommendations should only be considered if "not contrary to laws or national policies."[19] Finally, ASEAN's initiatives on regulating cross-border data flows indicate that a high priority should be given to ensuring that "safeguards are in place to protect and secure the information

---

[16] Noor, Elina, "Positioning ASEAN in Cyberspace," *Asia Policy* 15, no. 2 (April 2020), 108-109
[17] ASEAN Telecommunications and Information Technology Ministers Meeting, "Framework on Personal Data Protection," November 16th 2016, https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf, 3
[18] Ibid.
[19] ASEAN Telecommunications and Information Technology Ministers Meeting, "Framework on Digital Data Governance," December 6th 2018, https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf, 4

regardless of where the data goes," while also acknowledging that this will depend on the "different levels of maturity and local laws present" in the member-state.[20]

2.3. Explaining comparative variation in compliance with ASEAN

Ultimately, none of these findings ought to be surprising, given the nature of ASEAN as a regional organisation concerned with encouraging its member-states towards coordinating on common interests, as these policies have done, whilst also being constrained significantly by its major principle of non-interference. However, that ASEAN allows for national interests to supersede its regional recommendations therefore introduces the importance of this thesis's research question, in determining whether any patterns are present to account for this variation in member-state compliance with ASEAN's cyber strategies.

In this thesis, two competing explanations will be considered. The first is at a unit level of the ASEAN member-states, and it hypothesises that due to external actor influence, this presence of external leverage causes a decrease in member-state compliance with ASEAN recommendations on cyberspace regulation. As this external actor possesses leverage over the ASEAN member-state, they are able to influence the member-state into lower compliance with ASEAN as well as having closer written language in their own policies with the external actor's. It is useful at this juncture to provide a brief illustration of what leverage entails, in the context of this causal mechanism. Traditional literature in international relations has several methods of envisioning leverage: for instance, Waltz (1959, 1979) equates leverage with power in a Hobbesian sense where leverage can be seen as the ability to "produce an intended effect," in

---

[20] ASEAN Telecommunications and Information Technology Ministers Meeting, "Framework on Digital Data Governance," 6

this case lower compliance with ASEAN policies.[21] In ASEAN's case, this type of leverage may be seen in a security or military context, such as a dispute over contested territory such as the South China Sea. It may also be an economic type of leverage, where the external actor makes up such a high proportion of bilateral trade with the ASEAN member-state that failure to act similarly to the external actor's expectations would result in heavy economic loss.

On the other hand, external leverage might not necessarily be through force or coercion from the external actor, and so leverage may not always represent a negative relationship for the ASEAN member-state. Power and leverage may also result from ideas, interests, and institutions. As Wendt (1999) argues, power in international politics is derived partly from interests, which is also partly derived from ideas.[22] As such, external actor influence in this causal mechanism might also contain factors relating to domestic politics, where an ASEAN member-state believes it more useful to act similarly to the external actor in order to remain as part of this social group's constituted identity, rather than the regional organisation's identity. The normative pull to act similarly to an external actor to maintain a common identity may be stronger, and thus constitute the external leverage responsible for deviating from compliance to ASEAN recommendations on cyberspace governance. This might even have ramifications at a domestic political level, where failure to continue maintaining this common identity could result in a loss of political legitimacy and weaken the national government currently in power.

Therefore, the presence of external leverage may be one explanation for the comparative variation in ASEAN member-states' cyberspace policies. This thesis will select China as the

---

[21] Waltz, Kenneth N., *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1959), 205
[22] Wendt, Alexander, *Social Theory of International Politics* (Cambridge University Press, 1999), 135

external actor of interest with possible sources of external leverage among ASEAN member-states for the following reasons. First, China has historically been active in the Indo-Pacific region, with regards to key territorial conflicts in the South China Sea such as the Spratly and Paracel islands, both of which are also contested by ASEAN member-states.[23] This represents the first possible form of leverage to be studied. China, as a major economic power in the region, will also have potential to hold economic forms of leverage over ASEAN member-states. Finally, their current relationship with ASEAN member-states indicates that historically, China has been willing to exploit the "shallow institutionalism" seen in the regional organisation in order to employ strategies of coercion and inducement in order to increase its influence over ASEAN's member-states.[24] As such, while China exhibits no discernible leverage in a more normative or ideational sense, this thesis has decided to study China over the U.S. as the principal external actor exerting leverage over ASEAN member-states.

Moreover, another reason to examine China's relationships with various ASEAN member-states is their own role in cyberspace governance. In areas including maritime regions and cyberspace, it is well-documented that China selectively chooses to comply when it strategically benefits their national interests.[25] In other cases, China is willing to subvert other state actors' or non-state actors' attempts of setting global cyberspace governance norms or policies, eschewing the West and ASEAN's version of multi-stakeholder governance featuring coordination and cooperation in favour of "multilateral governance" which, for China, is akin to

---

[23] Jones and Jenne, 226
[24] Thu, Huong Le, "China's dual strategy of coercion and inducement towards ASEAN," *The Pacific Review* 32, no. 1 (2019), 22
[25] Govella, Kristi, "China's challenge to the global commons: compliance, contestation, and subversion in the maritime and cyber domains," *International Relations* 35, no. 3 (2021), 448

cyberspace being delegated as a sovereign responsibility of each state.[26] This effort of fragmenting governance into separate, sovereign spheres would importantly be diametrically opposed to the intent of ASEAN's recommendations towards a regional, cohesive form of cyberspace governance. As such, studying whether the possibility of Chinese external leverage observed leads to a pattern of member-states' varying, but decreased, compliance with ASEAN's recommendations will form the first major hypothesis to be tested. Formally, it will proceed as follows:

> **H1. The presence of Chinese external leverage over an ASEAN member-state leads to decreased compliance with ASEAN cyberspace recommendations.**

The next hypothesis, on the other hand, does not consider the unit level of individual member-states as the first hypothesis did. Rather, it examines the organisational dynamics of ASEAN itself, and considers whether it is ASEAN's own enshrinement of non-interference in sovereign affairs as well as consensus-based decision-making that leads its member-states to vary in compliance regarding any issues on regional, or global, governance.

These internal pillars holding up ASEAN as a regional organisation were originally created during ASEAN's inception as "de-escalation instruments" in order to bolster regional stabilisation and prevent overt conflicts.[27] By ensuring non-interference in one's sovereign political affairs, and focusing on bolstering efforts towards reaching common goals, this allowed ASEAN to attain stability in its early days. Moreover, enacting a policy of consensus-based

---

[26] Yau, Hon-min, "Fragmenting Cyberspace and Constructing Cyber Norms: China's Efforts to Reshape Global Cyber Governance," *Contemporary Chinese Political Economy and Strategic Relations: An International Journal* 7, no. 2 (2021), 694-95

[27] Aizawa, Nobuhiro, "Beyond the Non-Interference Dilemma: The Indonesian Initiative on ASEAN Charter, Nargis Crisis and Regionalism," *Australian Journal of Politics and History* 65, no. 3 (2019), 413

decision-making allowed all of ASEAN's member-states to be assured of "their equal voice," thus rendering size of state, military stature, or ideology irrelevant in decision-making.[28] It is true, however, that ASEAN has strayed from this set of guidelines at times, such as the 11th ASEAN Summit in 2005 where ASEAN openly encouraged for the release of political prisoners and expedition of democratic reforms in Myanmar.[29] For the most part, though, ASEAN has abided by its vaunted 'ASEAN Way' - the use of moral suasion in the hopes that its member-states will "do the right thing so as not to embarrass the collectivity."[30]

That being said, where this ASEAN Way encounters difficulties is where the organisation attempts to create areas of regional or global governance or tackle existing issues which require coordination to facilitate regional or global solutions. Cyberspace functions as one such area, as does climate change or perhaps traditional border disputes in contested maritime waters. As previously noted with ASEAN's guiding principles, non-interference in sovereign affairs and consensus-based decision-making were essential to getting the organisation started, but they may also constitute shackles moving forward. For instance, ASEAN has primarily set these policies on cyberspace as recommendations or optimal strategies to move towards, but always with the caveat that these should be ideally adopted in accordance with national laws where feasible. This caveat is necessary at an organisational level, so as to not appear as though ASEAN was mandating these policies on its member-states, which would be an instant breach of its own non-interference policy. Member-states could also use ASEAN's consensus-based decision-making

---

[28] Aizawa, 413
[29] Katanyuu, Ruukun, "Beyond Non-Interference in ASEAN: The Association's Role in Myanmar's National Reconciliation and Democratization," *Asian Survey* 46, no. 6 (November/December 2006), 839
[30] Simon, Sheldon, "ASEAN and Multilateralism: The Long, Bumpy Road to Community," *Contemporary Southeast Asia* 30, no. 2 (August 2008), 267

against the organisation, as an essential veto power in the event that a cyberspace regulation policy was attempted against the member-states' wishes.

Essentially, what this causal mechanism proposes is that while ASEAN may publish its cyberspace governance strategies, its own member-states may not necessarily see cyberspace as an area to be governed by regional or global means. As this would then contradict ASEAN's policies of respecting non-interference and sovereignty, these states would be free to ignore ASEAN's cyberspace recommendations and this would result in the variation in compliance ultimately seen. As such, this thesis's second hypothesis will formally be:

> **H2. ASEAN's internal dynamics on non-interference and sovereignty lead to decreased compliance with ASEAN cyberspace recommendations.**

Having introduced the two primary hypotheses, the following sections will now turn to studying the variation in compliance seen with ASEAN's cyberspace policies, briefly elaborating the methodology used to conduct this study. Then, it will test each hypothesis respectively, generating observable implications from both causal mechanisms and using process tracing to determine the validity of each hypothesis.

Section 3: External leverage as an explanatory variable (H1)

3.1. Measuring member-state compliance with ASEAN policies

First, it is necessary to determine what exactly constitutes 'compliance' with ASEAN's cyberspace governance policies. Since the quality of member-state data on their own national cyber policies tends to vary quite significantly across each ASEAN member-state, arranging any meaningful quantitative dataset on compliance would be difficult to impossible. Therefore, what this thesis has done is score member-state compliance on an ordinal scale, using qualitative methods. To reiterate, ASEAN's overall emphasis in cyberspace governance is to create a "rules-based order... that is open, secure, stable, accessible, interoperable, and peaceful" and built through "voluntary, non-binding norms of responsible State behaviour, confidence-building measures, and coordinated capacity-building."[31]

Compliance is scored on three levels, similar to a traffic-light scoring system, ranging from: (1) full, precise compliance, (2) vague, imprecise compliance, and finally (3) non-compliance or open defiance of ASEAN. The first level of full compliance refers to a state that makes explicit reference to ASEAN recommendations in their own cyber policy documents, which put forward a substantial effort to abide by them. The state may also include the names of other organisations or documents that are relevant and generally accepted in regional or global governance fora on cyberspace. This may include the UN Group of Governmental Experts, for example, or the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. In short, the 'green' level of compliance indicates that a state makes it very explicit that they

[31] ASEAN, "ASEAN Cybersecurity Cooperation Strategy (2021-2025)", 7

understand what the rules laid out by ASEAN are, and that they make a committed effort to abide by these rules with their own national policies.

Next, the 'amber' level of compliance would entail vague, imprecise compliance. By this, what is meant is a strategic level of ambiguity where member-states discuss the need to abide by international rules, norms, laws, or principles, but do not provide any specific examples. This is a critical component of imprecise compliance, as this demonstrates the cheap talk principle wherein states are free to continually shift their expectations and policies on what compliance with international rules actually entails, without suffering any meaningful consequences for having done so. There should be no reference whatsoever to ASEAN cyberspace strategies or, for that matter, any other institution or organisation relevant in cyberspace.

Finally, the 'red' level of compliance would demonstrate open non-compliance or defiance of ASEAN's recommendations. This is a theoretical level constructed to represent the end of the given categorical model's spectrum, and it is not expected to find any ASEAN member-state openly criticising the regional organisation on cyberspace policy in its documents.

At this point, however, it is imperative to note that one 'amber' state may not necessarily be the same as another in terms of compliance with ASEAN strategies. This is a reasonable flaw of the categorical model, and it will be partially addressed by the inclusion of Chen (2021)'s dataset from the World Bank's World Development Report 2021. This dataset sought to map data governance legal frameworks globally by having lawyers specialising in data governance and information and communications technology (ICT) assess states' national laws, regulations, and policies on given issue-areas in cyberspace regulation. Through assigning thirty-seven questions a binary score of 1 for the presence of good regulatory practices and 0 otherwise, Chen provides country scores for the following dimensions of cyberspace regulation: (1) personal data,

(2) cybersecurity, and (3) cross-border data transfers and flows.[32] As ASEAN's own policies pertain to the areas of personal data protection, data integrity, provisioning, and security, and finally cross-border data flows, these scores from the World Bank's dataset will allow for some possible separation between one 'amber' state and another, providing more contextual information on their specific policies.

The following table therefore comprises both the categorical scoring of an ASEAN member-state's compliance with ASEAN's cyber recommendations, as well as Chen's quantitative scoring of that given state's policies on each separate dimension of cyberspace regulation in order to separate similarly-complying states with others, where data is available. More information on how compliance with ASEAN policies was scored can be found in Appendix I at the conclusion of this paper.

Member-state	Compliance with ASEAN	Confidence	Personal data score	Cybersecurity score	Cross-border data transfer/flow score
Brunei	Amber	Medium	N/A	N/A	N/A
Cambodia	Amber	Low	4.17	30.36	0.00
Indonesia	Amber	Low	4.17	44.29	0.00
Laos	N/A	N/A	4.17	58.33	0.00
Malaysia	Green	High	66.67	47.86	38.10
Myanmar	Amber	Low	4.17	33.93	0.00
Philippines	Amber	Medium	83.33	95.00	50.00
Singapore	Green	High	66.67	67.50	62.50

[32] Chen, Rong, "World Development Report 2021: Mapping Data Governance Legal Frameworks Around the World," *World Bank Group* (April 2021), 5-6

Thailand	Green	Low	4.17	50.00	0.00
Vietnam	Amber	Low	4.17	90.83	0.00

Table 1. ASEAN member-states' compliance with ASEAN cyberspace regulation recommendations and quantitative scores on given issue-areas.[33]

Having generated this table, testing H1 will require several case studies of member-states. As it is unfeasible to examine the entire population of ASEAN member-states, this thesis will select a representative sample to gauge whether external leverage does, in fact, play a role in compliance with ASEAN. This thesis will select the following states for further analysis: (1) Malaysia, (2) the Philippines, and (3) Singapore. A main reason why these three states in particular were selected is due to limitations in data collection for the other ASEAN member-states. In particular, each state's set of governmental announcements and policy documents differed in quantity and in detail, leaving these three particular states with more evidence with which to test the first hypothesis. In addition to data-related reasons, it is also true that these three states possess a wide enough range of variation when it comes to compliance with ASEAN. Two states in Malaysia and Singapore are marked as 'green' compliers, but they vary to an extent with respect to Chen's scoring. On the other hand, the Philippines only scores an 'amber' in compliance, but their policies are markedly higher in several dimensions of Chen's scoring than the former 'green' states.

However, there is a cost to selecting these three case studies for H1. It is true that a prominent limitation in this analysis exists insofar as two of these case studies, Singapore and

[33] Chen, 42-43. See Appendix A for more details on how scoring by 'amber' or 'green' was conducted, as well as the amount of information that contributed to the ultimate 'Confidence' metric given for each state.

Malaysia, exhibit ‘green’ compliance. As this hypothesis is intended to test whether the presence of external leverage leads to a decreased compliance with ASEAN, it therefore seems counter-productive to have two of three case studies be an analysis of an *absence* of the independent variable which leads to an *absence* of the outcome variable. However, Table 1’s third column, titled ‘Confidence,’ addresses this matter with reference to this thesis’s Appendix A. The only other amber-scoring member-state besides the Philippines which received equal to or greater than a ‘Medium’ score in confidence was Brunei. Therefore, while the trade-off in this hypothesis testing is that it fails to test many ASEAN case studies with the explanatory variable present, the findings presented are made with higher confidence due to more data observed.

Having now established which states will be scrutinised to test the validity of H1, the next section will construct the observable implications generated by the prior causal theory and observe the results in these three case studies.

3.2. Testing H1

Previously, the causal theory elaborated that China’s own cyberspace policies were designed to support a sovereign version of cyberspace, counter to ASEAN. The mechanism also made note of the links between China holding external leverage of either a security, economic, or political nature over an ASEAN member-state, and thus concluded that greater amounts of external influence in one or multiple leverage areas should result in less and less compliance with ASEAN’s policies, as well as closer language to China’s own policies on cyberspace regulation.

The first observable implication that stems from this theory can be generated from the principle of external leverage being present since 2015. To be precise, the arbitrary date of 2015 was selected as a starting point for collecting data, as this is the year in which the ASEAN

Community was established in order to achieve a "truly rules-based, peoples-oriented, people-centred ASEAN" through integration, a principle that aligns with this thesis's causal theory on regional governance and cohesion.[34] If there really was leverage exerted by China over either Malaysia, the Philippines, or Singapore, one should expect to see a few possible indicators present. First, there might be visible signs of kowtowing from the ASEAN member-state towards China, and these signs should be linked to any recent issue-area in international politics regarding the forms of external leverage stated earlier. While not a case study in this particular thesis, one example of this might be the case where Cambodia, an ASEAN member-state with historically close diplomatic ties with China, is currently ASEAN Chair for the calendar year of 2022. External leverage and potential kowtowing could, therefore, represent certain shifts in policy away from traditional ASEAN maneuvers and towards Chinese policy directions.

Another case of leverage might also be weakly seen in the increasing of economic dependence on China over time, although this is not always a sufficient condition for leverage to form. If not the first or second sign, however, there could also be a more implicit shift that indicates a coercive leverage being used. For example, there might be a shift in member-state policy over time resulting in lower compliance with ASEAN and greater similarity with Chinese policy that correlates accordingly with a particular incident that occurred in a bilateral nature between that member-state and China.

3.2.1. Malaysia

---

[34] ASEAN, "2015 Kuala Lumpur Declaration on the Establishment of the ASEAN Community," November 22nd, 2015, https://www.asean.org/wp-content/uploads/2015/12/KL-Declaration-on-Establishment-of-ASEAN-Community-2015.pdf

Observing the independent variable in this hypothesis, external leverage, between Malaysia and China, is rendered more difficult by the fact that data on Malaysia's cyberspace policies tends not to be dated. This means that any time-series analysis examining shifting state policy over time cannot be utilised as an observable implication in Malaysia's case. This leaves two possible remaining means of observing external leverage, in that perhaps there are overt statements of deferment to China in foreign policy or evidence of deepening economic dependence on China.

Bilateral relations between China and Malaysia, at least at a diplomatic level, have been cordial between the two states. Malaysia reports that since the *Joint Communiqué* was signed between the two countries in 1974, bilateral relations have progressed at a substantial rate. This is aided by Malaysia's acknowledgement of the One China Policy, recognising the PRC as the sole legitimate government of China.[35] China similarly concurs with this sentiment, noting that they see the relationship as one of "good neighbors of mutual trust and good partners for win-win cooperation," particularly through cooperation efforts to combat the spread of COVID-19, promote economic recovery during the pandemic, and continue to establish partnerships between China and ASEAN.[36] Regarding economic relations, since 2016 Malaysia has continued to

[35] Ministry of Foreign Affairs Malaysia, "Overview of Malaysia-China Relations," accessed July 9th, 2022, https://www.kln.gov.my/web/chn_beijing/history

[36] Ministry of Foreign Affairs of the People's Republic of China, "Wang Yi and Malaysian Foreign Minister Dato' Saifuddin Abdullah Co-Chair the First China-Malaysia High Level Committee Meeting," November 4th, 2021, https://www.mfa.gov.cn/mfa_eng/zxxx_662805/202112/t20211205_10462618.html

expand its trade surplus bilaterally with China. From a surplus of eleven billion USD in 2016, this has increased to nineteen billion USD by 2019, the most recent year with data.[37, 38]

However, there have been recent instances where Malaysia has formally protested against Chinese action. For example, the Royal Malaysian Air Force lodged a complaint in June 2021 regarding sixteen Chinese aircraft from the People's Liberation Army Air Force entering Malaysian airspace without permission. In a strongly worded statement, the Malaysian Ministry of Foreign Affairs crucially said that while Malaysia was open to "friendly diplomatic relations" with any country, this would not come at the cost of compromising their own sovereignty.[39] Another instance can be seen in October of the same year, where Malaysia protested against Chinese naval incursion into Malaysia's claimed exclusive economic zone (EEZ) in the South China Sea. Of course, it is unfeasible to expect Malaysia to kowtow to China regarding issues of national sovereignty and defence. However, this indicates that while Malaysia does have fairly strong diplomatic ties with China, it does not indicate that there is any presence of external leverage in a political or economic form that would cause Malaysia to defer to China in cyberspace policy. Therefore, this independent variable is deemed to be absent for Malaysia, and one should expect their cyberspace policies to comply for the most part with ASEAN's own recommendations.

---

[37] World Integrated Trade Solution, "China trade balance, exports, and imports by country 2016," accessed July 11th, 2022, https://wits.worldbank.org/CountryProfile/en/Country/CHN/Year/2016/TradeFlow/EXPIMP/Partner/by-country#

[38] World Integrated Trade Solution, "China trade balance, exports, and imports by country 2019," accessed July 11th, 2022, https://wits.worldbank.org/CountryProfile/en/Country/CHN/Year/2019/TradeFlow/EXPIMP/Partner/by-country#

[39] Ministry of Foreign Affairs Malaysia, "Ministry of Foreign Affairs Will Issue A Diplomatic Protest and Summon the Ambassador of the People's Republic of China," June 2021, https://www.kln.gov.my/web/guest/-/ministry-of-foreign-affairs-will-issue-a-diplomatic-protest-and-summon-the-ambassador-of-the-people-s-republic-of-china

Malaysia's compliance with ASEAN's own cyberspace regulation policies appears, at first glance, to be ambiguously worded. Its domestic cyberspace policies are focused on attaining security for development strategies aimed to expand cyberspace's role in national life, such as the Cyber Security Framework For Public Sector which targets the risks associated with businesses and their assets when they begin increasing the digital aspect of their general operations.[40] Where common ground can be found between Malaysian policy and ASEAN's is in data integrity, provisioning, and personal data protection. Malaysia is focused on increasing the availability of intra-state data flows to be "shared and reused by the people, as well as the Government and public agencies for various purposes,"[41] whilst also maintaining guard against intentional or unintentional leakage of said data.[42] This does align closely with ASEAN's own statements on protecting personal data from "loss and unauthorised access" as outlined by the 2016 Framework on Personal Data Protection, although in no Malaysian policies observed here is ASEAN ever mentioned explicitly as a core reason of adoption.[43] Worth noting, however, is that Malaysia has no clear domestic policy on cross-border data flows, and so little can be said for their compliance towards ASEAN in this regard beyond the fact that Chen's data ranks Malaysia last out of the three case studies in terms of good regulatory practice on cross-border data flows. To summarise these policies, Malaysia does align with ASEAN cyberspace recommendations in development strategies, cybersecurity and national defence, and finally data

---

[40] The Government of Malaysia, "Cyber Security Framework For Public Sector," accessed July 7th, 2022, https://www.malaysia.gov.my/portal/content/30090
[41] The Government of Malaysia, "Open Data," accessed July 7th, 2022, https://www.malaysia.gov.my/portal/content/30024
[42] The Government of Malaysia, "Data Leakage Protection," (n.d.) accessed July 7th, 2022, https://www.malaysia.gov.my/portal/content/30088
[43] ASEAN Telecommunications and Information Technology Ministers Meeting, "Framework on Personal Data Protection," 3

integrity and protection, while it is unclear what their stance is on cross-border data transfers or flows.

On the other hand, their foreign policy is strongly dictated by a fierce belief in the core values of ASEAN as an organisation essential to upholding regional order in the Indo-Pacific. Noting that "ASEAN remains the cornerstone of Malaysia's foreign policy," and that the "nation's well-being is founded on the strong and friendly relations with other countries and its commitment to the multilateral system," it becomes less likely that Malaysia would adopt national policies, in any cyberspace-related capacity, contradicting their statements staunchly in favour of ASEAN's role in regional governance.[44] Indeed, its role as one of the founding members of ASEAN endows Malaysian foreign policy documents with a language of responsibility to ensure that the organisation is able to perform its duties as a "regional body in promoting peace and security in the region."[45] Their view of cybersecurity moving forward is one that indicates the necessity of regional solutions and international cooperation, rather than fragmented sovereignty.

In conclusion, this case study has illustrated that without the presence of the main independent variable of external leverage exerted by China, Malaysia does comply for the most part with ASEAN recommendations. No observable evidence indicates that China holds any meaningful economic or security-oriented leverage, as represented by the basic data of Malaysia

---

[44] Ministry of Foreign Affairs Malaysia, "Malaysia's Foreign Policy," accessed July 8th, 2022, https://www.pmo.gov.my/wp-content/uploads/2019/07/Malaysia-Foreign-Policy.pdf, 1-2

[45] Ministry of Foreign Affairs Malaysia, "Foreign Policy Framework of the New Malaysia: Change in Continuity" (June 2019), 19

holding a bilateral trade surplus as of 2019, and no overt dynamics of political kowtowing to China. Therefore, H1 is supported by this case study.

3.2.2. The Philippines

In viewing whether the presence of external leverage from China over the Philippines is present, it is first prudent to examine bilateral relations between these two countries since the election of then-President Rodrigo Duterte in 2016. China's version of events speaks of a glowing, productive relationship where significant progress was achieved through cooperation between China's Belt and Road Initiative (BRI) and the Philippines's own Build, Build, Build programmes.[46] More recently, coordination in combatting COVID-19 has also contributed to the strength of the bilateral relationship.

Even regarding territorial disputes and infringement upon sovereign territory, the Philippines have indicated a profound willingness to sweep territorial issues aside for the benefit of common cooperation. Regarding the South China Sea, the Philippines have been mired in a long-standing disagreement with China over the latter's 'nine-dash line,' a historic claim to areas rich in natural resources and strategic value such as the Spratly Islands and the Scarborough Shoal.[47] Despite this dispute, as well as the fact that the Permanent Court of Arbitration in the Hague ruled in favour of the Philippines in the 2016 landmark case *Philippines v. China* deciding on this issue, the Philippines have opted to use diplomatic, concessionary language to frame this

---

[46] Embassy of the People's Republic of China in the Republic of the Philippines, "China-Philippines Relations Shine Brighter in the Tempering of Time," June 9th 2021, https://www.mfa.gov.cn/ce/ceph/eng/sgdt/t1882350.htm

[47] Graham, Euan, "The Hague Tribunal's South China Sea Ruling: Empty Provocation or Slow-Burning Influence?", *Council on Foreign Relations*, August 18th, 2016, https://www.cfr.org/councilofcouncils/global-memos/hague-tribunals-south-china-sea-ruling-empty-provocation-or-slow-burning-influence

dispute delicately. From Duterte's presidency to the recently-elected Marcos's, the Philippines insist that this bilateral relationship ought to be characterised by "more than [just] a maritime dispute."[48] This already represents a significant divide from how Malaysia, earlier, approached similar issues of intrusions within claimed maritime territory. Economically, the Philippines have been registered at a $12 billion USD bilateral trade deficit with China as of 2016, and this has only increased to $20 billion USD by 2019, the last year currently with available data.[49, 50]

In terms of leverage as discussed by the observable implications of H1, political kowtowing to China is visible insofar as the Philippines have generally employed a strategy of containing the South China Sea dispute and isolating it so as to not inflame bilateral tensions. It is also visible from an economic standpoint, where the bilateral trade deficit has widened from 2016 to 2019, indicating the Philippines to be more dependent economically on China as a trade partner. As such, for the purposes of this thesis, the Philippines is one case study where the presence of external leverage is seen. From the causal mechanism, if this is the case, then one should expect to see lower compliance with ASEAN's recommendations on cyberspace governance.

Regarding personal data protection, the Philippines carefully balances the protection of an individual's privacy against the securing of "protection of information and data of the users" in its National Cybersecurity Plan 2022 (NCSP 2022).[51] This technically aligns with ASEAN's

---

[48] Lema, Karen, "China foreign minister seeks 'new golden era' of ties with Philippines," *Reuters*, July 6th, 2022, https://www.reuters.com/world/asia-pacific/china-foreign-minister-seeks-new-golden-era-ties-with-philippines-2022-07-06/

[49] World Integrated Trade Solution, "China trade balance, exports, and imports by country 2016."

[50] World Integrated Trade Solution, "China trade balance, exports, and imports by country 2019."

[51] Department of Information and Communications Technology (DICT), "National Cybersecurity Plan 2022," *Cybercrime Investigation and Coordination Center* (2022), 21

recommendation that personal data only be disclosed to an extent which a "reasonable person would consider appropriate in the circumstances," although it is quite unclear what this extent or what a reasonable consideration would amount to.[52] That being said, the Philippines' primary objective in their NCSP appears to be a staunch focus on national cyber defence capabilities, and so policies on cross-border data flows appear to be missing from this plan. While this is similar to Malaysia, Chen's scoring system elaborates further and provides some more context in that the Philippines scores higher in cross-border data transfer regulatory policies than Malaysia. Their overall objectives in the NCSP include consolidating existing strategies under a single blueprint, creating a synchronised defence mechanism, and ensuring that national laws are well-equipped to handle the protection of data and information by government agencies.[53]

In none of these policies within the NCSP, however, does the Philippines mention ASEAN or any other regional or global organisation recommending policies for cyberspace regulation. Their national policies are solely focused on their own sovereign needs in cyberspace, particularly cybersecurity. As such, the main observable implication to test the Philippines for determining H1's validity will be whether any similar language is used between the NCSP 2022 and any of China's cybersecurity laws from 2017 onwards.

Indeed, the 2017 Cybersecurity Law of the People's Republic of China contains several articles similar in wording to the Philippines' NCSP, written five years after the former document. Basic wording in both documents assigning personal data protection as the role of the state can be seen firstly in Article 8 of the Cybersecurity Law, which states that:

---

[52] ASEAN Telecommunications and Information Technology Ministers Meeting, "Framework on Personal Data Protection," 3

[53] Department of Information and Communications Technology (DICT), 2

> Cybersecurity protection, supervision, and management duties... at the county level or above will be determined by relevant national regulations.[54]

Similarly, the Philippines' memorandum released in August 2017, just one month after the Chinese law came into effect, states that:

> The privacy and sharing of personal data involving government agencies or a third party shall be in conformance with the issuances from the National Privacy Commission.[55]

Examining the Philippines' policy on having a synchronised defence in case of a cyberattack, through the necessity of having "roles, functions, objectives, and goals [which] are clear and well defined"[56] also weakly echo China's sentiments in Article 19, which states that:

> All levels of people's governments and their relevant departments shall organize and carry out regular cybersecurity publicity and education, and guide and stimulate relevant units in properly carrying out cybersecurity publicity and education work.
>
> The mass media shall conduct targeted cybersecurity publicity and education aimed at the public.[57]

However, these are fairly basic principles on state cyber defence, and may not necessarily reflect genuine leverage causing the Philippines to adopt similar language, even if the timing of the memorandum released is quite close to China's adoption of their Cybersecurity Law. In fact, there are some aspects that weaken the case for H1 being true. Specifically, China begins both the Cybersecurity Law (2017) and the Data Security Law (2021) by stressing that these laws are

---

[54] Cyberspace Administration of China (trans. by Creemers, Webster, and Triolo), "Translation: Cybersecurity Law of the People's Republic of China," *DigiChina: Stanford University*, June 29th, 2018, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

[55] Salalima, Rodolfo A., "Memorandum Circular No. 005: Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructure (CII) Stipulated in the National Cybersecurity Plan (NCSP) 2022," *Department of the Information and Communications Technology*, August 1st, 2017, 6

[56] Department of Information and Communications Technology (DICT), 45

[57] Cyberspace Administration of China (trans. by Creemers, Webster, and Triolo).

essential, among other reasons, to safeguard national sovereignty, security, and development interests.[58] Yet, in the Philippines' NCSP, no mention is made of the word 'sovereignty' whatsoever, a crucial term that one should expect to see if the primary theory of leverage causing the Philippines to pull away from ASEAN and move closer in policy wording to China were true.

What this qualitative analysis indicates is that while external leverage may exist between the Philippines and China, there is no strong evidence to link this independent variable to the Philippines' ambiguous compliance with ASEAN recommendations on cyberspace governance. The latter does not seem to be caused by the former, and so this particular case study thus lowers the credibility that H1 could potentially be true.

3.2.3. Singapore

Singapore's own bilateral relations with China are fairly warm, and both countries have celebrated milestones of diplomatic progress which include the 30th anniversary of establishing diplomatic relations in 2020.[59] From China's point of view, the presence of "close high-level contacts" between both countries have allowed for the deepening of strategic communication and the expansion of bilateral cooperation.[60] From the data available, it does not appear as though any current disputes are causing any political leverage to form for China over Singapore. Economically, Singapore's bilateral trade with China has gone from a deficit of $18 billion USD

---

[58] Cyberspace Administration of China (trans. by Creemers, Webster, and Triolo).
[59] Ministry of Foreign Affairs Singapore, "People's Republic of China," accessed July 12th, 2022, https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/Countries-and-Regions/Northeast-Asia/Peoples-Republic-of-China
[60] Ministry of Foreign Affairs of the People's Republic of China, "Wang Yi Meets with Singaporean Foreign Minister Vivian Balakrishnan," July 9th, 2022, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/202207/t20220710_10718059.html

in 2016 to $19 billion in 2019, a fairly small increase compared to the prior case studies.[61, 62] This suggests no presence of any leverage, and so with the independent variable absent, one would thus expect Singapore to be in strong compliance with ASEAN recommendations.

Indeed, Singapore's public statements have historically indicated a strong willingness to comply by internationally-defined standards with regards to cyberspace regulation. They pride themselves in playing "an active role in cybersecurity discussions" internationally by their inclusion in the UN Group of Governmental Experts, the Open-Ended Working Group on Developments in the Field of Information in the Context of International Security, and the Paris Call for Trust and Security in Cyberspace.[63] Regionally, Singapore also hosts the ASEAN-Singapore Cybersecurity Centre of Excellence to "strengthen regional cyber resilience" and work towards an "open and free digital environment" which is also secure.[64]

In terms of policy, Singapore has pledged to work towards the following aspects which are recommended by ASEAN: "fair and secure access to data, freer cross-border data flows, addressing misinformation and cyber threats, and strengthening multilateral cooperation to exploit digital technologies for sustainable development."[65] In particular, Singapore has cautioned that cyberspace possesses a borderless nature, which presents transnational problems which require regional or global solutions through the creation and maintenance of "global rules,

---

[61] World Integrated Trade Solution, "China trade balance, exports, and imports by country 2016."
[62] World Integrated Trade Solution, "China trade balance, exports, and imports by country 2019."
[63] Ministry of Foreign Affairs Singapore, "Cybersecurity," accessed July 12th, 2022, https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/International-Issues/Cybersecurity
[64] Prime Minister's Office Singapore, "PM Lee Hsien Loong at the APEC CEO Summit 2021," November 11th, 2021, https://www.pmo.gov.sg/Newsroom/PM-Lee-Hsien-Loong-at-the-APEC-CEO-Summit
[65] Ibid.

norms, governance principles, frameworks, and standards."[66] While Chen has scored Singapore lower than the Philippines in the dimensions of personal data and cybersecurity, Singapore has excelled in cross-border data transfers and flows.

Overall, the evidence presented here is strongly indicative that Singapore has been compliant with ASEAN recommendations on cyber policy, and in fact has been quite vocal in regional and global organisations' roles in creating a stable and desirable cyberspace governance regime. As such, this case study does strengthen H1's credibility.

3.2.4. Concluding remarks on H1

These three previous case studies of Malaysia, the Philippines, and Singapore, have sought to test the validity of whether external leverage exerted by China, as the first independent variable of this study, results in lower amounts of compliance with ASEAN policies on cyberspace regulation. To summarise, both Malaysia and Singapore have demonstrated that the absence of leverage has corresponded with strong compliance with ASEAN policies, corroborating H1 and strengthening its validity. On the other hand, it was argued that the Philippines could have been the subject of external leverage in both a political and economic dimension. For this reason that the independent variable was present in this case study and absent in the case of Malaysia and Singapore, a deeper analysis in comparing specific policy wording between the Philippines and China was conducted. Yet, no clear linkage to lower compliance with ASEAN was seen, thus lowering H1's validity.

---

[66] Prime Minister's Office Singapore, "SM Teo Chee Hean at TechX Summit 2022," April 5th, 2022, https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-TechX-Summit-2022

In conclusion, H1 has received weak levels of support. It cannot be stated explicitly that external leverage clearly leads to or does not lead to lower levels of compliance with ASEAN cyberspace governance policies, and the findings demonstrate that no ‘smoking guns’ were present in the evidence. However, political leverage of any kind is difficult to discern in international relations, and the implications remain that external influence is ultimately subtle, making it difficult to draw clear causal linkages. Having established weak support for H1, the next section will briefly consider an alternative, organisational-level explanation for the variation in compliance with ASEAN.

Section 4: ASEAN and non-interference in regional policy as an explanatory variable (H2)

4.1. Testing H2

If a state-level explanation for variance in cyberspace policy among ASEAN member-states has not sufficed in providing a full answer, then how might an organisational-level change this? Recalling that ASEAN is founded on the principles of non-interference in sovereign affairs as well as consensus-based decision-making, it is therefore these same principles that make the organisation unable to address any possible deviation from ASEAN policy.

Testing H2 will be derived from the earlier causal theory's observable implications. If ASEAN recommends policies on cyberspace governance, and its member-states reject these policies of regional governance on the basis that they believe cyberspace to be an issue-area for sovereign states, then one should expect to see one or both of the following. First, there may be explicit reference to the founding principles of ASEAN, specifically the aspect of non-interference in sovereign affairs, as an explanation for member-state's variance away from ASEAN's own policies. If this is not seen, however, one might also be able to see similar logic applied to other areas intended by ASEAN to be governed at a regional or even global level. For instance, climate change represents one such area that arguably ought to be governed regionally, if not globally. However, the ramifications of pushing policy recommendations seeking lowering carbon emissions, as one example, would be considered as an intrusion upon a state's sovereign policy decision-making.

The reason for which this second observable implication can be derived from the hypothesis's causal mechanism can be seen in ASEAN's internal dynamics. Through using ASEAN's principle of non-interference in a state's sovereign affairs, one can see variation in compliance with cyberspace governance policies by examining how this principle allows

different states to exercise non-compliance at different rates. As a result, while the overall hypothesis is aimed to test whether the variation in compliance is visible from organisational reasons, the logic it utilises still assumes variation in member-state behaviour. Moreover, if there exists a lack of data with regards to cyberspace as an issue-area, this hypothesis's logic can still be tested via using similar case studies of regional governance in international politics.

Following on this example, the next section will turn to analysing the case study of ASEAN's attempts to regulate transboundary haze in Southeast Asia, and test this second observable implication insofar as it seeks to discover whether ASEAN member-states vary in compliance with policies on regional governance due to its implied infringement on their sovereignty.

4.2. Transboundary haze and ASEAN

Transboundary haze in Southeast Asia can be characterised as a problem generated by the constant burning of peat land to clear vegetation for farmland or plantations. This burning, however, results in smoke pollution that leaves its country of creation and travels elsewhere in Southeast Asia, causing severe issues with respiratory quality and visibility. As such, it has simply been referred to as 'haze.'[67] While most of this haze is created on Indonesian land, the effects have been felt more drastically in Malaysia and Singapore, creating lingering regional impacts that an organisation such as ASEAN has stepped in to intervene.

Most prominently, ASEAN responded to the haze created over the 1990s with the seminal ASEAN Agreement on Transboundary Haze Pollution, ratified in 2002. Within this

---

[67] Cotton, James, "The "haze" over Southeast Asia: Challenging the ASEAN Mode of Regional Engagement," *Pacific Affairs* 72, no. 3 (Fall 1999), 331

document, ASEAN urged its member-states "in the spirit of solidarity and partnership" to coordinate in order to prevent and monitor haze, as well as collaborate to take precautionary measures in stopping the spread of haze if needed.[68] To address the roots causing the haze in the first place, ASEAN also declared that member-states should take responsibility for their own sovereign actions, and ensure that "activities within their jurisdiction or control do not cause damage to the environment and harm to human health of other States."[69]

As for whether this agreement and following set of recommendations listed by ASEAN were ultimately effective, the evidence seems unlikely. Malaysia and Singapore, being the closest and largest neighbours geographically to Indonesia, the primary culprit for much of the haze, have historically condemned the latter for not only refusing to address the problem, but also denying that it is their problem to begin with. In 2020, Indonesia's minister of forestry Siti Nurbaya Bakar insisted that the haze "could have originated from fires in Malaysia," despite Malaysian officials having cited data from the ASEAN Specialised Meteorological Centre conclusively indicating over three hundred times more hotspots creating haze in Indonesia than in Malaysia.[70] This was not the first time a strategy of deflection and denial was employed, as reflected by the same scenario occurring in Singapore seven years earlier where Indonesia suggested that Singaporean companies were to blame for the deteriorating air quality.[71]

However, what this suggests is that not only was ASEAN's original set of recommendations largely ignored by its member-state and culprit for much of the haze,

---

[68] ASEAN, "ASEAN Agreement on Transboundary Haze Pollution," June 10th, 2002, 4
[69] ASEAN, "ASEAN Agreement on Transboundary Haze Pollution," 4
[70] Reuters, "Malaysian PM to write to Indonesia's leader as row over haze flares," September 12th, 2019, https://www.reuters.com/article/us-southeastasia-haze-idUSKCN1VX0VE
[71] Lim, Kevin, "Singapore demands action from Indonesia on haze," *Reuters*, June 19th, 2013, https://www.reuters.com/article/southeastasia-haze-idUKL3N0EW0I420130620

Indonesia, but that Malaysia and Singapore alike were unable to shift Indonesian policy sufficiently to resolve the issue. This is largely due to the means in which ASEAN member-state conduct their bilateral and multilateral affairs, specifically how member-states must abide by the major principle of "non-interference in the internal affairs of one another" laid out by the 1976 Treaty of Amity and Cooperation in Southeast Asia.[72] Moreover, any escalation of disputes is to avoid the "threat or use of force," and at all times should be settled through "friendly negotiations," thus constraining member-states for the most part from pushing back against a deviating member-state over regional agreements on governance.[73]

As a result, the logic seen over ASEAN's attempted governance of transboundary haze failing to accomplish success among all of its member-states has been traced to an organisational level. The fact that ASEAN's own principles constrain it from constructing more binding agreements, and also constrain its member-states from being vocal regarding a non-complier, suggests that other areas of regional governance which ASEAN has also recommended best practices as policies may suffer similar results over time. Thus, the credibility of H2 is supported by the evidence seen in this case study, although with the caveat that this was merely a limited exploration.

4.3. Concluding remarks on H2

While the majority of ASEAN member-states may abide by the ASEAN Agreement on Transboundary Haze Pollution, that one member-state alone can deviate significantly from the agreed recommendations and also do so with relative diplomatic impunity is foreboding when

---

[72] ASEAN, "Treaty of Amity and Cooperation in Southeast Asia," 2
[73] Ibid.

this logic is applied to cyberspace regulation. ASEAN rests on moral suasion through their 'ASEAN Way,' and should this tactic of 'doing the right thing' fail to persuade a member-state into acting in compliance with its recommendations, ASEAN ultimately becomes ineffective in maintaining this policy or set of policies. The non-complying state would also be able to fully justify their deviation by invoking the principles upholding ASEAN as an organisation, and claiming that their policies align with national interests and laws. Consequently, this may also have a side effect of convincing other member-states that non-compliance with a policy recommendation which constrains the state's policy autonomy may be in their own best interests, causing a domino effect.

How this relates to the primary arena studied in this thesis, cyberspace, is that the guiding principle of non-interference in a member-state's sovereign affairs can already be utilised to justify non-compliance with ASEAN recommendations on personal data protection, cybersecurity, and cross-border data transfers and flows. Beyond this, the future of cyberspace governance regionally in the Indo-Pacific may become even more fractured, when ASEAN begins discussing more politically divisive policies beyond integrating cyberspace with member-state economic developmental strategies. For instance, in cross-border data transfers and flows, the policy of data localisation, the requirement of data to be collected and held within the physical geography of that member-state's territory, has already seen contentious debates between the US, EU, and China.[74] Should cyberspace regulation also become a politically sensitive discussion in the Indo-Pacific, as a result of push-pull dynamics between global powers

[74] Hufbauer and Lu, 2

like the U.S. and China as previously mentioned, what was seen regarding transboundary haze might come to represent future trajectories for cyberspace.

Section 5: Conclusions

This thesis has set out to situate ASEAN and its member-states in cyberspace, and determine the causes for the comparative variation between member-states in adhering to ASEAN's policy recommendations on cyberspace regulation in the following dimensions: personal data protection, data integrity, provisioning, and security, cybersecurity, and cross-border data transfers and flows. In doing so, it has noted primarily that ASEAN has first and foremost strictly maintained a moderate tone in its recommendations that is befitting of the 'ASEAN Way' concept of moral suasion. While this has allowed the recommendations to be palatable to its member-states, ASEAN has also steeped these policies in careful language that is strategically ambiguous in nature, allowing member-states to deviate from them using the reasoning of national security and compliance with domestic interests.

This thesis has identified two possible explanations for this comparative variance: first, it has hypothesised that the presence of external leverage exerted by China in a political or economic sense has caused it. It has also examined the possibility that ASEAN is limited in recommending policies on regional or global governance due to its status as an organisation constrained by its own founding principles of non-interference in sovereign affairs. In doing so, this paper has found that H1 has received weak support by means of case studies Singapore and Malaysia, while being weakened by the case study of the Philippines. It has also determined that the evidence seen on transboundary haze can be applied to strengthen H2 with regards to cyberspace governance.

The strengths of this paper have firstly been in the creation of a qualitative data table on member-state compliance with ASEAN on cyberspace recommendations since 2015, in conjunction with existing quantitative scoring from Chen's World Bank report. This will

contribute more clarity to future research dedicated to uncovering more factors for variation in comparative compliance with ASEAN, and can be updated relatively easily to provide a time-series analysis of compliance over time. In doing so, this may reveal new patterns on variation that can be observed with the data available. A secondary strength of this thesis has been in linking cyberspace as an issue-area salient to ASEAN with other matters of regional governance, such as haze management. This situates cyberspace governance as a political issue that ultimately can draw from and contribute to existing literature in other areas, rather than a niche and isolated field on its own, thus allowing for more data and research on the success of ASEAN regional governance as a whole.

Yet, having said this, some core limitations of this work have been largely driven by the inconsistency of acquiring state-level data. To measure compliance is a difficult task, especially when viewing this at a state level where the state in question would have no incentive to report non-compliance. As such, the qualitative data table generated only distinguishes between those who exercise ambiguous compliance and those who willingly bind themselves to certain principles suggested by international or regional organisations. Further research may be able to create more layers of separation in defining and operationalising compliance, therefore allowing the dependent variable to vary more effectively. This also applies to the definition of leverage given and used in this thesis, as other forms of leverage could have been examined, such as UN voting patterns for political leverage and the business interests of multinational corporations based in the external actor's territory for economic leverage. Another key limitation was the inability to study other actors' possible leverage over ASEAN member-states. For instance, the United States would have been an excellent counterpoint to juxtapose against China in this thesis, and should be the study of future research.

With regards to the implications of these findings, H1 having received weak support does not invalidate this hypothesis entirely. One area that will play a major role in the foreseeable future of this hypothesis will be as the Indo-Pacific continues to be a focal point for U.S.-China relations. For instance, again stating that this was outside the original scope of the thesis, Singapore noticeably demonstrated a clear desire to work with the Biden administration in the U.S. in cybersecurity,[75] and engaged in a "bilateral Cyber Dialogue" to share best practices.[76] If a push-and-pull dynamic continues to unfold in the Indo-Pacific, particularly with respect to the emergence of cyberspace governance, these tensions may exacerbate existing leverage further. As a result, the question to ask would then be whether either, or both, of the U.S. or China would court these ASEAN member-states to secure their support in a desired cyberspace governance structure. For instance, the partnerships that Singapore has made with the U.S. in this brief example are possible without the existence of leverage, but for a state such as the Philippines who currently has ongoing territorial disputes in the South China Sea, such a move would possibly inflame relations with China and contribute to the intensity of the disputes in question. In this regard, questions of 'digital decoupling' have already joined an existing discourse on deglobalisation, and this will likely remain relevant as cyberspace continues to grow. Therefore, the evidence seen in H1 may be weak now, but could be stronger in the future.

---

[75] Ministry of Foreign Affairs Singapore, "Transcript of Minister for Foreign Affairs Dr Vivian Balakrishnan's curtain raiser interview with SPH Media on the Visit of United States Vice President Kamala Harris at the MFA Exhibition Hall, 16 August 2021," August 17th, 2021, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2021/08/20210816-Minister-FA-Interview-with-SPH

[76] Prime Minister's Office Singapore, "PM Lee Hsien Loong at the Joint Press Conference with US Vice President Kamala Harris (Mar 2022)," March 30th, 2022, https://www.pmo.gov.sg/Newsroom/Remarks-by-PM-Lee-Hsien-Loong-after-the-meeting-with-US-Vice-President-Kamala-Harris-Mar-2022

Turning to H2, the conclusion that ASEAN as a regional organisation is constrained by its founding principles on non-interference is, to be sure, not a new finding. Yet, the implications are significant for cyberspace governance as this would indicate that ASEAN may not be effective in successfully recommending cyberspace policies at this regional level today, and that governance may continue to be fractured if cyberspace continues to be treated in the same light as an ultimately sovereign issue as issues such as transboundary haze are. Moreover, another implication complicating matters further is that this very outlook on H2 may be compounded by the findings for H1. To put this quantitatively, the presence of leverage as the first independent variable and ASEAN recommending policies on an issue deemed to be best suited for sovereign states as the second independent variable may create an interaction term that will need to be addressed in future research. It is possible that ASEAN member-states believing cyberspace governance to be better left in the hands of national policies rather than regional governance have some causal linkage with influence being exerted upon them. This would further contribute to existing literature on viewing external influence in international politics, and would illuminate future difficulties in cyberspace management as a whole.

Ultimately, cyberspace regulation and governance is undoubtedly complex at both a regional and a global level, but this should not dissuade states and organisations alike from seeking common solutions to common problems in its governance. In recalling the spirit of the 1976 Treaty of Amity and Cooperation's preamble, it will be imperative to focus on the promotion of regional peace and stability and the increasing of regional solidarity for Southeast Asian cyberspace governance. Indeed, the seeking of common interests rather than identities may yet accomplish a society of ASEAN member-states in cyberspace, each with their own sovereign

goals but with an overarching interest in regional stability in mind. This, after all, would be nothing short of the ASEAN way.

References

Aaronson, Susan Ariel. "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* 18, no. 4. 2019: 541-577.

Acharya, Amitav. *The Making of Southeast Asia: International Relations of a Region*. Ithaca: Cornell University Press. 2003.

Aizawa, Nobuhiro. "Beyond the Non-Interference Dilemma: The Indonesian Initiative on ASEAN Charter, Nargis Crisis and Regionalism." *Australian Journal of Politics and History* 65, no. 3. 2019: 412-429.

ASEAN. "2015 Kuala Lumpur Declaration on the Establishment of the ASEAN Community." November 22nd, 2015. https://www.asean.org/wp-content/uploads/2015/12/KL-Declaration-on-Establishment-of-ASEAN-Community-2015.pdf.

ASEAN. "ASEAN Agreement on Transboundary Haze Pollution." June 10th, 2002.

ASEAN. "ASEAN Cybersecurity Cooperation Strategy (2021-2025)." January 23rd, 2022. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-01-22.pdf.

ASEAN. "ASEAN Model Contractual Clauses for Cross Border Data Flows." 2021. https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf.

ASEAN. "Treaty of Amity and Cooperation in Southeast Asia." 1976.

ASEAN Telecommunications and Information Technology Ministers Meeting. "Framework on Digital Data Governance." December 6th, 2018. https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.

ASEAN Telecommunications and Information Technology Ministers Meeting. "Framework on Personal Data Protection." November 16th, 2016. https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

Chen, Rong. "World Development Report 2021: Mapping Data Governance Legal Frameworks Around the World." *World Bank Group*. April 2021.

Cotton, James. "The "haze" over Southeast Asia: Challenging the ASEAN Mode of Regional Engagement." *Pacific Affairs* 72, no. 3. Fall 1999: 331-351.

Cyberspace Administration of China (translated by Creemers, Webster, and Triolo). "Translation: Cybersecurity Law of the People's Republic of China." *DigiChina: Stanford University*. June 29th, 2018. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Defence Ministry of the Republic of Indonesia. "Defence White Paper." November 2015.

Department of Information and Communications Technology (DICT). "National Cybersecurity Plan 2022." *Cybercrime Investigation and Coordination Center.* 2022.

Embassy of the People's Republic of China in the Republic of the Philippines. "China-Philippines Relations Shine Brighter in the Tempering of Time." June 9th, 2021. https://www.mfa.gov.cn.ce/ceph/eng/sgdt/t1882350.htm.

Govella, Kristi. "China's challenge to the global commons: compliance, contestation, and subversion in the maritime and cyber domains." *International Relations* 35, no. 3. 2021: 446-468.

Graham, Euan. "The Hague Tribunal's South China Sea Ruling: Empty Provocation or Slow-Burning Influence?" *Council on Foreign Relations*. August 18th, 2016. https://www.cfr.org/councilofcouncils/global-memos/hague-tribunals-south-china-sea-ruling-empty-provocation-or-slow-burning-influence.

The Government of Malaysia. "Cyber Security Framework For Public Sector." Accessed July 7th, 2022. https://www.malaysia.gov.my/portal/content/30090.

The Government of Malaysia. "Data Leakage Protection." Accessed July 7th, 2022. https://www.malaysia.gov.my/portal/content/30024.

The Government of Malaysia, "National Defence Policy." Accessed July 8th, 2022.

The Government of Malaysia, "National Security Policy." Accessed July 8th, 2022.

The Government of Malaysia. "Open Data." Accessed July 7th, 2022. https://www.malaysia.gov.my/portal/content/30088.

The Government of Myanmar. "Law Protecting the Privacy and Security of Citizens." February 13th, 2021.

The Government of Myanmar. "Myanmar Cyber Legal and Policy Framework: Policies Related to e-Government, e-Commerce, and Cyber Security (Draft – 25 Jan 2019)."

Heinl, Caitríona. "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime." *Asia Policy* 18. July 2014: 131-160.

Hufbauer, Gary Clyde, and Zhiyao Lu. "Global E-Commerce Talks Stumble on Data Issues, Privacy, and More." *Peterson Institute of International Economics*. 2019.

Jones, David Martin, and Nicole Jenne. "Weak states' regionalism: ASEAN and the limits of security cooperation in Pacific Asia." *International Relations of the Asia-Pacific* 16. 2016: 209-240.

Katanyuu, Ruukun. "Beyond Non-Interference in ASEAN: The Association's Role in Myanmar's National Reconciliation and Democratization." *Asian Survey* 46, no. 6. November/December 2006: 825-845.

Lema, Karen. "China foreign minister seeks 'new golden era' of ties with Philippines." *Reuters*. July 6th, 2022. https://www.reuters.com/world/asia-pacific/china-foreign-minister-seeks-new-golden-era-ties-with-philippines-2022-07-06/.

Lim, Kevin. "Singapore demands action from Indonesia on haze." *Reuters*. June 19th, 2013. https://www.reuters.com/article/southeastasia-haze-idUKL3N0EW0I420130620.

Liu, Lizhi. "The Rise of Data Politics: Digital China and the World." *Studies in Comparative International Development* 56. 2021: 45-67.

Ministry of Defence of Brunei Darussalam. "Defence White Paper 2021: Defending the Nation's Sovereignty, A Secure and Resilient Future." 2021.

Ministry of Foreign Affairs Malaysia. "Foreign Policy Framework of the New Malaysia: Change in Continuity." June 2019.

Ministry of Foreign Affairs Malaysia. "Malaysia's Foreign Policy." Accessed July 8th, 2022. https://www.pmo.gov.my/wp-content/uploads/2019/07/Malaysia-Foreign-Policy.pdf.

Ministry of Foreign Affairs Malaysia. "Ministry of Foreign Affairs Will Issue A Diplomatic Protest and Summon the Ambassador of the People's Republic of China." June 2021. https://www.kln.gov.my/web/giuest/-/ministry-of-foreign-affairs-will-issue-a-diplomatic-protest-and-summon-the-ambassador-of-the-people-s-republic-of-china.

Ministry of Foreign Affairs Malaysia. "Overview of Malaysia-China Relations." Accessed July 9th, 2022. https://www.kln.gov.my/web/chn_beijing/history.

Ministry of Foreign Affairs of the People's Republic of China. "Wang Yi and Malaysian Foreign Minister Dato' Saifuddin Abdullah Co-Chair the First China-Malaysia High Level Committee Meeting." November 4th, 2021. https://www.mfa.gov.cn/mfa_eng/zxxx_662805/202112/t20211205_10462618.html.

Ministry of Foreign Affairs of the People's Republic of China. "Wang Yi Meets with Singaporean Foreign Minister Vivian Balakrishnan." July 9th, 2022. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/202207/t20220710_10718059.html.

Ministry of Foreign Affairs Singapore. "Cybersecurity." Accessed July 12th, 2022. https://www.mfa.gov.sg./SINGAPORES-FOREIGN-POLICY/International-Issues/Cybersecurity.

Ministry of Foreign Affairs Singapore. "People's Republic of China." Accessed July 12th, 2022. https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/Countries-and-Regions/Northeast-Asia/Peoples-Republic-of-China.

Ministry of Foreign Affairs Singapore. "Transcript of Minister for Foreign Affairs Dr Vivian Balakrishnan's curtain raiser interview with SPH Media on the Visit of United States Vice President Kamala Harris at the MFA Exhibition Hall, 16 August 2021." August 17th, 2021. https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2021/08/20210816-Minister-FA-Interview-with-SPH.

Ministry of Foreign Affairs Thailand. "Annual Report 2019." 2019.

Ministry of Foreign Affairs Vietnam. "Remarks by the Deputy Spokesperson of the Ministry of Foreign Affairs of Viet Nam Ngo Toan Thang about the US cyber security firm FireEye's statement that Viet Nam assisted the APT32 hacker group in conducting cyber-attacks targeting international government units and businesses." April 23rd, 2020. https://www.mofa.gov.vn/en/tt_baochi/pbnfn/ns200424144014/view.

Ministry of Foreign Affairs Vietnam. "Remarks by MOFA's Spokesperson Le Hai Binh during the 9th Regular Press Conference in August 4th 2016." August 4th, 2016. https://www.mofa.gov.vn/en/tt_baochi/nr140808202328/ns160804213736/view.

Ministry of Foreign Affairs Vietnam. "Viet Nam calls for enhanced solidarity to build strong, resilient ASEAN Community." February 17th, 2022. https://www.mofa.gov.vn/en/tt_baochi/tcbc/ns220218142224/view.

Ministry of Transport and Communications, "Cyber Legal and Policy Framework," *Myanmar National Portal*, https://myanmar.gov.mm/news-media/media//-asset_publisher/idasset290/content/cyber-law-and-policy-.

Narine, Shaun. "Forty years of ASEAN: a historical review." *The Pacific Review* 21, no. 4. 2008: 411-429.

Noor, Elina. "Positioning ASEAN in Cyberspace." *Asia Policy* 15, no. 2. April 2020: 107-114.

O'Hara, Kieron, and Wendy Hall. "Four Internets: The Geopolitics of Digital Governance." *Centre for International Governance Innovation*. 2018.

Prime Minister's Office Brunei Darussalam. "10.03.18 Issue of Cyber Security." https://www.pmo.gov.bn/Lists/2018%20PMO%20News/NewDispForm.aspx?ID=93&Source=https%3A%2F%2Fwww%2Epmo%2Egov%2Ebn%2FLists%2F2018%2520PMO%2520News%2FAllItems%2Easpx%23InplviewHasha19ab504%2D6624%2D496b%2D8871%2Dc9d8634ba4a9%3D&ContentTypeId=0x0100106B6B901C6AE64F9E659897FBEBB8C3.

Prime Minister's Office Singapore. "Meeting and Joint Leaders' Statement between PM Lee Hsien Loong and US President Joe Biden." March 30th, 2022. https://www.pmo.gov.sg/Newsroom/Meeting-and-Joint-Leaders-Statement-between-PM-Lee-Hsien-Loong-and-US-President-Joe-Biden-March-2022.

Prime Minister's Office Singapore. "PM Lee Hsien Loong at the APEC CEO Summit 2021." November 11th, 2021. https://www.pmo.gov.sg/Newsroom/PM-Lee-Hsien-Loong-at-the-APEC-CEO-Summit.

Prime Minister's Office Singapore. "PM Lee Hsien Loong at the Joint Press Conference with US Vice President Kamala Harris (Mar 2022)." March 30th, 2022. https://www.pmo.gov.sg/Newsroom/Remarks-by-PM-Lee-Hsien-Loong-after-the-meeting-with-US-Vice-President-Kamala-Harris-Mar-2022.

Prime Minister's Office Singapore. "SM Teo Chee Hean at TechX Summit 2022." April 5th, 2022. https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-TechX-Summit-2022.

Reuters, "Malaysian PM to write to Indonesia's leader as row over haze flares." September 12th, 2019. https://www.reuters.com/article/us-southeastasia-haze-idUSKCN1VX0VE.

Royal Government of Cambodia. "Rectangular Strategy for Growth, Employment, Equity and Efficiency: Building the Foundation Toward Realizing the Cambodia Vision 2050, Phase IV." http://cnv.org.kh/wp-content/uploads/2012/10/Rectangular-Strategy-Phase-IV-of-the-Royal-Government-of-Cambodia-of-the-Sixth-Legislature-of-the-National-Assembly-2018-2023.pdf

Salalima, Rodolfo A. "Memorandum Circular No. 005: Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructure (CII) Stipulated in the National Cybersecurity Plan (NCSP) 2022." *Department of the Information and Communications Technology*. August 1st, 2017.

Simon, Sheldon. "ASEAN and Multilateralism: The Long, Bumpy Road to Community." *Contemporary Southeast Asia* 30, no. 2. August 2008: 264-292.

Stubbs, Richard. "ASEAN's leadership in East Asian region-building: strength in weakness." *The Pacific Review* 27, no. 4. 2014: 523-541.

Thu, Huong Le. "China's dual strategy of coercion and inducement towards ASEAN." *The Pacific Review* 32, no. 1. 2019: 20-36.

Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis.* New York: Columbia University Press. 1959.

Waltz, Kenneth N. *Theory of International Politics*. New York: Random House. 1979.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge University Press. 1999.

World Integrated Trade Solution. "China trade balance, exports, and imports by country 2016." Accessed July 11th, 2022. https://wits.worldbank.org/CountryProfile/en/Country/CHN/Year/2016/TradeFlow/EXPIMP/Partner/by-country#.

World Integrated Trade Solution. "China trade balance, exports, and imports by country 2019." Accessed July 11th, 2022. https://wits.worldbank.org/CountryProfile/en/Country/CHN/Year/2019/TradeFlow/EXPIMP/Partner/by-country#

Yau, Hon-min. "Fragmenting Cyberspace and Constructing Cyber Norms: China's Efforts to Reshape Global Cyber Governance." *Contemporary Chinese Political Economy and Strategic Relations: An International Journal* 7, no. 2. 2021: 691-715.

Appendix: Constructing Table 1

This Appendix will elaborate further on how the data table used for H1 was constructed, in particular the section measuring a member-state's compliance with ASEAN policies on cyberspace regulation regarding personal data protection, data integrity, provisioning, and security, and finally cross-border data flows. This will be supplemented by a 'Confidence' column, which indicates the amount of reliability toward the overall compliance score generated by the data observed for each member-state. This score, ranging from 'Low' to 'High,' was determined by factors which included the numeric amount of data observations for each member-state and the amount of information the observations provided regarding each dimension on cyberspace regulation.

Member-state	Compliance with ASEAN	Confidence	Personal data score	Cybersecurity score	Cross-border data transfer/flow score
Brunei	Amber	Medium	N/A	N/A	N/A
Cambodia	Amber	Low	4.17	30.36	0.00
Indonesia	Amber	Low	4.17	44.29	0.00
Laos	N/A	N/A	4.17	58.33	0.00
Malaysia	Green	High	66.67	47.86	38.10
Myanmar	Amber	Low	4.17	33.93	0.00
Philippines	Amber	Medium	83.33	95.00	50.00
Singapore	Green	High	66.67	67.50	62.50
Thailand	Green	Low	4.17	50.00	0.00
Vietnam	Amber	Low	4.17	90.83	0.00

Table 1. ASEAN member-states' compliance with ASEAN cyberspace regulation recommendations and quantitative scores on given issue-areas.

As the data shows, evidence regarding compliance with ASEAN was gathered for every state but Laos. This was due to no state-level data from any government-affiliated website being publicly available from Laos, as opposed to other member-states which had a combination of (1) announcements, (2) policies, (3) white papers, or (4) declarations from important members of the state. To start, ASEAN data forming the policy recommendations used to ultimately compare member-state compliance with were located in the following documents:

ASEAN:

1. **Personal data protection**

"Framework on Personal Data Protection" (2016).

- An organisation should not collect, use or disclose personal data about an individual unless:
    - the individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of his/her personal data; or
    - the collection, use or disclosure without notification or consent is authorised or required under domestic laws and regulations. (3)

- An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

    - The personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal data is to be used or disclosed.
    - The personal data should be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks. (3)

- Upon request by an individual, an organisation should:
    - (i) provide the individual access to his/her personal data which is in the possession or under the control of the organisation within a reasonable period of time;

- and (ii) correct an error or omission in his personal data, unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in the particular circumstances. (3)

- Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles. (4)

- An organisation should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes. (4)

- An organisation should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control. An organisation should also make available information on how to contact the organisation about its data protection policies and practices. (4)

2. Data integrity, provisioning, and security

"Framework on Digital Data Governance" (2018).

- The Principle on data integrity and trustworthiness recognises that access to accurate and reliable data is critical, especially when the data is used to analyse and support business decisions such as product development, service delivery or market expansion. This would include:
    - Tracking and documenting data sources to account for when data is procured externally or generated internally;
    - Ensuring data accuracy, where practicable, over the entire data life cycle by implementing good data management practices, including managed data collection and creation, proper data recording and processing such that it does not affect the data quality, review and update internal databases to ensure data is up-to-date especially when the data is used to make a decision about individuals, and incorporate safeguards for data storage; and

- Promoting interoperability of standards by ensuring that data provided is in a structured, commonly used and machine-readable format. (3-4)

- The Principle on data use and access control promotes accountability in data processing, which is a key component in data governance. This would include:
  - Using and/or processing data only for purposes that are reasonable and appropriate; and which are not contrary to laws or national policies;
  - Assigning different access controls and levels of authorisations to personnel for access to different types or classifications of data; and
  - Ensuring that access to data should be adequate, relevant, and transparent. (4)

- The Principle on data security establishes the need to safeguard data, and any storage centres the data sits within, as well as the systems and platforms that handle the data. This would include:
  - Taking appropriate measures, including technical, procedural and physical measures, to ensure that they protect the confidentiality, integrity and availability of any data in their possession, or control against risks such as loss or unauthorised access, use, modification, disclosure, or destruction; and
  - Addressing data breaches promptly and effectively, by containing the breach and implementing mitigating measures to rectify the breach and where relevant, in accordance with national policies on data breach notifications. (4)

3. Cross-border data flows

"Framework on Digital Data Governance" (2018).

- Strategic Priority 2: Cross Border Data Flows
  - Data flows should be accompanied by assurances that safeguards are in place to protect and secure the information regardless where the data goes. These safeguards should be harmonised to prevent the development of fragmented regulatory regimes, which may negatively impact data flows and increase business compliance costs.
  - It should be emphasised that not all requirements imposed on cross border data flows are detrimental to the economy. Requirements may exist to ensure that there are safeguards to accord the necessary protection for the data being transferred. It is important for individual ASEAN Member States to review and minimise restrictions to cross border

data flows against the backdrop of its overall impact to data innovation and the goal of fostering a vibrant data ecosystem.

- The Principle on cross border data flows is intended to maximise the free flow of data within ASEAN to foster a vibrant data ecosystem but at the same time ensure that the data transferred is accorded the necessary protection. This would include:
    - Facilitating cross-border data flows within ASEAN by developing clear and unambiguous requirements and/or criteria and/or circumstances in which data can be transferred from one ASEAN Member State to another;
    - Evaluating and ensuring that the requirements on cross border data flows within ASEAN are proportionate to the risks associated with transferring the data, taking reference from the data classification framework; and
    - Building trust by ensuring an adequate level of protection is accorded to the transferred data. (5-6)

"ASEAN Model Contractual Clauses for Cross Border Data Flows" (2021).

- The MCCs are contractual terms and conditions that may be included in the binding legal agreements between parties transferring personal data to each other across borders. Implementing the MCCs and their underlying obligations helps parties ensure that the transfer of personal data is done in a manner that complies with the ASEAN Member States' (AMS) legal and regulatory requirements, protects the data of Data Subjects based on the principles of the ASEAN Framework on Personal Data Protection (2016) and promotes trust among citizens in the ASEAN digital ecosystem. (4)

4. Overall goals

"ASEAN Cybersecurity Cooperation Strategy (2021-2025)" (2022).

- "Regional organisations like ASEAN offer a platform for member states to share and offer regional perspectives, exchange information on emerging and existing threats, implement Confidence Building Measures (CBMs), and build capacity." (2)

- "However, State governments do not have a monopoly on the solutions to cyber and digital challenges. Leading technology companies' clout and influence over operations and development

of critical and emerging technologies have grown significantly, and industries have also helped build up cyber capacities and provide training in technical solutions." (6)

- "To support ASEAN's digital economy and ambitions, the 2021 – 2025 Strategy seeks to support the establishment of a rules-based multilateral order for cyberspace, one that is open, secure, stable, accessible, interoperable and peaceful; built through the application of voluntary, non-binding norms of responsible State behaviour, confidence building measures, and coordinated capacity-building by enhanced cooperation within ASEAN and with our ASEAN Dialogue Partners." (7)

- "Cybersecurity capacity building serves an effective tool, not only to strengthen collective cybersecurity posture, but also to enable countries to contribute meaningfully to international discussions, which is a key step towards achieving security and resilience in cyberspace. As such, it is important for ASEAN to continue such efforts and learn from each other's experiences through coordinated capacity-building to improve ASEAN's cyber resilience." (12)

ASEAN member-states:

The next section of this Appendix will provide the evidence that ultimately contributed to the assignment of a colour grade for the compliance of each ASEAN member-state to ASEAN's above policy recommendations. It will proceed in alphabetical order, starting from Brunei and ending with Vietnam. In each direct quotation from a state's announcement, policy, or document, the section pertaining to the scoring of compliance with ASEAN will be highlighted with the appropriate colour (amber or green). A brief explanation will be provided after each document.

Brunei:

Ministry of Defence of Brunei Darussalam, "Defence White Paper 2021: Defending the Nation's Sovereignty, A Secure and Resilient Future." (2021)

"To ensure that Defence can guard against disinformation, proper verification measures that check reports or news against credible sources of information must be in place. This remains pertinent in this digital era where disinformation can spread rapidly and uncontrollably. Defence must therefore strengthen its

conduct of audits, inspections, investigations, and its governance policies to be sufficiently robust in the future." (38)

"As information demands and the requirements for ever more capable communications systems increase in the future, there will continue to be a corresponding increase in security challenges… Military networks are also at risk from cyber-attacks from individuals, groups, or nation state sponsored hackers. As governments and militaries around the world move towards the digital usage, there is likely to be ever more reports of government network espionage activities as hackers try to steal state-sensitive information. As information technology demands and cyber risks increase, communication security's importance will increase as a core security theme for the future. The sometimes-contradictory relationship between individual privacy and national security will also become increasingly challenging, but important to balance correctly." (40)

"Develop enhanced preparedness to counter hostile cyber activity." (60)

10.03.18 Issue of Cyber Security. (2018)

"Yesterday morning's session also touched on the issues of cyber security. Responding to a query raised … the E-Government National Centre has carried out a number of security enhancement programmes for e-government systems to tackle cyber security issues.

The programmes cover a number of aspects include human resource and administration process system. Apart from that, several safety initiatives and activities were also introduced. One of them is the WSC safety standard for web applications, which is introduced as a guideline for implementing and auditing systems. All government web application must be tested for safety using the standard prior to its launch. At the same year, the e-government has provided another standard platform for government websites, which allows proper management and easy monitoring, especially in the IT security aspect. Meanwhile, in 2016, the e-government has implemented the manage security services project with the cooperation of ITPSS. The aim of the project is to monitor, protect and establish e-government infrastructure and assets. Meanwhile, activities to strengthen government asset management for server or network facilities are being carried out every quarterly."

For Brunei, their 2021 Defence White Paper represents most of the recent data available on cyberspace governance policy direction, which lowers the amount of confidence in the overall scoring on compliance. Their focus is primarily linked to cybersecurity, and individual privacy being balanced to national security. However, Brunei typically refers to improving on these

policies in a non-specific manner, and no reference to any specific type of improvement is made. For instance, “enhanced preparedness” (60) is not elaborated upon, nor is the methods to balance “individual privacy and national security.” (40) For this reason, as well as the fact that no reference to ASEAN or any international organisation involved in cyberspace governance was made, the White Paper was ultimately awarded an amber score for compliance. Similarly, one statement located from the Prime Minister’s Office elaborated on some mechanisms for improving state cybersecurity, and this included some specific plans. However, no real compliance with ASEAN was ultimately observed.

Cambodia:

Royal Government of Cambodia, “Rectangular Strategy for Growth, Employment, Equity, and Efficiency: Building the Foundation Toward Realizing the Cambodia Vision 2050, Phase IV.” (2018)

“Promoting the establishment of a legal framework to support digital development, including the implementation of digital government and information security strategy, E-Commerce law, the Law on Cybercrime as well as amending laws and related regulations, all of which will underpin the growth and prevent risks in the sector.” (44)

“Developing entrepreneurship and digital ecosystem conducive to the creation of new businesses, promoting the use of digital system in business, and establishing an entrepreneur cooperation mechanism within the RGC or some forms of partnership with the private sector.” (44)

Cambodia’s documentation on cyberspace is sparse, which is reflected in the low confidence score obtained, and nothing publicly available beyond this Rectangular Strategy plan announced in 2018 was noted in the thesis’s scoring of the country. As these two sections indicate, Cambodia has focused on establishing frameworks for their own digital economic development. This is in both a legal manner as well as a business-oriented one with regards to creating the new digital ecosystem for their businesses. However, as a whole, Cambodia does not

make explicit reference to the ASEAN recommendations above, and so they were given an amber score.

Indonesia:

Defence Ministry of the Republic of Indonesia. "Defence White Paper." November 2015.

"It is the perspective of defence that cyberspace has become the fifth domain used as a battlefield, excepts [sic] land, sea, air and space." (16)

Unfortunately, nothing beyond this brief quotation was observed for Indonesia. That they refer to cyberspace as a 'battlefield' does indicate that it ought to be given special attention in domestic governance, at least, but this is only an implication and little else is said regarding cyberspace governance. The amber grade assigned to Indonesia should therefore be taken with significant caution, as there is simply not enough sample size to justify the grade being a stable or accurate one.

Laos:

No data was observed from Laos's governmental websites.

Malaysia:

The Government of Malaysia. "Cyber Security Framework For Public Sector." Accessed July 7th, 2022.

- **Key Components**: Eight major components of this cybersecurity framework and the objective of these components are:
    - **Identify** which aims at identifying the business function environment, governance structure and policy as well as assets to be protected, the associated risks and risk management;
    - **Protect** requires the necessary security principles, technologies, processes and people competencies to be determined in order to mitigate the risks identified;

- Detect the objective of detecting malicious attacks through highlighting anomalies in usage and network traffic pattern;
- **Respond** on the other hand is to ensure responses to these malicious attacks are being taken and to escalate communications to the stakeholders and the general public (if required);
- **Recover** addresses the capability to be able to recover from the damages caused by malicious attacks and system failures to ensure availability of information;
- **Procure** is to ensure that security measures and requirements are enforced throughout the entire lifecycle of the system regardless of the manner of acquisition, be it through external acquisition or through in-house development. This is a very important component that covers procurement specifications, vendor management, footprint of resources, system development life cycle, commissioning and decommissioning processes and system disposal;
- **Security Audit** and
- **Enforce** cuts across all components to outline the scope of audit and enforcement carried out by the audit and enforcement agencies.

The Government of Malaysia. "Data Leakage Protection." Accessed July 7th, 2022.

- **What are Objectives DLP?:** Objectives of DLP implementations are:
  - To protect from and prevent intentional or unintentional leakage of electronic information;
  - To facilitate early detection of risky activity, thus allowing for the early initiation of actions to mitigate negative outcomes;
  - To reduce the cost of investigation on leakage and the cost to rebuild the organisational reputation in the event of information leakage; and
  - To increase confidence in the organisational management by setting protective security measures regarding electronic information in place.

The Government of Malaysia. "Open Data." Accessed July 7th, 2022.

- **What is Open Data?**
  - Open data is data that can be used freely, is able to be shared and reused by the people, as well as the Government and public agencies for various purposes. It acts as the catalyst in the Government's citizen-centric initiative. The implementation of Government open data

will improve the transparency of Government services delivery through sharing of data that is accurate, fast and relevant as well as increase the nation's digital economy productivity through new industries or innovations with the involvement of the people and the business community. It also places Malaysia on par with other countries in the Digital Government initiative.

  - The Public Sector Open Data (DTSA) portal was developed in 2014 to support this aspiration of implementing open data. The DTSA portal enables the government open data to be easily accessed centrally from an official source.

- **What are the Objectives of Open Data?**
  - The objectives for implementing the public sector open data are as follows:
  - To encourage the sharing of data between the public and private sector agencies, and the people.
  - To improve the quality and transparency of service delivery through online sharing of open data which is citizen-centric.
  - To encourage digital economy productivity through the creation of new industries or innovation with the involvement of the people and the business community.

The Government of Malaysia, "National Security Policy." Accessed July 8th, 2022.

"Strategy 18: Maintain Cyber Security and Defence Ensure a secured cyber environment through comprehensive risk management involving the consolidation of the security and defence infrastructure, especially the Critical Information Infrastructure of the country."

The Government of Malaysia, "National Defence Policy." Accessed July 8th, 2022.

"The development of a cyber-warfare capability is an important step towards counterbalancing the ability of other countries in the region and to defend important national targets from all forms of threats. It is important to stop any form of encroachment into national defence's computer systems and networks. Concurrently, it also provides the room for developing offensive capabilities for conducting cyberoperations when necessary. This capability would provide room for information fathering at strategic, operational and tactical levels."

Ministry of Foreign Affairs Malaysia. "Foreign Policy Framework of the New Malaysia: Change in Continuity." June 2019.

"As the reliance on information technology (IT), particularly the internet becomes greater, Malaysia is aware of the great risks involved in possible cyber attacks. Subversive, criminal or terrorist elements may cause crises and disruptions via unauthorised access or attacks to the related hardware, networks, programmes and data, owned by the government, businesses or private individuals. Therefore, there is an urgent need for attention to be given to cyber security."

Ministry of Foreign Affairs Malaysia. "Malaysia's Foreign Policy." Accessed July 8th, 2022.

"ASEAN remains the cornerstone of Malaysia's foreign policy and the establishment of the ASEAN Community in 2015 has significantly elevated Malaysia's approach and engagement at the regional level. Concurrently strengthening bilateral and multilateral aspects of Malaysia's engagement with the world will continue to be an important focus. The nation's well-being is founded on the strong and friendly relations with other countries and its commitment to the multilateral system."

Overall, Malaysia's compliance with ASEAN policies is not explicitly seen until their foreign policy document which outlines the significant role that ASEAN plays in Malaysian foreign policy. In terms of cyberspace, Malaysia is chiefly concerned with data protection, individual data privacy, cybersecurity, and the openness of data. In their documents, no reference to ASEAN or any other international organisation managing cyberspace is seen, which does provide an element of ambiguity insofar as Malaysia can define national cyber defence or other policy goals in their own terms.

That being said, what elevates them from an amber score to a green score is the fact that if Malaysia were truly going to commit to an amber country's methods of strategic compliance when it suited them, they would likely not have declared their fundamental compliance with ASEAN and a multilateral regional system. As such, because Malaysia has bounded their foreign policy to the constraints of compliance with ASEAN's multilateral norms of engagement, this represents a substantial shift in policy direction that puts them ahead of other states marked in the amber category. That there is significant amounts of data also provides Malaysia's score with a high confidence rating.

Myanmar:

It is first necessary to preface this country's data with the fact that their media publications are all in the native language, which cannot be read by the author. Therefore, the nuances observed and the sections highlighted should be taken with a sizable grain of salt, as the wording may not be entirely accurate with respect to the Burmese language. This lowers the confidence considerably, from what may have been a medium level to a low one.

Ministry of Transport and Communications, "Cyber Legal and Policy Framework," *Myanmar National Portal*, accessed July 6th, 2022.

"U Soe Thein, Permanent Secretary of the Ministry of Transport and Communications addressed the meeting. In this regard, the first meeting was held on December 7, 2018. The data collected from it is subject to international law and international law. He added that the meeting was held to compare the reports and prepare reports, and that the meeting was held to discuss the reports, and that the Cyber Law and Policy (first draft) would be further drafted based on the recommendations gained from the discussions."

The Government of Myanmar. "Myanmar Cyber Legal and Policy Framework: Policies Related to e-Government, e-Commerce, and Cyber Security (Draft – 25 Jan 2019)." (2019)

"Government institutions retain full control and ownership over their data. This is ensured through the Cloud Service Provider identity and access controls available to restrict access to customer infrastructure and data. CSPs should provide customers with a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity." (18)

"The government data manager can control where the data is being stored, including potentially choosing the jurisdiction where the data is located. Cloud customers that transfer personal information or other data that is subject to restrictions on cross border data transfers will need to ensure their data is stored and processed by a CSP that complies with the necessary certifications and requirements. For example, a cloud customer transferring data from the EU to Singapore should ensure their CSP complies with the EU regulations and, to the extent necessary, has obtained approval from the EU data protection authorities for transferring personal data from the EU to a non-EU jurisdiction. The Government Data Manager may also choose to require the CSP to disclose where data is being stored, processed and managed." (33)

The Government of Myanmar. "Law Protecting the Privacy and Security of Citizens." (2021)

"Every citizen has the right to enjoy the protection of his/her privacy and security in full, as set out in the Constitution of the Republic of the Union of Myanmar." (1)

The data demonstrates that for the most part, Myanmar's cyberspace regulations are intently focused on developing state capabilities and ensuring that their national laws are robust with regards to data protection and jurisdiction. While there is no reference to ASEAN or any other international organisation, the translated document does state that the findings from the meeting on the Framework are subject to international law. By the standards of the scoring practices in this thesis, this should be awarded an amber score due to its acknowledgement of international law whilst it is also non-specific in terms of which laws, and how it ought to comply to these laws to begin with. Again, a lack of data is visible here in the low sample size, and the amber score reflects this sample size as well as the findings visible from existing documents.

<u>The Philippines:</u>

Department of Information and Communications Technology (DICT). "National Cybersecurity Plan 2022." ***Cybercrime Investigation and Coordination Center.*** **2022.**

"Included in the mandates of DICT are to "ensure the rights of individuals to privacy and confidentiality of their personal information; ensure the security of critical ICT infrastructures including information assets of the government, individuals and businesses; and provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of the ICT sector."" (2)

"The rights of every individual to have equal access to the Internet are upheld at all times. However, balance must be made between protecting the privacy of the individual against securing protection of information and data of the users." (21)

"Admittedly, the Philippines' state of cybersecurity is still at its infancy stage, even though there have been previous initiatives that have already been undertaken through different agencies, including enabling

of the laws that have been promulgated to protect data and information. The NCSP 2022 shall provide the roadmap to make a coherent and cohesive strategy for cybersecurity and act as the enabler for institutionalizing all the initiatives and strategies that have already been started by different government agencies." (45)

Salalima, Rodolfo A. "Memorandum Circular No. 005: Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructure (CII) Stipulated in the National Cybersecurity Plan (NCSP) 2022." ***Department of the Information and Communications Technology.*** **August 1st, 2017.**

"The privacy and sharing of personal data involving government agencies or a third party shall be in conformance with the issuances from the National Privacy Commission."

Overall, as the NCSP admits, the Philippines is still also in a developmental phase of cyberspace, particularly with respect to cybersecurity. Most of their policies and documents, therefore, address the tenets mentioned by ASEAN's documents in a basic manner, although they do not mention ASEAN or any international organisation by name. For instance, the NCSP is geared towards creating a central state strategy on cybersecurity, and goals such as balancing data privacy of an individual with national security are also discussed. Due to this ambiguity in policy direction, the Philippines are awarded an amber score on compliance with ASEAN, and the overall lack of substantial data means that the confidence value in this score can only be a medium level.

<u>Singapore:</u>

Ministry of Foreign Affairs Singapore. "Cybersecurity." Accessed July 12th, 2022.

"Singapore is committed to the establishment of a rules-based multilateral order to build a secure and peaceful cyberspace. We play an active role in cybersecurity discussions at the UN. For example, Singapore participates in both the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security. In addition, Singapore and Estonia co-chair the UN Group of Friends

on e-governance and cybersecurity, and Singapore co-chairs the UN Group of Friends on Digital Technologies with Mexico and Finland. Singapore also hosts the annual Singapore International Cyber Week (SICW), and is a signatory of the Paris Call for Trust and Security in Cyberspace."

Ministry of Foreign Affairs Singapore. "Transcript of Minister for Foreign Affairs Dr Vivian Balakrishnan's curtain raiser interview with SPH Media on the Visit of United States Vice President Kamala Harris at the MFA Exhibition Hall, 16 August 2021." August 17th, 2021.

"Again, you know, that Singapore is engaged in Digital Economy Agreements (DEA) with Australia and New Zealand and other countries. We want to see or explore whether the US can be part of these emerging architecture for the digital economy.

The third area will be in the green economy. I think you have seen the latest Intergovernmental Panel on Climate Change (IPCC) report – climate change is an even more urgent and pressing problem. I believe the Biden Administration shares our view. We will be trying to explore opportunities for agreements on norms, and hopefully on global arrangements, which would help us transit more quickly into a greener, more sustainable economy. That is the third area of focus. The fourth area will include more topical and security-related issues like cybersecurity. As we become more dependent on the digital economy, we are also at greater risk. This (cybersecurity) is another area where we hope to collaborate more intensively and deeply with the US. Historically, we have a long, deep track record. Prospectively, there is a lot to explore in the near future as well."

Prime Minister's Office Singapore. "SM Teo Chee Hean at TechX Summit 2022." April 5th, 2022.

"Then we can develop the concepts, apply the technologies and break the cycle. Internationally, given the borderless nature of cybercrime, we need new global rules, norms, governance principles, frameworks, and standards. These will ensure that we are all aligned at the policy level to deal with these new threats. At the same time, even as technology has afforded us new capabilities to combat both physical and cyber crime, it is not an unalloyed good. For example, while surveillance cameras and facial recognition technology can keep us safer, they also raise concerns about privacy. We need to establish proper guidelines and standards on the use of technology to provide ample protection, and to preserve trust and confidence. Only with these in place can we make the best use of what technology can offer us, to improve our capability to protect our societies and people from the new dangers."

"Singapore has been trying to play our part – at the World Intellectual Property Organisation, at the United Nations Open-Ended Working Group on Cybersecurity, or OEWG, and the sixth Group of

Governmental Experts, or GGE. Our permanent representative to the UN in New York has been elected as the Chair of the 5-year Open-Ended Working Group on Cybersecurity (OEWG) on the security and use of ICT. We are committed to work together with the UN and other countries to establish a rules-based multilateral order for a secure and peaceful cyberspace. There is a lot of work to be done, and we hope that we can work together to make progress."

Prime Minister's Office Singapore. "PM Lee Hsien Loong at the Joint Press Conference with US Vice President Kamala Harris (Mar 2022)." March 30th, 2022.

"We [Singapore and the USA] established a bilateral Cyber Dialogue to work together on critical infrastructure protection, data security and sharing of best practices in support of a rules-based multilateral order in cyberspace."

Prime Minister's Office Singapore. "Meeting and Joint Leaders' Statement between PM Lee Hsien Loong and US President Joe Biden." March 30th, 2022.

"The United States and Singapore maintain a strong and growing partnership on cybersecurity. We seek global adherence to the UN framework of responsible state behavior in cyberspace and pledge to deepen our cooperation on combating cyber threats, promoting resilience, and securing our critical infrastructure, amongst other issues. We welcome the establishment of the United States-Singapore Cyber Dialogue to cement our cross institutional linkages to jointly tackle cybersecurity issues. We will continue to jointly lead critical efforts in the International Counter Ransomware Initiative to tackle the surge in ransomware attacks worldwide."

Prime Minister's Office Singapore. "PM Lee Hsien Loong at the APEC CEO Summit 2021." November 11th, 2021.

"My third suggestion, is that globally, we need a coherent and concerted response to manage the digital transition. Digital technologies have empowered millions of people, but the gulf of opportunities between digital haves and have-nots has also widened. Global digital standards and cooperation initiatives are important. They will enable more people to participate meaningfully in the digital economy. There are many areas to consider, for example, fair and secure access to data, freer cross-border data flows, addressing misinformation and cyber threats, and strengthening multilateral cooperation to exploit digital technologies for sustainable development. There are many overlapping discussions on digital issues, for example, at APEC, the World Economic Forum, the World Trade Organisation as well as the United Nations and its agencies. It is useful to bring them together in a coherent manner.

In our own region, Singapore is hosting the ASEAN-Singapore Cybersecurity Centre of Excellence to strengthen regional cyber resilience. Singapore will work closely with the international community towards not just an open and free digital environment, but also a secure and interoperable one."

Out of the 10 ASEAN states surveyed for data (9, excluding Laos which had no data), Singapore is by far the best complier with ASEAN policies on cyber governance, according to this thesis's scoring metrics. Their public statements and announcements on policy directions have been detailed and informative, insofar as they have discussed all four areas of governance in which ASEAN has recommended policies. More than this, however, Singapore has repeatedly made reference to ASEAN, to the UN Group of Governmental Experts, and other international bodies and fora on cyberspace governance in which they play a significant role. This is an important dynamic of the scoring system, as it indicates that Singapore is willing to constrain themselves in state policy to adhere to regional or global bodies' governance recommendations. Therefore, they are given a strong 'green' score in Table 1, and the significant amount of data is reflected in the high confidence score obtained.

Thailand:

Ministry of Foreign Affairs Thailand. "Annual Report 2019." (2019)

"The two leaders expressed satisfaction with the close and comprehensive relations between Thailand and Singapore, especially in the areas of economic and defence cooperation, which have been underpinned by frequent exchanges of high-level visits and close contacts within ASEAN. Their discussions focused on security cooperation, trade and investment, digital economy and start-up businesses, cybersecurity and cooperation within ASEAN frameworks."

Conversely, Thailand suffers from a significant lack of data. The only report pertaining to cyberspace was the Annual Report 2019, in which the country reported cordial discussions with Singapore on cybersecurity development within an ASEAN-centric framework. By the letter of

the law as the thesis's scoring standards were concerned, this met the standards for a score of green. However, realistically the low sample size indicates that Thailand being assigned a green standing for compliance may not particularly be accurate, especially when considering that Thailand has not published any public data regarding their own policy directions and current goals. As such, the confidence level in this compliance result remains quite low.

Vietnam:

Ministry of Foreign Affairs Vietnam. "Remarks by the Deputy Spokesperson of the Ministry of Foreign Affairs of Viet Nam Ngo Toan Thang about the US cyber security firm FireEye's statement that Viet Nam assisted the APT32 hacker group in conducting cyber-attacks targeting international government units and businesses." April 23rd, 2020.

"This is groundless information. Viet Nam strictly bans all cyber-attacks against organizations and individuals in any form. Cyber-attacks and security threats are to be strictly condemned and punished in accordance with the laws. In 2018, Vietnamese National Assembly has ratified the Law on Cyber Security and is completing legal documents to prevent cyber-attack attempts.
Viet Nam stands ready to collaborate with the international community in combating cyber-attacks in all forms."

Ministry of Foreign Affairs Vietnam. "Remarks by MOFA's Spokesperson Le Hai Binh during the 9th Regular Press Conference in August 4th 2016." August 4th, 2016.

"As you may be aware, Vietnamese competent agencies have speedily taken necessary measures to protect network security and to ensure safety and normal operation at our airports. At the same time, investigations by Vietnamese cyber security forces on the attacks have been underway. The Vietnamese functioning bodies, including the Ministry of Foreign Affairs, are willing and ready to work closely with the international community to prevent and fight against any forms of hacking and cyber attacks, including the recent incident."

Ministry of Foreign Affairs Vietnam. "Viet Nam calls for enhanced solidarity to build strong, resilient ASEAN Community." February 17th, 2022.

"Regarding the Myanmar issue, Minister Son affirmed Viet Nam's readiness to join hands with other countries to assist Myanmar to overcome these trying times, voicing support for the continued effective implementation of the Five-Point Consensus.

He also proposed stronger cooperation within ASEAN and between the bloc and partners to deal with emerging non-traditional security challenges, including those related to cyber security, maritime security, water resource security, climate change, and environmental pollution, as well as new challenges caused by the COVID-19 pandemic."

Again, Vietnam is a country which has little substantive data with regards to country policy direction on cyberspace. It is unclear, from the data observed, where Vietnam wishes to proceed with their own policies on data protection, privacy, and integrity, as well as cross-border data flows. However, the statements seen do indicate that they are agreeable to working with 'the international community' to prevent against cyber attacks. While this may be the case, as mentioned in the scoring criteria, the amber score is deliberately designed to account for potential cases of strategic ambiguity, where it is not certain what lengths the state will go to in order to meet their own standards. In this case, working with the international community, as Vietnam phrases it, is unclear in how it ultimately would look like from a policy-based perspective.

One aspect worth mentioning is that Vietnam did propose cooperation within an ASEAN-based framework to deal with non-traditional security issues like cybersecurity. However, this is once again ambiguous insofar as Vietnam's proposal is not clear on how it will cooperate in an ASEAN-driven set of guidelines, given the context of its other policy statements observed. This particular statement will provide strength towards the argument that Vietnam should be somewhere between a strong amber score and a weak green score, but more so towards the former due to a conclusive lack of more evidence scoring Vietnam with a green record of compliance. Due to this, a low amount of confidence is given to Vietnam's compliance score.