PACIFIC FORUM

The role of regional organizations in building cyber resilience: ASEAN and the EU

By
Eugenio Benincasa

ISSUES & INSIGHTS

WORKING PAPER

VOL. 20, WP3 | June 2020

Pacific Forum

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

TABLE OF CONTENTS

ABSTRACT

This paper explores the role of regional organizations in crafting solutions that are able to address both the scale and cross-border nature of cyber threats, as well as the challenges inherent to an anarchical international system. It focuses on the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) and the cybersecurity frameworks they have developed in the last few years. The EU has significantly improved regional cyber resilience and cooperation by setting out ambitious goals, enhancing information sharing and harmonizing practices across its member states. In contrast, ASEAN has a lack of a strong unifying governance or legal framework, which limits the collective capability of the region to capitalize on shared knowledge to prevent and mitigate cyber threats. The paper aims to elaborate on relevant measures that could be implemented in ASEAN based on a comparative analysis with the EU. Despite the stark differences between the two organizations, there is common ground in some areas for the development of policy recommendations aimed at enhancing ASEAN's cyber resilience, eliminating the need to reinvent the wheel in key policy areas. To this end, this paper analyzes the two organizations' cybersecurity frameworks in line with the four pillars of cyber capacity building identified by the European Institute for Security Studies (EUISS) and adjusted to a regional context: overarching regional strategy, institutional framework for cyber threat prevention and response, harmonization of cybercrime and data privacy legislation, and cyber awareness and hygiene.

1. INTRODUCTION

Today's international landscape is characterized by countries with varying levels of cyber maturity, threatened by a myriad of state and non-state actors with different intentions and offensive capabilities. The scale and cross-border nature of these threats are such that international cooperation has become essential, as major threats often affect multiple jurisdictions at the same time, propagating rapidly across networks and computer systems. An example is the 2017 WannaCry ransomware attack, which spread across 150 countries in just a few days, affecting around 230,000 computers and causing an estimated $4 billion in losses worldwide[1]. These complexities are further exacerbated by the problems of attribution and jurisdictional access, as perpetrators can be difficult to identify and prosecute due to the use of anonymity-enhancing techniques and the lack of unfettered access to singular state jurisdictions to investigate transnational cyber offenses. Despite these challenges, to date there is no effective mechanism or framework for international cooperation in cybersecurity due to irreconcilable differences across states globally and rising tensions between great powers competing for different visions of cyberspace.

This paper explores the role of Regional Organizations (ROs) in crafting solutions that are able to address both the scale and cross-border nature of cyber threats, as well as the challenges inherent to an anarchical international system, including:

Ideological Inconsistency: As of today, there exist no binding multilateral cybercrime agreement that has been able to bring most countries together. Countries often disagree due to divergent priorities and views on critical principles, including over the applicability of existing international law to cyberspace. Given this global fragmentation, it is unrealistic to hope that global consensus will emerge either in the short or medium term. The recent failure of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) to reach an agreement on international norms and confidence building measures (CBMs) in 2017 [2] exemplifies this problem.

The Coordination Dilemma: Ensuring protection from cyber exploitation is a problem all states have to tackle, but no actor can address the vulnerabilities in cyberspace on its own. At the same time, there is no "one-size-fits-all" approach to build cyber resilience, as it is not plausible to suggest that the same standardized measures be adopted in every jurisdiction and implemented according to the same mechanisms. States have significant differences in culture, geography, economic development, structural organization and form of government, or conflicting interests, which will inevitably result in different strategic and operational frameworks, institutions, legislation, and capabilities. The absence of a global solution to these challenges and its associated risks will become ever more relevant as new technologies are developed and the world becomes more interconnected, exposing us to new vulnerabilities.

[1] Kaspersky: What is WannaCry ransomware? https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry
[2] Sukumar, *The UNGGE Failed. Is International Law in Cyberspace Doomed as Well?* (*Lawfare*, 2017)

Neighboring countries are more likely to share greater similarities and interests: they are more likely to have interconnected infrastructures and economies, leaving them vulnerable to the same threat actors[3] and cyberattacks that spill across borders[4]. These commonalities make it easier to work toward a common strategy, develop common standards, and coordinate incident response and capacity-building. As stated by a Microsoft report on Critical Infrastructure Protection, "regional elements are important… as they provide us with an opportunity to investigate whether the solutions to global cybersecurity challenges need to be tailored to a particular context to be effective, whilst at the same time allowing us to retain a level of scale[5]."

Needless to say, cybersecurity is a common societal challenge that requires all layers of government, economy, and society to be involved, especially the private sector. These layers include ROs, defined as international associations linking together geographically and ideologically related states[6]. This paper will examine the role of ROs and how they can contribute to cyber resilience—defined as the ability to prepare for, respond to and recover from cyberattacks[7]—by focusing on the Association of Southeast Asian Nations (ASEAN) and the European Union (EU). ASEAN and the EU are often referred to as the two most successful regional organizations in the world[8]. ASEAN is a regional intergovernmental organization comprising 10 countries in Southeast Asia. It has a total population of about 659 million (around 200 more than the EU) and is the world's third most populous region and seventh largest market. The EU is a political and economic union of 27 member states with an estimated population of 446 million. It is the world's largest trading bloc and second largest economy, after the United States[9]. ASEAN and the EU were both founded to foster peace and seek economic integration of their member states into a single market.

The EU has developed a solid and comprehensive cybersecurity framework in the last few years, setting out ambitious goals, enhancing information sharing, and harmonizing practices across its member states, marking a significant improvement for regional cyber resilience and cooperation. In contrast, ASEAN has no strong unifying governance or legal framework, limiting the collective capability of the region to capitalize on shared knowledge to prevent and mitigate cyber threats. Despite the great benefits brought about by fast technological change in the last few years, there remains a huge gap in the cybersecurity policy framework of many ASEAN member states, making the region particularly vulnerable to cyber risks and exploitation by state and non-state actors alike[10]. Besides being primary targets for cyberattacks, countries such as Malaysia, Indonesia, and Vietnam are global hotspots for suspicious web activities, indicating that these countries are being used as launchpads for attacks by cybercriminals and hacktivists[11]. Another threats stem from state-sponsored cyberattacks, such as those from North Korea which aims to gain financial resources to support its nuclear and missile programs[12]. Additionally, the Chinese group APT40 has recently been accused of

[3] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Cyber Conflict Studies Association, 2013)
[4] Nicholas, *The role that regions can and should play in critical infrastructure protection (Microsoft*, 2018)
[5] Nicholas, *The role that regions can and should play in critical infrastructure protection (Microsoft*, 2018)
https://sites.google.com/site/walidabdulrahim/home/my-studies-in-english/20-introduction-to-regional-organizations
[6] Dr. Abdulrahim: Private Site for Legal Research and Studies: Introduction to Regional Organizations
[7] IT Governance: What is cyber resilience. https://www.itgovernance.co.uk/cyber-resilience
[8] *ASEAN and the EU: Differences and challenges, (The Straits Times, 2017)*
[9] *ASEAN and the EU: Differences and challenges, (The Straits Times, 2017)*
[10] Dobberstein, Gerdemann, Pereira, *Cybersecurity in ASEAN: An Urgent Call to Action*, (AT Kearney, 2018)
[11] Dobberstein, Gerdemann, Pereira, *Cybersecurity in ASEAN: An Urgent Call to Action*, (AT Kearney, 2018)
[12] *North Korea could target Southeast Asia's vulnerable crypto sector, says defense think tank* (*CNBC*, 2019)

conducting cyber espionage against countries strategically important to China's "Belt and Road Initiative" in Southeast Asia, organizing campaigns against maritime, defense, aviation, government, and technology organizations[13].

Besides undermining regional security, the combination of criminal and state-sponsored threats magnifies ASEAN's risk profile, hindering foreign investment and economic growth. Overall, the estimated exposure of ASEAN's top companies amounts to $750 billion, and an overwhelming majority of industry leaders claim that concerns over cybersecurity are impeding innovation, particularly in technology products, business, retail, and banking services[14]. This situation is exacerbated by an underinvestment in cybersecurity. Most ASEAN countries—with the exception of Singapore—fall well below the global average of cybersecurity spending as percentage of GDP despite the deteriorating threat landscape[15].

In ASEAN, the last few years have witnessed steady and significant progress as cybersecurity policy gained important momentum, giving rise to new institutions and relevant discussions. As the region puts forward new policies and coordination mechanisms to boost its resilience, this paper aims to explore opportunities for elaborating relevant measures that could contribute to this goal based on a comparative analysis of the EU experience. Despite the stark differences between the two organizations, there is common ground in some areas for the development of policy recommendations aimed at enhancing ASEAN's cyber resilience, eliminating the need to reinvent the wheel in key policy areas. To this end, it will be essential to take into account the peculiarities of the institutions and procedures at the basis of the ASEAN decision-making process, and how they differ from the EU. In the words of Singapore's former Minister for Communications and Information Dr. Yaacob Ibrahim, "…while staying plugged in to the global conversations, [ASEAN] should also make sure that norms and behaviors are kept relevant and applicable to our unique ASEAN context and cultures[16]."

Based on an analysis of methods and approaches adopted by different countries and organizations, the European Union Institute for Security Studies (EUISS) identified the following pillars of national cyber capacity building: national strategic framework, incident management, criminal justice in cyberspace, and cyber hygiene and awareness[17]. As this paper focuses exclusively on the role of ROs and their contribution to enhancing cyber resilience, this paper adapts these pillars to a regional governance context, emphasizing the following policy areas:

- Overarching regional strategy (derived from national strategic framework);
- Institutional framework for cyber threat prevention and response (derived from incident management);
- Harmonization of cybercrime and data privacy legislation (derived from criminal justice in cyberspace).
- Cyber hygiene and awareness (unvaried)

[13] FireEye, Inc: M-Trends 2019, https://content.fireeye.com/m-trends
[14] Dobberstein, Gerdemann, Pereira, *Cybersecurity in ASEAN: An Urgent Call to Action*, (AT Kearney, 2018)
[15] Dobberstein, Gerdemann, Pereira, *Cybersecurity in ASEAN: An Urgent Call to Action*, (AT Kearney, 2018)
[16] CSA Singapore: Opening Speech by Dr Yacoob Ibrahim, https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2016
[17] Pawlak, *Operational Guidance for the EU's international cooperation on cyber capacity building,* (EUISS, 2018)

For each of the four strategic aspects listed above, this paper analyzes the current situation in both regions, starting with the EU then turning to ASEAN. While the topics of these sections are not mutually exclusive, they are arranged in a way that prioritizes flow and cohesion. Finally, this paper will conclude with policy recommendations based on the preceding analysis.

2. OVERARCHING REGIONAL STRATEGY

Cyberspace in the EU and ASEAN carries several risks and challenges that need to be addressed by a collective regional response through a coherent plan of action, adequate institutions, and a common stance on fundamental issues. To that end, adopting a regional cybersecurity strategy is an essential cornerstone of cyber resilience. Michael Watkins, Professor of Leadership and Organizational Change at IMD Business School, defines strategy as a set of guiding principles that when communicated and adopted in the organization generates a desired pattern of decision making[18]. It provides a clear roadmap based on a set of guiding principles and priorities that define the actors involved in the process and the actions they should take—individually and collectively—based on available resources. In the context of cybersecurity, a regional strategy should highlight the role of member states and the private sector as the key actors in enhancing cybersecurity. This is due to the fact that, despite the different levels of regional integration, member states still retain the majority of decision-making power in both the EU and ASEAN, and that the large majority of network and information systems are privately owned and operated. At the regional level, given the cross-border nature and scale of the threat, the strategy should aim to set a shared vision and principles and create an enabling environment to facilitate coordination and cooperation, harmonize practices, raise awareness, and build capacity across member states.

2.1 EU Cybersecurity Strategy: "An open, safe, and secure cyberspace"

In its 2013 Cybersecurity Strategy, the European Commission (EC) identified core principles and strategic priorities to guarantee an open, safe, and secure cyberspace in the EU. To this end, it outlined the roles and responsibilities that EU agencies and institutions, member states, industry, and academia should play[19]. It outlined five main objectives:

1) Achieving cyber resilience: This first EU strategic goal focuses on capacity development, awareness raising, and partnership building between public authorities and the private sector[20]. More specifically, it lays down a detailed plan of action aimed at developing a robust regional architecture to intensify strategic and technical cooperation among member states and to strengthen national capabilities. It also highlights the importance of establishing an effective incentive scheme for private companies to invest more in security solutions. Finally, cooperation between the public and private sector is emphasized and considered essential since the large majority of network and information systems are privately owned and operated[21].

A critical milestone in this effort was reached with the adoption of the 2016 Network and Information Security (NIS) Directive, the first piece of EU-wide cybersecurity legislation aimed at consolidating national capabilities, cross-border collaboration, and national supervision of critical sectors. In addition, the EU also passed the 2019 Cybersecurity Act to strengthen the mandate of ENISA, its Cybersecurity Agency in charge of coordinating response to large-scale cyber incidents affecting multiple EU member states. ENISA is also responsible for raising

[18] Watkins, *Demystifying Strategy: The What, Who, How, and Why*, (Harvard Business Review, 2007)
[19] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[20] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[21] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

cybersecurity awareness through reports, workshops, and public-private partnerships, and offering recommendations and independent advice on several ICT issues.

2) Drastically reducing cybercrime: The EU aims to significantly reduce cybercrime by means of strong and effective legislation, operational capability, and improved coordination at the regional level[22]. With regard to national legislation, the EC urged all of its member states to ratify the Budapest Convention and implement its provisions within their domestic frameworks. As of today, the 2004 Budapest Convention is the only existing multilateral legal instrument to address cybercrimes and international cooperation in cyberspace. To date, only 64 states have ratified the convention. Many important global actors (China, Russia, India, and Brazil) declined to adopt it for different reasons, such as not having been involved in the drafting process, but mainly because of perceived sovereignty violations within Article 32 which permits extraterritorial searches[23].

To enhance regional capability and coordination, the EU Cybersecurity Strategy emphasizes the need to identify and strengthen skill gaps across member states to investigate and combat cybercrime by working closely with relevant EU agencies such as EUROPOL's European Cybercrime Centre (EC3), which coordinates cross-border law enforcement activities against computer crimes and acts[24].

3) Developing cyber defense policy and capabilities: Cyberspace is considered to be the fifth domain of warfare on par with air, sea, land, and space, as success of military operations in the physical world is increasingly dependent on the availability of, and access to, cyberspace[25]. EU cyber defense efforts seek to promote the development of capabilities and technologies to protect member states' national security interests, as well as the networks of EU-wide missions and operations[26]. Key priorities include the elaboration of cyber defense strategies, especially since most EU member states do have a cyber defense doctrine in place as of today[27].

The EU adopted a cyber defense policy framework in 2014 (updated in 2018), identifying six priority areas. The primary focus is the development of cyber defense capabilities and the protection of the EU communication and information networks. Other priorities include training and exercises, research and technology, civil-military cooperation, and international cooperation[28]. The European Security and Defence College (ESDC), the European Defence Agency (EDA), and the European External Action Service (EEAS) are the main actors in this effort.

4) Developing industrial and technological resources for cybersecurity: The EU seeks to promote a single market for cybersecurity products and incentivize R&D investments and

[22] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[23] Hakmeh, *A New UN Cybercrime Treaty ? The Way Forward for Supporters of an Open, Free, and Secure Internet*, (Council on Foreign Relations, 2020)
[24] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[25] Rand Corporation: Examining the EU's Military Capabilities for Cyber Defence. https://www.rand.org/randeurope/research/projects/eu-military-cyber-defence.html
[26] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[27] European Defence Agency: Cyber Defence. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence
[28] European Council: Cyber defence: Council updates policy framework. https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/

innovation to fill the gaps in ICT security market, as well as prepare for the next generation of security challenges. To this end, the EU aims to adopt higher supply chain security standards and establish voluntary EU-wide certification schemes by means of appropriate cybersecurity performance requirements across the whole value chain[29]. The 2019 EU Cybersecurity Act has therefore increased the resources and authority of ENISA and established an EU cybersecurity certification framework for digital products, services and processes, introducing common requirements and evaluation criteria across the region[30]. As part of its mandate, ENISA is also tasked with preparing draft cybersecurity certification schemes in consultation with the private sector and other relevant stakeholders.

5) Establishing a coherent international cyberspace policy for the European Union and promote core EU values: The EU does not wish to create new international legal instruments to deal with cybersecurity. In its international cyberspace policy, the EU supports the application of existing international law in cyberspace and aims to participate in international efforts to build cybersecurity capacity[31]. It also advocates for the widespread adoption of the Budapest Convention as the best way to address cybercrime, and it believes International Humanitarian Law and Human Rights law to be applicable when armed conflict extends into the cyber sphere[32]. In addition, a state victim of an "internationally wrongful act" (the breach by a State of an international obligation) may, depending on the case at hand, respond appropriately to a cyberattack following the proportionality principle[33]. To better define threat factors and available means, the EU developed a "cyber diplomacy toolbox," a framework to encourage cooperation, facilitate threat mitigation, and influence the behavior of potential aggressors in the long term.

The EU Cybersecurity Strategy also touches on the protection of personal data and privacy, stating that "any information sharing for the purposes of cybersecurity should be compliant with EU data protection law and take full account of the individuals' rights in this field[34]." To better address this issue and strengthen existing legislation, in 2018, the EU initiated and adopted aground-breaking privacy framework called General Data Protection Regulation (GDPR) to give EU citizens more control over their personal data.

Since the enactment of the EU cybersecurity strategy in 2013, significant steps forward have been made with regard to each of the five main goals by means of new laws, projects, the empowerment of existing institutions, and the creation of new ones. Some of these developments have been mentioned in the previous paragraphs and will be further analyzed throughout the remaining sections of this paper. What is clear is that by adopting a regional strategy with a defined timeline and plan of action, the EU was able to set the ground for the achievement of critical goals to enhance its cyber resilience.

[29] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[30] European Commission: The EU cybersecurity certification. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[31] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[32] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[33] Delerue, Kulesza, Pawlak, *The Application of International Law in Cyberspace: Is there a European Way?,* (EU Cyber Direct. 2019)
[34] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

2.2 ASEAN: The case for a regional strategy

Over the last ten years, ASEAN's strategic efforts have been mostly directed towards the development of a strong Information and Community Technology (ICT) ecosystem and promoting innovation, reaching remarkable results. Since the launch of the ASEAN ICT Masterplan 2015, ICT has become an engine for economic growth, resulting in increased Internet penetration, infrastructure development and lower costs of mobile cellular services[35]. The gap of the digital divide has also narrowed, although significant differences among member states still remain. Yet this plan did not include cybersecurity as a strategic priority. The following paragraphs will look at ASEAN's strategic effort based on the categories of analysis contained in the EU Cybersecurity Strategy. The sections on "developing cyber defense policy and capabilities" and "developing industrial and technological resources for cybersecurity" are not included, given that the region has not yet made any collective effort toward the creation of a common cyber defense framework or cybersecurity single market.

Achieving cyber resilience: Cyber threats were first officially recognized as a "threat that could impede ASEAN's progress as a digitally-enabled community" in the ASEAN ICT Masterplan 2020, in which Information Security and Assurance was included as one of the eight main strategic thrusts[36]. More specifically, four action points were outlined: 1) Develop regional data protection principles; 2) Develop regional network security best practices; 3) Develop regional critical information infrastructure resilient practices; and 4) Strengthen cyber incident emergency response collaboration[37]. Major initiatives that were included in the 2020 plan included the potential creation of a regional ASEAN Computer Emergency Response Team (CERT) - composed of representatives of the member states' CERTs - to enhance collective readiness, and the development of an Incident Reporting Framework. Despite the fact that some progress has been made in some of these areas, ASEAN has yet to develop a region-wide comprehensive cybersecurity strategy outlining a shared vision, scope, objectives and priorities with a clear governance structure and defined roles and responsibilities. The 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation highlighted the need to build on some of these issues, identifying priorities and key stakeholders[38]. As of now, however, it is unclear how different institutions interoperate and what future developments will entail, since cybersecurity is not covered within the most recent Masterplan on ASEAN Connectivity 2025. This Masterplan only briefly mentions in Chapter 3, G.13 that "Additional challenges include establishing a policy framework for data sharing, online privacy, and cybersecurity...[39]." It does, however, include an initiative calling for the creation of a regional framework for personal data protection by exploring possible areas of harmonization of member states' legislation.

Some ASEAN member states do not have a national strategy in place to date, such as Myanmar, Laos, Cambodia, or Vietnam. In addition, legislative and enforcement measures vary greatly

[35] ASEAN: ICT Masterplan 2015 Completion Report https://www.asean.org/storage/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf
[36] ASEAN: ICT Masterplan 2015. https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf
[37] ASEAN: ICT Masterplan 2015. https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf
[38] ASEAN: ASEAN Leaders' Statement on Cybersecurity Cooperation. https://asean.org/storage/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf
[39] Master Plan on ASEAN Connectivity 2025. https://asean.org/storage/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf

across the region. Regional strategic and legal divergence are structural challenges that have a major impact on regional cybersecurity. As intra-ASEAN trade and investment increase, the region increases its overall vulnerability stemming from its less protected member states, intensifying systemic risk, and making the region "only as strong as its weakest link[40]." Indeed, threat actors need not target a business' core system located in a "cyber mature" state to exploit its vulnerabilities but can instead target its weaker components in countries with lower regulatory and/or supply chain security standards. Critical information infrastructure (CII) remains at an elevated risk of cyberattack as different member states have not yet adopted a CII identification and protection mechanism and there is no region-wide coordination mechanism to address it.

International cyberspace policy: With regard to international cyberspace policy, in 2018 ASEAN endorsed in principle the 11 voluntary, non-binding norms recommended by the 2015 UNGGE, signaling a growing awareness that cybersecurity is a region-wide strategic matter that needs to be addressed as a whole. These norms focus on rules and principles for the behavior of states, confidence-building measures (CBMs), international cooperation and capacity-building, and the applicability of international law to cyberspace. Further determination towards the development of a unified approach was shown in the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation, where state leaders urged "the need for ASEAN to speak with a united voice at international discussions." This statement demonstrated the ambition to develop international cybersecurity policy and capacity building frameworks to more effectively advance regional interests at such discussions[41].

Key platforms to advance engagement in international cyberspace policy have been 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. The ARF-ISM has focused on the development of CBMs to reduce the risk of conflict stemming from the use of ICTs, identifying the following priority areas: i) Establishment of a Coordination Mechanism within the ARF; ii) Awareness Building and Exchange of Best Practices; iii) Computer Emergency Response Team (CERT)-CERT Cooperation Frameworks; iv) Critical Information Infrastructure Protection Frameworks and Mechanisms; and v) Combating Criminal and Terrorist Use of ICTs[42]. CSCAP study groups also conducted substantial work on CBMs. However, at the CSCAP Cybersecurity Workshop in Semarang, Indonesia (2017), it was noted that ASEAN member states' diverging views on some critical matters had impeded the successful implementation of CBMs[43]. Since "progress ultimately depends on shared priorities, a shared vocabulary, a multi-stakeholder approach, and a

[40] Dobberstein, Gerdemann, Pereira, *Cybersecurity in ASEAN: An Urgent Call to Action*, (AT Kearney, 2018)
[41] ASEAN: ASEAN Leaders' Statement on Cybersecurity Cooperation. https://asean.org/storage/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf
[42] ASEAN 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). http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-12.pdf
[43] Council for Security Cooperation in the Asia Pacific: 1st Meeting of the CSCAP Study Group on International Law and Cyberspace. http://www.cscap.org/uploads/CSCAP%20Co-chairs%20Report%20for%20First%20Study%20Group%20.pdf

readiness to tailor solutions to the particular needs of individual states[44]," it was suggested that CSCAP study groups tackle some of these issues first. At the end of its first meeting, the main challenges to the application of international law in ASEAN identified by CSCAP participants were the following: i) Definition of cyberspace; ii) Concept of sovereignty; iii) Concept of due diligence; iv) Concept of state responsibility; v) Espionage; and vi) What constitutes use of force[45]. ASEAN member states have yet to achieve convergence on these issues.

Reducing cybercrime: As of today, some ASEAN member states do not have relevant cybercrime legislation in place. Nine out of ten have not ratified the Budapest Convention. So far, the Philippines has been the only ASEAN member state to ratify it. Different conceptions of cyberspace have given rise to different ideas about cooperation to tackle cybercrime, and the main point of contention has long been the issue of sovereignty and the perceived violations to this principle within Article 32 of the Budapest Convention, which permits extraterritorial searches. In December 2019, Cambodia and Myanmar joined Russia and China in sponsoring the United Nations resolution "Countering the use of information and communications technologies for criminal purposes", which aims to establish principles of sovereignty in cyberspace. The resolution passed 79-60 with 33 abstentions, with all ASEAN member states voting in favor—except the Philippines, which abstained[46]—successfully establishing a committee of experts that will meet from August 2020 to consider a new UN cybercrime treaty that could serve as an alternative to the Budapest Convention. This latest development signals the region's long-standing adherence to the principles of non-interference in the internal affairs of other states, and a closer alignment with the Sino-Russian view.

In summary, despite the significant progress made in the last few years, the cybersecurity landscape in ASEAN still lacks clear direction. The lack of direction has been further confirmed by the omission of cybersecurity-related provisions or statements in the recent Master Plan on ASEAN Connectivity 2025, and by the lack of substantial coordination and harmonization of practices. Progress in advancing the strategic efforts analyzed in his section is made more difficult by the nature of the ASEAN decision-making process and diverging national priorities of its member states, which I will analyze in detail in the following section. Nonetheless, ASEAN has been able to adopt regional strategies to tackle cross-border security threats in the past, such as the 2018 ASEAN Plan of Action to Prevent and Counter the Rise of Radicalization and Violent Extremism. The work plan identified core objectives and priority areas and envisioned the establishment of new entities to reduce terrorism in the region. It also provided a clear roadmap based on a set timeline and activities assigning specific responsibilities to the actors involved in the process and the actions they should take—individually and collectively—based on available resources[47].

---

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

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

[46] United Nations Digital Library: Countering the use of information and communications technologies for criminal purposes: resolution / adopted by the General Assembly. https://digitallibrary.un.org/record/3841023?ln=en

[47] Work Plan of the ASEAN Plan of Action to Prevent and Counter the rise of Radicalisation and Violent Extremism (2019-2025). https://asean.org/storage/2012/05/Bali-Work-Plan-Narrative-and-Matrix-adopted-27November2019.pdf

3. INSTITUTIONAL FRAMEWORK FOR CYBER THREAT PREVENTION AND RESPONSE

As defined by the US Department of Homeland Security, cybersecurity involves **preventing**, **detecting**, and **responding** to cyberattacks that can have wide ranging effects on the individual, organizations, the community, and the national level[48]. After setting out a strategy aimed at reaching cyber resilience, the next step is to empower relevant actors with the resources, roles, and responsibilities they need to reach strategic goals. As concerns prevention and response, ROs can play a critical role in establishing mechanisms given their ability to facilitate coordinated action and resource allocation across member states through information sharing, harmonization of practices and collective response. In contrast, detection of threats relies on the use of appropriate software and hardware mechanisms or other advanced technologies. While regional organizations can play an important role in providing guidance on the adoption of such technologies, there are structural difficulties that make it impossible for regional institutions to directly monitor all vulnerable access points in real time. Therefore, the subsequent analysis will focus on prevention and response.

This section will specifically analyze the set of institutions that are involved in enhancing regional prevention and response capabilities in the EU and ASEAN. In particular, the subsection on **prevention** will analyze the role played by decision-making entities that can propose or adopt laws, common standards, and engage in high-level strategic and technical discussions. The subsection on **response** will analyze the role played by law enforcement and the judicial system to prosecute cybercrime. This analysis will not include responses to state-to-state attacks and potential acts of war, since the role ROs can play in this domain remains limited, both strategically and operationally. Most states in both regions do not even have a cyber warfare doctrine in place[49].

3.1 EU: Towards enhanced cyber resilience

EU cybersecurity legislation has aimed at building a comprehensive and resilient policy framework and institutional architecture by means of EU directives and regulations. In European Union law, these are different legislative acts that are adopted following one of the legislative procedures set out in the EU treaties. More specifically, directives outline objectives or results that must be achieved by all member states but leave each state substantial flexibility to decide what measures to adopt to reach them considering different national circumstances. EU countries must incorporate the selected measures into their national law by a set deadline. Regulations, in contrast, are legal acts that apply automatically and uniformly to all EU countries as soon as they enter into force. They are binding in their entirety and do not need to be transposed into national law. The EC is the EU sole body that holds the power of legislative initiative, while the European Parliament (EP) and the Council of the European Union vote on legislation while retaining powers of amendment and veto throughout the legislative process. The Directive on Security of Network and Information Systems (the NIS Directive) and the 2019 Cybersecurity Act are the most relevant pieces of cybersecurity legislation that played a

[48] US Department of Homeland Security: Cybersecurity. https://www.ready.gov/cybersecurity
[49] Rand Corporation: Examining the EU's Military Capabilities for Cyber Defence https://www.rand.org/randeurope/research/projects/eu-military-cyber-defence.html

key role in reshaping the EU cybersecurity governance framework by creating new institutions and common standards.

Prevention: The NIS Directive is the backbone of EU legislation on cybersecurity, as discussed earlier. Proposed by the EC, it was adopted in 2016 and has been fully implemented by all 27 EU member states. At the national level, its main provisions include:

- The identification of operators of essential services (or critical infrastructure). While these are not explicitly defined, the directive provides member states with the criteria they need to apply to identify them[50]. For example, a service can be considered essential if it is needed for the maintenance of critical societal and/or economic activities and an incident would result in large disruptive effects.
- The elaboration of a national cybersecurity strategy outlining scope and objectives, as well as roles and responsibilities of all the actors involved[51]. Strategies must also include response and recovery measures, public-private cooperation planning, education/awareness programs, and risk assessment plans, among other things.
- The establishment of National Competent Authorities (NCAs) and single points of contact (SPoCs) for cybersecurity monitoring, reporting, incident response, and cross-border coordination[52]. These can take different forms, such as ministries of communication, intelligence services, etc.
- A computer security incident response team (CSIRT or CERT) to monitor national security incidents, provide early warnings and conduct risk analysis[53].

As far as cross-border cooperation is concerned, the NIS directive has given rise to two relevant platforms to enhance regional strategic and operational cooperation:

- The Computer Security Incident Response Teams (CSIRTs) Network, composed of representatives of the member states' CSIRTs and CERT-EU, aims to "to provide swift and effective operational cooperation," provide a forum for technical cooperation and information sharing, and improve collective incident response on the basis of voluntary mutual assistance[54].
- The Cooperation Group, composed of representatives of member states, the EC and ENISA, provides strategic guidance for the activities of the CSIRTs Network and provides a forum where member states can share good practices on several matters, including awareness-raising, training, R&D, and exchange information on risks and incidents[55].

[50] 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
[51] 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
[52] 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
[53] 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
[54] 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
[55] 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

The directive further outlines security and incident notification requirements for digital service providers, which have the obligation to notify the competent authority/CSIRT in the case of any incident having a "substantial impact" on the provision of a service. In addition, if a digital service provider is headquartered in a member state, but its networks and information are in a different member state, the competent authorities of the two member states must cooperate "as necessary[56]."

The 2019 EU Cybersecurity Act also proved important to further consolidate the EU's cybersecurity institutional framework. It strengthened the mandate of ENISA, the EU Agency for Cyber Security, increasing its resources and authority, and established a European cybersecurity certification framework for digital products, services and processes[57]. ENISA is tasked with increasing operational cooperation at EU level, helping EU member states who would request it to handle cybersecurity incidents and supporting the coordination of the EU in case of large-scale cross borders cyberattacks and crises. The EU certification framework consists of cybersecurity certification schemes that introduced common requirements and evaluation criteria across the bloc. The creation of these standards is facilitated by ENISA, which is tasked with preparing draft cybersecurity certification schemes in consultation with industry, standard groups, and relevant stakeholders[58]. The Cybersecurity Act also established the European Cybersecurity Certification Group (ECCG), composed of representatives from national cybersecurity certification authorities, and a Stakeholder Cybersecurity Certification Group (SCCG), both tasked with advising the EC and ENISA on this matter.

Response: The fast-paced and cross-border nature of cybercrime creates specific challenges for judicial and police authorities, such as the need to act quickly, overcome the differences in legislation between countries concerning how to collect and secure e-evidence, ensure swift cooperation with third countries and actors in the private sector, and ensure data security[59]. To effectively counter cyber threats and bring perpetrators to justice, the EU has established relevant departments within EUROPOL and EUROJUST, its region-wide law enforcement and judicial institutions, assigning them key roles and responsibilities. In 2013, EUROPOL set up the European Cybercrime Centre (EC3) to strengthen law enforcement response to cybercrime, facilitating coordination between national law enforcement agencies. In 2016, EUROJUST established the European Judicial Cybercrime Network (EJCN) to increase cooperation and efficiency in cybercrime investigations and prosecutions.

The 2013 EU Cybersecurity strategy identified EC3 as the European "focal point" in the fight against cybercrime. It provides analysis and intelligence, support to investigations, high level forensics, and information sharing between law enforcement agencies and with the private

[56] 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
[57] 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 certification and repealing Regulation
[58] 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 certification and repealing Regulation
[59] 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 certification and repealing Regulation (EU) No 526/2013

sector across the region[60]. The Head of EC3, or Programme Board, sets the guidelines and direction to fulfill the center's main goals and priorities, which include the following three main areas of work:

1) Strategy, composed of two teams[61]:
   - Outreach & stakeholder management: in charge of establishing partnerships and coordinating prevention and awareness measures
   - Strategy and Development: in charge of strategic analysis, the formulation of policy and legislative measures, and the development of standardized training.
2) Forensic Expertise, composed of two teams[62]:
   - Digital forensics: focuses on operational support
   - Document forensics: focuses on research and development
3) Operations, divided into three main areas[63]:
   - High-tech crimes (AP Cyborg)
   - Payment fraud (AP Terminal)
   - Online child sexual abuse (AP Twins)

In addition, the Joint Cybercrime Action Taskforce (J-CAT) works on the most relevant international cyber incidents that have a significant impact on EU member states and its citizens. Moreover, since the large majority of network and information systems are privately owned and operated, cooperation between law enforcement and industry is essential. In that respect, EC3 has established public-private partnerships through a network of Advisory Groups comprising more than 80 private companies in three major industries: Internet Security, Financial Services, and Communication Providers, to successfully identify operational priorities and industry-specific threats[64].

To facilitate and enhance cooperation between competent judicial authorities, ECJN promotes the exchange of expertise, good practices and other relevant knowledge regarding the investigation and prosecution of cybercrime[65]. One of the most effective tools employed by investigators confronted with the challenge of fighting cybercrime is to form joint investigation teams (JITs): "legal agreements between two or more countries to undertake joint transnational criminal investigations during a fixed period of time, which provide for the possibility to directly exchange data and evidence, cooperate in real time and successfully carry out urgent operations. JITs also allow for parties to be present during investigative measures on each other's territories, and to therefore share their technical and human resources more efficiently[66]." To tackle

[60] EUR-Lex: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[61] European Cybercrime Centre – EC3: About. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[62] European Cybercrime Centre – EC3: About. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[63] European Cybercrime Centre – EC3: About. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[64] European Cybercrime Centre – EC3: About. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[65] Eurojust: About Eurojust. http://www.eurojust.europa.eu/about/background/Pages/History.aspx
[66] 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 certification and repealing Regulation (EU) No 526/2013

cybercrime more effectively, EUROJUST also provides JITs with financial and operational support, as well as expertise and judicial analysis.

To enhance collaboration and tackle key challenges, such as access to and sharing of electronic evidence (e-evidence), in 2017 EUROPOL and EUROJUST established the SIRIUS Project, a platform "that helps investigators to cope with the complexity and volume of information in a rapidly changing environment by providing guidelines and tools, and by sharing experiences with peers, both online and in person[67]." Besides e-evidence, other common challenges identified by EC3 and EJCN institutions include: i) discrepancies in national legislation among member states; ii) internet governance-related challenges, such as the widespread implementation of Carrier Grade Network Address Translation (CGN); iii) use of encryption to hide relevant data and communications evidence; and d) the increase in use of cryptocurrencies for illicit transactions[68].

In summary, the EU has established a robust framework of interoperational institutions as envisioned in its 2013 strategy. While there is still a lot of room for progress, the current framework has so far resulted in stronger national capabilities and the creation of platform for effective coordination at the strategic and operational level, with a specific focus on national supervision of critical infrastructure. These developments have been complemented by region-wide law enforcement and judicial cooperation to prosecute cybercrimes which coordinate the enforcement of relevant legislation across multiple jurisdictions.

3.2 ASEAN: Building effective institutions

Contrary to the EU's decision-making mechanism based on the qualified majority voting in most areas, ASEAN's institutional voting operates based on mutual understanding and informal procedures that do not impose legally binding measures on its member states. This framework for cooperation is commonly referred to as the "ASEAN way," according to which all decisions must be based on consensus[69]. Occasionally, the "ASEAN minus X" formula is employed, allowing a few member states to move forward on the basis that other member states will follow at a later stage. This more flexible modus operandi forms part of a deliberate effort by ASEAN to avoid becoming as bureaucratic and legalistic as its counterpart in Europe, and the outcomes of its decisions are largely political and non-binding. However, this does not mean that ASEAN is not able to agree on binding instruments when there is enough political will and serious security concerns arise. In fact, it has already done so with respect to transnational crime. Two recent examples include the 2007 ASEAN Convention on Counter Terrorism and the 2015 ASEAN Convention Against Trafficking in Persons, Especially Women and Children. The grounds for these agreements included deep concern over the dangers to infrastructure, regional/international stability, and economic development, as well as human rights violations.

---

[67] Eurojust: SIRIUS Project. http://www.eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx

[68] Europol and Eurojust Public Information: Common challenges in combating cybercrime http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF

[69] ASEAN: The ASEAN Way and the Rule of Law. https://asean.org/?static_post=the-asean-way-and-the-rule-of-law

Prevention: As of today, ASEAN national capabilities and institutions as well as regional cooperation platforms present varying levels of sophistication, ranging from intermediate and advanced, to nascent or even absent in certain cases. Nonetheless, the last few years have witnessed an increased effort in building a more robust and resilient institutional architecture, showing significant improvement in different areas. ASEAN's current structure comprises three main pillars, i.e., the ASEAN Economic Community (AEC), the ASEAN Political-Security Community (APSC), and the ASEAN Socio-Cultural Community (ASCC). The third pillar, the ASCC, does not deal with cybersecurity. Within the first two pillars, the following entities specifically deal with cybersecurity:

- The ASEAN Telecommunications and IT Minister's meeting (TELMIN), under the AEC pillar, is a platform for ICT cooperation between ASEAN member states. Meeting at least once a year, TELMIN's areas of engagement encompass a wide portfolio of different ICT issues, including infrastructure development, human capital development, bridging the digital divide, economic transformation, innovation, people empowerment and engagement[70]. Its portfolio has also included cybersecurity in more recent years. In support of TELMIN, the Telecommunications and Information Technology Senior Officials Meeting (TELSOM) is tasked with coordinating and implementing policies and activities for ICT cooperation in ASEAN, following the directions and priorities set by TELMIN [71] . TELSOM comprises Senior Telecommunications Officials from ASEAN member states and meets about once a year, providing a forum for exchange of views and information sharing on major international issues and developments in the realm of ICTs. It also promotes participation of the private sector and regional/international organizations and non-governmental organizations in the development and implementation of its programs and activities[72]. Finally, ASEAN has also established the ASEAN Network Security Council (ANSAC) to establish a common framework for cybersecurity focused on national CERTs cooperation and capacity building. It has convened annual meetings since 2013[73].
- The ASEAN Ministerial Meeting on Transnational Crime (AMMTC), under the APSC pillar, is a platform for cooperation to prevent and combat transnational crimes including cyber exploitation. It is the entity that oversees the two above-mentioned Conventions on terrorism and human trafficking. As for TELMIN, its structure also includes another entity, the Senior Officials Meeting on Transnational Crime (SOMTC), which is tasked with coordinating and implementing policies and activities cooperation in ASEAN following the directions and priorities set by AMMTC. SOMTC is subdivided into various mechanisms and working groups that deal with different issues, ranging from arms smuggling to counterterrorism and human trafficking. Since 2013, it also includes a working group on cybercrime, providing a platform for ASEAN member states to discuss and adopt a coordinated approach to deal with cybercrime and collaborate with Dialogue Partners[74].

[70] ASEAN TELMIN 2017: About ASEAN TELMIN. https://www.aseantelmin17.gov.kh/page/about-asean-telmin
[71] ASEAN TELMIN 2017: About ASEAN TELSOM. https://www.aseantelmin17.gov.kh/page/about-asean-telsom
[72] ASEAN TELMIN 2017: About ASEAN TELSOM. https://www.aseantelmin17.gov.kh/page/about-asean-telsom
[73] Heinl, *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime*, (National Bureau of Asian Research, 2014)
[74] ASEAN: ASEAN Ministerial Meeting on Transnational Crime. https://asean.org/asean-political-security-community/asean-ministerial-meeting-on-transnational-crime-ammtc/

- The ASEAN Defence Ministers Meeting (ADMM-Plus), also under the APSC pillar, is the highest defense consultative and cooperative mechanism in ASEAN. It focuses on seven areas of cooperation, including cybersecurity, promoting cooperation and signaling greater attention to cybersecurity as a key defense issue. Its structure includes the Experts' Working Groups on Cyber Security (EWG on CS), which is in charge of coordinating training exercises, meetings, workshops, and seminars[75].

Notwithstanding the role played by TELMIN and AMMTC, there is no official regional institution or ministers' meeting dealing exclusively with cybersecurity under any of the three pillars. Nevertheless, important advancements have been made in that respect in the last few years, especially under Singapore's chairmanship in 2018. These include the establishment of the ASEAN Ministerial Conference on Cybersecurity (AMCC) in 2016, a key platform for the advancement of cybersecurity cooperation that takes place once a year during the International Cyber Week in Singapore. At its first meeting, member states agreed to develop a set of practical cybersecurity norms of behavior in ASEAN, proposing that TELMIN take up responsibility to identify measures to move cybersecurity cooperation forward[76]. This commitment was further confirmed at the second AMCC, and at the third AMCC they finally agreed to subscribe in principle to 11 voluntary, non-binding norms recommended in the 2015 Report of the UNGGE. Asia Pacific Center for Security Studies (APCSS) faculty member and cybersecurity expert Elina Noor praised this development, claiming that "the seeds of a more strategic conversation on positioning ASEAN within the norm-setting agenda in cyberspace have now finally been sown[77]." This was even more remarkable considering that out of the 10 member states, only Malaysia and Indonesia had taken part in some of the UNGGEs sessions convened between 2004 and 2017[78]. Finally, during the fourth and latest AMCC meeting in 2019, Singapore put forward a draft of an ASEAN Cybersecurity "Coordination Mechanism Paper," which will be reviewed by TELMIN and other relevant stakeholders before being submitted to ASEAN Leaders[79]. While it is not completely clear yet what this will entail, it might lead to the creation of an "ASEAN Cross-Sectoral Coordinating Committee" with relevant representatives from sectoral bodies to be set up for cybersecurity[80].

Given that ASEAN, unlike the EU, is not able to directly impose legally binding measures on its member states, it is important to have deeper insight into ASEAN member states' national capabilities to understand their different circumstances and how these differences impact the ASEAN as a whole. Considering the four main EU NIS directive national capability components and applying them to ASEAN member states results in Table 1.

[75] ASEAN: ASEAN Defence Ministers Meeting (ADMM). https://asean.org/asean-political-security-community/asean-defence-ministers-meeting-admm/
[76] CSA Singapore: ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN. https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean
[77] Noor, *ASEAN Takes a Bold Cybersecurity Step,* (The Diplomat, 2018)
[78] Noor, *ASEAN Takes a Bold Cybersecurity Step,* (The Diplomat, 2018)
[79] CSA Singapore: ASEAN Member States agree to move forward on a formal cybersecurity coordination mechanism. https://www.csa.gov.sg/news/press-releases/amcc-release-2019
[80] CSA Singapore: ASEAN Member States agree to move forward on a formal cybersecurity coordination mechanism. https://www.csa.gov.sg/news/press-releases/amcc-release-2019

Table 1 - National Capabilities of ASEAN Member States

	National Strategy	*CII Identification*	*National Agency*	*CSIRT*	*GCI*
Singapore					6
Malaysia					8
Thailand					35
Indonesia					41
Philippines					50
Brunei					58
Vietnam					64
Cambodia					120
Laos					128
Myanmar					131

Established Draft Absent

Table 1 shows that most ASEAN member states have been able to establish the essential policies and institutions for cyber resilience identified by the NIS directive. Nonetheless, despite this positive development, there are still important differences in capabilities and national priorities affecting the degree of effectiveness and enforcement according to which these entities operate, revealing a much more fragmented scenario. For example, the CSIRT in Singapore is better equipped and has more resources than the one in Indonesia, which comprises a small group of people, some of which are volunteers. This disparity is better reflected by the Global Cybersecurity Index (GCI), a trusted reference developed by the International Telecommunications Union (ITU) that measures the commitment of countries to cybersecurity along five factors: legal measures; technical measures; organizational measures; capacity building; and cooperation[81]. According to this ranking of 155 countries, Singapore and Malaysia excel at the global level and significantly outperform their regional partners, while Cambodia, Laos and Myanmar are among the lowest performing states globally. Thailand, Indonesia, the Philippines, Brunei, and Vietnam fall somewhere between the 35th and 64th spots.

Response: In tackling cross-border cybercrime, there are no ASEAN equivalents to EC3 or EUROJUST/ECJN. Even if the National Police Organization for the Association of Southeast Asian Nations (ASEANAPOL) – ASEAN's law enforcement agency – is conceptually similar to EUROPOL, it does not match its European counterpart in terms of cybersecurity-related functions and capabilities, and mostly serves as a platform to enhance trust and information sharing among its members. Nonetheless, the involvement of regional and international networks greatly facilitates assistance in tackling cybercrime.

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

To enhance coordinated action among law enforcement agencies in the region, in 2018 INTERPOL established the ASEAN Cyber Capability Desk[82]. Its main functions include:

- Enhancing cybercrime intelligence: provide ASEAN authorities with cybercrime intelligence at the strategic, operational, and tactical levels leveraging the capabilities of the INTERPOL Cyber Fusion Centre and public-private partnerships[83];
- Joint cybercrime operations: deal with the challenges posed by jurisdictional differences among member states by conducting joint operations targeting the most relevant cyberthreats[84].

Regarding judicial cooperation, the Council of ASEAN Chief Justices (CACJ) was established in 2013 to strengthen collaboration and information sharing to enhance economic growth and development in the region. It has recently launched the ASEAN Judiciaries Portal (2018) for member states to share experience, good practices, and training. As of today, CACJ does not hold or offer cybersecurity-related legal assistance to its member states, but it committed to continue its efforts in training judges and judicial officers on the topics of emerging legal-technologies[85].

In summary, ASEAN's institutional framework has been improving steadily in the last few years, creating key institutions that have been essential for enhancing regional cyber resilience. Nonetheless, the interoperability framework of the current institutional system still appears limited and fragmented, due to varying priorities and national capabilities of ASEAN member states.

[82] INTERPOL: ASEAN Cyber Capability Desk. https://www.interpol.int/en/Crimes/Cybercrime/Investigative-support-for-cybercrime/ASEAN-Cyber-Capability-Desk
[83] INTERPOL: ASEAN Cyber Capability Desk. https://www.interpol.int/en/Crimes/Cybercrime/Investigative-support-for-cybercrime/ASEAN-Cyber-Capability-Desk
[84] INTERPOL: ASEAN Cyber Capability Desk. https://www.interpol.int/en/Crimes/Cybercrime/Investigative-support-for-cybercrime/ASEAN-Cyber-Capability-Desk
[85] Council of ASEAN Chief Justices (CACJ): Announcements. https://cacj-ajp.org/announcements

4. HARMONIZATION OF CYBERCRIME AND DATA PRIVACY LEGISLATION

Data security and data privacy have long been treated as two separate domains that operate independently of each other. Since the rise of big data and machine learning, they are steadily being considered two sides of the same coin as they are both critical for protecting sensitive data[86]. Nonetheless, despite sharing the same goal, they are not interchangeable concepts, and they should therefore be addressed in different ways through tailor-made legislation. While the former focuses on protecting data from unauthorized access, the latter governs how data is collected, shared, and used. In particular, the greater risk to unregulated data collection and processing is the threat of "unintended inference," i.e., the ability of increasingly sophisticated and widespread machine learning techniques to elaborate predictions on sensitive information, such as political affiliations and behavioral patterns[87]. A case in point is the 2018 Cambridge Analytica scandal, a British political consulting firm that illicitly harvested the personal data of millions of Facebook users without their consent. It used this data to create political advertisements aimed to manipulate the electorate and swing elections in favor of the party that bought their services. When international cybercrime or privacy security threats like that arise, it is essential for states to collaborate and adopt effective preventive and response measures through relevant legislation. Unfortunately, divergences on critical principles and incompatibility of legal provisions often complicate cooperation in this area. The EU and ASEAN should aim to harmonize as much as possible cybercrime and data privacy legislation in their respective regions to overcome some of these obstacles.

4.1 EU: Filling the gaps in sensitive data protection

The NIS Directive and the Cybersecurity Act have been important steps forward in the EU cybersecurity ecosystem, creating a sophisticated governance structure and strong capabilities. Nonetheless, for the effective functioning of these frameworks and institutions, it is essential to have solid cybercrime and data privacy legislation in place that can be enforced at the national level. In that respect, the EU has encouraged its member states to transpose the cybercrime-related provisions contained in the Budapest Convention within their national legal systems and has taken active steps to harmonize practices among member states.

Cybercrime: The Budapest convention focuses on cybercrime offences against confidentiality, integrity and availability (CIA) of computer data and systems, forgery and fraud, and illegal content, such as child pornography.

Key EU legislation in these areas includes[88]:

- 2011 Directive on Combating the Sexual Exploitation of Children Online and Child Pornography;
- 2013 Directive on Attacks Against Information Systems;

[86] Burt, *Privacy and Cybersecurity are Converging. Here's Why That Matters for People and for Companies,* (Harvard Business Review, 2019)
[87] Burt, *Privacy and Cybersecurity are Converging. Here's Why That Matters for People and for Companies,* (Harvard Business Review, 2019)
[88] Pawlak, *Operational Guidance for the EU's international cooperation on cyber capacity building,* (EUISS, 2018)

- 2018 Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters;
- 2019 Directive on Combating Fraud and Counterfeiting of Non-Cash Means of Payment.

The adoption of these measures has created common standards and ensured consistency with respect to the same legal framework of reference. However, many challenges and discrepancies across national legal frameworks remain. Among them is the complex and lengthy process to request and access electronic evidence (e-evidence) for criminal investigations from other member states or third parties, which can be impeded by legal limitations imposed under some jurisdictions[89]. While there are operational processes aimed at streamlining cooperation in this area, such as the mutual legal assistance process (MLA), there exist no international common legal framework for the expedited sharing of evidence, which implies that the outcome of cooperation will depend on differences in specific legal systems and frameworks of the requesting and receiving countries. In the context of the EU, cooperation in this area is facilitated by the Budapest Convention, which contains both general and specific provisions for the successful implementation of MLA legislation to tackle cybercrime. These provisions include measures for the effective preservation and disclosure of traffic data, as well as trans-border access to computer data and real-time collection and interference of relevant information[90]. In addition, the EJCN encouraged member states to implement Article 26 of the Budapest Convention, which regulates the spontaneous exchange of information, in the "broadest possible sense" to simplify the process of exchanging evidence[91]. In 2018, the EC presented a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, allowing member states' relevant authorities to request directly from a service provider located in a different member state access to or preservation of electronic data (emails, texts, etc.) relevant to the investigation[92].

Data privacy: For years, Europe has been at the forefront of privacy regulations that have often become the standard for many countries worldwide. The EU General Data Protection Regulation (GDPR) is the region's latest and most robust effort to enhance the protection of personal data across the region and in its relationship with third parties. Personal data, in this case, refers to things like a person's name, email, and IP address, but also pseudonymized information that could be traced back to a specific individual. Building on the 1995 EU Data Protection Directive, GDPR's most important features include its extraterritorial application,

[89] Europol and Eurojust Public Information: Common challenges in combating cybercrime. http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF

[90] Council of Europe: Convention on Cybercrime ETS No. 185.

[91] Europol and Eurojust Public Information: Common challenges in combating cybercrime. http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF

[92] European Parliament: Legislative Train Schedule – Area of Justice and Fundamental Rights. https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence

new rights to data subjects, new obligations for data controllers and processors, and onerous penalties for noncompliance[93]. In particular, the following provisions stand out:

- Territorial scope: GDPR applies to the activities of all entities, inside or outside of the EU, which process personal data of EU citizens and residents[94]. These include the offering of goods and services—paid or free—or the monitoring of individual behavior. This also includes social media.
- Data retention: Personal data cannot be kept in a form which permits identification of an individual longer than it is necessary for the purpose for which the personal data was processed in the first place[95].
- Conditions for consent: An individual must consent to the processing of her/his personal data, which should be given in the context of a written declaration "in an intelligible and easily accessible form, using clear and plain language[96]," specifying what use will be made of her/his personal data. In addition, opting out of this consent must be as easy as to give it[97]. People can also object to personal data being used for specific purposes, like direct marketing.
- Right to data portability: An individual can request a controller to receive the personal data concerning her/him in a commonly used format and to transmit it to another controller[98].
- Data protection by design and by default: Data controllers and processors should implement data privacy technical and organizational measures at an early stage of the design of the processing operations, as well as ensuring the highest protection when processing personal data[99].
- Notification of a personal data breach: It is mandatory when a data breach is a risk to the rights and freedom of individuals. In this situation, relevant data controllers/processors must notify the supervisory authority and affected individuals within 72 hours[100].
- Transfers based on an adequacy decision: Personal data can be transferred to a third country or international organization only if the EC determines that they ensure an adequate level of protection[101].

[93] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[94] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[95] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[96] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[97] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[98] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[99] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[100] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[101] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)

- Penalties: Failing to comply with GDPR may turn out to be significantly onerous and will expose businesses to substantial penalties of up to 20 million euros or 4 percent of the annual global turnover, in some circumstances[102].

According to a January 2020 report by Cisco, the rate of breach notification has increased by over 12 percent compared to the same period last year, testament to the ability of personal data regulations like GDPR to raise awareness and enforce privacy[103]. Higher awareness is also making organizations better equipped to manage and protect personal data and to avoid being fined, despite the high cost of compliance with this regulation. In fact, depending on the amount of data that is processed by any given organization, the implementation of GDPR provisions can cost from hundreds to tens of thousands of US dollars[104]. Costs may include hiring new people, updating/installing new technologies, and seeking legal advice or consulting services.

4.2 ASEAN: Challenges to regulatory harmonization and standard setting

In the 2017 Declaration to Prevent and Combat Cybercrime, ASEAN member states agreed to enhance cooperation in preventing and combating cybercrime by means of various measures, including the harmonization of laws related to cybercrime and electronic evidence. However, given ASEAN's inability to impose legally binding measures on its member states and the lack of a Cybersecurity Convention, the outcome will largely depend on political will and national priorities, which will be analyzed in this subsection.

Cybercrime: Based on the major cybercrime provisions contained within the Budapest Convention, the current legislative landscape in ASEAN member states is shown in Table 2.

[102] EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation)
[103] Cisco: From Privacy to Profit: Achieving Positive Returns on Privacy Investments – Cisco Data Privacy Benchmarks Study 2020. https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf
[104] TDS: The Positive and Negative Implications of GDPR. https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr

Table 2 - Cybersecurity and Data Privacy Legislation across ASEAN

	CIA attacks	*Fraud and Forgery*	*Child pornography*	*Data privacy*	*Breach Notific. Law*	*GCI*
Singapore						6
Malaysia						8
Thailand						35
Indonesia						41
Philippines						50
Brunei						58
Vietnam						64
Cambodia						120
Laos						128
Myanmar						131

Established Draft Absent

Even though most member states have established legislative frameworks in most of these areas, their legislative scope and cybersecurity capabilities vary greatly across the region. For example, data privacy in Laos includes only basic regulations to protect personal information, whereas Singapore's regulations approximates GDPR standards. In addition, there are important differences among ASEAN member states' legislative instruments with respect to the criminalization of conduct in cyberspace and provisions to investigate cybercrime and collect e-evidence, which can render cooperation lengthy and complex.

It is important to reiterate that when there exists no international common legal framework for the expedited sharing of evidence, the outcome of cooperation will depend on the differences in the specific legal systems and frameworks of the requesting and receiving countries, or on the existence of bilateral agreements. Therefore, the most effective way of obtaining data today remains that of being part of a mutual legal assistance treaty[105]. The only existing one in the world today is the Budapest convention, which no ASEAN member state except the Philippines has ratified. In 2004, ASEAN member states agreed on a regional Treaty on Mutual Legal Assistance in Criminal Matters (MLA Treaty), but its application to cybercrime remains quite limited because it lacks important provisions that underlie the transnational nature of cyberthreats, such as retention of and access to e-evidence[106]. These provisions are important because e-evidence is stored online by service providers that are often based in a different country than the requesting one. In particular, in comparison with the Budapest Convention, the ASEAN MLA treaty lacks the following provisions to deal effectively with cybercrime:

[105] Kent, *The Mutual Legal Assistance Problem Explained*, (The Center for Internet and Society, 2015)
[106] ASEAN: Treaty on Mutual Legal Assistance in Criminal Matters, 2004

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[107].

Data privacy: The absence of ASEAN region-wide legislation is also reflected in data privacy issues as member states have adopted different measures regarding the handling of personal data. Major differences include varying degrees of responsibility for data processors and controllers, individuals' rights, conditions and timeframes to report data breaches, and penalties for privacy infringements. Nonetheless, two non-binding frameworks have been developed to harmonize personal data privacy legislation at the regional level. The first is the 2016 ASEAN Framework on Personal Data Protection, which establishes a set of principles to guide the implementation of measures at both national and regional levels to promote and strengthen personal data protection in the region[108]. The second is the ASEAN Framework on Digital Data Governance endorsed at the ASEAN TELMIN meeting in December 2018. It is intended to enhance data management, facilitate harmonization of data regulations among ASEAN member states and promote intra-ASEAN flows of data[109].

As the EU moved forward with the implementation of GDPR, advancing comprehensive data privacy legislation became a more pressing issues for other regions in the world, and many ASEAN countries started adapting their own regulatory framework to be more aligned with EU regulations[110]. This development is largely due to the extraterritorial scope of GDPR which, as mentioned, extends legal obligations to organizations which, even if not based in the EU, offer goods or services to EU citizens/residents or monitor their online behavior. GDPR is particularly relevant in this context given the robust economic ties between ASEAN and the EU[111]. In fact, ASEAN represents the EU's 3rd largest trading partner outside Europe (after the US and China) with more than US$ 260 billion worth of trade in 2018. The EU is ASEAN's second largest trading partner after China, accounting for around 14 percent of ASEAN trade[112]. As far as Foreign Direct Investment (FDI) is concerned, the EU is by far the largest investor in ASEAN countries. In 2017, FDI stocks into ASEAN accounted for $372 billion[113]. Although a more recent phenomenon, ASEAN investment in Europe has also been growing steadily to a total stock of over $155 billion in 2017[114]. While it is burdensome for many countries to adapt to GDPR regulations, from both an administrative and financial point of view, doing so has the potential to bring the world together under a common regulatory framework while also enhancing ASEAN interoperability[115]. Higher operational costs for

[107] ASEAN: Treaty on Mutual Legal Assistance in Criminal Matters, 2004
[108] ASEAN: ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) – Framework on Personal Data Protection, 2016
[109] ASEAN: ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) – Framework on Digital Data Governance, 2016
[110] Tan, Azman, *The EU GDPR's impact on ASEAN data protection law*, (Financier Worldwide, 2019)
[111] European Parliament: Fact Sheets on the European Union – Southeast Asia. https://www.europarl.europa.eu/factsheets/en/sheet/183/southeast-asia
[112] European Parliament: Fact Sheets on the European Union – Southeast Asia. https://www.europarl.europa.eu/factsheets/en/sheet/183/southeast-asia
[113] European Parliament: Fact Sheets on the European Union – Southeast Asia. https://www.europarl.europa.eu/factsheets/en/sheet/183/southeast-asia
[114] European Parliament: Fact Sheets on the European Union – Southeast Asia. https://www.europarl.europa.eu/factsheets/en/sheet/183/southeast-asia
[115] Sagar, *The EU's GDPR – opportunities outweigh the challenges in ASEAN*, (OpenGov, 2019)

businesses will mostly derive from the need to hire new personnel, update/install new technology, and seek legal advice or consulting services[116].

The Asia-Pacific Economic Cooperation (APEC) established in 2011 an alternative model to regulate cross border data transfer and protection of personal data, called the Cross-Border Privacy Rules System (CBPRs). It is a voluntary, accountability-based certification scheme that allows companies to transfer personal data (inter- and intra-company) in a safe manner with other CBPRs-certified member economies[117]. By only outlining minimum standards that can be adopted by different states, CBPRs' great advantage lies in its flexibility, making it much more conducive to trade and investment than GDPR[118]. As explained by US Court of Appeals Law Clerk A. Gribakov, "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[119]." The CBPRs system does not provide any affirmative rights to consumers, but it also does not prevent a member economy from adopting its own enhanced privacy standards.

More specifically, the following GDPR areas are not covered by CBPRs: the principle of storage limitation, mandatory data breach notifications, restrictions for automated processing and profiling, special categories, onward transfers, and the direct applications of these obligations to data processors[120]. It might therefore still be necessary for joining states to adopt more comprehensive legislation to fill the gap with EU regulations or to negotiate partial agreements. An example is the EU-US Privacy Shield Framework, designed to provide companies with a mechanism to comply with data protection requirements when transferring data from the EU to the US[121]. To date, only 23 companies and nine states are part of the CBPRs initiative, including two ASEAN member states: USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, the Philippines, and Chinese Taipei[122].

[116] Callo-Müller, *GDPR and CBPR: Reconciling Personal Data Protection and Trade. Asia-Pacific Economic Cooperation*, (APEC, 2018)
[117] Callo-Müller, *GDPR and CBPR: Reconciling Personal Data Protection and Trade. Asia-Pacific Economic Cooperation*, (APEC, 2018)
[118] Callo-Müller, *GDPR and CBPR: Reconciling Personal Data Protection and Trade. Asia-Pacific Economic Cooperation*, (APEC, 2018)
[119] Gribakov, *Cross-Border Privacy Rules in Asia: An Overview*, (*Lawfare*, 2019)
[120] Callo-Müller, *GDPR and CBPR: Reconciling Personal Data Protection and Trade. Asia-Pacific Economic Cooperation*, (APEC, 2018)
[121] Privacy Shield Framework: Home Page. https://www.privacyshield.gov/welcome
[122] Cross Border Privacy Rules System (CBPRs): About CBPRS. http://cbprs.org/

5. CYBER AWARENESS AND HYGIENE

Cyber awareness means knowing about the existence and likelihood of cyber threats and understanding their impact on a given organization or institution. It can be promoted at the regional level by publishing detailed reports and research on relevant cybersecurity matters and resources, organizing workshops and events, and creating public-private partnerships. It is nonetheless essential for member states to take the lead in raising awareness, targeting communication to their specific language, culture, priorities, and threat scenarios. Cyber hygiene comprises the practices and steps that users take to maintain system health and enhance online security. In both the EU and ASEAN, there is no unified approach to cyber hygiene. The role of ROs in these area remains quite limited overall because these practices must be enforced through security and data protection policies adopted by organizations and institutions in their relations with employees or clients. People are in fact considered as the weakest link in the cybersecurity chain. Social engineering attacks try to lure users into committing human error or engaging in irresponsible behavior. According to some estimates, about 80 percent of exploitable computer vulnerabilities are the direct result of poor or no cyber hygiene[123]. Nevertheless, ROs can contribute to enhance cyber hygiene and awareness through joint exercises, publications, and other initiatives. This section will analyze ongoing initiatives in the EU and ASEAN to complement the efforts of member states in these domains.

5.1 EU: Promoting cyber awareness and hygiene

The EU defined the promotion of cyber hygiene and awareness as a key objective in its 2017 joint communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. It stated that "people need to develop cyber hygiene habits and businesses and organizations must adopt appropriate risk-based cybersecurity programs and update them regularly to reflect the evolving risk landscape.[124]" This statement emphasizes the leading and self-regulating role of organizations and institutions in implementing effective cyber hygiene practices.

In the EU, ENISA is responsible for raising cybersecurity awareness through reports, workshops, and public-private partnerships. Its activities also seek to promote good health online and skills development to address the shortage of cybersecurity talent in the EU. ENISA's most relevant initiatives include the European Cybersecurity Month (ECSM), the European Cybersecurity Challenge (ECSC), NIS in Education, and the Cybersecurity Education Database. These are described in more detail below.

European Cybersecurity Month (ECSM) is an awareness campaign that promotes cybersecurity among citizens and organizations, emphasizing the importance of information security and highlighting the steps that individuals can take to protect their personal, financial, ad/or professional data[125]. ECSM takes place annually in October, and it consists of different

[123] Pawlak, *Operational Guidance for the EU's international cooperation on cyber capacity building,* (EUISS, 2018)
[124] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN/2017/0450 final
[125] ENISA: European Cybersecurity Month https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

online activities, webinars, and events to raise awareness and change individuals' behavior to promote better cyber hygiene practices. The objectives of ECSM[126] are:

- generate general awareness about cybersecurity;
- generate specific awareness on NIS;
- promote safer use of the Internet for all users;
- build a strong track record to raise awareness through the ECSM;
- involve relevant stakeholders;
- increase national media interest through the European and global dimension of the project;
- enhance attention and interest about information security through political and media coordination.

European Cybersecurity Challenge (ECSC) is an annual European event that brings together young talent from across the EU to engage in cybersecurity competitions. It promotes friendly relations between attending countries, where top cyber talents from each member state collaborate and compete against each to win the final prize. Contestants solve security related challenges in different domains, such as: web and network security, mobile security, crypto puzzles, reverse engineering, and digital forensics[127].

NIS in Education: ENISA has created a "Network and Information Security" quiz for people to test their privacy and general online security skills, providing resources and courses for long-term learning[128].

Cybersecurity Higher Education Database gives access to a comprehensive list of cybersecurity degrees in European countries. A dedicated search tool provides users with the possibility to discover cybersecurity degrees filtering them by country, type of program, and delivery method. Up-to-date information on each degree is gathered, organized and displayed in order to provide a comprehensive overview of the programs proposed. This database allows young talents to browse through the various possibilities offered by higher education in cybersecurity in Europe, and helps universities attract students motivated to learn cybersecurity skills[129].

These initiatives have complemented the efforts of single member states to enhance cyber awareness in the EU. In addition, recognizing that there is no unified approach to cyber hygiene in the EU, in 2017 ENISA published a report that analyzed the leading cyber hygiene programs across member states and provided recommendations on how it can be improved in the region (https://bit.ly/2XHTaDg).

5.2 ASEAN: Bridging the digital divide

In ASEAN, there is no unified agency that coordinates awareness campaigns or promotes cybersecurity hygiene across the region. ASEAN member states present different levels of

[126] ENISA: European Cybersecurity Month https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month
[127] ENISA: About ENISA https://www.enisa.europa.eu/about-enisa
[128] ENISA: About ENISA https://www.enisa.europa.eu/about-enisa
[129] ENISA: About ENISA https://www.enisa.europa.eu/about-enisa

economic development and technological capabilities that shape their national priorities and perceived threats to the socio-economic impact of cyberspace. These affect the overall level of awareness and investment in cyber hygiene practices.

INTERPOL has launched its own regional cybercrime strategy for ASEAN, highlighting that the region is today the fastest-growing digital market in the world, increasing its projected regional GDP by US$ 1 trillion over the next ten years. At the same time, cybercrime is expected to rise exponentially and become more sophisticated. To face current and emerging cyber threats, INTERPOL has included in its strategy the need to promote good cyber hygiene "by supporting the next global awareness campaign in 2020 to reduce the impact of cybercrime in the region through awareness and preventive measures.[130]"

Overall, ASEAN countries except for Singapore fall well below the global average of cybersecurity spending as percentage of GDP despite the deteriorating threat landscape. Depending on the different benefits and dangers stemming from cyberspace across the region, ASEAN member states have invested varying amounts of resources to address cyber threats. ASEAN member states can be divided into three groups based on how much they are investing[131].

- **High Investors:** Includes Singapore, Malaysia, Brunei Darussalam, and Thailand. These states depend more heavily on the benefits and dangers posed by cyberspace and have invested a larger amount of resources to enhance security[132]. In particular, Singapore has played an important role in promoting cyber awareness at both the local and regional level. Important regional advancements have been made under Singapore's ASEAN chairmanship in the last few years, as discussed in Section 3.
- **Medium Investors:** Vietnam, Philippines, and Indonesia. These states recognize the threats stemming from cyberspace but have only invested a limited amount of resources to enhance security[133].
- **Low Investors:** Myanmar, Cambodia, and Laos. These states do not perceive cyber threats as an imminent danger given the lack of widespread technological assets and lower economic benefits they derive from cyberspace. Thus, they do not spend enough resources to enhance security. In addition, only 24.17 percent of this group's population benefits from the socio-economic benefits of Internet access, as opposed to an average of 70.83 percent of high investor countries[134]. The absence of breach notification legislation in Myanmar, Cambodia, and Laos further exacerbates the lower level of awareness. Breach notification requirements, such as those contained within GDPR, play an important role in raising awareness.

As discussed in Section 2 and in the previous paragraphs, there is a wide technology gap between ASEAN member states. According to the Internet Society[135], the digital divide of the future will no longer be only about connectivity but will be linked to security as well. Although

[130] ENISA: Cyber Hygiene https://www.enisa.europa.eu/publications/cyber-hygiene
[131] Dai, Gomez, *Challenges and Opportunities for Cyber Norms in ASEAN*, (Journal of Cyber Policy, 2018)
[132] Dai, Gomez, *Challenges and Opportunities for Cyber Norms in ASEAN*, (Journal of Cyber Policy, 2018)
[133] Dai, Gomez, *Challenges and Opportunities for Cyber Norms in ASEAN*, (Journal of Cyber Policy, 2018)
[134] Dai, Gomez, *Challenges and Opportunities for Cyber Norms in ASEAN*, (Journal of Cyber Policy, 2018)
[135] Internet Society: Digital Divide https://future.internetsociety.org/2017/introduction-drivers-of-change-areas-of-impact/areas-of-impact/digital-divides/

the gap of the digital divide in ASEAN has been narrowing since the implementation of its ICT Master Plan 2015, significant differences among member states remain, which inevitably translate into different levels of cyber awareness and hygiene.

6. POLICY RECOMMENDATIONS

The previous sections have analyzed the strategic, institutional, legal and awareness-raising measures adopted by ASEAN and the EU to enhance cyber resilience considering their different organizational structures.

Based on these insights and comparison, this paper offers eleven policy recommendations that could be relevant as ASEAN moves forward in proposing new solutions and mechanisms to deal effectively with the challenges it faces in this domain, eliminating the need to reinvent the wheel in certain policy areas. The first six recommendations are short-term policy considerations, while the remaining five focus on medium- to long-term aspects.

In the short term, ASEAN member states could consider:

a) **Establishing a regional cybersecurity strategy outlining a shared vision, scope, objectives, and priorities:** Following i) the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation and ii) the endorsement of the UNGGE 11 non-binding norms, a unified strategy on this matter is an important next step to provide a clear direction and detailed action plans to enhance cyber resilience in the region. It would allow ASEAN to prioritize and align organizational activities across member states and the private sector, define accountabilities, as well as draw a roadmap and timeline for expected outcomes. To this end, it should set up a clear governance structure and assign specific roles and responsibilities to relevant stakeholders to avoid duplication and create new roles and responsibilities where needed. The overall aim should be to create a legal and institutional environment that facilitates information sharing, coordinated response and public-private cooperation.

b) **Setting out a region-wide comprehensive framework to assist member states in protecting critical information infrastructure and help reduce vulnerabilities:** Develop procedures for the identification and designation of critical information infrastructures and the assessment of the need to improve their protection. Measures could include the development of a body modelled after the European Reference Network for Critical Infrastructure Protection (ERNCIP) to carry different research activities such as the development of methods and tools for regional cybersecurity exercises, the assessment of the vulnerability of networked infrastructures in case of extreme scenarios, and knowledge and expertise sharing across member states to better align protocols throughout the region[136]. This would be particularly beneficial to countries at the lower end of the digital divide to efficiently secure their systems as they modernize their economy by benefiting from other member states' expertise and cooperation.

c) **Streamlining the MLA process wherever possible to ensure effective coordination:** This could be done by aligning and using existing model requests and a common taxonomy of cybercrime terminology. Alternatively, ASEAN could consider amending the 2004 Treaty on Mutual Legal Assistance in Criminal Matters to include cybercrime-related

[136] EU Science Hub: Critical Infrastructure Protection. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

provisions. As mentioned in Section 4, the MLA's application to cybercrime purposes remains quite limited due to the lack of important provisions that underlie the transnational nature of cyberthreats, such as retention of and access to e-evidence. E-evidence is stored online by service providers that are often based in a different country than the requesting one. In particular, potential amendments could include the following provisions to deal effectively with cybercrime: 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.

d) **Remodeling ASEANAPOL's e-ADS mechanism around EUROPOL's SIRIUS project to exchange information more efficiently:** To facilitate criminal investigations that require cross-border requests and meet the increasing need of ASEAN law enforcement agencies to access e-evidence. The updated platform could include guidelines on the type of data stored by Online Service Providers (OSP) and how to request access to it, templates for OSP data requests; and a library of the terms and conditions of the largest OSPs[137]. It could also extend information sharing to INTERPOL and the CACJ.

e) **Developing a blueprint for coordinated response to cybersecurity emergencies to apply to cybersecurity incidents causing extensive disruptions to two or more member states:** A blueprint should describe how existing and potentially new cybersecurity mechanisms interoperate at the political, operational, and technical level to enable an effective response in case of emergency. Based on the "EU Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises"[138], it could complement ASEAN's annual CERT incident drills (ACID).

f) **Initiating region-wide cyber awareness campaigns:** This could be done by entrusting newly formed institutions, such as the ASEAN-Singapore Centre of Excellence (ASCCE), with the responsibility of conducting cyber awareness initiatives. ASEAN member states could also collaborate with INTERPOL in its 2020 awareness campaign. Following ENISA's example, ASCEE could raise cyber awareness through detailed reports, workshops, and public-private partnerships to promote good health online and skills development to address the shortage of cybersecurity talent in the ASEAN.

In the medium- to long-term, ASEAN member states could consider:

g) **Drafting a regional Convention on Cybercrime:** Given the important differences among ASEAN member states' legislative instruments and capabilities, a legally binding convention would facilitate the harmonization of legislation and adoption of common standards to fight cybercrime. ASEAN member states have varying national priorities, capabilities, and conceptions of cyberspace. Therefore, in absence of convergence on a unified text, the "ASEAN Minus X" formula could be employed to allow willing member states to move forward in this area. While historically this mechanism has mostly been

[137] Eurojust: SIRIUS Project. http://www.eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx

[138] European Commission: Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C(2017) 6100 final ANNEX I

employed to deal with economic matters, it is important to remember that cybersecurity is as much an economic issue as a security one. As reported by the consulting firm AT Kearney, the estimated exposure of ASEAN's top companies amounts to $750 billion, and an overwhelming majority of industry leaders claimed that concerns over cybersecurity are impeding innovation, particularly in technology products, business, retail, and banking services[139]. In addition, ASEAN Minus X has already been used in the past to pass legally binding conventions to counter cross-border security threats, such as the 2007 Convention on Counter Terrorism and the 2015 Convention Against Trafficking in Persons, Especially Women and Children.

h) **Strengthening the mandate of the AMCC:** AMCC has proven to be the most relevant regional cybersecurity platform in the last few years. Since TELMIN appears to be too IT-focused and holds a very wide portfolio, while AMMTC focuses exclusively on cybercrime, AMCC could take the leading effort in this area and be granted a stronger mandate. This would allow it to focus on relevant cybersecurity issues in a more comprehensive way, avoiding overlapping roles and responsibilities with other institutions. This could be done by integrating AMCC within the Political-Security pillar, entrusting it with greater authority, resources, and influence.

i) **Strengthening the role of CACJ to provide cybersecurity-related legal assistance to ASEAN member states and increase judicial cooperation in sharing information and good practices:** CACJ should form part of an integrated network that includes law enforcement agencies to overcome the obstacles posed by e-evidence access and sharing.

j) **Exploring the development of an ASEAN-EU joint privacy framework to obtain GDPR adequacy status:** Given the strong economic ties between the two blocs, ASEAN could engage the EU to develop a privacy framework that could provide companies in both regions with a mechanism to comply with data protection requirements when transferring personal data from the EU to ASEAN. This could be modelled after the EU-US Privacy Shield Framework.

Seeking common ground on the main principles regarding the applicability of international law to cyberspace to build regional CBMs: Further study and analysis could be undertaken by additional sessions of the CSCAP Study Group on International Law and Cyberspace, which has so far been able to start a wide-ranging debate on ASEAN member states' main internal challenges to the application of international law to cyberspace. Doing so would facilitate the work of ARF-ISM to elaborate CBMs and complement the work conducted by the ASEAN working level committee formed at the latest AMCC in October 2019 to come up with a practical set of actions to develop norms of responsible state behavior.

[139] Dobberstein, Gerdemann, Pereira, *Cybersecurity in ASEAN: An Urgent Call to Action*, (AT Kearney, 2018)

7. CONCLUSION

Despite their internal divergences and different levels of integration, ROs are in a favorable position in the fight against cyber exploitation. They enjoy a higher level of structural similarities and shared interests that make them better suited to address the scale and cross-border nature of the threat, and to tackle the challenges to cooperation posed by an anarchical international system, such as the coordination dilemma and ideological inconsistencies.

The previous sections have analyzed the four pillars of cyber capacity building identified by EUISS, applied to the regional contexts of the EU and ASEAN. The first pillar addresses the benefits of adopting a comprehensive strategy that can outline a clear roadmap, principles and priorities, as well as the roles and responsibilities of the main actors involved. By adopting a regional strategy, the EU was able to set the groundwork for the achievement of critical goals to enhance its cyber resilience, making significant steps forward. In contrast, ASEAN, despite the progress made in the last few years, still lacks a clear direction, resulting in a fragmented cybersecurity architecture.

The second and third pillars address the creation of an interoperational institutional framework that can prevent cyber threats and respond to malicious actors by means of strategic and technical information sharing platforms, as well as harmonized cybercrime and data privacy legislation. In the EU, such a framework has resulted in stronger national capabilities and the creation of platforms for effective coordination, complemented by region-wide law enforcement and judicial cooperation through harmonization of relevant legislation across multiple jurisdictions. ASEAN's institutional and legal framework has also been improving steadily, creating key institutions that have been essential to enhancing regional cyber resilience. Nonetheless, the interoperability framework of ASEAN's current institutional system still appears limited and fragmented due to varying priorities and national capabilities of ASEAN member states.

Finally, the fourth pillar addresses cyber awareness and hygiene. Despite the limited role ROs can play in these areas, they can contribute to enhancing cyber hygiene and awareness in different ways. In the EU, ENISA is responsible for promoting cybersecurity awareness and hygiene through reports, workshops, and public-private partnerships. In ASEAN, there are significant differences among member states in terms of the benefits and dangers they derive from cyberspace, translating into different levels of cyber awareness and hygiene.

Therefore, notwithstanding the sharp differences among the two organizations, it is possible to address some of ASEAN's challenges by scrutinizing the measures adopted by its European counterpart, eliminating the need to reinvent the wheel in certain areas. Some of these opportunities were elaborated into policy recommendations tailored to the context of ASEAN in the previous section.

The questions and risks posed by cyber threats will be ever more relevant as new technologies are developed and adopted. In the near future, the convergence of Big Data, Artificial Intelligence, and other disruptive technologies powered by 5G networks will give rise to the so-called "Fourth Industrial Revolution," which will expose us to new vulnerabilities and

fundamentally alter the way we live, work, and relate to one another[140]. In that respect, Singapore's Foreign Minister Dr. Vivian Balakrishnan has emphasized the need to enhance cyber resilience and "to step up, and to step up urgently, collaboration on cybersecurity, because you can't have a smarter world, you can't have e-commerce, you can't have seamless digital transactions if you don't have cybersecurity. It's the flip side of the coin[141]."

[140] Schwab, *The Fourth Industrial Revolution: what it means, how to respond*, (World Economic Forum, 2016)
[141] Lung, *ASEAN leaders issue statement on cybersecurity cooperation*, (OpenGov, 2018)

REFERENCES

- Kaspersky: What is WannaCry ransomware? https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed April 12, 2020)

- Sukumar, Arun. The UNGGE Failed. Is International Law in Cyberspace Doomed as Well? *Lawfare*, July 4, 2017.

- Healey, J. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, 2013.

- Nicholas, P. The role that regions can and should play in critical infrastructure protection *Microsoft*, March 5, 2018.

- Dr. Walid Abdulrahim - Private Site for Legal Research and Studies: Introduction to Regional Organizations. https://sites.google.com/site/walidabdulrahim/home/my-studies-in-english/20-introduction-to-regional-organizations (accessed April 16, 2020)

- IT Governance: What is cyber resilience. https://www.itgovernance.co.uk/cyber-resilience (accessed April 16, 2020)

- Dobberstein, N, Gerdemann, D, Pereira, G. *Cybersecurity in ASEAN: An Urgent Call to Action*. AT Kearney, 2018.

- North Korea could target Southeast Asia's vulnerable crypto sector, says defense think tank [editorial]. *CNBC*, (14 April 2019).

- FireEye, Inc: M-Trends 2019. https://content.fireeye.com/m-trends. (accessed April 16, 2020)

- Asean and the EU: Differences and challenges [opinion]. The Straits Times, (22 August 2017)

- CSA Singapore: Opening Speech by Dr Yacoob Ibrahim, Minister for Communications and Information and Minister-In-Charge of Cybersecurity, at the Asean Ministerial Conference on Cybersecurity.https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2016 (accessed April 16, 2020)

- Pawlak, P. *Operational Guidance for the EU's international cooperation on cyber capacity building*. EUISS, 2018, pp. 12-14.

- Watkins, M. *Demystifying Strategy: The What, Who, How, and Why*. Harvard Business Review, 2007.

- EUR-Lex: 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. /* JOIN/2013/01 final */

- Hakmeh, J. *A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet*. Council on Foreign Relations, 2020.

- European Defence Agency: Cyber Defence. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence (accessed April 16, 2020)

- Rand Corporation: Examining the EU's Military Capabilities for Cyber Defence. https://www.rand.org/randeurope/research/projects/eu-military-cyber-defence.html (accessed April 18, 2020)

- European Council: Cyber defence: Council updates policy framework. https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/ (accessed April 18, 2020)

- European Commission: The EU cybersecurity certification. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (accessed April 18, 2020)

- Delerue, F, Kulesza, J, Pawlak, P. *The Application of International Law in Cyberspace: Is there a European Way?* EU Cyber Direct, 2019, pp. 4.

- ASEAN: ICT Masterplan 2015 Completion Report. https://www.asean.org/storage/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf (accessed April 16, 2020)

- ASEAN: ICT Masterplan 2015. https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf (accessed April 16, 2020)

- ASEAN: ASEAN Leaders' Statement on Cybersecurity Cooperation. https://asean.org/storage/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf (accessed April 16, 2020)

- ASEAN: Master Plan on ASEAN Connectivity 2025. https://asean.org/storage/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf (accessed April 16, 2020)

- ASEAN 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). http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-12.pdf (accessed April 16, 2020)

- Council for Security Cooperation in the Asia Pacific: 1st Meeting of the CSCAP Study Group on International Law and Cyberspace. http://www.cscap.org/uploads/CSCAP%20Co-chairs%20Report%20for%20First%20Study%20Group%20.pdf (accessed April 16, 2020)

- United Nations Digital Library: Countering the use of information and communications technologies for criminal purposes: resolution / adopted by the General Assembly. https://digitallibrary.un.org/record/3841023?ln=en (accessed April 18, 2020)

- US Department of Homeland Security: Cybersecurity. https://www.ready.gov/cybersecurity (accessed April 18, 2020)

- 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 OJ L 194, 19.7. 2016, pp. 1–30.

- 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 certification and repealing Regulation (EU) No 526/2013.

- Eurojust: Tackling cybercrime through joint investigation teams. http://www.eurojust.europa.eu/press/News/News/Pages/2019/2019-06-07_JITs-experts-meeting.aspx (accessed April 20, 2020)

- European Cybercrime Centre – EC3: About. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (accessed April 20, 2020)

- Eurojust: About Eurojust. http://www.eurojust.europa.eu/about/background/Pages/History.aspx (accessed April 20, 2020)

- Eurojust: SIRIUS Project. http://www.eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx (accessed April 20, 2020)

- Europol and Eurojust Public Information: Common challenges in combating cybercrime. http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF (accessed April 20, 2020)

- ASEAN: The ASEAN Way and the Rule of Law. https://asean.org/?static_post=the-asean-way-and-the-rule-of-law (accessed April 20, 2020)

- ASEAN TELMIN 2017: About ASEAN TELMIN. https://www.aseantelmin17.gov.kh/page/about-asean-telmin (accessed April 20, 2020)

- ASEAN TELMIN 2017: About ASEAN TELSOM. https://www.aseantelmin17.gov.kh/page/about-asean-telsom (accessed April 20, 2020)

- ASEAN: ASEAN Ministerial Meeting on Transnational Crime. https://asean.org/asean-political-security-community/asean-ministerial-meeting-on-transnational-crime-ammtc/ (accessed April 20, 2020)

- ASEAN: ASEAN Defence Ministers Meeting (ADMM). https://asean.org/asean-political-security-community/asean-defence-ministers-meeting-admm/ (accessed April 20, 2020)

- Heinl, C. Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *National Bureau of Asian Research (NBR)*, NO. 18, 2014, pp. 131-160.

- CSA Singapore: ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN. https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean (accessed April 20, 2020)

- Noor, E. *ASEAN Takes a Bold Cybersecurity Step*. The Diplomat, 2018.

- CSA Singapore: ASEAN Member States agree to move forward on a formal cybersecurity coordination mechanism. https://www.csa.gov.sg/news/press-releases/amcc-release-2019 (accessed April 20, 2020)

- UNIDIR: Cyber Policy Portal. https://cyberpolicyportal.org/en/ (accessed April 20, 2020)
- ITU: Global Cybersecurity Index (GCI) 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed April 20, 2020)
- Dai, C, Gomez, M. Challenges and Opportunities for Cyber Norms in ASEAN. *Journal of Cyber Policy*, Vol. 3, Issue 2, 2018.
- ASEANAPOL: ASEANAPOL Bulletin 8th Edition. http://www.aseanapol.org/activities/8th-edition-aseanapol-bulletin (accessed April 21, 2020)
- INTERPOL: ASEAN Cyber Capability Desk. https://www.interpol.int/en/Crimes/Cybercrime/Investigative-support-for-cybercrime/ASEAN-Cyber-Capability-Desk (accessed April 21, 2020)
- Council of ASEAN Chief Justices (CACJ): Announcements. https://cacj-ajp.org/announcements (accessed April 3, 2020)
- Burt, A. Privacy and Cybersecurity are Converging. Here's Why That Matters for People and for Companies. *Harvard Business Review*, 2019.
- Council of Europe: Convention on Cybercrime ETS No. 185.
- European Parliament: Legislative Train Schedule – Area of Justice and Fundamental Rights. https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence (April 21, 2020, last accessed)
- EUR-Lex: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Cisco: From Privacy to Profit: Achieving Positive Returns on Privacy Investments – Cisco Data Privacy Benchmarks Study 2020. https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf (accessed April 21, 2020)
- TDS: The Positive and Negative Implications of GDPR. https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr (accessed April 21, 2020)
- Kent, G. The Mutual Legal Assistance Problem Explained. *The Center for Internet and Society*, 2015.
- ASEAN: Treaty on Mutual Legal Assistance in Criminal Matters, 2004.
- ASEAN: ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) – Framework on Personal Data Protection, 2016.
- ASEAN: ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) – Framework on Digital Data Governance, 2016.
- Tan, S, Azman, N. The EU GDPR's impact on ASEAN data protection law. *Financier Worldwide*, 2019.

- European Parliament: Fact Sheets on the European Union – Southeast Asia. https://www.europarl.europa.eu/factsheets/en/sheet/183/southeast-asia (accessed April 22, 2020)
- Sagar, M. The EU's GDPR – opportunities outweigh the challenges in ASEAN. *OpenGov*, 2019.
- Callo-Müller, M. GDPR and CBPR: Reconciling Personal Data Protection and Trade. Asia-Pacific Economic Cooperation (APEC), #218-SE-01.10, 2018.
- Gribakov, A. Cross-Border Privacy Rules in Asia: An Overview. *Lawfare*, 2019.
- Privacy Shield Framework: Home Page. https://www.privacyshield.gov/welcome (accessed April 22, 2020)
- Cross Border Privacy Rules System (CBPRs): About CBPRS. http://cbprs.org/ (accessed April 22, 2020)
- EU Science Hub: Critical Infrastructure Protection. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection (accessed April 22, 2020)
- European Commission: Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C(2017) 6100 final ANNEX I.
- Schwab, K. The Fourth Industrial Revolution: what it means, how to respond. *World Economic Forum*, 2016.
- Lung, N. ASEAN leaders issue statement on cybersecurity cooperation. *OpenGov*, 2018.

ABOUT THE AUTHOR

Eugenio Benincasa is a resident WSD-Handa Fellow at Pacific Forum. He holds an M.A. in International Affairs from Columbia University in New York, where he focused on International Security Policy, and a B.A. in Politics, Philosophy and Economics from LUISS University in Rome, Italy. During his B.A., he also took part to a one-semester exchange program at Sciences Po University in Paris, France. Eugenio worked as a Crime Analyst at the New York Police Department and contributed to shaping the initial defense and security policy of Volt Europa, a new pan-European political movement. He also completed internships at the Delegation of the European Union to the United Nations, Morgan Stanley's Financial Crimes Unit and at the Asia-Pacific Center for Security Studies. His research interests include the role of regional organizations in strengthening cybersecurity. He is fluent in Italian (native), English, French and Spanish.