Jagiellonian University in Kraków
Faculty of International and Political Studies
Institute of European Studies

Mariam Bochoidze

student ID number: 1199504

Field of study: European Studies

From Cybersecurity Laggard to Normative Leader.
EU becoming a digital regulatory power.
Magister (MA) Thesis

Thesis written under the supervision of
Dr. Błażej Sajduk

06.2024
Krakow, Poland

Table of Contents

Abstract 1

List of Abbreviations 3

Definition of Concepts 4

List of Tables 5

Introduction 6

Literature Review 9

Theoretical Framework 14

Chapter 1. The Tendency of Cyber Politicization 17

Chapter 2. Cybersecurity Trajectory and Regulatory Landscape of EU 20

Early Beginnings 20

Key Regulations and Strategies 21

Chapter 3. ASEAN and Cyberspace 26

ASEAN's Positioning and Engagement in Cyberspace 26

ASEAN Cybersecurity Mechanism 30

ASEAN Regional Cybersecurity Framework 31

Chapter 4. Cybersecurity Chronicles: Unveiling EU and ASEAN Policies 35

Connecting Nodes: EU-ASEAN Relations 35

Cyber Policy Perspectives: EU-ASEAN Comparison 38

EU: Towards enhanced cyber resilience 45

Chapter 5. Guiding ASEAN Cybersecurity: The EU's Influence 51

Analysis and Conclusion 60

Bibliography 64

Appendices 75

Abstract

The paper studies the EU’s transformation from a cybersecurity laggard to a normative leader and examines its dominant digital regulative power in the international arena. Considering the fast-changing and increasing nature of cybercrime and cyber threats, it is essential to know the EU’s methods to influence global cybersecurity norms. The study focuses on the main question: How the EU’s role is shaping the development of global cybersecurity norms? For this reason, the paper also investigates how the European Union has used its internal market power, regulatory expertise, and diplomatic networks to influence cybersecurity policies beyond borders. This part focuses mainly on its impact on the Association of Southeast Asian Nations.

Moreover, this paper employs agenda-setting theory as a theoretical framework and analyzes features of policy windows, institutional roles, and transnational dimensions that have contributed to the EU’s dominance. This research mainly focuses on GDPR’s influence on ASEAN. Therefore, the association member state’s data privacy legislations are discussed in detail and compared to the GDPR. Different methods were used to collect data. The primary official documents from both organizations and secondary literature were thoroughly examined. Therefore, this work intends to contribute to our understanding of the global cybersecurity landscape and the EU’s pivotal role in it.

W rozprawie zbadano transformację Unii Europejskiej z instytucji w dziedzinie bezpieczeństwa cybernetycznego zapóźnionej w jej legislacyjnego lidera, oraz zbadano dominującą cyfrową siłę regulacyjną tej instytucji na arenie międzynarodowej. Biorąc pod uwagę szybko zmieniający się charakter i rosnącą intensywność cyberprzestępczości i zagrożeń cybernetycznych, niezbędne wydaje się zdobycie znajomości metod stosowanych przez Unię Europejską w celu wpływania na globalne normy cyberbezpieczeństwa. Badanie koncentruje się na głównym pytaniu: jak rola wspólnoty europejskiej kształtuje rozwój globalnych norm cyberbezpieczeństwa? Z tego powodu w rozprawie zbadano również, w jaki sposób Unia Europejska wykorzystała swoją siłę na rynku wewnętrznym, znajomość regulacji i istniejące sieci dyplomatyczne, aby wpłynąć na politykę cyberbezpieczeństwa poza swoimi granicami. Rozparawa koncentruje się się na wpływie zjednoczonej Europy na Stowarzyszenie Narodów Azji Południowo-Wschodniej.

Jako ramę teoretyczną niniejszym artykule wykorzystano teorię ustanawiania agendy. Analiza skupia się na segmentach legislacyjnych, rolach instytucjonalnych oraz kontekstach ponadnarodowych, c które przyczyniły się do dominacji Unii Europejskiej w dziedzinie cyberbezpieczeństwa. Badanie koncentruje się głównie na wpływie RODO na ASEAN. Dlatego też przepisy dotyczące ochrony danych obowiązujące w państwach członkowskich stowarzyszenia są szczegółowo omawiane i porównywane z RODO. W pracy zastosowano różne metody gromadzenia danych. Dokładnie zbadano również najważniejsze oficjalne dokumenty obu organizacji oraz literaturę przedmiotu. Celem niniejszej pracy jest przyczynić się do lepszego zrozumienia globalnej sytuacji cyberbezpieczeństwa i kluczowej roli, jaką odgrywa w niej Unia Europejska.

Key terms: Cybersecurity, EU-ASEAN relations, cyber maturity, GDPR
Kluczowe pojęcia: Cyberbezpieczeństwo, stosunki UE-ASEAN, dojrzałość cybernetyczna, RODO

List of Abbreviations

ADGMIN - ASEAN Digital Minister's Meeting

ADGSOM - ASEAN Digital Senior Official's Meeting

ADMM - ASEAN Defence Ministers Meeting

AEC -ASEAN Economic Community

AFR - ASEAN Regional Forum

AI - Artificial Intelligence

AMMTC - ASEAN Ministerial Meeting on Transnational Crime

ANSAC – ASEAN Network Security Action Council

APEC - The Asia-Pacific Economic Cooperation

APSC - ASEAN Political-Security Community

ASCC - ASEAN Socio-Cultural Community

CBM - confidence-building measures

CBPR - Cross-Border Privacy Rules System

CERT - Computer Security Incident Response Team

CSCAP - Council for Security Cooperation in the Asia Pacific

EC - European Commission

EC3 - European Cybercrime Center

ECCG - European Cybersecurity Certification Group

EJCN - European Judicial Cybercrime Network

EP - European Parliament

FDI - Foreign Direct Investment

GCI - Global Cybersecurity Index

GDPR - General Data Protection Regulation

ICPC - International Cyber Policy Center

ICT - Information and communications technology

IoT - Internet of Things

ISM - Information Security Manual

ITU - International Telecommunication Union

JCC - ASEAN-EU Joint Cooperation Committee
PDPA - Personal Data Protection Act
SOMTC - Senior Officials Meeting on Transnational Crime
TELMIN - ASEAN Telecommunications and Information Technology Ministers Meeting

Definition of Concepts

Cyber Maturity - refers to the level of preparedness and capability of an organization, sector, or nation to effectively manage cyber risks and respond to cyber incidents (Feakin et al., 2016).

E-commerce - commerce conducted via the Internet (Merriam-Webster. (n.d.).

End-users - The ultimate consumer of a finished product (Merriam-Webster. (n.d.)).

Cyber hygiene - The steps that computer and device users take to maintain system health and improve online security. Good cyber hygiene practices include updating software regularly, using strong passwords, and being cautious about email attachments and links (National Institute of Standards and Technology. (n.d.)).

Interoperability - the ability of computer systems or software to exchange and make use of information", (Merriam-Webster. (n.d.)).

List of Tables

Table 1 - National Capabilities of ASEAN Member States 49

Table 2 - Cybersecurity and Data Privacy Legislation across ASEAN 52

Introduction

Cyber security is yet another challenge that transforms international relations in the modern world, which is so diverse and multifaceted. In response to growing threats and attacks on IT systems and infrastructure, there is greater development of what is referred to as 'the norms of cyberspace' and international cooperation. These norms are for reducing conflicts and harmonizing the digital domain, but they are quite challenging as there are multiple actors and multiple interests.

As more people use digital services, solving cybersecurity problems becomes critical to protecting national security, international cooperation, and the EU's digital transformation agenda. Therefore, the European Union (EU) has recently stepped up its involvement in cybersecurity issues, realizing the urgency of the situation. In the beginning, the EU had an introverted approach, which mainly focused on cyber resilience and strategic autonomy. Now, it is clear that the EU is setting the agenda and guiding the creation of an open, free, stable, and secure cyberspace beyond its borders. Despite a delayed start, the EU's cyber strength is becoming strategically responsible.

With the increase in the incidences and sophistication of cyber threats, the EU is now participating in cybersecurity forums. This study aims to analyze the evolution of the EU from a cybersecurity laggard to a normative power, focusing on its role as a digital standard-setting authority. This, together with the fact that cyber risks are constantly developing and increasing, makes it essential to understand the EU's mechanisms and its influence on global cybersecurity. Therefore, the paper examines the EU's journey and the factors that supported the European Union in becoming the cyber normative authority. Moreover, the paper explores how the EU used its internal market power, regulatory expertise, and diplomatic networks to influence cybersecurity norms beyond its borders, with a particular focus on the Association of Southeast Asian Nations. This research is highly relevant because it addresses the modern issue of cybersecurity. It also shows how the European Union nowadays plays a bigger role in creating a safer digital space for the globe. Besides, the paper studies ASEAN and demonstrates how regional integration efforts influence cooperation mechanisms of cybersecurity and its strategies. The case of the Association of Southeast Asian Nations is crucial for this work for the following reasons. First, it shows how the European Union is pulling all the power into this region to overcome the influence of other dominant cyber actors. Second, the EU and ASEAN have very different governing systems, and this case study shows how the European Union deals with them in a very effective manner. Third, in most of the existing literature, the authors compare the ASEAN and EU cyber governance. This work compares the sensitive data regulations of ASEAN member states and the GDPR and fills the significant gap by providing insights into their similarities and differences. Moreover, the offered study will be useful to those interested in this topic and may be employed as supporting literature for future research.

Hence, against this backdrop, the research aims to address the question: How the EU's role is shaping the development of global cybersecurity norms?

Methodology

The paper analyzes the EU's role in shaping global cybersecurity norms while focusing on ASEAN member states. For this reason, the research employs multiple designs, namely document analysis, content analysis, and case study to answer the main question. First, the current state of cyber norms is studied using document analysis. Official cybersecurity policy documents issued by the European Union, ASEAN, and its member states are examined in order to understand their approaches and key cyber issues. Namely, the ASEAN Cybersecurity Cooperation Strategy 2021-2025 helps us identify where the association puts cybersecurity on its agenda. Another significant document that illustrates how the data protection legislation works in that region is the Framework on Personal Data Protection. Moreover, the ASEAN-EU Plan of Action of 2018 and 2019 presents valuable information for the research. Several official documents issued by the European Commission and the European Council are used. The paper also analyzes one of the significant primary sources - the NIS Directive, which clearly shows RU's regulative approach. Furthermore, the work comprises other important documents concerning the GDPR and EU Cybersecurity Strategy.

Second, the research design will take the form of a qualitative comparative case study. Specifically, the ASEAN case study addresses the similarities and differences between the approaches of the EU and the Association. The comparison is an essential part of the paper to find the gaps between the two countries' cyber strategies and how the EU influences them. In this respect, both primary and secondary literature are reviewed. This paper also examines bilateral and multilateral fora, which focus on cybersecurity and where the EU directly participates, projecting its normative power. However, as the ASEAN does not have a common cyber defense framework, the research does not cover “developing cyber defense policy and capabilities” and “developing industrial and technological resources for cybersecurity.”

Theoretical framework

The research employs agenda-setting theory as a foundational framework to show how the European Union prioritizes cybersecurity in domestic and foreign relations. The theory focuses on policy windows, which helps us see how the EU has put certain cybersecurity issues on the agenda. Moreover, the agenda-setting theory offers insights into the roles of various actors and institutions. This, indeed, is essential to analyze the complex dynamic of EU policymaking. Also, the theory is relevant because it touches on aspects of transnational dimensions and supports the paper to explore the EU's influence beyond its borders and in regard to ASEAN.

Limitations

A notable limitation of the research is the absence of explicit assignment of duties among the EU and its Member States in the field of cybersecurity. While the EU positions itself as a significant actor, the practical responsibility for cybersecurity is largely delegated to Member States and the private sector. Thus the decentralized approach unables us to fully capture the complexity of EU's cybersecurity initiatives.

Literature Review

Mass communications and digital technology have recently penetrated practically every industry, including national security. States are now confronted with cyber issues that might escalate into broader cyber wars in the future. Joseph Nye was the first to describe cyberspace and conceive the notion of cyber power. Power based on information resources, he claims, is not new, but cyber power is. There are several definitions of cyberspace, but “cyber” generally refers to electronic and computer-related activity. In a sense, “cyberspace is an operational domain framed by the use of electronics to …exploit information via interconnected systems and their associated infrastructure.” (Nye, 2011, p.18). Power is determined by context, but cyber power is determined by the resources that define the realm of cyberspace. This definition will guide the research paper in the course of the work.

Notably, in her examination of the cyberspace revolution in international relations, Nazli Choucri (Choucri, 2012) does not confine herself to low politics but also realizes its impacts on high politics and sensitive matters of national security and decision-making processes. Choucri challenges conventional state-centric viewpoints by emphasizing the necessity of openly integrating cyberspace into the study of global politics. The book looks at online conflict and collaboration, how sustainability and cyberspace might intersect, and how cyberspace and international initiatives to promote sustainable development are starting to work together. Above all, this material is essential to my work because it emphasizes how the internet is becoming a more significant factor in determining international relations.

Despite the perception that cyberspace has little strategic significance, Francis C. Domingo’s (2016) study investigates why powerful governments engage in cyber capabilities for military domination. Based on a neorealist paradigm, the paper argues that strong governments would unavoidably expand their cyber warfare capacity, retain their cyberspace hegemony, and maybe intensify cyberattacks into kinetic attacks. This is relevant to my work as it clarifies the strategic actions of strong nations in the digital sphere and adds important context to the geopolitical environment of cyberspace.

The development of EU cybersecurity policies has been a subject of growing academic interest over the past two decades. Christou (2016) provides a complete overview of the EU's cybersecurity policy evolution in his book "Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy." He characterizes the EU's cybersecurity approach as a steady transition from a fragmented, sector-specific approach to a more inclusive and unified strategy. Carrapico and Barrinha (2017) also share the same view while analyzing the EU's efforts to establish itself as a powerful cybersecurity actor. They highlight the challenges the EU faces in balancing the diverse interests of its member states while striving for a unified approach to cybersecurity.

The introduction of crucial legislative measures, such as the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR), has been vital in shaping the EU's cybersecurity landscape. Wessel (2015) discusses the legal consequences of these developments, arguing that they represent a significant step towards an EU cybersecurity law. Similarly, Fahey (2014) explores the EU's rule-making process in cybercrime and cybersecurity, focusing on domestic and foreign policy interaction. This work is important for the paper as it helps to show how the EU creates the norms internally and how they influence the ASEAN. Robert Siudak (2022) further contributes to this discussion by studying cybersecurity discourses and their policy implications, offering valuable information on how different narratives shape EU cybersecurity policies. To understand the mechanisms of how cybersecurity issues become a priority in EU policy-making processes, Sebastiaan Princen (2007), in his work on agenda-setting theory, lays a perfect theoretical foundation. These works collectively highlight the complex nature of developing an inclusive cybersecurity framework within the EU's multi-level governance structure.

The EU's emerging role as a global regulatory power, particularly in the digital domain, has gained considerable scholarly attention. Bradford's (2020) persuasive work, "The Brussels Effect: How the European Union Rules the World," effectively analyzes the EU's ability to shape global standards through its market power and regulatory expertise. While not exclusively focused on cybersecurity, Bradford's insights into the mechanisms of EU influence are highly relevant to this study as his paper supports understanding the EU's impact on global cybersecurity norms. In the specific context of cybersecurity, Bendiek and Pander Maat (2019) examine the EU's regulatory approach and its implications for global cyber partnerships. They argue that the EU's focus on sensitive data protection and privacy gave the EU the image of an influential and unique participant in global cybersecurity debates. This perspective is complemented by Liaropoulos (2017), who analyzes the EU's cybersecurity strategy as a form of soft power projection, highlighting how the EU leverages its normative influence in the absence of traditional hard power capabilities in cyberspace. The global impact of EU regulations, particularly the GDPR, is further explored by Callo-Müller (2018), who shows how personal data protection and trade are harmonized and highlights the far-reaching effects of EU data protection standards. Gribakov (2019) extends this analysis to the Asian context, discussing the implications of cross-border privacy rules in Asia and how they interact with EU standards.

The EU's influence on ASEAN's cybersecurity policies is an emerging area of research that falls within the broader context of EU-ASEAN relations. Benincasa (2020) provides a valuable analysis of the role of regional organizations in building cyber resilience, offering a comparative perspective on EU and ASEAN approaches. Chen and Yang (2022) also add significant data to this analysis by comparing the different approaches of the EU and ASEAN to cyber governance, highlighting areas of convergence and divergence. Furthermore, Tan and Syahirah Azman (2019) specifically examine the EU GDPR's impact on ASEAN data protection law, showing the wide-range effects of EU regulations beyond its borders. This is complemented by Noor's (2018) analysis of ASEAN's steps towards cybersecurity, providing context for understanding how EU influences interact with regional initiatives. As mentioned previously, this research shows how the EU effectively influences the ASEAN cybersecurity policies, namely the data privacy legislation. Therefore, the above-listed author's work is essential supportive literature for my paper.

Feakin, Hawkins, and Nevill (2016) explore the unique challenges and characteristics of cybersecurity in the Asia-Pacific region in their assessment of cyber maturity in the region. Their work provides an important background for understanding the context in which EU influence operates. Molthof's (2012) evaluation of ASEAN's principle of non-interference offers additional insights into the regional dynamics that shape ASEAN's approach to cybersecurity and its openness to external influences.

The research paper of Kasper and Vernygora (2021) gives a detailed examination of the dynamic growth of cybersecurity policy within the European Union (EU). The EU's journey, which began in the mid-1990s with an emphasis on data protection and telecommunications, is characterized by several significant turning points, such as the 2013 Cybersecurity Strategy and the far-reaching 2020 Cybersecurity Strategy for the Digital Decade. Placing great emphasis on an all-inclusive cross-government strategy, the EU presents itself as a normative authority, setting domestic and international agendas. The European Union's dedication to integrated governance and system capabilities is demonstrated by establishing organizations such as the European Network and Information Security Agency (ENISA). Nonetheless, there are difficulties in establishing strategic autonomy, particularly in "hard" cyber defense, which reflects conflicting future visions. Therefore, this historical background is critical for understanding the EU's involvement in defining international cybersecurity standards, giving significant insights for policy analysis, strategic planning, and predicting the EU's stance in global cybersecurity governance talks.

It is important to have the broader context of global cybersecurity governance because it provides an essential background for understanding the EU's role and influence in shaping international cyber norms and policies. Nye's (2014) seminal work on the regime complex for managing global cyber activities offers a thorough framework for understanding the multi-stakeholder nature of global cybersecurity governance. He argues that cybersecurity governance is characterized by a complex ecosystem where regimes sometimes overlap and even compete with state actors, international organizations, private sector entities, and civil society groups. This perspective is crucial for situating the EU's efforts within the broader international context, as it highlights the multiple channels through which the EU can exercise influence. Cyberspace has a unique characteristic of rapid technological change, low barriers to entry, and attribution difficulties, which indeed need a flexible and adaptive governance approach. Nye's "regime complex" model recognizes the diverse array of formal and informal institutions and norms that collectively shape cybersecurity governance, providing a valuable lens through which we are able to analyze the EU's role in global cyber diplomacy and its potential influence on regions like ASEAN.

Moreover, with a particular emphasis on the multi-stakeholder approach, Richard Hill (2014), in his article, offers a clear overview of the main concerns surrounding Internet governance. It explores definitions of the internet, identifies distinctive features, explains the multi-stakeholder method, and evaluates its results. The outcomes highlight the unique characteristics of the internet and offer ways to strengthen governance systems, including giving more weight to established institutions like international organizations. The article's original observations are meant to stimulate more investigation and conversation. This source is particularly relevant to my study on the EU's backing of a multi-stakeholder internet governance strategy and is useful for comparing it to the ASEAN governing style.

In this literature review, I have drawn upon a diverse array of secondary sources to establish the theoretical and empirical foundation for my research. These sources encompass scholarly articles, books, and policy papers that explore the EU's cybersecurity policies, its role as a global regulatory power, and its influence on ASEAN. I have identified key themes, debates, and gaps in the existing literature by critically examining works from authors such as Christou, Bradford, Nye, and others. This comprehensive review has not only informed my understanding of the current state of research but also highlighted areas where my study can make significant contributions to the field of EU-ASEAN cybersecurity relations and global digital governance.

Theoretical Framework

This paper adopts the agenda-setting theory in order to examine the European Union's rising role as a normative leader in cybersecurity and its influence on data privacy regulations in ASEAN. This theoretical framework offers useful perspectives on the EU's position as a worldwide regulatory power and its subsequent influence over other regions. It is crucial to learn how the EU's regulatory mechanism works, especially in order to understand global cybersecurity governance in the fast-evolving digital world.

According to Princen, the agenda-setting theory in the European Union portrays the mechanism via which certain topics gain attention and are regarded as priorities for policymakers (Princen, 2017). Indeed, this process influenced the EU's domestic and foreign cybersecurity policies and deepened ties with ASEAN. According to Sebastiaan Princen, agenda-setting in the EU happens in two main ways. The first is "High politics," in which national political leaders support certain issues to be part of the agenda. The second approach is "low politics," in which communities of experts and advocacy networks are mainly responsible for putting issues on the agenda. Both methods had a significant impact on the cybersecurity field (Princen, 2017). The increased cyberattacks and cyber incidents caught national leaders' attention, while a group of experts always stood for more significant cybersecurity measures. Therefore, these dynamics have greatly shaped the EU's internal approach to cybersecurity and its interaction with ASEAN.

To comprehend the EU's cybersecurity policy-making process and its impact on ASEAN, it is crucial to employ the policy window concept. This concept is borrowed from Kindon's (2011) multiple-stream approach and relates to the circumstances when certain solutions or issues should be put on the agenda. In the case of the EU cybersecurity framework, many vital policy windows can be revealed. First, the increased complexity and frequency of cybercrimes and cyberattacks against EU institutions and member states have generated a sense of urgency. The cyberattacks on Estonia in 2007 and Georgia in 2008 can be a primary example of this, as they alerted many EU policymakers (Christou, 2019). Second, increased sensitive data violations and public concern over it opened a new window for solid data protection regulations, which resulted in the establishment of the General Data Protection Regulation (GDPR) (Fahey, 2014). Finally, the EU's initiative to create a Digital Single Market offered chances to consider cybersecurity an essential element of the trusted digital ecosystem (Bendiek & Pander Maat, 2019). The above-mentioned policy windows influenced both the EU's internal strategies and its cooperation with ASEAN on cybersecurity issues. It also played a crucial part in positioning the EU as a role model for cybersecurity regulations and sensitive data protection. Indeed, the European Union took advantage of this window and enhanced its cybersecurity agenda. Moreover, it demonstrated how policy opportunities can assist in spreading the norms and regulations inside and outside the borders.

The EU institutions and their interactions also played a crucial role in determining the EU's external cybersecurity strategy. Namely, the European Commission has proposed vital cybersecurity legislation along with strategies for cooperating with third countries, including ASEAN (Carrapico & Barrinha, 2017). As for the European Parliament, it notably modified the cybersecurity laws and even pushed for stricter personal data protection, which also impacted the EU's stance in dialogues with the Association of Southeast Asian Nations (Wessel, 2015). The Council of Europe, representing the interests of the member countries, has been very active in negotiations. It balances national security concerns with pan-European approaches to cybersecurity, which is crucial for the EU's united position (Christou, 2019). The interplay among the institutions led to a complete and strong cybersecurity approach. Moreover, it enabled the European Union to establish strategies and policies for combating cybersecurity threats and address the concerns of stakeholders. Furthermore, it gave the EU a chance to become a role model for other regions, including ASEAN.

The European Union's influence goes beyond its borders and presents itself as a leading regulation power. Its relations with ASEAN are a perfect example of the transnational dimension of EU agenda-setting in the cybersecurity area. Also, the EU is actively engaged with different international organizations, such as NATO and the UN, to shape global cyber security norms. Even though indirectly, this engagement has also influenced the ASEAN's approaches toward cyber issues. In addition, the EU has created dialogues with ASEAN and individually with its member states, enabling it to advocate for regulations more directly (Bendiek & Pander Maat, 2019). By creating solid regulations such as GDPR, the European Union presents itself as a norm entrepreneur in the digital sphere and strives for global influence (Bradford, 2020). The ASEAN case is a clear example of the EU’s role as a normative leader in cybersecurity. Moreover, the EU’s GDPR influence on the association’s members can be examined via agenda-setting theory. The European Union facilitated the enforcement of similar regulations in ASEAN through capacity-building and policy transfers (Bradford, 2020). Another important mechanism is the EU’s market size and establishment of GDPR. The market access encouraged ASEAN member states to create data protection legislation if they did not have one and harmonize it with EU standards (Viola de Azevedo Cunha, 2017). Furthermore, the EU’s portrait as a leader in data protection led the association’s members to adopt a similar model on national instances, which shows how the European Union shapes global cybersecurity norms.

According to Princen, the policymakers, apart from gaining attention, should be convinced that the EU is a credible venue for addressing that issue. They should be assured that the EU is a proper venue. This, however, should be backed up by its legal competence, such as having enough expertise and capabilities or no competing venues. The EU came up with the data privacy legislation known as GDPR, which is one of the influential frameworks in the cyber sphere and which showed that the EU was sufficiently equipped to deal with cybersecurity issues. Moreover, by creating a legal base, the European Union ensured it was less controversial and had fewer competitors (Princen, 2017). Again, the positive effect of the EU on ASEAN cybersecurity, specifically member states’ data privacy laws and cyber capacity-building, shows the European Union’s power to leverage its domestic frameworks to promote global cybersecurity norms. The association’s member states and their national PDPAs are actual examples of the EU’s successful influence. Therefore, the ASEAN case study shows that EU agenda-setting greatly and positively impacts global cybersecurity.

Chapter 1. The Tendency of Cyber Politicization

Having established itself as an acute policy issue in the last few decades, cybersecurity has pervaded national security, diplomacy, and people's lives globally. Today, it is possible to observe the intensive application of ICTs in almost all aspects of politics and society. Thus, the need to protect such systems has become not only important for the public sector but also for the private sector as well. However, the concept of cybersecurity itself remains contested, with multiple explanations which open up space for debates. The landscape of cybersecurity is extremely complex and challenging to explore. "There is no single universal understanding of cybersecurity" (Siudak, 2022, p. 319). Currently, it is even harder to regulate cyberspace without the involvement of different actors, such as the EU and NATO, in order to ensure cybersecurity by developing necessary policies. From the original perspective, it has been considered that multiple competing discourses shape cybersecurity policy. Each is framing the issues and solutions in a different way. At the same time, this perspective challenges the dominance of threat-oriented national security narratives that have often characterized cybersecurity discussions in political science and international relations literature (Buchanan, 2017).

In an increasingly interconnected world, where digital technologies permeate all aspects of social, economic, and political life, understanding the diverse discourses shaping cybersecurity policies is cardinal. Generally, we face five key discourses shaping cybersecurity debates in today's world. These dimensions are technical, national security, civil-social, international relations, and economic. Each of these proposes different referent objects, threats, and solutions, leading to varied policy outcomes. As a result, they are contributing to shaping the state's cybersecurity and operating system for critical infrastructure. Due to the rising role of cyberspace in the security domain, a place for debating on cybersecurity has always been opened as the discussion is formed by the ongoing struggles between various discourses (Kaider, 2015). For deeper and more comprehensive research, it is better to explore cybersecurity as a policy area because politics is one of the most influential dimensions when discussing security dynamics.

Cybersecurity as a concept should be defined in various ways. One of them is purely technical, which mentions the practice of finding and fixing some vulnerabilities in the computer system(Dunn Cavelty, 2018). Others explain that in terms of managing the process of alleviating risk against threats in cyberspace (Swinfen Green, 2015). Another view of the term is the dimension of national security, which encompasses the ability of countries to defend themselves from malicious cyber activities, such as cyberwarfare, digital espionage, cyber crime, etc. Threats coming from cyberspace are almost always cross-border, so cyberattacks on one facility might cause damage to others simultaneously. This is why it is so hard to fight and shape a specific approach in order to tackle all coming cyber threats. However, prominent actors in the security field are trying to counter it and create common norms to fight against it. Countries are developing and adopting different policies and regulations against cyber threats to be more responsible. For prominent actors, such as the European Union, it is crucial to work and cooperate with counterparts by sharing information and experience. In this matter, the EU evolves some policies and supervises member states to maintain security in the cyber landscape. Considering the scale, cybersecurity is one of the largest fields on the market. It is undisputed that risks and threats ought to be mitigated, at least on a national level.

However, fighting alone in this field mentioned above is risky and even meant to be losing. The European Union is one of the actors that take steps toward cyber threats, and even though it develops policies for member states, it is involved in global initiatives and, at the same time, sharing good practices and supporting partners. For its member states, the EU has come up with different initiatives such as Cybersecurity and Cyber Solidarity acts, which aim to improve response to cyber threats and step up at the operational level as well as in crisis management overall. Shaping the space where different actors will share their experiences is the best practice for tackling cyber threats, as it is a complex issue requiring strong governmental bodies to address it immediately.

The tendency to politicize cyber refers to the growing integration of cybersecurity topics and issues into decision-making processes and political debates. This tendency gained massive attention because digital technologies are becoming more involved in national security and economic relations. Cyber Politicization may take many forms, portraying cyber threats as a national security concern and even integrating them into foreign policy agendas (Dunn Cavelty, 2013). This tendency has also influenced the sphere of international affairs. According to political scientists, this phenomenon also fueled the debates regarding digital governance and its sovereignty over state-sponsored cybercrimes, which also contributed to developing national cybersecurity strategies (Barrinha & Renard, 2020). Moreover, this created a new demand for a governance model that addresses newly emerged cyber threats (Nye, 2014). Besides the governing style, new initiatives and frameworks were adopted to address the cyber challenges. Therefore, the following chapters discuss those regulations initiated by the EU and explain their influence on other regions.

Chapter 2. Cybersecurity Trajectory and Regulatory Landscape of EU

Early Beginnings

Technological advancements and increased reliance in the late 1990s have increased cyber threats. Therefore, protecting personal information and critical infrastructure has become important. However, it took quite a while for the European Union to use the concept of cybersecurity in their official documents. The first encounter happened in 2001 within Network and Information Security: Proposal for A European Policy Approach. This paper served as a foundation for the EU's emerging approach to cybersecurity and showed the need for new mechanisms to protect member state's networks and information systems. Other important events, such as the establishment of the European Network and Information Security Agency in 2004, followed this process. However, the cyberattacks on Estonia in 2007 and Georgia in 2008 turned out to be a wake-up call for the European Union. Even though Estonia at that time held the status of a digitally advanced state, the cyber intrusions caused significant damage. Especially in the banking system, government websites, and media outlets (Traynor, 2007). This was when the EU realized it underscored the massive danger of cyberattacks and that firm counter-measures and cooperation were necessary. Therefore, the EU began to enforce a more developed approach to cybersecurity. Namely, in 2013, it adopted the first EU Cybersecurity Strategy outlining its vision and priorities (*EUR-Lex - 52013JC0001,* 2013). The Cooperation Group and the Computer Security Incident Response Teams (CSRTs) were created using this strategy. Later, it was followed by the NIS Directive of 2016 and the European Cybersecurity Act of 2019. All these essential strategies and regulations are briefly discussed in the following section. It allows us to understand the evolution of cybersecurity policies in the EU and later compare them with ASEAN.

Key Regulations and Strategies

The European Union in 2018 adopted a Data protection law known as the *General Data Protection Regulation* (GDPR). It is clear that with the rise of technology, concerns over privacy and data protection increases, and therefore, this law is important to grant citizens more control of their own rights. The GDPR strongly restricts data subjects and entities from processing all sensitive information. Some of its key features are as follows: The extraterritorial nature of the law means that it applies to any entities that process the data of EU residents, no matter their location (GDPR, 2016). Failure to do so can result in heavy fines, namely up to 4% of their total global turnover or €20 million, whichever is more prominent. The GDPR also obliges companies to ask for approval from individuals, and respectively, individuals also have the right to erasure, access, correct, and restrict the procession of their sensitive information. Furthermore, GDPR also obliges certain organizations to have Data Protection Officers (DPOs) to ensure that the institutions are following the rules. The General Data Protection Regulation is one of the significant pieces of legislation in the cyber domain. Not only does it guarantee the protection of the residents' sensitive data, but it is also a role model for the rest of the world to harmonize their respective laws or create new ones (Voigt & Bussche, 2017).

The Digital Operational Resilience Act (DORA) is a regulation of the European Union that helps the financial service industry secure its digital security and continue doing business safely. The primary purpose of DORA is to strengthen the resilience and recovery of financial bodies, including banks, insurance companies, and investment firms, so that they can quickly recover from cyber incidents. To address this, DORA proposes an all-encompassing framework that outlines guidelines for handling and avoiding ICT risks for financial firms. This includes having ICT risk management systems as well as incident reporting mechanisms and regularly exercising ICT systems and procedures. Third-party risk management is another aspect the proposed regulation underlines because financial entities often rely on outside ICT service providers. This means that under DORA, outsourcing arrangements that expose financial entities to certain risks must be monitored and managed successfully. In addition, DORA seeks to enable effective cooperation between the different financial entities and supervisory authorities, as well as other entities that may be interested in the matter. This is possible by setting up a single EU-level body with supervisory powers and encouraging communication and cooperation in the financial sector (Clausmeier, 2022).

Another important framework that the European Union created is the *Cyber Diplomacy Toolbox.* It is a model that defines strategies for combating and responding to malicious cyber operations. It aims to promote international cooperation, norms of responsible state behavior in cyberspace, and the resilience of critical infrastructure. The toolbox contains a range of diplomatic, political, and technical instruments that may be used for prevention and response to cyber risks. These measures include both preventive and restrictive measures. The first one covers policies, such as capacity-building and confidence-building measures, as well as reactive tools like public statements, diplomatic démarches, and the former - sanctions. This framework also allows the European Union to have a coordinated and proportionate response to cyber incidents depending on the events and political environment. The Cyber Diplomacy Toolbox shows how important cybersecurity is in the international arena. As cyber challenges grow daily, the document also draws attention to the need for an inclusive approach to addressing these issues. Moreover, it presents the European Union as a key actor that seeks to establish and protect the rules-based order in cyberspace (Rehrl, 2019).

The European Union has implemented several cybersecurity laws that, with the use of EU directives and regulations, aim to establish an inclusive and powerful policy framework and institutional structure. Within European Union law, these are distinct legislative actions implemented per one of the legislative processes outlined in the EU treaties. These directives serve as guidelines that lay out the specific goals or outcomes that member states must accomplish, but this document also takes into account different national circumstances and allows each state significant autonomy in determining what measures or tactics they can employ (Benincasa, 2020). Moreover, they have a certain time limit under which member states are required to integrate the specified measures into their domestic legislation. On the contrary, regulations are legislative measures that, once they become effective, are binding and consistently applicable to all EU countries. Currently, the only institution in the EU that has the power to introduce new laws is the European Commission. On the other hand, the European Parliament (EP) and Council of the EU are able to approve legislation and retain the right to amend and reject legislation at each step of the legislative process. Additionally, there are two key influencers of the EU cybersecurity governance: The Directive of Security of Network and Information Systems (the NIS Directive) and the 2019 Cybersecurity Act. These two critical legislations created new organizations and laid down standardized procedures (Benincasa, 2020).

The NIS Directive is regarded as the backbone of the European Union's cybersecurity legislation. As the European Commission holds the initiative power, it enforced the NIS Directive in 2016 and gave the member states a two-year time frame. At the national level there are several vital components to mention: *Identification of OES* - the member states are responsible for finding operators of essential services. In this context, the essential services are the ones that are crucial for social and economic activities and may also cause disruption. *Development of a national cybersecurity strategy* - the member states are required to have proper guidelines that define the roles of the network actor, aims, strategies for recovery measures as well as risk assessment plans. *Founding National Competent Authorities (NCAs) and single points of contact (SPoCs)* - states must create designated agencies that can also include other ministries and intelligence services and that are responsible for cross-border issues, incident response, and monitoring. *Establish a Computer Security Incident Response Team (CSIRT or CERT)* - with the major task of controlling security incidents as well as providing early warnings with risk analysis (Council Directive 2016/1148).

The NIS directive also highlights the two major platforms for cross-border cooperation. The first one is composed of member states CSIRTs and CERT-EU and is called the Computer Security Incident Response Teams (CSIRTs) Network. It is a forum where different entities voluntarily exchange information and work together for incident response and other cyber issues. The second one, the Cooperation Group, includes the representatives from the European Commission and ENISA. This group serves as a knowledge provider as it guides states and allows them to share their own best practices with each other (Council Directive 2016/1148).

In 2023, a more improved version of the NSI Directive came into force, known as NIS2. According to the European Union Agency For Cybersecurity, this new directive has developed the EU's cybersecurity status in many different ways. Namely, it creates a cyber crisis management structure (CyCLONe); encourages the member countries to develop a new sphere of interest in the supply chain, cyber hygiene, and vulnerability management, and suggests employing a peer review mechanism to develop collaboration and knowledge exchange between members; also the new directive covers more socio-economic bodies which means more entities are obliged to take specific measures of cybersecurity. From now on, NIS2 will also equip ENISA with new tasks, such as being the secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe). ENISA will also have to publish annual reports on the cybersecurity environment in the EU as well as organize the previously mentioned peer reviews between states. Additionally, ENISA will be responsible for maintaining the European vulnerability registry and registry for entities providing cross-border services. The NIS and NIS2 Directives together have a preventive nature (ENISA, 2023).

Another vital piece that significantly contributed to the development of the EU cybersecurity framework is the EU Cybersecurity Act adopted in 2019. It expanded ENISA's legal remit by boosting its status and funding and established a European cybersecurity certification scheme for products, services, and processes (European Parliament Regulation 2019/881). As mentioned previously, ENISA's primary goal is to increase operational collaboration within the EU level. This means that in case the member states cannot deal with cyber incidents, they can always ask for help from ENISA. It also takes part in large-scale cross-border cyberattacks. Apart from this, ENISA engages with different groups and relevant stakeholders to create the drafts of the cybersecurity certification scheme. Therefore, it is a creator of common requirements and evaluation criteria that are part of the EU certification framework. The Cybersecurity Act also created the European Cybersecurity Certification Group (ECCG). The members of this group are the representatives of the national cybersecurity certification team and Stakeholder Cybersecurity Certification Group (SCCG) that give advice to ENISA and EC, respectively (Benincasa, 2020).

The European Union, under its law enforcement and judicial institutions, created EUROPOL and EUROJUST, which have a responsive nature. Later, these institutions will be compared to the ones from ASEAN. EC3 plays a crucial role as it is a bridge between law enforcement agencies and the private sector. Besides coordinating these relations, EC3 is a focal point in the fight against cybercrime. On the other hand, ECJN serves as a practice and knowledge exchange between the judicial authorities. It helps them during the investigation process so that the prosecution is successful. Additionally, there are Joint Investigation Teams (JITs) that, with EUROJUST, conduct transnational crimes. EUROPOL and EUROJUST have a joint project known as SIRIUS, and they help investigators with e-evidence and provide tools for them (Benincasa, 2020).

Nowadays, the EU's digital regulations pay great attention to cybersecurity. They prioritize privacy data protection along with digital resilience. For this reason, the EU established influential measures like GDPR and NIS Directive that create the standards for other cyber actors. The Digital Operational Resilience Act further strengthens cybersecurity in the banking and financial sector. The initiatives and regulations, as mentioned above, aim to create an open, secure digital environment not only for the EU but for the whole world.

Chapter 3. ASEAN and Cyberspace

ASEAN's Positioning and Engagement in Cyberspace

The Association of Southeast Asian Nations (ASEAN), which consists of ten Southeast Asian states, is distinguished by an elevated degree of economic heterogeneity. This attribute is entirely mirrored in the region's governments' maturity concerning the sectoral development of information and communication technologies (ICT), adoption of computerized goods, and expansion of the digital economy. As a result of diverse political regimes, different political will, and dedication of the member states, the Association developed a vast range of approaches towards cyber policy and security, equaling cyber maturity. In contrast to Myanmar, which is more focused on setting protective measures for national infrastructure and, in reality, needs to enhance its cyber maturity**,** Singapore, a nation with a high capacity for cyber maturity, is more prone to push for adoption regulations, capacity-building initiatives, and different cyber policy elements. Therefore, commitment to cyber policy issues in this region is heavily influenced by the cyber maturity of each state. According to the International Cyber Policy Center's (ICPC) report on cyber maturity in the Asia-Pacific region at the Australian Strategic Policy Institute, the extensive majority of states fall in the medium-level category, while Singapore occupies the high status, followed by Malaysia, Thailand (above the average range), Indonesia, Philippines, Brunei and Vietnam. Furthermore, Laos, Myanmar, and Cambodia are completing the list (Feakin et al., 2016).

Even though this report presents the fundamental disparity between the member states, the broader sub-regional initiative under the ASEAN framework shows that these nations have been working hard to enforce a joint vision of digital adoption and digital transformation. This common goal was foreseen in the early 2000s and set in November 2000, when member states signed the e-ASEAN Framework Agreement. The document aspired to trade liberalization in ICT products and services, the advancement of e-commerce, and the strengthening of ICT infrastructure construction in the region. Since that day, ASEAN has undertaken a consistent effort to advance and enhance the 'connectivity' of the region (ASEAN 2011, 2015). Additionally, on December 31, 2015, they established the ASEAN Economic Community (AEC), making the above imperative more crucial.

This, along with solid aspiration in the digital sphere, constitutes the integration of SouthEast Asia. Looking closely at ASEAN's approach to the digital domain, it is clear that issues concerning cyberspace have a more economic tone than political security, making this association even more appealing to foreign institutions such as the European Union (Tran Dai & Gomez, 2018).

The Region is ambitious and displays favorable conditions for developing digital economies and societies. It also encompasses significant digital potential that can enable the growth of the e-economy, for which, however, digital confidence is essential. ASEAN has only recently begun to tackle cybersecurity issues, personal data protection, and privacy at the regional level, while at the national instances, the strategies and capabilities of each nation vary. The region has also faced a few wake-up calls in recent years, mainly with cyber criminality, espionage, hacktivism, and notable cyber incidents.

It should be noted that cyber threats are not isolated from political, geopolitical, and economic realities; more importantly, they often represent either escalation or extension of the previous tensions or conflicts (Tran Dai & Gomez, 2018). Thus, cyberspace can be seen as a revealing element of the region's dynamics. In South East Asia, these kinetics are mainly influenced by three contextual factors. First concerns the increase of digitized economies; second - growing military expenditure and modernization of armies; and third - territorial conflicts, which evolve into geopolitical tension. The region's economic prosperity seems to become attractive to cyber threats that are driven by economic competition and desire for financial gain. Bearing in mind that the fast development of the Web Economy and societies in the association has increased reliance on ICT for Economic means. Hence, for some members, information and communication technologies have already been integrated into their socio-economic plan. Apart from an economic point of view, military expenditure has notably increased around the region. Which points toward geopolitical tensions related to the South China Sea and not only. This unfavorable military-political environment complicates the situation by encouraging patriotic hackers who act independently to get involved. Above all, in the region, the absence of regulative mechanisms of state behavior in cyberspace poses a massive threat to countries' economic and political stability (Tran Dai & Gomez, 2018).

It is quite a challenging scenario for Southeast Asia to maintain its goal of growing the digital economy and safeguarding cyberspace. Nevertheless, cybersecurity has been addressed at the regional level since the early 2000s. More specifically, in 2003, during the third meeting of Ministers of Telecommunications and Information Technology (TELMIN), the Singapore Declaration underlined the importance and the need to establish ASEAN's information infrastructure (ASEAN, 2003). Moreover, the meeting's main objective was to encourage the region's networks to be interconnected, secure, and reliable. Initially, the association's policy on cyberspace and its protection was based on regional cooperation, through which the national system became more resilient. Developing national cybersecurity capabilities remains one of the key priorities in this respect; however, in recent years, the ideas of a regional approach to cybersecurity have become prevailing. The ASEAN ICT Master Plan 2015 also mandated an integrated framework for network safety and the establishment of the ASEAN Network Security Action Council (ANSAC) (ASEAN, 2015).

Moreover, the association places a significant value on enforcing confidence-building measures (CBMs). Since 2004, the ASEAN Regional Forum (AFR) has been very active in this field and has hosted conferences, seminars, and workshops regarding cyber incident response, national capacity-building, cyber terrorism, cyber espionage, and other threats (AFR, 2012). It could be seen that the forum has a genuine desire to operationalize cyber confidence-building measures. Furthermore, cybercrime was placed among the eight priorities during the ASEAN Ministerial Meeting on Transnational Crime (AMMTC). Eventually, the regional cooperation directed toward cyber issues is concentrated on strengthening national capabilities while mobilizing joint forces to fight against cyber threats and keep the digital economic development of the whole region secure. Thus, building capacity continues to play a crucial role as it supports the development of stakeholders' abilities so they can respond appropriately to emerging cyber trends and keep up resources.

Several events have also highlighted a vital turning point in the association's approach to cyberspace. Back in May 2016, in Vientiane, Laos, at the ASEAN Defence Ministers Meeting (ADMM), a cybersecurity working group named the ADMM-Plus Experts (proposed by the Philippines) was established (Tran Dai & Gomez, 2018). The following years can be characterized as digitally transformative for the member states. 2018-2019 is regarded as the Digital ASEAN

Initiative era, which was launched by the World Economic Forum. Namely, in November 2018, in Bangkok, the ASEAN Digital Skill Vision 2020 was established. Its main goal was to equip the ASEAN workforce with the necessary digital skills through training. Over 16 million people, including general workers, students, and broader citizens, were trained by 23 different organizations (World Economic Forum, n.d.). A year later, in March 2019, the ASEAN e-Payments Coalition was created. Its main objective was facilitating smooth and secure cross-border e-commerce transactions and developing a more harmonious digital payment framework. Such an initiative is directed toward the economic integration of the whole region, which also interconnects its association with the global digital world (World Economic Forum, n.d.). This initiative was followed by various capacity-building programs supporting the cybersecurity framework of the association, as well as addressing issues concerning cyber threats and enhancing awareness among the states.

Moreover, from 2019 onwards, topics such as cross-border data flows have become significant. ASEAN Framework on Digital Data Governance came into force, which comprises mechanisms like ASEAN Certification and supports the harmonization of data exchange and data privacy within the region. Against this backdrop, the main aim of these initiatives was economically motivated to enhance e-business and the integration of the region (The ASEAN Magazine, 2022). Since 2021, the ASEAN Cybersecurity Task Force has mainly focused on cyber intelligence sharing and collaborative aspects. These initiatives are beneficial for member states as they improve their collective ability to detect, prevent, and respond to cyber threats; therefore, they are highlighted in the ASEAN Cybersecurity Cooperation Strategy of 2021-2025 (ASEAN, 2022). The endeavors mentioned above serve as proof of ASEAN’s proactive stance towards the cyber domain and its security. The Association is actively laying the groundwork for a more interconnected digital economy by improving the digital skills of the region’s population, integrating e-payments, and advancing capacity building and data governance. The association’s efforts are empowering the region’s resilience and raising global digital competitiveness (Tran Dai & Gomez, 2018).

ASEAN Cybersecurity Mechanism

A considerable number of ASEAN sectoral institutions and ASEAN-led mechanisms have been working on improving cyber policies and cyber security. Among them worth mentioning are the ASEAN Digital Minister's Meeting (ADGMIN) along with the ASEAN Digital Senior Official's Meeting (ADGSOM), the ASEAN Regional Forum (ARF), the ASEAN Defence Minister's Meeting (ADMM), the East Asia Summit (EAS) and the ASEAN Ministerial Meeting on Transnational Crime (AMMTC). The last one has the mandate to discuss and consult about cybercrime. Within this framework, back in 2017, the association adopted the Declaration to Prevent and Combat Cybercrime. In the same year, due to the rise in cyber threats toward the region, the ASEAN Regional Forum launched the ARF Inter-Sessional Meeting on Security of and in the Use of ICTs (Sari, 2023). It is a platform used by the ARF members to promote trust and confidence via capacity building, foster mutual trust, and carry out the ARF Work Plan on Security of and in the Use of ICTs. In order to direct the work of the Information Security Manual (ISM) on ICTs, in 2015, the Plan on Security of and in the Use of ICTs came into force. Again, this framework uses capacity building to promote a peaceful, open, secure, and cooperative ICT environment. It also helps to prevent cyber conflicts by improving transparency and confidence-building measures. Moreover, in September 2020, ARF adopted "ARFT Terminology in the Field of Security of and in the use of ICTs," enabling member states to share their domestic perspectives and definitions of essential terms linked to ICTs (Sari, 2023).

Turning toward the ASEAN Digital Minister's Meeting (ADGMIN), they supervise the mechanism of cybersecurity initiatives, which the ASEAN Economic Community runs. This instrument was previously known as the ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN); however, in 2019, the name was changed to mirror ICT ministers' expanding scope and responsibilities beyond the ASEAN (ASEAN Secretariat, n.d.). A few years later, in 2021, the concept papers regarding the ASEAN Cyber Defence Network and the ADMM Cybersecurity and Information Center of Excellence were accepted as significant steps in encouraging real-world cybersecurity collaboration in the association. These initiatives are fostering confidence-building measures across the region, and the ASEAN wishes to inspire other nations to take similar actions and facilitate a peaceful cyber environment at the global level (Sari, 2023).

Within the three pillars of ASEAN, with the objective of promoting discussions on cybersecurity cooperation, the association has several cyber-related mechanisms and institutions in place. Since the cyber domain is a multidisciplinary topic, in 2020, the association decided to form the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) and handle issues such as coordination, promote cross-pillar and cross-sectoral collaboration, and enhance the broad cyber security in the region. To support this new mechanism and assist with eleven non-binding, voluntary norms that concern the State Behaviour in the use of ICTs, the association is now working hard on prioritizing and developing a Regional Action Plan on implementing the Norms of Responsible State Behaviour in Cyberspace. The above-mentioned sectoral bodies of the ASEAN are not just simply producing the Chairman's statement or enforcing agreed documents. Indeed, numerous informal and side-line interactions occur in this so-called diplomatic ecosystem, which is held regularly and hosts officials and regional leaders. All these meetings generate a sense of familiarity and foster the mentality of a give-and-take approach, which translates into solving complex issues with consensus. Moreover, these mechanisms are regarded as a forum for discussing cyber-related topics with the member states and foreign partners (Sari, 2023).

ASEAN Regional Cybersecurity Framework

The above text mentioned the different important initiatives; however, it is essential to highlight some of the additional regional frameworks. First, the association, in response to the new cyber challenges in the region, has modified its cybersecurity cooperation strategy. Strengthening regional efforts to secure the cyber domain and promoting the development of the digital economy with its community is well reflected in the ASEAN Cybersecurity Cooperation Strategy 2021-2025. The updated version of this document covers the following topics: 1. advancing cyber readiness cooperation, 2. strengthening regional cyber policy coordination, 3. enhancing trust in cyberspace, 4. regional capacity building, and 5. international cooperation (ASEAN, 2022).

It is extremely important to mention that the ASEAN is the only regional organization subscribing to the United Nations' principle 11 concerning the non-binding norms of responsible state behavior in cyberspace. This is a crucial step toward ASEAN's proactive role in safeguarding cyberspace.

Against this backdrop, the association is forming the ASEAN Regional Plan on the IMplementation of UNGGE Norms of Responsible State Behaviour in Cyberspace. This initiative is divided into different focus areas: cybercrime legislation, incident response and coordination, awareness-rising, policy development, and founding a reliable ecosystem. This plan acts as a valuable guide in implementing norms for the association, and the member states now have a better understanding of critical cybersecurity challenges (ASEAN, 2022).

Lastly, the association is creating the ASEAN Regional Computer Emergency Response Team (CERT) and ASEAN CERT Information Exchange Mechanism. The member states have acknowledged the urgency of protecting the growing digital economy, especially in times of massive trans-border cyber attacks. Thus, ASEAN CERT will be a valuable asset to the region's security as it will enable the timely exchange of critical information (cyber threat and attack-related) between member nations and CERT representatives (ASEAN, 2022).

Adopting and implementing the cyber norms in ASEAN requires overcoming several regional challenges. As previously stated, the region is encompassed by mosaic states with various political and economic regimes and diverse cyber capabilities. However, due to distinct approaches to cyber threats and cybersecurity, which are merely characterized by disparities in the perception of the cyber domain and cyberspace, regional variation forms obstacles to cyber governance. The cybersphere is becoming an arena where states exhibit their unique visions and ambitions. Furthermore, the character of political regimes and their approaches toward the information flow can be mirrored in diverse strategies of online content control and censorship politics in the member states. In their work about "Challenges and Opportunities for Cyber Norms in ASEAN," Tran Dai and Miguel Alberto Gomez doubt the association would reach a joint position. They argue that due to the non-interference principle in the internal affairs of member states, harmony over this issue would not be possible (Tran Dai & Gomez, 2018). However, this paper proves otherwise and shows how EU regulatory influence changes the ASEAN's atmosphere. A more detailed explanations of EU-ASEAN cyber relations are presented in the following section.

When discussing limitations, the question arises of whether the "ASEAN way" is helpful in addressing cybersecurity issues. In addition, as reported by the ITU Global Cybersecurity Index

(GCI) 2020, the disparities among member states range from 4 to 131 among a total of 194 countries (Table 1) (ITU, 2020). Furthermore, the association states have not allocated enough funds to close the investment gaps or maintain a cybersecurity domain commitment. To delve into more detail, according to A.T. Kearney's assessment, from 2017 through 2025, the member states should allocate between 0.35 and 0.61 percent of their GDP, or US$171 billion, to cybersecurity to ensure the investment gap is closed and ensure the successive commitment to the cyber field (Cisco & A.T. Kearney, 2018). Following Palo Alto Network's report on the State of Cyber Security in ASEAN 2020, cybersecurity has become a high-priority concern among many ASEAN businesses. Namely, 92% of them are convinced that the area should be prioritized in their industries due to the increased number of cyber attacks and threats. As stated by the survey, in 2019, the security expenditures increased for most of the ASEAN organizations. Indeed, most of them (46%) distributed much of their IT budgets to cybersecurity. It is crucial to highlight one of the biggest jumps in ASEAN history between 2019 and 2020. In particular, more than half (53%) of Singaporean enterprises spent over half their IT budgets on cybersecurity, while 84% of Indonesian business firms increased their cybersecurity funding (Palo Alto Networks, 2020). Turning more toward the member state's governments, Singapore, as a leading country in cyber maturity, for its 2020-2023 budget, has set aside US$1 billion to enhance the government's cyber capabilities and security measures (Lim Min Zhang, 2020). Meanwhile, in 2021, for cyber capacity building, Malaysia set aside US$6 million (Yeoh, 2020), and Indonesia provided US$ 89 million for ICT development (Indonesia Ministry of Finance, 2020). These numbers seem very promising. However, the other member nations have not allocated an identical ratio of their cybersecurity budgets.

The range of approaches to cyber challenges also reflects both the human and financial resources that member states have at their disposal. It is essential to highlight the diverse political will of the states. Not all of them prioritize the same cyber issues nor share similar objectives. Some members may be willing to concentrate on certain cyber aspects, such as safeguarding information infrastructures, or work more on regulatory frameworks. In contrast, others favor to stress on a different aspect of the cyber security industry and the organization of military cyber command. As mentioned during the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), finding shared objectives and priorities is crucial, as cyberspace happens to be one of the priorities among the other eight (Tran Dai & Gomez, 2018).

It was said before that one potential obstacle might be the value of non-interference in domestic matters, though the principle of consensus in decision-making procedures might complicate things more. In order to make decisions based on the consensus principle, the member nations must come to an understanding of a shared cyber identity and set of common expectations for the cyber domain. For the sake of consensus, countries may abide by the rules and guidelines. In the worst-case scenario, this may lead to following norms without fully comprehending them. Needless to say, the mistrust toward the supranational institution, as well as poor coordination and compliance mechanisms for decision implementation, lead to the fact that decisions taken on the regional level in most cases still depend on their successful implementation and regulatory translation at the national level. Therefore, persuading ASEAN members to follow the guidelines might be challenging.

In recent years, national security issues have heavily influenced cyber governance as state-sponsored cyber crimes and espionage have become increasingly prominent. This tendency is not new to ASEAN, though most members have recently begun to recognize the strategic significance of the cyber domain. Strong nationalism still dominates in Southeast Asia, and ASEAN has always respected preserving national sovereignty (Molthof, 2012). Therefore, within this framework, the development and implementation of cyber norms - specifying appropriate state conduct in cyberspace will definitely rely on the genuine political willingness of member nations (Tran Dai & Gomez, 2018). Nonetheless, we should not forget successful past decisions. In 2018, the association adopted the ASEAN Plan of Action to Prevent and Counter the Rise of Radicalization and Violent Extremism to address cross-border cyber threats. This work plan outlined the vital objectives and priority spheres and called for the creation of a particular agency responsible for terrorism reduction in the region (ASEAN, 2019).

Chapter 4. Cybersecurity Chronicles: Unveiling EU and ASEAN Policies

Connecting Nodes: EU-ASEAN Relations

The relationship between the European Union (EU) and the Association of Southeast Asian Nations (ASEAN) dates back to 1972. The longstanding partnership started with informal cooperation and has, over time, enlarged in scope and depth. In the process of diminishing the Soviet Union's influence in the region and, at the same time, developing its foreign policy image, the European Community transformed this casual interaction into eco-political cooperation. Even though both parties condemned Vietnam's invasion of Cambodia in 1975, it did not delete the fact that they still had very distinct and opposing ideologies (Flers, 2010).

On March 7, 1980, the two organizations signed an agreement in Kuala Lumpur to expand their economic and political relations. This year has been described as a favorable period during which the Cold War and US troop withdrawal from Vietnam allowed the European Community to be more actively involved in the region (Forster, 2000). The European Community tactically used its chance and began supporting authoritarian nations regardless of their stance. Although this event improved the relations between the two groups, the developmental aid recipient states were still transformed into less powerful negotiators (Flers, 2010).

At the end of the 1990s, the relationship between the two organizations significantly improved when, eventually, the EU took a more practical approach and delved into the region's economic potential. This economic focus was also documented in the EU's paper - "Towards a New Asia Strategy." Moreover, Singapore's Prime Minister Goh Chok Tong suggested creating a non-formal platform called the Asia-Europe Meeting (ASEM), which allowed leaders of both regions to expand their relationships and foster cooperation. Obviously, the EU benefited a lot from this initiative given its absence from other regional conferences (Hwee, 2010). Several political changes, namely Indonesia's democratization, gave the EU an opportunity for more engagement. Furthermore, September 11, 2001, highlighted the importance of addressing non-traditional security concerns together (at that time, pollution, terrorism, and piracy). In 2003, the relations from simple economic objectives shifted to non-traditional security (Abdul Rahman, 2022).

In Bandar Seri Begawan (Brunei), in April 2012, the two organizations agreed to enforce a five-year Plan of Action that defined the guidelines to enhance communications between the parties. This document expands on the 2007-2012 ASEAN-EU Plan of Action to adopt the Nuremberg Declaration on an EU-ASEAN Enhanced Partnership. The EU's desire to connect more with the association is well reflected in the new plan, as it mainly focuses on various topics beyond trade. Although it attempts to formalize the partnership by listing socio-cultural and politico-security initiatives and programs on which both sides can work together, it does not entirely represent a major step toward new collaboration. Besides the yearly EU-ASEAN Foreign Ministers Meeting, the parties have established another annual review mechanism, which is carried out via the ASEAN-EU Joint Cooperation Committee (JCC) and the ASEAN-EU Senior Officials Meeting (SOM). February 2014 counts as the first meeting in Brussels for the EU and ASEAN Committees of Permanent Representatives. The partnership enters into a new chapter with the Bandar Seri Begawan Plan of Action, which recognizes the notable developments on both sides, mainly with regard to ASEAN's regional integration objectives, which cover the ASEAN Community by 2015 and beyond (Wong, 2019).

The EU started supporting ASEAN in fields such as the fight against organized crime, piracy, migration, and human rights. With this, the EU proved its understanding of the importance of political stability and prosperity in the region (Wong, 2019). In order to facilitate the sharing of best practices and expertise in fighting against human trafficking and migrant smuggling, ASEANPOL and EUROPOL signed a letter of Intent in 2016. Against this backdrop, in 2018, the two organizations met in Hanoi to strengthen collaboration under the EURASEAN Investigative Network on Payment Card Fraud, which strives to combat organized cyber fraud from groups with European origins setting up cells in Asia (Abdul Rahman, 2022).

The traditional type of cooperation occasionally incorporates new dimensions of issues. From 2018 to 2020, the EU, Vietnam, and Australia co-chaired the ASEAN Regional Forum (ARF) on maritime security. Moreover, the two organizations enforced the Statement of Cybersecurity

Cooperation in 2019, covering information and cybersecurity topics. Due to recently emerging cyber threats and crimes, they adopted the initiative in a timely manner. According to the 23rd ASEAN-EU Ministerial Meeting (AEMM) in December 2020, the EU has actively supported the Association of Southeast Asian Nations in dealing with maritime security, terrorism, transnational crimes, and cybersecurity (Abdul Rahman, 2022).

Since the early 2010s, EU-ASEAN cyber relations have greatly improved, culminating in the adoption of the EU-ASEAN Dialogue on Cybersecurity in 2019. The dialogue allows for information exchanges on cyber practices, initiatives, and policies. Crucial projects include the ASEAN Cyber Capacity Programme (ACCP) and Enhanced EU-ASEAN Dialogue Instrument (E-READI), which aims to improve members' cyber capabilities and capacity-building skills. While discussing cyber relations between these organizations, it is essential to point out the EU-Singapore Digital Partnership, which sets the standard for broader regional involvement and demonstrates a close partnership on digital economy and cyber resilience. Furthermore, the EU's support for ASEAN's cybersecurity strategy is visible in different fields, such as intelligence sharing, joint drills, and cyber incident response. The advanced AI and IoT security technologies are also the subject of joint research funded by programs like Horizon 2020. All in all, the EU's participation in advancing stability and security is highlighted by its contributions to the ARF. Besides, public-private collaborations are essential for comprehensive strategies (to tackle cyber threats) and strong cyberinfrastructure development, which covers relations between the private and public sectors and academia. These initiatives demonstrate the shared objective of founding a safe and resilient digital space (EEAS, 2019).

Starting from a narrow focus on economic partnership and market access, the EU-ASEAN partnership nowadays covers political, security, and cyber dialogues and participation in Ministerial and other types of dialogues. Thus, the EU and the ASEAN have dynamic relations which advance as both organizations grow. Moreover, it opens up many possibilities for creativity and innovation. The value parallels of identity and aspirations between the two bodies, with the addition of both groups advocating for regional cooperation, served as a foundation for the development of their partnership. Despite employing different approaches to regional integration, both parties aim to enhance the region's security, stability, and economic prosperity. Also, the

European projects serve as an inspiration for ASEAN due to its advanced status. The regional integration cooperation can be regarded as a bastion of EU-ASEAN relations. It is noteworthy that the EU is not only a financial sponsor for the ASEAN, but it has also mentored and supported the association via practice exchanges and various projects. Consequently, the Association of Southeast Asian Nations today is regarded as the most progressive regional organization globally, of course, after the European Union (Khandekar, n.d.).

Cyber Policy Perspectives: EU-ASEAN Comparison

Cyberspace in the ASEAN and EU faces several dilemmas and difficulties that can only be managed through well-thought-out action plans, joint response, sufficient institutions, institutions, and shared positions on vital concerns. Therefore, implementing a regional cybersecurity strategy is an essential component. According to Michael Watkins, IMD Business School professor of Leadership and Organizational Change, strategy is a prerequisite for the desired pattern of decision-making as it allows the guiding principles to be communicated and enforced (Watkins, 2007). Based on the series of guiding principles and preferences, it offers a clearly arranged path that identifies the process's participants as well as their individual or collective actions in light of available resources. In the case of cybersecurity, the regional framework should cover the critical role of vital cyber actors, such as the member states and the private sector. This type of arrangement is especially essential for both the EU and ASEAN as member states whose regional integration levels are different still maintain the majority of decision-making authority, and most network and information systems remain privately owned and run.

EU Cybersecurity Sheme: "An open, safe, and secure cyberspace"

In order to guarantee an open, reliable, and secure cyberspace in the EU, in 2013, the European Commission established fundamental principles and objectives. This document identified the roles and obligations of the member states, EU agencies, the private sector, and academia (EUR-Lex, 2013). It consists of five main objectives:

Achieving cyber resilience: According to this first EU strategy, the main goals are as follows: increasing awareness and strengthening capacity and partnership building among public and private authorities. More precisely, it aims to create a robust regional architecture through which the member nations can boost their national capabilities and deepen their strategic and technological relations. Moreover, with the emphasis on founding effective incentive programs it encourages private businesses to invest more in security solutions. In this part, the EC also mentions the significance of private and public sector cooperation, as most network and information platforms are privately owned (EUR-Lex, 2013).

Following this trend, the Network and Information Security (NIS) Directive was adopted in 2016, becoming the first legislation on EU-wide cybersecurity. The document concerned the topics of cross-border cooperation, national capacity-building, and domestic regulation of crucial sectors. The EU took another brave step in 2019 by passing the Cybersecurity Act, which further strengthened the authority of ENISA, the Cybersecurity Agency, which is in charge of cyber response and coordination of member states. ENISA is also in charge of workshops, reports, and recommendations, via which it promotes cybersecurity awareness and gives advice on ICT issues (Benincasa, 2020).

Minimizing Cybercrime: The second important goal of the EU is to reduce cybercrime through the use of better coordination and operational capabilities and robust legislation. Therefore, the EC encouraged its member states to enforce and integrate the Budapest Convention into their national legal frameworks. Thus, experts regard the 2004 Budapest Convention as the sole multilateral legal document addressing cybercrimes and cyber cooperation. However, only sixty-four states have ratified it, while such significant actors as China, Russia, India, and Brazil refused to do so. There are different reasons for the decline, one of which is connected to not being a part of the drafting process, while a more reliable issue seems to be Article 32 of the convention (permits extraterritorial searches), which, according to these countries, violated their sovereignty (Hakmeh, 2020). The EU Cybersecurity Strategy also identifies the necessity of eliminating skill gaps among the member states. This may happen via close collaboration with relevant EU agencies, namely EUROPOL’s European Cybercrime Center (EC3), which is responsible for coordinating cross-border law enforcement proceedings regarding digital crimes (EUR-Lex, 2013).

Expanding Cyber Defense Capabilities: Due to the accessibility and high dependency on cyberspace, it is becoming a crucial part of warfare along with land, air, sea, and space. Moreover, its accomplishment of military operations in the real world gives it the title of the fifth domain (Rand Corporation, n.d.). The main goal of EU cyber defense initiatives is to protect member states as well as their national security interest and networks that support missions across the European Union. Therefore, it seeks to advance the region's cyber capabilities and technological tools. In this part of the document, one of the most meaningful goals is the enhancement of cyber defense plans, given that majority of EU members nowadays have cyber defense doctrines (European Defence Agency, n.d.).

In 2014, the European Union implemented cyber defense policy guidelines identifying six priority areas, which were revised four years later. The framework mainly focuses on safeguarding the communication and information infrastructure in the region and developing cyber defense capabilities. More practical activities such as drills, research, and civil-military cooperation are among the other priorities (European Council: , n.d.). The credits for this endeavor go to the European Defense Agency (EDA), the European Security and Defence College (ESDC), and the European External Action Service (EEAS).

Fostering Industrial and Technological Growth for Cybersecurity: As expected, the EU encourages a single market for cybersecurity solutions and delivers incentives for R&D spending and innovation to close the gaps in the ICT security sphere and prepare for future challenges. To do so, the European Union aspires to create a voluntary certification plan and enforce stronger supply chain security regulations by introducing suitable cybersecurity performance criteria (EUR-Lex, 2013). Consequently, the 2019 EU Cybersecurity Act powered ENISA and its jurisdiction. It also created broad shared guidelines and assessment criteria for the region and formed an EU cybersecurity certification system for digital goods, services, and procedures (European Commission, n.d.). Indeed, ENISA closely cooperates with private and other commercial sectors to draft cybersecurity certification projects.

Building a Harmonized International Cyberspace Policy for the EU promoting core values: In reality, the European Union does not intend to establish new legal rules for cybersecurity issues. It has already expressed its support toward current international cyberspace law and intends to participate in global initiatives while increasing the region's cyber capabilities. Another significant framework under EU guidance is the “cyber diplomacy toolbox,” which enables threat reduction, encourages collaboration and has influence over prospective opponents. This mechanism also defines threat variables and accessible tools more precisely. It is noteworthy that the strategy mentioned earlier addresses personal data privacy safety. More precisely, it stipulates that any data exchange for cybersecurity goals should first be consistent with the EU’s data safety legislation and second take into consideration the individual’s rights (EUR-Lex, 2013). For this reason and to allow the European people to have greater control over their personal information, the EU introduced and enforced the General Data Protection Regulation (GDPR), otherwise known as groundbreaking privacy legislation, in 2018.

The year 2013 became pivotal in addressing these five primary goals. They have made significant progress by establishing new strategies, initiatives, and legislation and empowering existing ones. Several of them are discussed at the beginning of the paper, while the others are detailed in the following paragraphs. This evidence proves the EU’s power to set the foundation for accomplishing significant objectives and enhancing its cyber resilience by defining the timeline and course of action in its regional strategy (Benincasa, 2020).

ASEAN: Advocating for a Regional Strategy: It is essential to mention that in the past ten years, the ASEAN has primarily focused on forming a strong ICT ecosystem. After enacting the ASEAN ICT Masterplan 2015, the information sphere became economically beneficial, leading to infrastructure development, higher internet usage, and decreased cellular service prices (ASEAN, 2015b). Even though, as mentioned in the upper block of the paper, the member nations greatly differ from each other, these guidelines still narrow the gap in the digital space. However, unlike the European Union, the association did not incorporate cybersecurity as a strategic priority. Therefore, in the following sections, ASEAN’s efforts will be explored according to analytical categories in the EU Cybersecurity Strategy.

Achieving cyber resilience: As mentioned before, the ASEAN ICT Masterplan 2020 listed Information Security and Assurance as one of the eight essential objectives. This was the first time the document officially acknowledged the cyber threats as “threats that could impede ASEAN’s progress as a digitally-enabled community” (ASEAN, 2015b). Unlike the European Union, this framework came into force almost a decade later and outlined four main points: first, developing regional data protection principles on which a detailed description is provided in the subsequent paragraph; second, establishing best practices for regional network security; third, founding critical infrastructure and information resilience and forth reinforcing coordination for cyber incident emergency response (ASEAN, 2015b). The establishment of the ASEAN Computer Emergency Response Team (CERT) was part of the 2020 Masterplan. It is made up of representatives from member states (CERTs) to start developing an Incident Reporting Framework and promote collective readiness. The information provided above shows the progress of the Association of Southeast Asian Nations in certain areas, whereas it has not yet come up with a complete cybersecurity strategy outlining a joint vision, scope, priorities, and organized governing structure. Back in 2018, the ASEAN Leaders' Statement on Cybersecurity Cooperation identified a few key challenges that needed to be addressed (ASEAN, 2018)y. It should be noted that the newest Masterplan of 2025 does not cover cybersecurity in detail; however, it proposes to explore possible areas of harmonization concerning GDPR and potentially establish a framework for it.

Regrettably, some member nations, namely Cambodia, Vietnam, Myanmar, and Laos, do not enforce a national strategy. Moreover, significant differences in law and enforcement practices are visible in the region. Clearly, these structural differences and challenges greatly affect regional cybersecurity. Due to the weak safety mechanisms of nations and the increased volume of trade investment, ASEAN has grown more vulnerable and escalated the systematic risk (AT Kearney, 2018). It is clear that the member states with lower cyber maturity are easier cyber attack targets than those located in the core system. As no region-wide coordination guidelines exist and not all members have enforced CII identification, the critical information infrastructure became vulnerable to cyberattacks.

International cyber domain Policy: By voluntarily accepting principle 11, ASEAN once again confirmed its stance on cybersecurity importance. Moreover, during the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation, the association members once again expressed their commitment to establishing a unified plan and urged "the need for ASEAN to speak with the united voice at international discussions." (ASEAN, 2018). With this, they clearly conveyed the need to develop an international cybersecurity policy and capacity-building guidelines for sufficient regional interests.

The section on ASEAN in cyberspace mentioned several central bodies working on cyber security issues. However, a few more are important to note such as the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the use of Information And Communication Technologies (ARF-ISM on ICTs Security) and the Council for Security Cooperation in the Asia Pacific (CSCAP) Study Group in International Law and Cyberspace. In order to reduce the tension and risk caused by the use of ICTs, the ARF-ISM has concentrated on establishing CBMs, whereas it prioritizes the following areas: the creation of a coordination mechanism for ARF, raising awareness and exchange of best practices, cooperation guidelines among the computer emergency response team (CERT), frameworks and mechanisms for protecting critical infrastructure and fight against the cybercriminals and terrorists (ASEAN, 2018b). Even though the region has established different platforms for cybersecurity management, the study conducted by CSCAP in Semarang, Indonesia (2017) shows that the implementation of CBMs has been interrupted by the opposite perspectives of the member nations (Council for Security Cooperation in the Asia Pacific, 2019). As the "progress ultimately depends on shared priorities, a shared vocabulary, a multi-stakeholder approach, and readiness to tailor solutions to the particular needs of individual states," the CSCAP study group received the recommendation to address these issues first. The CSCAP, during its first meeting, did a great job identifying primary obstacles to international law application. They are as follows: i) Definition of Cyberspace; ii) Concept of sovereignty; iii) Conceot of due diligence; iv) Concept of State responsibility; v) Espionage; and vi) What constitutes use of force. (45) As demonstrated, the association member states have to find common ground concerning these issues (Council for Security Cooperation in the Asia Pacific, 2019).

Reducing cybercrime: Some association members do not have applicable cybercrime legislation. Only one country - Philiphines has ratified the Budapest Convention. Due to the different perspectives on the cyber domain, the opinions on how to combat cybercrimes have also diverged. As mentioned previously, one of the main reasons was Article 32 of the Budapest Convention, which allows extraterritorial searches and is regarded as causing issues of sovereignty. Countries such as Myanmar and Cambodia in December 2019 joined hands with China and Russia to sponsor the United Nations resolution on “Countering the use of information and communications technologies for criminal purposes,” which, in fact, intends to determine the principles of sovereignty in the cyber domain. The resolution for creating the panel of experts who will gather and work on the UN cybercrime treaty, regarded as an alternative, was passed 79-60, with a total of 33 abstentions. The Philipines, which abstained forty-six times, was the only exception as all other member nations voted in favor. These activities clearly show that the region has high respect for the rule of non-interference in the internal affairs of other nations and leans more toward the Sino-Russian view (Benincasa, 2020).

Threat Prevention and Response Institutions: As defined by the US Department of Homeland Security, consists of preventing, detecting, and responding mechanisms to cyberattacks that could affect a broad range of communities, companies, people, and the federal government (US Department of Homeland Security, 2022). Once the cyber resilience strategy is built, the following step is to empower the suitable players with their duties, resources, and obligations so they can achieve the desired goals. Due to the RO’s capacity to promote coordinated activities and allocate resources between member states via information exchange, joint response, and harmonized practices, it plays a crucial role in establishing preventive and responsive mechanisms. On the other hand, the detection of cyber threats mostly depends on high technologies and relevant software and hardware methods. Although regional organizations play a valuable role in the adoption of such technologies, structural challenges still prevent them from being able to monitor all illegal activities in real time. For this reason, the following parts will focus merely on prevention and response.

The following sections discuss EU and ASEAN institutions that work on developing regional prevention and response capabilities. The part on prevention examines the function of decision-making bodies, which are in charge of proposing and enforcing the laws and have the authority to create common frameworks and hold high-level strategic and technical meetings. The second section on response concentrates more on law enforcement and the legal system as they prosecute cybercrime. Because ROs have limited operational and strategic power in these fields, the subsequent parts do not cover state-to-state attacks and possible acts of war. Not to mention that the majority of countries of both regions do not have cyber warfare doctrines (Rand Corporation, n.d.).

EU: Towards enhanced cyber resilience

Through EU directives and guidelines, the European Union's regulation on cybersecurity strives to establish an inclusive and solid policy framework and institutional architecture. To explain the complicated procedure, in European Union law, the above-mentioned judicial acts are all different and are adopted in accordance with one of the legislative techniques that are outlined in the EU treaties. Generally, the directives determine the goals or the outcomes that all member states should meet; however, they are free to decide the measures and mechanisms they want to employ according to their national environment. They are also obliged to incorporate these measures into their national law within a certain period of time (Benincasa, 2020). In contrast, regulations are a type of law that is enacted and applied to all member states automatically and are binding in nature; therefore, it does not require states to incorporate them into their national legislation. Even though the European Commission (EC) is the sole entity with the power to initiate laws, the European Parliament (EP) and the Council of the European Union are responsible for voting and maintain the authority to amend or veto it at any point during the legislative procedure. The Directive on Security of Network and Information Systems (the NIS Directive) and the 2019 Cybersecurity Act are named as the most significant cybersecurity laws that played an essential role in creating modern institutions with common standards and modifying EU cybersecurity governance architecture. Overall, the primary mechanism for prevention is the NIS Directive, which is also the backbone of EU cyber legislation and is fully implemented by all member states. The 2019 EU Cybersecurity Act also strengthened the organization's cybersecurity architecture. Moreover, it empowered the EU Agency for Cyber Security, ENISA, and increased its capabilities while also creating a European cybersecurity certification system for digital goods, services, and procedures (Benincasa, 2020).

The cross-border nature of cyber crimes that are characterized by being fast-paced turns out to be very challenging for law enforcement and judicial representatives. They have to deal with third countries and actors in the private sector and have to be operative in addressing the differences in legislation between the states on how to acquire and secure e-evidence. Therefore, the European Union established region-wide institutions, such as EUROPOL and EUROJUST, with crucial roles and obligations. Their main objective is to combat cyber attacks and bring culprits to light effectively. In order to support law enforcement authorities in strengthening their response abilities, the European Cybercrime Center (EC3) was established in 2013. After three years, EUROJUST also founded the European Judicial Cybercrime Network (EJCN) to achieve effectiveness in cybercrime investigation and prosecution (Benincasa, 2020). Most of the initiatives are already discussed in Chapter One; however, it should be noted here as well that the EU built a robust framework of interoperational institutions. It is clear that the existing guidelines still need to be refined, but so far, they have positively affected the national capabilities and created a platform for adequate coordination both at the strategic and operational levels with a focus on national oversight of cyber critical infrastructure. The regionwide law enforcement and judicial collaboration were attached to this initiative in order to coordinate the implementation of relevant laws across the region and adequately hold the prosecution procedures (Benincasa, 2020).

ASEAN: Institutional Progress: It is well known that the EU's decision-making happens through qualified majority voting, while the ASEAN process is more informal and based on mutual understanding. This means that these procedures are not legally binding for the member nations. This type of consensus is referred to as the "ASEAN way." Hence, sometimes an "ASEAN minus X" formula is employed, which permits some countries to move forward on the understanding that other member states will eventually follow. The ASEAN is trying to avoid becoming as bureaucratic as the organizations in Europe (Benincasa, 2020). Thus, most of its decisions are of a political nature rather than being legally binding. This does not imply that when a significant security concern arises, and there is a common political will, the association can not come to an agreement on binding mechanisms. On this note, the association already did so regarding transnational crime when, in 2007, it adopted the ASEAN Convention on Counter Terrorism and in 2015 - the ASEAN Convention Against Trafficking in Persons, Especially Women and Children. The concerns such as human rights, infrastructure, and regional stability served as the foundation for these conventions.

Prevention measures within the association: The current state of the association's regional collaboration platforms, along with member states' capabilities and institutions, can be characterized by varying degrees, starting from very complex to intermediate to fledging or even nonexistent in certain areas. Despite that, noticeable improvements have been visible in some areas over the past years, especially in establishing stronger and more resilient institutional architecture, leading to considerable improvements in other spheres as well. The association's current structure covers the three primary pillars, which are as follows: the ASEAN Economic Community (AEC), the ASEAN Political-Security Community (APSC), and the ASEAN Socio-Cultural Community (ASCC). The last pillar does not handle issues connected to cybersecurity, while the other two employ organizations that address the cybersecurity concerns of the Association. The entities working on preventive measures are briefly discussed below which clearly shows their working methods and how different they are from the ones of the European Union (Benincasa, 2020).

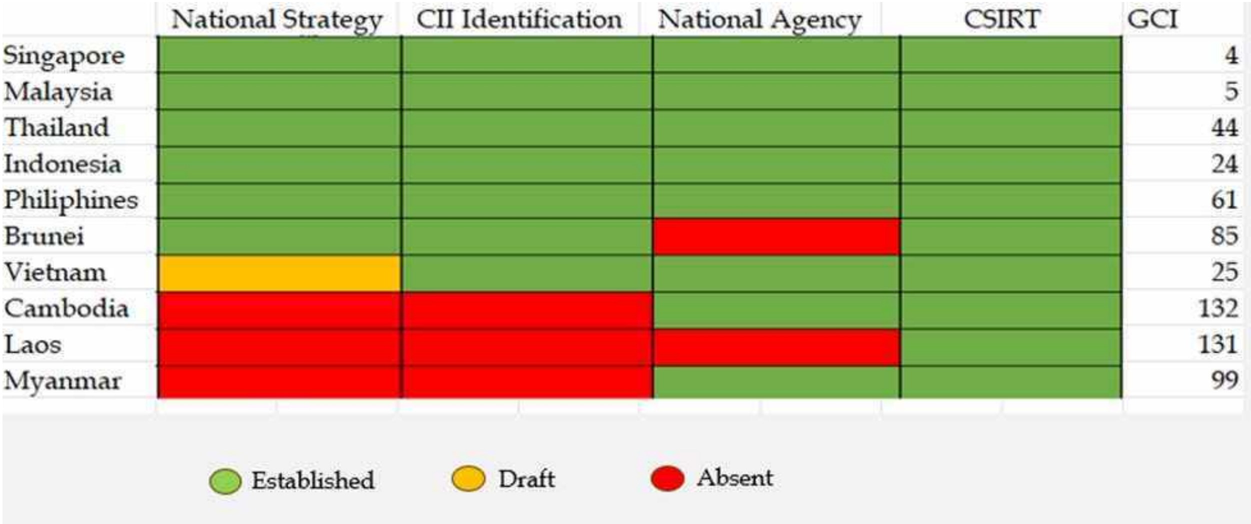
The main forum for ICT cooperation among the association's members is the ASEAN Telecommunications and IT Minister's Meeting (TELMIN), which works under the AEC pillar. The main responsibilities under this body are diverse ICT issues, namely human capital development along with empowering them and their engagement; critical infrastructure development; connecting the digital divide and economic well-being (ASEAN TELMIN, 2017). Recently, the cybersecurity area has also become part of it. The TELMIN has another body working under its directions and priorities, called the Telecommunications and Information Technology Senior Officials Meeting (TELSOM). This institution is entrusted with managing and implementing activities connected to the ICT sphere and carrying out Infrormation and Communication Technology cooperation policies in the region. TELSOM is comprised of Senior Telecommunications Officials from member nations who meet once a year to exchange ideas on crucial international challenges and advancements in ICT. Moreover, it encourages participation from the private sector, NGOs, and other organizations in its projects and activities (ASEAN TELMIN, 2017). Lastly, the ASEAN Network Security Council (ANSAC), which meets annually since 2013, was established to create a shared framework for cybersecurity, emphasizing national CERT collaboration and capacity building (Heinl, 2014).

The second pillar of APSC has the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) under its wing. This is a collaborative forum working on the prevention and reduction of transnational crimes with an emphasis on cyber exploitation. It is this body that is in charge of the two Conventions on terrorism and human trafficking listed above. AMMTC sets the guidelines and priorities for the Senior Officials Meeting on Transnational Crime (SOMTC), which is another entity under TELMIN's umbrella and is in charge of managing and carrying out ASEAN-wide policies and initiatives. The SOMTC itself encompasses different working groups and mechanisms that address various issues, including human trafficking, arms smuggling, and counterterrorism. It is not surprising that it also features a team that works on cybercrime and allows the association's member nations to discuss it with partners and then decide on appropriate approaches (ASEAN, 2013).

The APSC pillar also includes the ASEAN Defence Ministers Meeting (ADMM-Plus), which is the association's most elevated defense consultative and cooperative instrument. Its main focus is cybersecurity and promotes cooperation in cyber defense in seven different areas. This institution also has another body under its supervision, which is responsible for administrative tasks, coordinating meetings, workshops, seminars, and training. It is called the Experts' Working Group on Cyber Security (EWG on CS) (ADMM, 2010).

It is clear that AMMTC and TELMIN play a crucial role; however, no official regional organization or league exclusively addresses cybersecurity issues. Regardless, significant progress has been made in the cyber area since Singapore took a chairman position in 2018. One of them is the founding of the ASEAN Ministerial Conference on Cybersecurity (AMCC), another vital platform that takes place annually on International Cyber Week in Singapore and supports the advancement of cybersecurity cooperation. In the beginning, the member nations proposed to create simple, pragmatic cybersecurity norms of behavior and measures led by TELMIN (Noor, 2018). Another fact to highlight is the fourth AMCC meeting held in 2019, where Singapore proposed a draft of an ASEAN Cybersecurity "Coordination Mechanism Paper," and the ministers agreed to endorse it but with the condition that it is not copying existing ASEAN sectoral institutions' work (CSA Singapore, 2019). This process has ended with establishing an ASEAN Cross-Sectoral Coordinating Committee that works on cyber issues without duplicating other bodies.

Since the Association of Southeast Asian Nations does not have the authority to impose legally binding documents directly like the EU, examining each member's national capabilities is crucial. This analysis helps to understand each state's different realities and how these diversities affect the region. For this reason, in the table below, the four main national capability components are considered (according to the EU NIS directive) and applied to ASEAN member countries.



	National Strategy	CII Identification	National Agency	CSIRT	GCI
Singapore	🟩	🟩	🟩	🟩	4
Malaysia	🟩	🟩	🟩	🟩	5
Thailand	🟩	🟩	🟩	🟩	44
Indonesia	🟩	🟩	🟩	🟩	24
Philiphines	🟩	🟩	🟩	🟩	61
Brunei	🟩	🟩	🟥	🟩	85
Vietnam	🟨	🟩	🟩	🟩	25
Cambodia	🟥	🟥	🟩	🟩	132
Laos	🟥	🟥	🟥	🟩	131
Myanmar	🟥	🟥	🟩	🟩	99

🟩 Established 🟨 Draft 🟥 Absent

Table 1 - National Capabilities of ASEAN Member States

Note. Sourced from ITU: Global Cybersecurity Index (GCI) (2020)

The table illustrates that the majority of association members were able to enact the vital institutions and their policies for cyber resilience mentioned in the NIS directive. Despite these positive updates, the scenario in this region is fragmented due to differences in national capabilities and priorities, which also negatively affect the degree of effectiveness and enforcement. In contrast, CSIRT in Indonesia mainly comprises small groups of volunteers, while Singapore is well-equipped and has plenty of resources. To reflect on the disparity, the International Telecommunications Union (ITU) created a reliable reference - the Global Cybersecurity Index (GCI). This platform assesses the member states' cybersecurity commitment based on five aspects: technical measures, legal measures, organizational measures, capacity-building, and cooperation (ITU, 2020). As shown in the table, Singapore and Malaysia are taking leading positions both globally and regionally. In the 2018 report, Singapore ranked 6th, while Malaysia 8th. Only after two years did both of them advance into fourth and fifth places, respectively. While these two countries have seen significant development, others, such as Thailand, Cambodia, Philippines, Brunei, and Laos, have lowered their ranks drastically (ITU, 2018).

Responsive measures within the association: The ASEAN's law enforcement agency - the National Police Organization for the Association of Southeast Asian Nations (ASEANPOL), conceptually is close to EUROPOL; however, in terms of functions and capabilities related to cybersecurity, it differs a lot from its European counterpart and primarily focuses on exchanging information and enhance trust between its members. Thus, no entity is equivalent to EUROJUST or EC3 in combating cross-border cybercrime. Still, the participation of regional and international networks in tackling cybercrime is highly appreciated (Benincasa, 2020). In 2018, as a responsive mechanism for law enforcement and a means of developing coordinated action between them, INTERPOL founded the ASEAN Cyber Capability Desk. It has two key responsibilities, among which the first is to *enhance cybercrime intelligenc*e through utilizing the INTERPOL Cyber Fusion Center and private-sector partnerships. It also provides the ASEAN leaders with cybercrime intelligence at different levels. Another function is *joint cybercrime operations*, which addresses the differences of jurisdiction between the association members through joint operations targeting the most pertinent cyber threats (INTERPOL, 2020).

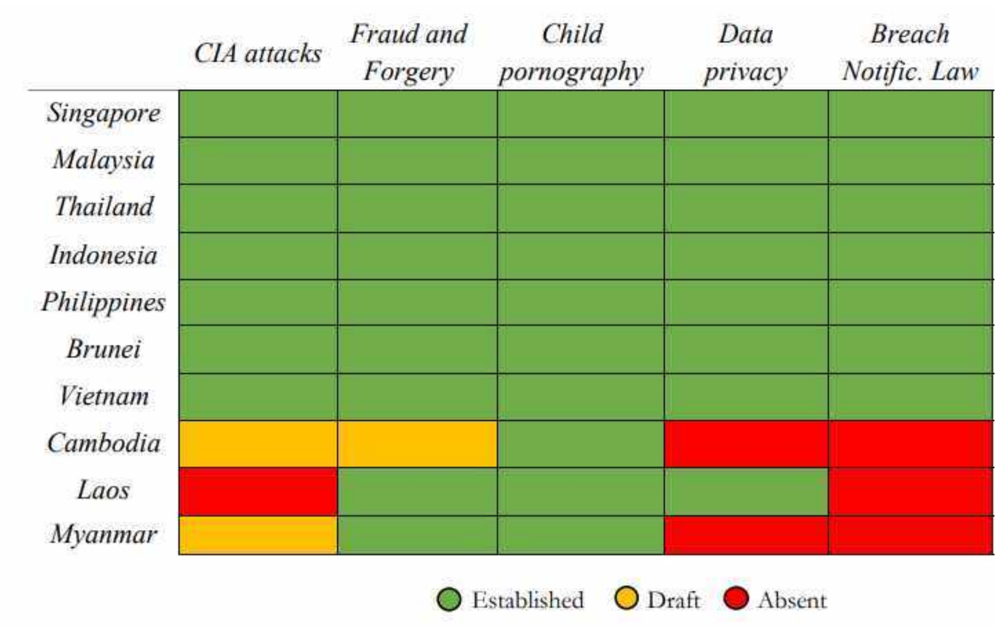
It is noteworthy that in 2013, another institution, the Council of ASEAN Chief Justices (CACJ), was founded with the goal of supporting regional economic growth through collaboration and information exchange. Furthermore, in 2018, they also launched the ASEAN Judiciaries Portal, which serves as a platform for sharing best practices and experiences. Nowadays, the Council of ASEAN Chief Justices provides more practical support by educating judicial representatives on the terms and issues of the cyber arena rather than providing legal assistance to the association's members (CACJ, 2013).

All in all, the Association of Southeast Asian Nations has been working hard on improving its institutional framework and establishing key entities that greatly influence cyber resilience. It is apparent that ASEAN takes the EU as a role model and tries to harmonize its institutions and frameworks with the European one. The data of this chapter show how well the EU has influenced ASEAN and how productive the European Union has been.

Chapter 5. Guiding ASEAN Cybersecurity: The EU's Influence

For quite a while, data security and privacy were regarded as two distinct fields that function independently from each other. Ever since artificial intelligence and big data gained popularity, they have become complementary parts of sensitive data protection (Burt, 2019). However, they can't be viewed as interchangeable, moreover, they should be addressed separately with appropriate tailor-made legislation. While data security protects data from illegal access, data privacy controls how it is gathered, shared, and utilized. More precisely, accidental interference can lead to a bigger risk of illegal data gathering and processing. For example, with their intelligence capabilities, the new technologies can easily predict sensitive information regarding political memberships and their activity patterns (Burt, 2019). The Cambridge Analytica Scandal of 2018 can be a prime example, as this political consulting firm in Britain collected the personal information of millions of Facebook users without authorization (Benincasa, 2020). They used smart machines to target and manipulate the electorate by creating political advertisements and swaying the outcome of the whole election. Another incident happened in 2017 when Equifax got hacked, and hackers acquired the credit card information and other sensitive data of 147 million Americans. Due to Equifax's vulnerable system, the information was leaked, and the US Fair Trade Commission (FTC) fined the company with $700 million (Tan & Syahirah Azman, 2019). In similar times, when the sensitive information is at stake the states must work together to establish efficient preventative and responsive measures and apply the applicable laws. Unfortunately, as mentioned many times before, huge gaps in the legislation and significant principles make collaboration hard. The majority of scientists suggest these two organizations harmonize as much as possible. Therefore, this section discusses what preventive measures the Association of Southeast Asian Nations has at its disposal in terms of cybercrime and data security and how the European Union positively influenced it.

The members of the Association of Southeast Asian Nations (ASEAN), under the 2017 Declaration to Prevent and Combat Cybercrime, decided to enhance their relations through a range of strategies, such as harmonizing legislation regarding cybercrime and electronic evidence to prevent and combat cybercrime. The result, however, will mostly depend on political will and national priorities due to the association's governing nature and incapacity to enforce legally binding measures on its member nations and the absence of a Cybersecurity Convention. The following sections examine the result of this cooperation with a focus on GDPR regulations and the EU's influence over it (Benincasa, 2020).



	CIA attacks	Fraud and Forgery	Child pornography	Data privacy	Breach Notific. Law
Singapore	🟩	🟩	🟩	🟩	🟩
Malaysia	🟩	🟩	🟩	🟩	🟩
Thailand	🟩	🟩	🟩	🟩	🟩
Indonesia	🟩	🟩	🟩	🟩	🟩
Philippines	🟩	🟩	🟩	🟩	🟩
Brunei	🟩	🟩	🟩	🟩	🟩
Vietnam	🟩	🟩	🟩	🟩	🟩
Cambodia	🟨	🟨	🟩	🟥	🟥
Laos	🟥	🟩	🟩	🟩	🟥
Myanmar	🟨	🟩	🟩	🟥	🟥

🟩 Established 🟨 Draft 🟥 Absent

Table 2 - Cybersecurity and Data Privacy Legislation across ASEAN

Note. Sourced from Benincasa, E. (2020, p.24)

Cybercrime: Table 2 illustrates the present legislative measures in the association's member states based on the main cybercrime provisions found in the Budapest Convention. The graph also shows that most of the nations have developed frameworks for legislation in most of these areas, while they still significantly differ in terms of cybersecurity capabilities and legislative range. In contrast to Singapore's laws, which is very similar to the EU's GDPR criteria, Laos's data privacy laws only have fundamental features for personal data protection. Moreover, there are significant differences even between the legal frameworks of ASEAN members which makes cooperation difficult and time-consuming. Namely, they differ in legal provisions that are about the investigation and prosecution of certain online behaviors as well as the collection of e-evidence (Benincasa, 2020).

It is noteworthy that sometimes, these legal system and framework differences may even result in deepening cooperation or another type of agreement between the countries, while international common legal guidelines for expedited sharing of evidence are absent. Thus, membership in a mutual legal assistance agreement (Kent, 2015) remains the most efficient means of acquiring data at this time. In this case, it is the Budapest Convention that is only ratified by the Philippines. Although the association's members signed the Mutual Legal Assistance in Criminal Matters (MLA Treaty) in 2004, its application to cybercrime is limited as it lacks the crucial parts for transnational cyber threats, such as retaining and accessing e-evidence (ASEAN, 2004). These clauses are especially important due to the fact that the service providers that keep electronic evidence online most of the time are located outside the country making the request. More precisely, the ASEAN MLA treaty, compared to the Budapest Convention, lacks the following provisions. "expedited preservation of stored computer data, expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, trans-border access to stored computer data with consent or where publicly available, and mutual assistance in the real-time collection of traffic data"(ASEAN, 2004).

The ASEAN and the European Union have long-lasting relations, and they recently recognized the importance of working together on cyber issues as well. The EU, on its end, with different initiatives, tries to support the association as a whole, and one of them that concerns cybercrime and cyber data protection is YAKSHA (CybersecuritY Awareness and Knowledge Systemic High-level Application). This project started in January 2018 and lasted till December 2020 and was fully funded by the European Union and European Commission under Horizon 2020 (EEAS, 2021). The main goal of YAKSHA is to improve the general cybersecurity process in both regions and specifically deter cyber-attacks and crimes and avoid the prospective danger in this field. As mentioned many times before, the EU and ASEAN in 2019 adopted the Ministerial ASEAN-EU Statement on Cybersecurity Cooperation, and this joint project was part of it. To be more precise, under YAKSHA, both organizations received cybersecurity software solutions that were validated in their respective real-world pilot schemes. Also these pilots were tested by end-users who found out possible cybersecurity risks and allowed the consortium to enhance the current software and make it ready for the launch. Even though the 2019 Covid pandemic brought some challenges to the working group, they still managed to solve it and deployed the software in Greece, Vietnam, and Malaysia (EEAS, 2021).

This software is a tool for gathering cybersecurity intelligence and helping organizations control and utilize honeypot virtual devices, which mainly create an artificial environment to trap attackers who threaten the publicly available services provided by the institution. Here are a few beneficial features that software has: "YAKSHA Honeypot management platform, Honeypots, Automated binary decompiler, Honey analyzer, Honey maker, and a Correlation engine that implements malware behavior analysis." There are many innovative results to point out, among which are the dataset generated by the pilot deployment in Malaysia and Vietnam (EEAS, 2021). This project sent 103 ambassadors who were recruited on a voluntary base to ASEAN countries. The representatives from both sides had access to European and ASEAN-wide networks that were actively engaged in cyber technology. The high representatives of both organizations made a positive statement about the project and welcomed YAKSHA's role in strengthening their cybersecurity cooperation. This project is a practical representation of the ASEAN-EU Statement on Cybersecurity Cooperation, which prepares the region for cybercrime and threats. According to the European Union External Action, YAKSHA's solutions will be commercialized once the project is finalized. Thus, this project is another evidence of the EU's positive influence over ASEAN, in this case through building joint software and knowledge exchange. That can also be a reason for YAKSHA receiving the label of Excellence (EEAS, 2021).

Data Privacy: It is not surprising that since the association's member nations have enforced varying policies over managing and processing personal information, ASEAN does not possess a region-wide legislation. Mainly, the differences are the personal rights, requirements for reporting the data violations, penalties for it, and different degrees of accountability for data controls and processors. However, the association still managed to adopt two non-binding frameworks to harmonize the region's personal data privacy legislation at a certain level. One of them is the ASEAN Framework on Personal Data Protection, which was created in 2016 and lays out a number of clauses for strengthening sensitive data protection both at national and regional scales (ASEAN, 2016b). Another one, the ASEAN Framework on Digital Data Governance, was created at the TELMIN meeting in 2018. It aims to improve data management, make it easier for ASEAN member nations to harmonize their data legislation, and encourage intra-ASEAN data flows (ASEAN, 2016a).

The Asia-Pacific Economic Cooperation (APEC) established an alternative model called Cross-Border Privacy Rules System (CBPR) in 2011 to protect sensitive data and regulate its cross-border transfer. It is an optional certification program where its members, usually the private companies that own CBPR certificates, can securely exchange personal data (both inside and across firms). Many organizations choose CBPR over GDPR for their trade and investment activities. Simply because CBPR just specifies minimal criteria that can be easily adopted by different states or companies and seems more flexible than GDPR (Callo-Müller, 2018). However, the reality is more complex, and as A. Gribakov mentions it

"fundamentally, the GDPR and CBPRs frameworks represent competing views on the trade-offs between privacy and economic growth. The CBPRs system arose from APEC's desire to increase information flows and trade, while the GDPR arose out of the Charter of Fundamental Rights of the European Union, which includes the right to privacy and data protection." (Gribakov, 2019).

Also, the CBPR does not give its customers any special affirmative rights nor prevent them from enforcing their own standards. As said before, the CBPR is more flexible, but it does not cover certain areas of GDPR, such as restrictions on the automatic handling of data and limitations on its storage, onward transfers, and even applying these obligations to data processors (Callo-Müller, 2018). For this reason, the states have to enact legislation with a more comprehensive character and fill the gap with EU regulations or even negotiate partial agreements with it. A successful example of the EU-US Privacy Shield Framework should not be forgotten as it equips businesses with special mechanisms that are used during data transfer from the EU to the US (DPF, 2020). Only 9 states and 23 private companies are holders of CBPR certificates, including Singapore and the Philippines of ASEAN, and other influential countries like Japan, Mexico, Canada, USA, the Republic of Korea, Chinese Taipei and Australia. (CBPR, 2011).

As said earlier, the EU serves as a role model for many other organizations, and ASEAN is no exception. Since the EU advanced with the GDPR's implementation, the other world actors also began to prioritize enacting comprehensive data privacy laws, among which there are several ASEAN nations that also began modifying their own legal systems to be more in line with EU directives (Tan & Syahirah Azman, 2019). It is important to mention that political players were mainly encouraged by the GDPR's extraterritorial character. As previously mentioned, it imposes legal responsibilities on businesses that provide any kind of products or services to EU people or track their online activity even if they are not positioned in the European Union. Thus the GDPR is even more crucial in this context, given the solid economic relations that exist between the EU and ASEAN (European Parliament, 2022). Indeed, with over €271.8 billion in trade in 2022, ASEAN is the EU's third-largest trading partner outside of Europe, after the US and China. The same rank applies to the EU, as it accounts for 10.2% of ASEAN trade. Apart from trade, the organizations take leading positions in terms of FDI. According to the European Commission, the EU's Foreign Direct Investment in 2020 accounted for €350.1 billion; while ASEAN investment for the same year was lower than the former, it is still going progressively and accounted for over €172.4 billion (European Commission, 2022). Despite the administrative and financial challenges faced by many nations in adjusting to GDPR standards, doing so might contribute to ASEAN interoperability and unite the world under a single regulatory framework. Moreover, they will need to hire new personnel, upgrade their software, or even install new technologies, as well as get legal advice, and of course, operational costs will rise accordingly (Callo-Müller, 2018).

Generally, the Data Protection laws that are active in ASEAN do not have a mandatory nature, thus, not all member states are part of it. For instance, Singapore recommends that its organizations notify the Personal Data Protection Commission (PDPC) in case there is any data breach. The PDPC is also working on giving this recommendation an obligatory nature. In the Philippines, they only have 72 hours after discovering the data breach or a potential threat to notify the regulator. It also ensures that the leak victims are informed within the same time frame. The same policy applies in Thailand to inform the Office of Personal Data Protection Commission and the subject under the risk, respectively (Tan & Syahirah Azman, 2019). As ASEAN trade heavily depends on Europe, the businesses connected to it realized they needed to comply with EU regulations. Therefore, the member states started to adopt GDPR, and this section provides detailed information about them that also shows the EU's positive effect.

Malaysia is currently in the process of considering amendments to its Personal Data Protection Act 2010 (PDPA) to align with the GDPR. The minister of the communications and multimedia ministry, which is responsible for the protection of sensitive data, told the media that this reviewing process aims to harmonize the clauses of the privacy data protection with international requirements among which is GDPR as well. He also added that nine years after the PDPA was established, the world has developed, and many things have changed that require their legislation to be up-to-date. The examination process started in 2018 and is still ongoing (Tan & Syahirah Azman, 2019).

Moving towards the top-ranked member state to *Singapore*, its Personal Data Protection Act 2012 (PDPA) has many similarities with GDPR provisions. Namely, both documents ask for consumer consent on data gathering, as well as on its processing and disclosure. Moreover, they recently introduced a data portability that allows users to transfer their personal data across different service providers. It is not surprising that Singapore also joined the US and Japan in enforcing the CPBR system through the Asia-Pacific Economic Cooperation (APEC) and became the third biggest economy in the group. Also, the country's IMDA agents ensure that participating organizations are following the APEC's regulations for which they use third-party assessments (Tan & Syahirah Azman, 2019). APEC representative Shannon Coe praised Singapore's move and said that the country shows a genuine commitment to employing decent protective measures along with developing its technologies. Apart from being an active participant, Singapore has a strong commitment to its PDPA. For instance, in 2019, the government fined five different companies for breaching sensitive data policies as they failed to safeguard the privacy information of their customers. The fine amounted to S$117,000, from which S$54,000, the biggest, went to Horizon Fast Ferry (ferry service provider) as they did not provide any protection policies or practices, nor did the protection officer, therefore, let all the sensitive data be leaked (Tan & Syahirah Azman, 2019).

Unlike its member states, *Thailand's* Personal Data Protection Act came into force quite late in 2019, but the EU strongly influenced it. Thus it offers its citizens similar protection measures as GDPR. Thailand also stands out as the association's third-largest EU trade partner and of course, its private and public businesses have to obey GDPR requirements. It is essential to mention that even though the Thai PDPA mirrors many principles of the General Data Protection Regulation, its PDPA is still created in a way that fits the Thai nation. Meaning that it has concepts developed from the Thai view, and its compliance with GDPR does not necessarily mean it complies with PDPA. Therefore, there is still a long way to go so both acts are fully compilable (Tan & Syahirah Azman, 2019).

Continue to the countries with the least similarities to EU regulations. The *Philippines* adopted its first Data Privacy Act in 2012, which, after four years, was supplemented to reflect the principles of GDPR. However, it does not fully comply with higher standards. As for *Laos*, it does not have specific legislation for sensitive data protection. Though the following documents, the law on Prevention and Combating of Cybercrime 2015 and the law on Electronic Data Protection 2017, contain clauses that partially forbid the harmful use of personal information and protect individual's privacy (Tan & Syahirah Azman, 2019). A similar situation is in *Vietnam*, where the principles of data protection are simply spread over different legislation, and they do not have a single law that controls it. Moreover, in 2019, their government adopted a cyber security law that caused controversy among experts. Especially the conditions under the law that do not allow cross-border data exchange as well as oblige data to be localized. To simplify it, all the sensitive data collected by foreign entities should be kept locally in Vietnamese territory. Also, if the government needs this information, the private sector representatives should share it with them, which does not sound very protective. Following this trend, neither *Brunei* nor *Myanmar* has a law for data protection. In *Cambodia*, at least, the national constitution, along with the Cambodian Civil Code and some other sectors that provide banking or medical services, include the principles of privacy and confidentiality (Tan & Syahirah Azman, 2019).

Indonesia was among the members without a specific law regulating and protecting personal data until 2022. As of today, the country has enacted the Personal Data Protection Act, which is valid for any organization that operates within or outside Indonesia and possesses sensitive data. Before that the country only had some sector-based laws like Vietnam. Two players mainly influenced this development. In 2008, Google invested $1bn in Go-Je, which increased the investment in the whole country (Tan & Syahirah Azman, 2019). Therefore, the House of Representatives of Indonesia has to make sure that they are well-prepared for future challenges and that their citizen's data are not processed without consent. For the same reason, the Ministry of Communication and Information Technology encouraged different innovative initiatives under which the Institute for Community Studies & Advocacy, the Indonesian E-Commerce Association, and ICT Watch were established. The second influencer is the EU with its economic ties. That is why some of the similar GDPR features that Indonesia's PDPA has are the right to be informed, erasure, access, right to the data port, ability, and objection. Moreover, this document requires certain companies to assign Data Protection Officers (DPO) and monitor their activities (Tan & Syahirah Azman, 2019).

Analysis and Conclusion

The main part of the research already discussed EU's and ASEAN's strategies and initiatives and in the following section the paper analyzes their relations in the cyber domain, which are influenced by many factors. Through the trade links, the EU shaped the ASEAN's cybersecurity policy and, at the same time, advocated for regulatory standards such as the General Data Protection Regulation (GDPR). This effect is clearly visible in the frameworks, guidelines, technical assistance, capacity-building programs, and recommendations. It is important to mention that the European Union employs a multifaced approach towards the association. The EU fosters its cybersecurity strategies and regulations by creating solid economic ties and ensures that the association's member states incorporate the best practices in their national policies. The European Union may not be a leading cyber power; however, it is indeed a normative power. A great example of this is GDPR, which emerged as a global standard for sensitive data protection. As said before, several ASEAN nations implemented similar principles in their national laws. For example, the Philippines' and Singapore Data Privacy Acts are mostly harmonized with the GDPR. Indonesia's latest data protection laws also demonstrate the EU's massive impact on the region with its trade links.

Apart from the commercial approach, the EU employs several other cooperative initiatives to show its dedication to promoting cyber resilience in the ASEAN. Once again, Indonesia and its engagement in the Cyber4Dev project serve as a prime example. This project offers knowledge exchange, training, and experts to strengthen the cybersecurity norms and regulations in the ASEAN. This initiative aims to support the association's members so they can align their norms more closely with the European Union (Chen & Yang, 2022). Moreover, the EU pulled out all sources in ASEAN due to the association's geopolitical preference for Sino-Russian interests. The European Union uses most of its capabilities so that Southeast Asian countries do not entirely depend on Chinese or Russian models. The European Union, as a normative power, is ready to counterbalance other cyber actors and affirm its presence in the region. Research shows that the EU's actions are quite successful and different from its opponents. For example, both the EU and China use economic means to promote their own type of cyber governance and cybersecurity norms. However, while China tries to influence each association member separately, the European Union regards the ASEAN as a united organization and communicates with it as a whole institution. This approach is applied not only to cyber relations but also to other economic and social relations. It is known that the ASEAN does not have a binding nature and is voluntary based. However, since the association's trade with the EU is quite significant, the member nations are trying to benefit from it, which also encourages them to adopt similar standards as in Europe. The EU promotes its norms by respecting the target's unity. Furthermore, it has a diplomatic and economic presence in the region, not a military. This means that the EU can be regarded as a safe partner and also says a lot about its intentions.

The EU's approach to the ASEAN strategy places great importance on technical assistance and capacity-building. Therefore, it created many initiatives to enhance cybersecurity in the region. One of the EU-sponsored projects, YAKSHA, improves cyber resilience within the ASEAN and serves as a knowledge exchange platform. These initiatives positively influence association members as they support them in developing effective cybersecurity preventive and responsive measures. Moreover, the EU's legal and regulatory advising services have a vital impact on ASEAN's cybersecurity domain. The European Union sends the experts to association member states who support them in implementing EU standards. The EU tries to influence cybersecurity norms and regulations by employing an advisory role so they are more harmonized with European standards. Furthermore, the ASEAN-EU Plan of Action proves that the EU-ASEAN cyber relations are a priority. For instance, in the 2018-2022 action plan, the term cybersecurity is used only once in regard to combating cybercrime. Moreover, it is discussed under the political and security cooperation section, precisely where it addresses non-traditional security concerns and terrorism (ASEAN-EU Plan of Action 2018). In contrast, the 2023-2027 Plan of Action mentions cybersecurity in the same part where security architecture is discussed, but it also highlights the importance of cyber capacity-building and awareness-raising programs. This document uses cybersecurity terms eight times and addresses many details regarding it. Such as digital governance and cross-border travel through the digital economy. The current Plan of Action also has a separate section about cybersecurity cooperation, which shows different spheres of collaboration and implementation of the agreed norms.

In 2020, EU-ASEAN relations upgraded to establish a "strategic partnership." Indeed, this strengthened their existing mutual agreements and opened up the chances for future cooperation in new spheres such as digital connectivity, cybersecurity, and even green growth (EEAS, 2024). The process of their engagement with cyber and digital governance can be regarded as a "two-way socialization." Meaning that both actors constantly work to influence the outcome and the content of the norm distribution in this field (Xiaoyu, 2012). As this kind of cooperation between the EU and ASEAN promotes the exchange of best practices and mutual understanding, it may also assist in bridging the normative gap between Western and non-Western cyber governance.

The Association of Southeast Asian Countries has always shown a great interest in learning from the EU's strategies and practices in digital economy and connectivity, including the spheres of the digital ecosystem and its regulation. One example can be its willingness to participate in EU-initiated programs about digital benchmarking indexes as well as gaining knowledge via the EU's experience in measuring the digital economy (European Commission, 2019). Moreover, policy-makers and researchers in ASEAN encourage the association to take lessons from the EU concerning the data privacy policy and comprehend similar policies. Not only does the ASEAN show an interest in EU-led policies, but the European Union likewise became aware of ASEAN-specific norms and initiatives. Therefore, it impacted the EU's view towards the association, and after a better understanding of the association's approaches and norms, ASEAN gained the title of a partner rather than a norm recipient (Xuechen, 2018). This is also demonstrated by the EU's active participation in the ASEAN Regional Forum's Inter-Sessional Meeting on ICT Security. Besides, the EU is supportive of the association's non-binding and voluntary nature, which also shows massive respect for ASEAN centrality.

The cooperation between the EU and ASEAN can be described as similar to some extent and diverse to other extents. Furthermore, their relationship also highlights the spheres of mutual independence of both regions in the context of China and the U.S. confrontation and the changing landscape of cyber threats. Despite these complexities, ASEAN and the EU still effectively manage situations while carefully balancing values. By doing this, they demonstrate their ability to function independently while tackling common cyber challenges. Both the European Union and the ASEAN have immense opportunities to enhance their collaboration further. This may assist both organizations in successfully tackling cybersecurity threats and formulating a strategy that covers normative principles and practical factors. Increased cooperation will lead to a long-term advantage for both the European Union and ASEAN.

By analyzing both organizations' distinct norms and approaches toward cybersecurity, this research challenged the existing scholarly views, stating that ASEAN's non-binding nature is an issue. It demonstrated that the European Union made considerable efforts to familiarize itself with ASEAN approaches and that its voluntary nature is well-respected by the EU. Moreover, as the main focus of the research is GDPR, the paper showed a positive influence of it by comparing the data privacy laws in each member state. Economic ties play a significant and influential role in the EU's strategies. However, unlike other actors, the European Union respects the unity of the association, and according to my work, it has a successful outcome. By employing a multifaced approach, the European Union tries to promote its cybersecurity regulations worldwide, and ASEAN is a great example of it. In conclusion, the EU's impact on the cybersecurity policy of the ASEAN is significant and diverse as it fosters the spread of cybersecurity norms and regulations utilizing trade links, technical assistance, capacity-building, and legal advice.

Bibliography

Abdul Rahman, M. F. B. (2022). *Enhancing ASEAN-EU cooperation in non-traditional security*. https://dr.ntu.edu.sg/bitstream/10356/164282/2/BC%204b%20Muhammad%20Faizal%20bin%20Abdul%20Rahman_ASEAN-EU%20NTS%20cooperation.pdf

ADMM. (2010). *ADMM-Plus - ASEAN Defence Minister's Meeting (ADMM)*. Admm.asean.org. https://admm.asean.org/index.php/about-admm/about-admm-plus.html

AFR. (2012). *Co-Chairs' Summary Report of the ARF Seminar on Confidence Building Measures in Cyberspace.* https://aseanregionalforum.asean.org/wp-content/uploads/2019/03/Annex-3-Co-Chairs-Summary-Report-ARF-ISG-on-CBMs-and-PD-Bandar-Seri-Begawan-20th-ARF.pdf

ASEAN. (2000). *e-ASEAN FRAMEWORK AGREEMENT Preamble*. https://agreement.asean.org/media/download/20140119121135.pdf

ASEAN. (2003). *Joint Media Statement of the 3rd ASEAN Telecommunications and Information Technology Ministers Meeting, Singapore*. Asean.org. https://asean.org/joint-media-statement-of-the-3rd-asean-telecommunications-and-information-technology-ministers-meeting-singapore/

ASEAN. (2004). *Treaty on Mutual Legal Assistance in Criminal Matters*. https://agreement.asean.org/media/download/20160901074559.pdf

ASEAN. (2013). *ASEAN Convention on Counter-Terrorism Completes Ratification Process*. Asean.org. https://asean.org/asean-convention-on-counter-terrorism-completes-ratification-process/

ASEAN. (2015a). *ASEAN ICT Masterplan 2020*. https://asean.org/wp-content/uploads/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf

ASEAN. (2015b). *ICT Masterplan 2015 Completion Report*. https://asean.org/wp-content/uploads/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf

ASEAN. (2016a). FRAMEWORK ON DIGITAL DATA GOVERNANCE. In *TELMIN*. https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf

ASEAN. (2016b). *Framework on Personal Data Protection*. TELMIN. https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

ASEAN. (2018a). *ASEAN Leaders' Statement on Cybersecurity Cooperation*. https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf

ASEAN. (2018b). *Co-chairs Summary Report: 1st ASEAN Regional Forum Inter-sessional meeting on security of and in the use of information and communication technologies (ARF ISM ON ICTs SECURITY)*. https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-12.pdf

ASEAN. (2019). *WORK PLAN OF THE ASEAN PLAN OF ACTION TO PREVENT AND COUNTER THE RISE OF RADICALISATION AND VIOLENT EXTREMISM (2019 – 2025)*. https://asean.org/wp-content/uploads/2012/05/Bali-PCRVE-Work-Plan-2019-2025_asof11Dec2019.pdf

ASEAN. (2022). *ASEAN CYBERSECURITY COOPERATION STRATEGY 2021-2025*. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf#:~:text=URL%3A%20https%3A%2F%2Fasean.org%2Fwp

ASEAN . (2013). *Ministerial Meeting on Transnational Crime.* Asean.org. https://asean.org/meetingreportparent/asean-ministerial-meeting-on-transnational-crime-ammtc/

ASEAN Secretariat. (n.d.). Asean.org. Retrieved June 11, 2024, from https://asean.org/our-communities/economic-community/asean-digital-sector/major-sectoral-bodies-committees/

ASEAN TELMIN . (2017). *About ASEAN TELMIN*. https://asean.org/wp-content/uploads/2012/05/14-TELMIN-17-JMS_adopted.pdf

ASEAN-EU Plan of Action. (2018). https://www.eeas.europa.eu/sites/default/files/asean-eu_plan_of_action_0.pdf

AT Kearney (2018). Dobberstein, Gerdemann, Pereira, Cybersecurity in ASEAN: An Urgent Call to Action. https://www.kearney.com/service/digital-analytics/article/-/insights/cybersecurity-in-asean

Barrinha, A., & Renard, T. (2020). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 6(2), 115-129.

Bendiek, A., & Pander Maat, M. (2019). The EU's regulatory approach to cybersecurity. EU Cyber Partnerships, 1-14.

Benincasa, E. (2020). *The role of regional organizations in building cyber resilience: ASEAN and the EU*. Pacific Forum. https://pacforum.org/wp-content/uploads/2020/06/issuesinsights_Vol20WP3-1.pdf

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Buchanan, B. (2017). The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press.

Burt, A. (2019). *Privacy and Cybersecurity Are Converging. Here’s Why That Matters for People and for Companies.* Harvard Business Review. https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

CACJ. (2013). *Announcements – CACJ*. Council of ASEAN Chief Justices . https://cacj-ajp.org/announcements/

Callo-Müller, M. V. (2018). *GDPR and CBPR: Reconciling Personal Data Protection and Trade*. Asia-Pacific Economic Cooperation (APEC). https://www.apec.org/docs/default-source/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade/218_PSU_Policy-Brief_GDPR_CBPR.pdf

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? Journal of Common Market Studies, 55(6), 1254-1272.

CBPR. (2011). *Cross Border Privacy Rules System*. https://cbprs.org/

Chen, X., & Yang, Y. (2022). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *The International Spectator*, 1–18. https://doi.org/10.1080/03932729.2022.2066841

Choucri, N. (2012). *Cyberpolitics in International Relations*. MIT Press. https://mitpress.mit.edu/9780262517690/cyberpolitics-in-international-relations/

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. West European Politics, 42(2), 278-301.

Cisco, & A.T. Kearney. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action*. https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-in-asean/files/assets/common/downloads/publication.pdf

Clausmeier, D. (2022). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review*, *4*. https://doi.org/10.1365/s43439-022-00076-5

Council for Security Cooperation in the Asia Pacific. (2019). *1 st Meeting of the CSCAP Study Group on International Law and Cyberspace DRAFT PROCEEDINGS*. http://www.cscap.org/uploads/CSCAP%20Co-chairs%20Report%20for%20First%20Study%20Group%20.pdf

CSA Singapore. (2019). *ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism*. https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Multilateral/ASEAN+Member+States+Agree+to+Move+Forward+on+a+Formal+Cybersecurity+Coordination+Mechanism.pdf

Domingo, F. C. (2016). Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy*, (2), 154–168. https://doi.org/10.1080/01495933.2016.1176467

DPF. (2020). *Data Privacy Framework*. Www.dataprivacyframework.gov. https://www.dataprivacyframework.gov/

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, 15(1), 105-122.

Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance*, *6*(2), 22. https://doi.org/10.17645/pag.v6i2.1385

EEAS. (2019). *ASEAN-EU Statement on Cybersecurity Cooperation | EEAS*. Www.eeas.europa.eu. https://www.eeas.europa.eu/node/66196_en

EEAS. (2021). *EU and ASEAN develop joint software against cyberattacks | EEAS*. Www.eeas.europa.eu. https://www.eeas.europa.eu/eeas/eu-and-asean-develop-joint-software-against-cyberattacks_en

EEAS. (2024). *EU-ASEAN Relations | EEAS*. Www.eeas.europa.eu. https://www.eeas.europa.eu/eeas/eu-asean-relations_en#:~:text=Dialogue%20between%20the%20EU%20and

ENISA. (2023). *NIS2 Directive*. ENISA. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? International Political Science Review, 27(3), 221-244.

EUR-Lex. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Europa.eu. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

EUR-Lex - 52013JC0001 - EN - EUR-Lex. (2013). Eur-Lex.europa.eu. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

Eur-Lex: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Eur-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity

European Commission. (n.d.). *The EU cybersecurity certification.* Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

European Commission. (2019). *The EU and ASEAN: Building stronger digital economy & connectivity cooperation | Shaping Europe's digital future*. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/library/eu-and-asean-building-stronger-digital-economy-connectivity-cooperation

European Commission . (2022). *EU trade relations with Association of South East Asian Nations (ASEAN)*. Policy.trade.ec.europa.eu. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/association-south-east-asian-nations-asean_en#:~:text=ASEAN%20as%20a%20whole%20represents

European Council: (n.d.). *Cyber defence: Council updates policy framework*. Www.consilium.europa.eu. https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/

European Defence Agency: (n.d.). *Cyber Defence*. Default. Retrieved June 11, 2024, from https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

European Parliament. (2022). *Fact Sheets on the European Union - Southeast Asia*. Www.europarl.europa.eu. https://www.europarl.europa.eu/factsheets/en/sheet/183/southeast-asia

Fahey, E. (2014). The EU's cybercrime and cyber-security rule-making: Mapping the internal and external dimensions of EU security. European Journal of Risk Regulation, 5(1), 46-60.

Feakin, T., Hawkins, Z., & Nevill, L. (2016). *CYBER MATURITY IN THE ASIA-PACIFIC REGION* . https://ad-aspi.s3.ap-southeast-2.amazonaws.com/import/ASPI-Cyber-Maturity-2016.pdf?VersionId=rL6DRSNr06xET_0OEycZuhHj_54SLbC1

Flers, N. A. de . (2010). *EU-ASEAN Relations: The Importance of Values, Norms and Culture* . EU Center in Singapore. https://aei.pitt.edu/14480/1/EUASEAN%2DAlecuFlers%2D8June2010.pdf

Gribakov, A. (2019). *Cross-Border Privacy Rules in Asia: An Overview*. Lawfare. https://www.lawfaremedia.org/article/cross-border-privacy-rules-asia-overview

Hakmeh, J. (2020). *A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet*. Council on Foreign Relations. https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet

Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *Asia Policy*, *18*, 131–160. https://www.jstor.org/stable/24905282

Hill, R. (2014). The Internet, its governance, and the multi-stakeholder model. *The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media Preview Publication Details*, (2), 16–46. https://doi.org/10.1108/info-05-2013-0031

Hwee, Y. L. (2010). *The EU as a Security Actor in Southeast Asia Reorientation*. https://www.kas.de/documents/252038/253252/Panorama_2-2010_SecurityPolitics_Hwee.pdf/c91fa8f2-b317-1152-63ba-e97e7e0248fe

Indonesia Ministry of Finance. (2020). *The Government of ICT and Electricity Development Go Up to the Village for Digital Transformation*. https://kemenkeu.go.id/informasi-publik/publikasi/berita-utama/pemerintah-kejar-pembangunan-ict-dan-listrik-hingg

INTERPOL. (2020). *ASEAN Cybercrime Operations Desk*. Www.interpol.int. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk

ITU. (2018). *Global Cybersecurity Index (GCI) 2018* . https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ITU. (2020). *Global cybersecurity index 2020* . https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

Kaider, R. (2015). "The Birth of Cyberwar." Political Geography 46: 11–20. doi:10.1016/j.polgeo. 2014.10.001

Kasper, A., & Vernygora, V. (2021). The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? *Cuadernos Europeos de Deusto*, (65), 29–71. https://doi.org/10.18543/ced-65-2021pp29-71

Kent, G. (2015). *The Mutual Legal Assistance Problem explained*. The Center for Internet and Society. https://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained

Khandekar, G. (n.d.). *EU-ASEAN Relations*. AGORA Asia-Europe. https://www.files.ethz.ch/isn/177603/Mapping%20EU-ASEAN%20relations.pdf

Kingdon, J. W. (2011). Agendas, alternatives, and public policies. Longman.

Lim Min Zhang. (2020). *Singapore Budget 2020: $1b over next 3 years to shore up cyber and data security capabilities*. The Straits Times. https://www.straitstimes.com/singapore/singapore-budget-2020-1b-over-next-3-years-to-shore-up-cyber-and-data-security

Merriam-Webster. (n.d.). E-commerce. In Merriam-Webster.com dictionary. Retrieved June 23, 2024, from https://www.merriam-webster.com/dictionary/e-commerce

Merriam-Webster. (n.d.). End user. In Merriam-Webster.com dictionary. Retrieved June 23, 2024, from https://www.merriam-webster.com/dictionary/end%20user

Merriam-Webster. (n.d.). Interoperability. In Merriam-Webster.com dictionary. Retrieved June 23, 2024, from https://www.merriam-webster.com/dictionary/interoperability

Molthof, M. (2012). *ASEAN and the Principle of Non-Interference*. E-International Relations. https://www.e-ir.info/2012/02/08/asean-and-the-principle-of-non-interference/

National Institute of Standards and Technology. (n.d.). Cyber hygiene practices

Noor, E. (2018). *ASEAN Takes a Bold Cybersecurity Step*. Thediplomat.com. https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/

Nye, J. S. (2014). The regime complex for managing global cyber activities. Global Commission on Internet Governance Paper Series, 1.

Palo Alto Networks. (2020). *The State of Cybersecurity in ASEAN.* https://www.paloaltonetworks.sg/apps/pan/public/downloadResource?pagePath=/content/pan/en_SG/resources/whitepapers/the-state-of-cybersecurity-in-asean-2020

Plan of Action to Implement the ASEAN-EU Strategic Partnership (2023-2027)

Princen, S. (2007). Agenda-setting in the European Union: A theoretical exploration and agenda for research. Journal of European Public Policy, 14(1), 21-38.

Rand Corporation. Examining the EU’s Military Capabilities for Cyber Defence. https://www.rand.org/randeurope/research/projects/eu-military-cyber-defence.html

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Rehrl, J. (Ed.). (2019). *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union*. Federal Ministry of Defence of the Republic of Austria.

Robert Siudak (2022) Cybersecurity discourses and their policy implications, Journal of Cyber Policy, 7:3, 318-335, DOI: 10.1080/23738871.2023.2167607

Sari, M. (2023). ASEAN Regional Effort on Cybersecurity and its Effectiveness. *KEIO SFC JOURNAL*, *23*(1). https://gakkai.sfc.keio.ac.jp/journal/.assets/SFCJ23-1-02.pdf

Swinfen Green, J. (2015). *Cyber Security: An Introduction for Non-Technical Managers*. Routledge & CRC Press. https://www.routledge.com/Cyber-Security-An-Introduction-for-Non-Technical-Managers/Green/p/book/9780367606114

Tan, S., & Syahirah Azman, N. (2019). *The EU GDPR's impact on ASEAN data protection law*. Financier Worldwide. https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law

The ASEAN Magazine. (2022). *ASEAN Revs Up. Digital Transformation*. https://asean.org/wp-content/uploads/2022/11/Issue-23-Digital-Transformation-digital-version.pdf

Tran Dai, C., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217–235. https://doi.org/10.1080/23738871.2018.1487987

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. https://www.theguardian.com/world/2007/may/17/topstories3.russia

US Department of Homeland Security. (2022). *Cybersecurity*. Ready.gov. https://www.ready.gov/cybersecurity

Viola de Azevedo Cunha, M. (2017). The GDPR and the export of data protection norms. In G. González Fuster, R. van Brakel, & P. De Hert (Eds.), Research Handbook on Privacy and Data Protection Law. Edward Elgar Publishing.

Voigt, P., & Bussche, A. von dem . (2017). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Watkins, M. D. (2007). *Demystifying strategy: The what, who, how, and why*. Harvard Business Review. https://hbr.org/2007/09/demystifying-strategy-the-what

Wessel, R. A. (2015). Towards EU cybersecurity law: Regulating a new policy field. In N. Tsagourias & R. Buchan (Eds.), Research Handbook on International Law and Cyberspace. Edward Elgar Publishing

Wong, R. (2019). The European Union in the Asia-Pacific: Rethinking Europe's strategies and policies. In *JSTOR*. Manchester University Press. https://www.jstor.org/stable/j.ctv18b5hpk.17

World Economic Forum. (n.d.). *Digital ASEAN*. World Economic Forum. https://www.weforum.org/projects/digital-asean/

Xiaoyu, P. (2012). Socialisation as a Two-way Process: Emerging Powers and the Diffusion of International Norms. *The Chinese Journal of International Politics*, *5*(4), 341–367. https://doi.org/10.1093/cjip/pos017

Xuechen, I. C. (2018). The Role of ASEAN's Identities in Reshaping the ASEAN–EU Relationship. *Contemporary Southeast Asia*, *40*(2), 222–246. https://www.jstor.org/stable/26539179?seq=1

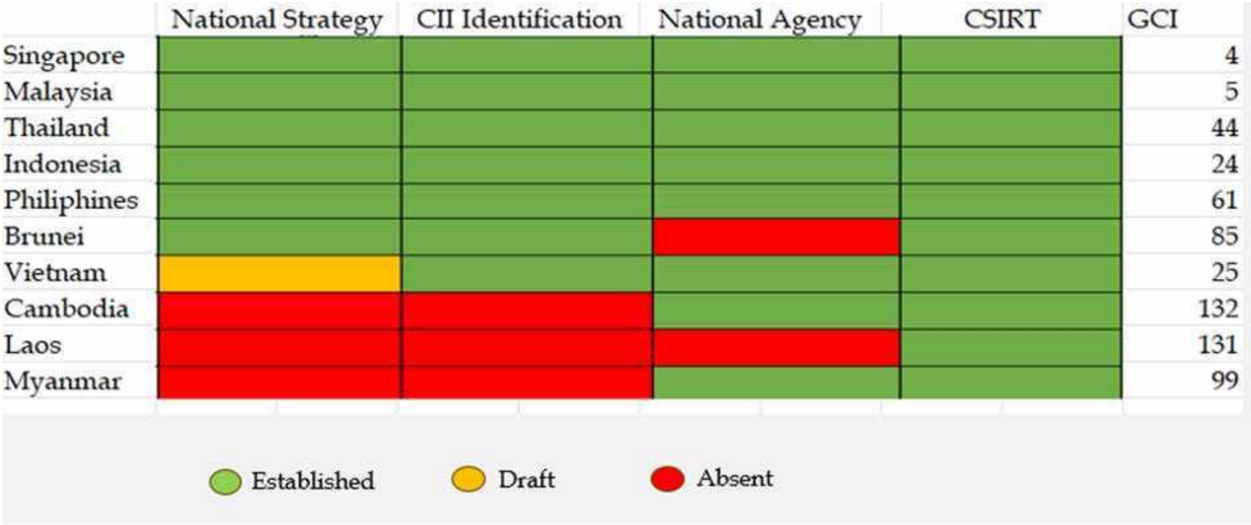
Yeoh, A. (2020). *Budget 2021: RM27mil allocation for CyberSecurity Malaysia hailed by industry players*. The Star. https://www.thestar.com.my/tech/tech-news/2020/11/06/budget-2021-rm27mil-allocation-for-cybersecurity-malaysia-hailed-by-industry-players

Appendices

Appendix 1

Table 1 - National Capabilities of ASEAN Member States

Note. Sourced from ITU: Global Cybersecurity Index (GCI) (2020)



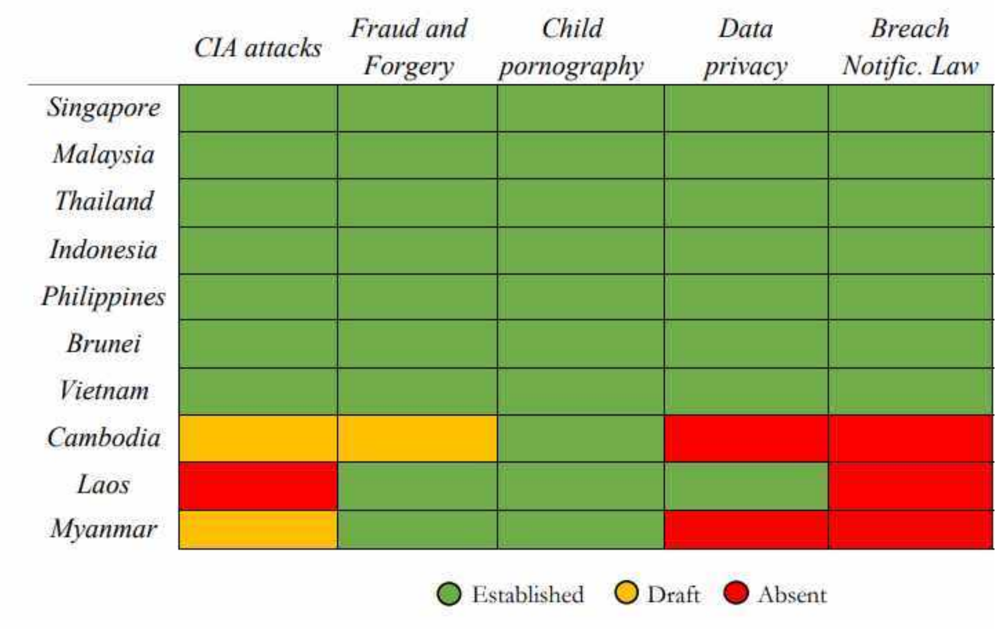
	National Strategy	CII Identification	National Agency	CSIRT	GCI
Singapore	🟩	🟩	🟩	🟩	4
Malaysia	🟩	🟩	🟩	🟩	5
Thailand	🟩	🟩	🟩	🟩	44
Indonesia	🟩	🟩	🟩	🟩	24
Philiphines	🟩	🟩	🟩	🟩	61
Brunei	🟩	🟩	🟥	🟩	85
Vietnam	🟨	🟩	🟩	🟩	25
Cambodia	🟥	🟥	🟩	🟩	132
Laos	🟥	🟥	🟥	🟩	131
Myanmar	🟥	🟥	🟩	🟩	99

🟢 Established 🟡 Draft 🔴 Absent

Appendix 2

Table 2 - Cybersecurity and Data Privacy Legislation across ASEAN

Sourced from Benincasa, E. (2020, p.24)



	CIA attacks	*Fraud and Forgery*	*Child pornography*	*Data privacy*	*Breach Notific. Law*
Singapore	🟩	🟩	🟩	🟩	🟩
Malaysia	🟩	🟩	🟩	🟩	🟩
Thailand	🟩	🟩	🟩	🟩	🟩
Indonesia	🟩	🟩	🟩	🟩	🟩
Philippines	🟩	🟩	🟩	🟩	🟩
Brunei	🟩	🟩	🟩	🟩	🟩
Vietnam	🟩	🟩	🟩	🟩	🟩
Cambodia	🟨	🟨	🟩	🟥	🟥
Laos	🟥	🟩	🟩	🟩	🟥
Myanmar	🟨	🟩	🟩	🟥	🟥

🟢 Established 🟡 Draft 🔴 Absent