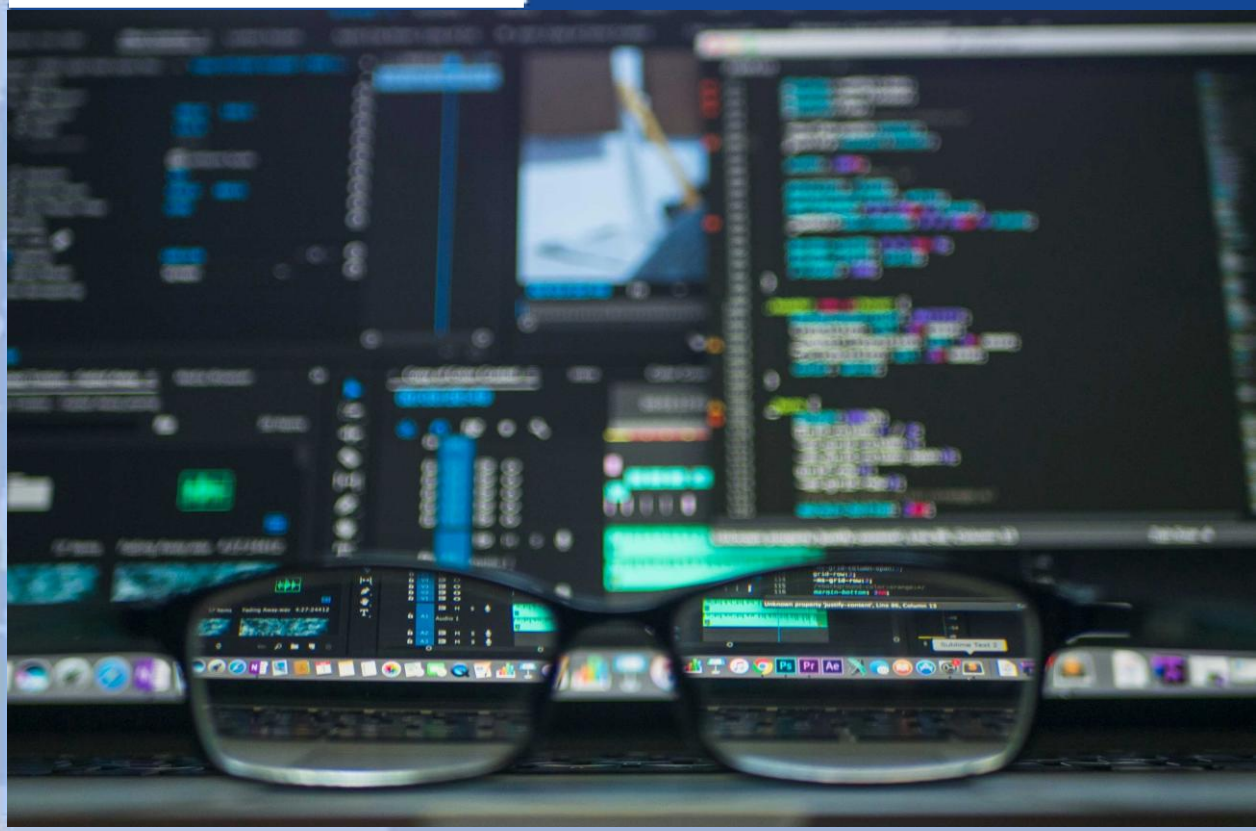
Southeast Asian Perspectives on Cybersecurity

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Eric Siyi Zhang
Rogier Creemers



June, 2025

The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website:

www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

Doelensteeg 16, 2311 VL Leiden, The Netherlands

LEIDEN ASIA CENTRE

Partners in Research and Knowledge

Executive Summary

This report examines how ASEAN and its member states understand the issue of cybersecurity, and how they navigate the growing geopolitical situation around this issue. It also discusses how Europe can best find its role in cybersecurity cooperation with the region.

Rather than pursuing security as an end in itself, ASEAN considers cybersecurity as a key enabler of economic progress and the betterment of living standards in the digital economy.[1] The grouping attaches great value to a cyberspace that is open, secure, interoperable, peaceful, and most importantly not fragmented along geopolitical lines. This enables non-alignment in cyberspace in the geopolitical sense, and 'technological hedging' in a geo-economic sense. At least tacitly, ASEAN (and its member states[2]) aims to adopt a 'selective hedging' strategy in managing its external relations, where it chooses to cooperate with external powerful nations in areas where it suits its own interests the most. While China is a pivotal actor in the digital economy in the region, the US and its allies are preferred partners on the issue of security. However, there is also significant variation among ASEAN member states in their geopolitical orientation.

Most ASEAN nations generally share a non-aligned geopolitical outlook and an economic-developmental approach to cybersecurity, but this hides a vastly diverse range of approaches on specific cybersecurity issues. Firstly, the region lacks a shared understanding of the scope of 'cybersecurity', and multiple states blur the line between 'cybersecurity' and 'information security'. Secondly, there is no consensus on whether cybersecurity should be addressed primarily through the lens of cybercrime or as an issue of national security, which can be explained by the region's diverse levels of digital maturity, political regimes, institutional set-up, and path dependency of past policies.

Public cyber attributions conducted directly by national governments to state actors are extremely rare. However, it should not be assumed that states in the region do not make such public attributions[3] purely out of deference. Countries in the region also view public

[1] ASEAN (2020), 'ASEAN Cybersecurity Cooperation Strategy (2021-2025)'. ASEAN.

[2] with different degrees of success

[3] to China or any other states

attribution as ineffective and political. Beyond their stance on public attribution, most states in the region also simply lack the cyber forensic capacities.

Policy recommendations

1. Europe should be aware of a fairly common perception in the region that European countries 'do not partner but only preach'. However, provided that European practitioners take the aforementioned sensitivity into account, an increased European role in non-traditional security (including cybersecurity) is generally welcomed. ASEAN states are particularly keen to bolster their neutrality and counterbalance major superpowers.
2. Policy should prioritise providing more capacity-building to countries in the region, particularly to those with a low level of digital maturity. This should also be done with more coordination with like-minded partners. In the long term, training the region's cybersecurity practitioners will contribute to aligning the region's and Europe's perspectives on cybersecurity. Capacity-building could also enable the region to conduct effective attribution of cyber incidents.
3. In the long-term, European industry-actors need to become more active and economically competitive in the region, in order to be able to provide enticing alternatives to digital solutions provided by Chinese actors. As the region's approach to cybersecurity focuses on economic and developmental issues, the viability of an external power as an economic partner would have ramifications regarding how the region manages security relations with it.
4. Public cyber attribution is considered to be ineffective, sensitive, and driven by geopolitical considerations, and pursuing collective attribution against China with countries in the region with territorial disputes would be highly counter-productive. However, European Actors should also actively discuss with their counterparts in the region China's own public cyber attribution, as the awareness of China's shifting approach to attribution remains low.
5. Currently, there is a lack of English-language literature studying the region based on a country-specific approach. Analysing ASEAN as a monolithic group risks underappreciating its diversity in domestic factors such as geopolitical outlooks, political regime, or the priorities of national law enforcement agencies. Future

research on the topic is however crucial and should be conducted in an extensively country-specific manner.

Contents

Introduction

In November 2020, the Netherlands released its Indo-Pacific Guidelines, calling for increased Dutch and EU engagement in the region to promote economic and political interests, as well as cooperation with 'like-minded democracies and countries with open-market economies'.[4] The strategy emphasises cooperation in maritime security, digital connectivity, and adherence to multilateral rules, positioning the Netherlands and the EU as key players in shaping the region's stability and technological governance.[5] In cyberspace specifically, the Netherlands offers various forms of capacity building for the ASEAN region, in the area of international law, threat landscape, CIIP, cybercrime, etc. Besides, the Netherlands also aims to play an active role in engaging with the region on a wide range of regulatory and normative themes, from cybersecurity and internet regulation to innovation, artificial intelligence, e-commerce, cross-border data transfer, privacy and national digital sovereignty.[6]

As a LeidenAsiaCentre report from 2021 pointed out, an issue that implicitly runs through European Indo-Pacific strategies is the China factor. While some Indo-Pacific strategies call for a more inclusive vision for the region, China remains what necessitated such a strategy in the first place.[7] While this is a reasonable policy logic that aims to adapt to new geopolitical and geoeconomic realities, it does mean that Chinese policy-makers will be carefully scrutinising our intent and formulating China's own responses accordingly.

Based on a review of existing literature, semi-structured interviews conducted with researchers on cybersecurity as well as with Dutch and European policy-makers, and a brief comparative study of cybersecurity strategies of selected ASEAN member states, this report aims to provide a better understanding of the region's conceptualisation and approaches to cybersecurity, as well as the diversity therewithin. The rest of this report proceeds as follows: first, it highlights that ASEAN's approaches to cybersecurity follows an economic-

[4] Ferchen, M. (2021), European Indo-Pacific Strategies in Comparative Perspective. LeidenAsiaCentre.

[5] Okano-Heijmans, M. (2021), The Netherlands and the EU turn to the Indo-Pacific, Clingendael. Available at: https://www.clingendael.org/publication/netherlands-and-eu-turn-indo-pacific.

[6] Government of the Netherlands (2020), 'Indo-Pacific: Guidelines for strengthening Dutch and EU cooperation with partners in Asia'. Government of the Netherlands.

[7] Ferchen, M. (2021) European Indo-Pacific Strategies in Comparative Perspective, p. 7.

development logic, where security is a means to realise its ambitions in the digital economy. Adopting this perspective, the report will then explain ASEAN's geopolitical outlook in cyberspace and how the group approaches its external relations. At the same time, it is important to bear in mind that the region is highly diverse in terms of political institutions, level of economic development, as well as geopolitical outlook. The following section therefore discusses how domestic factors in countries in the region can lead to distinctive conceptualisations and threat perceptions in cyberspace. Next, the report summarises the perspectives from the region on the issue of public cyber attribution, and explains why it is unlikely that countries in the region will pivot to public attribution in the near future as the following three key issues remain unresolved, i.e. capabilities, effectiveness, and geopolitical sensitivity. The conclusion and discussion of this report explore what Europe's future role in cybersecurity cooperation with Southeast Asia could be.

1. Southeast Asian approaches to security in cyberspace

This section addresses why ASEAN and its member states want security in cyberspace. Although the question may seem banal, an accurate understanding of security requires a critical look at its building blocks, as security is embedded within local perceptions and priorities. Cybersecurity strategy documents often contain problem statements that fundamentally shape policy options. For example, the Netherlands applies a normative logic about securing the public values of an 'an open, free, stable and secure digital world',[8] whereas the US's national security-oriented view highlights the tension between the US and its allies in promoting 'democracy, free speech, innovation, and equality' and what it refers to as 'authoritarian states that go against our national interests'.[9] It also needs to be highlighted that there are differences in scope through threats in cyberspace is understood. Both the EU and the US primarily adopt a technical definition and focus on hacks or other forms of unauthorised access, whereas China focuses on particular kinds of harm, whether they involve hacks or not.

As the rest of this chapter will show, ASEAN's approach to cybersecurity is characterised by the following three guiding principles: first, ASEAN regards cyberspace as a key enabler for economic prosperity and is more concerned with tangible economic cooperation in cyberspace rather than hard security questions. Second, ASEAN adopts a non-alignment approach towards external powers, primarily between the US and China in cyberspace. Third, this entails in practice that ASEAN and its member states adopt a strategy of 'selective hedging' in persuing cooperation with external powers: while the US and its allies

[8] 'We must not forget, however, that the ultimate objective is to safeguard our public values. We want to create an open, free, stable and secure digital world in which companies and individuals can participate as securely as in the physical world.' In

NCTV (2022) 'Netherlands Cybersecurity Strategy 2022-2028'. Ministry of Justice and Security.

[9] 'In doing so, the digital ecosystem has come to reflect the values of its architects and its users. Technologies have promoted democracy, free speech, innovation, and equality. But they also have been misused to enable transnational repression and digital authoritarianism… And we've worked with our allies and partners around the world to improve our capacity to collectively defend against and respond to cyber threats from authoritarian states that go against our national interests.' In

White House (2023), 'National Cybersecurity Strategy'.

are preferred partners in security issues, they often turn to China for economic and development issues.

ASEAN's approach to cybersecurity is primarily one that operates according to an economic-developmental logic, which is notably different from aforementioned Western cybersecurity strategies. For readers more accustomed to Western cybersecurity perspectives, an adequate appreciation of this often-overlooked fact aids understanding why the region's positions, interests, and needs in cyberspace appear different. As pointed out in the ASEAN Cybersecurity Cooperation Strategy (2021-2025), cybersecurity is a key enabler of economic progress and the betterment of living standards through the digital economy,[10] which supports ASEAN's digital ambitions in the areas of smart cities network, Industry 4.0, and a digital ecosystem.[11] In part, this builds on the future prospects of ASEAN's economy and favourable demographic conditions: ASEAN has a population of more than 670 million, the third largest in the world, and is expected to become the world's fourth largest economy. Among its population, 224 million are young people aged between 15 and 35, with high digital consumption and innovation potential and innovation vitality.[12] Scholars in the region view cybersecurity and information security as essential to the digitalisation ambitions of the ASEAN countries,[13] underpinning businesses and citizens' trust in the use of technology. The proliferation of new digital technologies in Southeast Asia such as 5G and IoT is making the economy and public life increasingly more dependent on cyberspace. Digital trust is also considered a key factor in driving digital economic growth, as the extent of users' trust in digital products and services can be either a growth enabler or a significant impediment with regard to the digital economy.[14]

In the area of cyber norms and global cyber governance, ASEAN member states in principle prefer a cyberspace that grants relatively high levels of autonomy for small and middle powers, which enables non-alignment and 'hedging' in cyberspace. This is crucial

[10] ASEAN (2020), 'ASEAN Cybersecurity Cooperation Strategy (2021-2025)'. ASEAN.

[11] Ibid. p.8.

[12] ASEAN (2022), Asean Youth Development Index 2022 the 2nd Report.

[13] Rahman, M.F.A. (2023) *Advancing Cyber and Information Security Cooperation in ASEAN*. RSiS IDSS Paper.

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

from an economic and developmental perspective in the digital context, as it has become the reality that digital solutions are developed by a mere handful of tech-giants, native to different great powers that are growing increasingly hostile to each other.

Strategic non-alignment is a fundamental principle of ASEAN's foreign policy.[15] In this context, a key term often invoked by official documents and academic publications is 'ASEAN Centrality'. The term originates from the ASEAN Charter, which states that ASEAN's main objective is to maintain ASEAN's centrality and proactive role as the main driving force in its relations and cooperation with external partners, in an open, transparent, and inclusive regional architecture,[16] in which ASEAN member states support and strengthen each other.[17] Rather than understanding 'ASEAN centrality' as a modus operandi for the group's conduct of diplomacy, it should be seen through the wider strategic purpose it serves: ASEAN's geopolitical orientation in cyberspace can be summarised as applying 'ASEAN centrality' in cyberspace.[18] This can be interpreted as maintaining ASEAN's agency in geopolitical contestation and avoiding becoming a pawn in great-power rivalry in cyberspace, thereby safeguarding its relative autonomy to pursue its (mostly economic) digital ambitions and other public policy goals. ASEAN centrality is being pursued in several ways when it comes to the grouping's management of external relations.

First, in its most literal reading, ASEAN centrality entails consolidating ASEAN's place at the centre of the region's diplomatic architecture where most multilateral diplomacy takes place,[19] as well as the institutional architecture of wider regional cooperation initiatives in the Asia–Pacific region.[20] This is an important principle informing the grouping's

[15] ASEAN (2012), ASEAN Security Community Plan of Action.

[16] Kominfo, K. (2023). ASEAN Centrality, What Does It Mean?. ASEAN Indonesia 2023. Available at: https://asean2023.id/en/news/asean-centrality-what-does-it-mean

[17] ASEAN (2008), The ASEAN Charter. Art. 15.

[18] Lu, C. and Zhang, S. (2024), 'Strategic Conception and Implementation Path of ASEAN Digital Geopolitics[东盟数字地缘政治的战略构想与实施路径]', *Nanyang Wenti Yanjiu*, 197, pp. 45–60.

[19] Kominfo, K. (2023), ASEAN Centrality, What Does It Mean?. ASEAN Indonesia 2023. Available at: https://asean2023.id/en/news/asean-centrality-what-does-it-mean

[20] Chen, X. and Yang, Y. (2022), 'Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance', *The International Spectator*, Vol.57(3), pp. 48–65. Available at: https://doi.org/doi.org/10.1080/03932729.2022.2066841. p.59.

management of external relations, particularly with more powerful actors such as the US and China. As ASEAN consists exclusively of small and middle powers, the benefit of engaging with great powers outside of the region as a unified bloc is self-evident: it would provide ASEAN as a whole the optimal possible power balance in such engagements. Besides, individual member states, through ASEAN's rotating chairmanship,[21] are able to socialise their priorities with counterparts within the region and incorporate their priorities in ASEAN's engagement with great powers outside the region. ASEAN centrality empowers its member states with agenda-setting powers which otherwise propense to be passive objects of great-power diplomacy.[22]

Second, the non-alignment principle shared by Southeast Asian countries also means that they in general avoid taking a clear stance on the divisive issues that have been internalised as an integral part of geopolitics in cyberspace. One of those divisive issues is between multilateralism and multi-stakeholderism. Some existing literature suggests that instead of choosing between an exclusively state-centric multilateral cyber governance approach versus a market-based multi-stakeholder approach, ASEAN seeks to be a 'broker' between the Chinese and US approaches to cyber governance.[23] Also, the voting behaviour of South-East Asian states at international fora tends to reflect this balancing exercise, brokering between proposals that reflect a state-centric view of cybersecurity governance and a market-based multi-stakeholder view of cyberspace.[24] The most recent ASEAN Cybersecurity Cooperation Strategy contains elements from both multilateral and multi-stakeholder models. While it supports a multilateral rules-based order in cyberspace, the course of action for regional cyber capacity building laid down in the document seems to have a mostly multi-

[21] ASEAN (2008). The ASEAN Charter. Art. 31.

[22] Connelly, A. (2022), *The often-overlooked meaning of 'ASEAN centrality'*. IISS. Available at: https://www.iiss.org/online-analysis/online-analysis/2022/06/the-often-overlooked-meaning-of-asean-centrality/.

[23] Van Raemdonck, N. (2021), Cyber Diplomacy in Southeast Asia. EU Cyber Direct. Available at: https://eucyberdirect.eu/content_research/cyber-diplomacy-in-southeast-asia/.

[24] Ibid.

stakeholder approach, referring to AJCCBC[25], ASCCE[26] and ACICE[27] as multidisciplinary, modular, multi-stakeholder and measurable programmes.[28] However, rather than a 'norm-hybridisation', this might be more indicative of the heterogeneity of digital maturity among ASEAN member states, and to a lesser extent might also be related to selective 'hedging' tactics in different issues in cyberspace. This argument will be revisited in greater detail in subsequent sections of this report.

Experts in the region have also voiced concerns that external efforts aimed at placing ASEAN in the US-China dichotomy deprives ASEAN countries of their agency. Policy makers and the public in Southeast Asia are very cognizant of the dangers of alignment with the different power plays regarding cyberspace.[29] In terms of cyber norms, the rivalry between China and the U.S. in cyberspace could significantly increase tensions in the region and relegate ASEAN to the role of normative recipient rather than of proactive agent.[30] Another sentiment generally shared by ASEAN countries is a concern for the seemingly already ongoing process of fragmentation of the global market of digital goods and services, exacerbated by the great power competition between the US and China, and how this ongoing process will impact small and middle powers.[31] Regulations such as the US's CHIPS Act will likely complicate ASEAN countries' access to certain critical technologies,[32] as they entail export controls aimed at curtailing the availability of certain technologies to geopolitical adversaries.

---

[25] ASEAN-Japan Cybersecurity Capacity Building Centre

[26] ASEAN-Singapore Cybersecurity Centre of Excellence

[27] ADMM Cybersecurity and Information Centre of Excellence

[28] ASEAN (2020), 'ASEAN Cybersecurity Cooperation Strategy (2021-2025)'. ASEAN.

[29] Noor, E. (2024). *[CSA series] Will ASEAN Seek Alignment or Independence When Pursuing Emergent Technologies?* [Video]. Available at: https://www.youtube.com/watch?v=fuhzCYPLw1Y (Accessed: 14 May 2024).

[30] Rahman, M. F. A. (2024), ASEAN Should Watch the China-US Cyber Competition More Closely. The Diplomat.

[31] Gomez, M.A. (2024), 'Will ASEAN Seek Alignment of Independence When Pursuing Emergent Technology?', *Counterpoint Southeast Asia*. Issue 10, March, pp. 2–20.

[32] Gomez, M.A. (2024), 'Will ASEAN Seek Alignment of Independence When Pursuing Emergent Technology?', *Counterpoint Southeast Asia*. Issue 10, March, p.3.

This report emphasises that the general consideration of non-alignment and the geopolitical orientation of maintaining neutrality in the US-China rivalry seem to be shared by all countries in the region, even though it is true that the positions of ASEAN countries on the US-China spectrum (to the extent that such placement is appropriate and informative) are very different, especially when it comes to security. As two cases in point, this also applies to the Philippines and Vietnam, which have at times bitter territorial disputes with China in the South China Sea, with the Philippines even enjoying a close security relation with the US. However, during the interviews conducted for this study, several interlocutors mentioned that territorial disputes in the South China Sea would be an inaccurate indicator if used to characterise the Philippines or Vietnam's overall relation with China.[33] One Vietnamese official was even quoted as saying that 'South China Sea is only 1% of our relation with China'.[34] There appear to be both (geo-)economic and purely geopolitical considerations behind this approach: revisiting the argument on ASEAN's economic-developmental policy logic of their approaches to cybersecurity, it should be emphasised that most ASEAN countries are developing countries, which are primarily looking for trade and investment to bring tangible economic benefits. In this regard, China is ASEAN's largest trading partner, while about 40% of official development finance of ASEAN comes from China.[35] In terms of geopolitical considerations, while the US seems to be a more trusted partner in security (a point to be elaborated in the following paragraphs of this report),[36] it is also considered to be a distant and, according to some, declining power, whose commitment to the region is becoming increasingly uncertain.[37]

In practice, this means that ASEAN[38] selectively adopt practices of hedging in order to maximise their autonomy in cyberspace. ASEAN's selective hedging with major powers

[33] Gomez, M. A. (23 July 2024), Personal Communication.

Domingo, F. (6 September 2024), Personal Communication.

Anonymised interlocutor (23 July 2024), Personal Communication.

[34] Yaacob, A. R. (2024), Asian countries: pro-US or pro-China? Studio Asia.

[35] Ibid.

[36] Yusof Ishak Institute (2024), The State of Southeast Asia 2024 Survey Report. Available at: https://www.iseas.edu.sg/wp-content/uploads/2024/03/The-State-of-SEA-2024.pdf.

[37] Ibid.

[38] For clarification, in the context of 'hedging' ASEAN refers only to the organisation, not its member states.

in cyberspace is neither equidistant foreign policy – where countries walk the thin line of a perfect middle way between major powers – nor can it be characterised as diversification, where countries engage on various issues with multiple major powers simultaneously. ASEAN has different preferences and adopts different strategies of engagements with external powers, depending on what specific issues are at hand according to its own interests and needs.

An analysis of which external power ASEAN has concluded bilateral agreements and cooperation mechanisms with in the areas of cybersecurity, economic development, and governance and norms suggests that ASEAN may have different preferences and priorities on issues when they engage with the US and China. Thus, ASEAN has habitually cooperated with China on economic and development issues and with the US on cybersecurity and the governance of cyberspace.[39] The most important element of ASEAN's economic cooperation with China seems to be the deployment of digital infrastructure, including submarine optic cables, computing power infrastructure and navigation satellite systems.[40] This is in line with ASEAN'S own digital strategies – the ASEAN Digital Masterplan 2025 and its two ICT Masterplan predecessors from the 2010s, which aim to build 'high quality and ubiquitous connectivity throughout ASEAN, delivered through the underlying telecommunications infrastructure' – in part through attracting investment in digital infrastructure and ICT.[41] In this context, it should be reiterated that enhancing connectivity through investment and deployment in infrastructure lies at the core of China's signature BRI and Digital Silk Road initiatives.[42] Although the BRI and Digital Silk Road have received at best mixed feedback in the West, the reception of those initiatives by experts from Southeast Asia seems positive overall,[43] with the Philippines as the only outlier due to unfinished projects and concerns over

[39] Lu, C. and Zhang, S. (2024), 'Strategic Conception and Implementation Path of ASEAN Digital Geopolitics[东盟数字地缘政治的战略构想与实施路径]', Nanyang Wenti Yanjiu, 197, pp. 45–60.

[40] Ibid.

[41] ASEAN (2021), ASEAN Digital Masterplan 2025. p.5.

[42] Dekker, B., Okano-Heijmans, M. and Zhang, E.S. (2020), 'Unpacking China's Digital Silk Road'. Clingendael Report.

[43] e.g. SIIA. (2024), Understanding the "Digital Silk Road": Implications for ASEAN. Available at: https://www.siiaonline.org/understanding-the-digital-silk-road-implications-for-asean/;

the involvement of illicit capital in the Philippines.[44] At the official level, ASEAN and China have also signed an MoU on synergising the ASEAN Master Plan on ASEAN Connectivity (MPAC) 2025 and the BRI in 2019.[45] Although the shortfall between pledges and implementations is a lingering issue for BRI infrastructural projects, China is still by far the largest country of origin of investments in infrastructure projects in Southeast Asia between 2015 and 2021. It should also be pointed out that the second and third largest investor in infrastructure projects are Japan and Japanese-led ADB, with France and Germany only taking sixth and seventh place respectively.[46]

Regarding the issues of cybersecurity and the international governance of cyberspace, ASEAN has habitually engaged more with the US and its allies, apart from cooperation on cyber capacity-building within the region, such as the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) launched in October 2019. Together with the US, Singapore also provides capacity building training to Southeast Asia, including in the areas of cybersecurity and cyber defence, through the Third Country Training Programme (TCTP).[47] In 2018, ASEAN and the US also established the ASEAN-US Cyber Policy Dialogue, which serves as a primary platform for advancing cybersecurity cooperation, where both sides emphasise maintaining an open, stable, and secure cyberspace aligned with the norm of responsible state behaviour.[48] This exemplifies a comprehensive approach that combines capacity building with alignment on international governance of cyberspace, such as cyber norms. Besides, there has been strong regional cybersecurity engagement with ASEAN by Japan, Korea and

Zheng, W. (2024), 2024/1 "China's Digital Silk Road (DSR) in Southeast Asia: Progress and Challenges". Yusof Ishak Institute. Available at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-1-chinas-digital-silk-road-dsr-in-southeast-asia-progress-and-challenges-by-wang-zheng/.

[44] Camba, A. et al. (2023), 'How Has China's Belt and Road Initiative Impacted Southeast Asian Countries?' Carnegie China.

[45] ASEAN (2019), ASEAN-China Joint Statement on Synergising the Master Plan on ASEAN Connectivity (MPAC) 2025 and the Belt and Road Initiative (BRI).

[46] Dayant, A. and Stanhope, G. (2024), Mind the gap: Ambition versus delivery in China's BRI megaprojects in Southeast Asia. Lowy Institute.

[47] Ministry of Foreign Affairs of Singapore (2018), Singapore - United States Third Country Training Programme. Available at: https://www.mfa.gov.sg/Newsroom/Announcements-and-Highlights/2018/08/TCTPsigning.

[48] ASEAN (2023), Co-Chairs' Statement on the Third ASEAN-U.S. Cyber Policy Dialogue. Available at: https://asean.org/co-chairs-statement-on-the-third-asean-u-s-cyber-policy-dialogue/.

Australia. Japan has assisted ASEAN in various areas of cooperation and has pursued activities to build technical capacities and capacities to support norms and confidence-building measures.[49] Some ASEAN member states also cooperate with China in the area of responding to threats in cyberspace, mainly in the area of tackling cybercrime.[50] However, instead of a deliberate act of diversification on security issues, this is likely a logical expansion of the ASEAN-Chinese cooperation on tackling transnational crime that has been in place since the early 2000s. However, it also needs to be highlighted that the cyber threats in Southeast Asia are more often perceived and addressed through the lens of tackling crime rather than as a national security or geopolitical issue. This argument will be discussed in greater detail in the next section of this report.

The pattern of ASEAN's selective hedging when it comes to its engagement and cooperation with external powers is characterised by a China-leaning approach to economic and developmental issues, and a Western-leaning approach on security issues. This approach is driven by a desire to maximise its interests in the relations with both China and the US, and reflects the region's view of those two great powers. China is seen as an economic opportunity and an irreplaceable source of investment in digital infrastructure, which is key to ASEAN's own digital ambitions. At the same time, according to the Southeast Asia Situation Report released by the Yusof Ishak Institute in 2024 there are growing concerns about China's increasing economic, political and strategic influence in the region, coupled with declining trust in the country.[51] Growing economic dependence on China seems to have become a growing concern more recently. Accordingly, ASEAN has more actively involved US actors in the field of digital economy and digital infrastructure, which some scholars interpret as aiming to introduce American power to balance China's digital influence in an area with relatively low sensitivity, in order to avoid antagonising China.[52] Regarding ASEAN's current Western-leaning outlook on security issues, especially concerning cybersecurity, the pivotal role played by Singapore also cannot be understated, as a significant

[49] Van Raemdonck, N. (2021), *Cyber Diplomacy in Southeast Asia*. EU Cyber Direct. p.34.

[50] Lu, C. and Zhang, S. (2024), 'Strategic Conception and Implementation Path of ASEAN Digital Geopolitics[东盟数字地缘政治的战略构想与实施路径]', Nanyang Wenti Yanjiu, 197, pp. 45–60.

[51] Yusof Ishak Institute (2024), The State of Southeast Asia 2024 Survey Report.

[52] Bi, S., Li, G. and Shen, S. (2024), 'US-ASEAN Digital Economy Co-operation: The Conflict between Security and Development[美国—东盟数字经济合作: 安全与发展的冲突]', *Nanyang Wenti Yanjiu*, 2024(1), pp. 85–99.

part of ASEAN-central cooperation mechanisms with the US and its allies in the area of cyber capacity-building are initiated and coordinated by Singapore.

2. Regional diversity in conceptualisations an threat perception

The preceding section of this report intentionally adopted an angle that analyses ASEAN as a whole, in order to sketch a generalisable picture of some of the shared positions and considerations underlying the group's approach to security in cyberspace. However, ASEAN member states' specific approaches to countering threats in cyberspace are distinct from each other. All South-East Asian countries face a dilemma of priorities along two lines: firstly regarding the nature of the threat – whether these fall under the narrow and technical sense of 'cybersecurity' (correct functioning of internet and telecommunication) or also pertain to wider content-related information security (e.g. disinformation, influence operations, or terrorism) – and secondly regarding the nature of actors, specifically whether they are cybercriminals or state-sponsored/state-affiliated actors.[53] These different approaches can often be linked to the region's diversity in terms of their political institutions, digital maturity, as well as the question of which governmental agency is tasked with tackling threats in cyberspace. While those variables do not always conclusively explain the variations in ASEAN member states' approaches to cyberspace, appreciating country-specific contexts can contribute to understanding why their approaches to threats in cyberspace are different.

Following the developments in UN cyber-processes in recent years such as the UN norms of responsible state behaviour in cyberspace and the UN cybercrime convention, policy-makers and researchers in the West are all too familiar with the major lines of division regarding the question of 'what constitutes cyberspace with regards to state interests'. This largely boils down to the range of constructs in cyberspace that should be securitised: whether it is only the infrastructure that allows access to cyberspace, or both the infrastructure and the social interaction taking place in cyberspace, should fall under states' own remit of security.[54] Among major powers in cyberspace, positions on this debate largely coincide with the geopolitical division lines. While the former perspective is mostly adopted by Western nations and its like-minded partners that promote the free flow of information in cyberspace with limited government oversight, Russia and China perceive information as an inherent source of threat from hostile powers: this view was accentuated in an SCO project (Shanghai

[53] Van Raemdonck, N. (2021), *Cyber Diplomacy in Southeast Asia*. EU Cyber Direct.

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

Cooperation Organisation) for responsible state behaviour back in 2011 - the International Code of Conduct for Information Security, submitted to the UN - which called on states 'not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'.[55]

In the Global South, however, the dividing line between 'cybersecurity' and 'information security' is much blurrier. During the interviews conducted for this study, various interlocutors referred to the confusion around the definition of 'cybersecurity' in the context of multilateral cooperation under the ASEAN framework, while the 'like-minded' technical definition of cybersecurity is currently still dominant.[56] In practical terms, the existence of these two definitions is notable as it offers not only different conceptualisations of cyberspace, but also implies a possible divergence in threat perception.[57] It should also be pointed out that the concern within ASEAN about information operations is genuine; campaigns of disinformation have been blamed for social unrest and violence in Indonesia and the Philippines.[58] In Philippines and Malaysia, political influencing and information manipulation are not automatically seen as a threat by foreign actors, as such tactics are also commonly used by domestic political parties and businesses against their own population.[59] Interviewees from the Philippines and Vietnam also shared concerns over info-operations ostensibly conducted by foreign actors: website-deface operations often coincide with high tensions in territorial disputes in the South China Sea,[60] and the Philippines in particular has

[55] SCO (2011), International Code of Conduct for Information Security.

[56] Anonymised interlocutor (23 September 2024), Personal Communication;

Domingo, F. (6 September 2024), Personal Communication;

Anonymised interlocutor. (25 July 2024), Personal Communication

[57] Tran Dai, C. and Gomez, M.A. (2018), 'Challenges and opportunities for cybernorms in ASEAN', *Journal of Cyber Policy*, 3(2), pp. 217–235. Available at: https://doi.org/10.1080/23738871.2018.1487987.

[58] Van Raemdonck, N. (2021), *Cyber Diplomacy in Southeast Asia*. EU Cyber Direct.

[59] Anonymised interlocutor (25 July 2024), Personal Communication.

[60] Tran, B. (23 July 2024), Personal Communication;

Gomez, M. A. (23 July 2024), Personal Communication.

experienced election interference in support during its last presidential election campaign.[61] Here, it is generally believed that either actors that sympathise with China or Chinese state-affiliated actors are behind these campaigns, although it was difficult to establish the real-world identity of the perpetrators due to a lack of cyber forensic capabilities. The complexity and heterogeneity in conceptualisation of threats

in cyberspace is also reflected in cooperation on cybersecurity under the ASEAN framework. ASEAN's latest Cybersecurity Cooperation Strategy summarises the changing threat perception in the region as follows:

> *'Traditional cyber and digital risks issues are no longer as straightforward as they used to be as these domains have evolved to be more cross-cutting and complex. International and domestic conversations on the correlation between cyber and digital issues like data security, misinformation and disinformation, influence operations and fake news, to name a few, are gradually gaining more traction in cybersecurity discussions.'*[62]

As non-interference is one of the founding principles of ASEAN, it is recognised in the grouping that information/content-related threats in cyberspace are more politically contentious, and regional cooperation under the ASEAN framework to tackle those threats is confined mostly to information sharing, with no capacity-building component.[63]

The table below provides a preliminary overview of selected ASEAN member states' approaches to tackling threats in cyberspace, in terms of what those states aim to secure in cyberspace, specific governmental institutions delegated to tackle threats in cyberspace, and their most recent cybersecurity strategy documents. This comparison is in no way intended to be comprehensive, but rather offers some rudimentary country-specific contexts.

[61] Gomez, M. A. (23 July 2024), Personal Communication

[62] ASEAN (2020), p.6.

[63] Anonymised interlocutor.

Table 1: Cyber strategy of selected ASEAN countries

	Cybersecurity strategy	Objectives	Specialised insitutions responsible for tackling threats in cyberspace
Singapore	The Singapore Cybersecurity strategy 2021	Protecting critical information infratstructures, devices, and applications that power the digital economy[64]	Cyber Security Agency of Singapore Singapore Armed Forces – Digital and Intelligence Service
Malaysia	Malaysia Cyber Security Strategy 2020-2024[65]	Safeguard critical information infrastructures essential for national security, economic stability, and public safety	National Cyber Securtiy Agency (NACSA) [66] Ministry of Defence – Cyber Defence Operation Center
The Philippines	National Cybersecurity Plan 2023-2028	Securing government network Protecting crititcal infrastructure Counter disinformation[67]	Department of Information and Communications Technology[68]
Vietnam	National Cyber Security and Safety Strategy, Proactively Responding to Challenges From Cyberspace to 2-25, With a Vision to 2030[69]	Protecting regime security[70] Defending cyber sovereignty[71] Defending territorial integrity in cyberspace Protecting critical infrastructure Economic development	Ministry of Public Security Ministry of Defence – Taskforce 47 – Cyberspace Operations Command Ministry of Information and Communciations
Cambodia	Cambodia Digital Economy and Society Policy Framework 2021-203572	Developing infrastructures Building legal systems and raising awareness of digital security Promoting digital leadership and mobilizing digital talents Building digital public services Encouraging enterprises to adopt digital technologies73	CamCERT

[64] Cyber Security Agency of Singapore (2021), The Singapore Cybersecurity Strategy 2021. Available at:https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021
[65] National Security Council of Malaysia (2020), Malaysia Cyber Security Strategy 2020-2024. Available at: https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf.
[66] Ibid.
[67] DICT (2022), National Cybersecurity Plan 2023-2028.
[68] Domingo, F. (6 September 2024), Personal Communication.
[69] Prime Minister of Vietnam (2022), Approving the National Cyber Security and Safety Strategy, Proactively Responding to Challenges from Cyberspace to 2025, with a Vision to 2030. Available at: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-964-QD-TTg-2022-phe-duyet-Chien-luoc-An-toan-An-ninh-mang-quoc-gia-den-2025-525540.aspx
[70] Tran, B. (2024), Vietnam Strengthens Cyber Capabilities for Political Stability, National Defence, and Socio-economic Development. Yusof Ishak Institute. Available at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-78-vietnam-strengthens-cyber-capabilities-for-political-stability-national-defence-and-socio-economic-development-by-bich-tran
[71] Ministry of Science and Technology (11 August 2022), Gov't issues new national cybersecurity strategy. Available at: https://english.mic.gov.vn/govt-issues-new-national-cybersecurity-strategy-197154584.htm.

[72] Supreme National Economic Council of Cambodia (2021), Cambodia Digital Economy and Society Policy Framework 2021-2035. Available at: https://asset.cambodia.gov.kh/mptc/media/EN-Policy-Framework-of-Digital-Economy-and-Society.pdf.
[73] Ibid.

A less context-sensitive angle that researchers and policy-makers can use to understand these differences is through ASEAN member states' distinctive level of digital maturity. Countries with high digital maturity, most notably Singapore, will have more vested interests in advancing norms adoption, capacity-building measures and other cyber policy aspects. In comparison, countries with low digital maturity do not recognise the threat due to the absence of assets that are placed in harm's way, and will tend to prioritise digitisation.[74] Digital maturity can be measured by various indicators, such as the population's connectivity to the internet, or more comprehensive indicators such as the ITU's Global Cybersecurity Index. We will not address this point extensively in this report, as it is already discussed in existing literature.[75] Briefly, there are anomalies at both the high end of digital maturity - Singapore, which plays an exceptionally active, if not central, role in regional cooperation on cybersecurity - and at the low end of digital maturity, e.g. Myanmar, Laos, and Cambodia.

This report instead highlights the necessity of considering country-specific contexts, including the political regime, institutional set-up, and path dependency of existing policies when appreciating their divergent approach to cybersecurity. Perhaps one of the most notable cases in this context is Vietnam, which has the most distinctive conceptualisations and threat perceptions of cybersecurity in the region, due to its regime type. Apart from the common denominator in the region – safeguarding a secure and trustworthy cyberspace for the development of the digital economy – Vietnam's approach to cybersecurity is also prompted by the goal of protecting the leadership of the Communist Party of Vietnam.[76] In this regard, Vietnam's threat perception in cyberspace has an 'endogenous' focus on information security, which is not a response to emerging challenges (e.g. misinformation during COVID pandemic) as is the case in other ASEAN countries, but is pre-determined by the needs of its own political institutions. A unique set-up of the Vietnamese cyber forces that is absent in other ASEAN member states is a unit tasked with domestic public opinion control, named Task Force 47, after its Directive No. 47 issued in 2016. The unit operates under the military's chain of command with over 10,000 members. Rather than the technical aspects of cyberspace, they

[74] Tran Dai, C. and Gomez, M.A. (2018), 'Challenges and opportunities for cyber norms in ASEAN', Journal of Cyber Policy, 3(2), pp. 217–235. Available at: https://doi.org/10.1080/23738871.2018.1487987. p.272.

[75] E.g. Dai & Gomez (2018).

[76] Tran, B. (2024), Vietnam Strengthens Cyber Capabilities for Political Stability, National Defence, and Socio-economic Development. Yusof Ishak Institute.

often act as internet commentators who 'counter unfavourable views' by propping up voices of support for the regime.[77] Vietnam's approach to cybersecurity is also guided by the principle of cyber-sovereignty, which, similar to the Chinese approach, stipulates states' jurisdiction over cyberspace as another form of territory just like land, sea and air. At the same time, there seems to be another aspect to Vietnam's understanding of cyber-sovereignty which is absent in the Chinese conceptualisation - i.e. protecting sovereignty/the idea of territorial integrity in cyberspace. In 2019, the movie 'Abominable', which showed a map with the nine-dash-line, was shown in Vietnamese cinemas for a week before the film was banned.[78] The incident was perceived from the perspective of defending national territorial integrity in Vietnam, as 'the inclusion of the line in the movie was seen as an attempt by China to legitimise its territorial claims, which serves as clear examples of how cyberspace has become an arena in the territorial disputes.'[79] Vietnam's political institution that is particular in the region also has ramifications when it comes to how the country addresses the issue of economic dependence in cyberspace. As mentioned in the previous section of the report, there are growing concerns in the region about over-dependence on Chinese solutions particularly when it comes to 5G telecommunication infrastructure: considerations of costs and economic development mean that countries in the region often prefer 5G telecommunication infrastructure provided by Chinese companies in spite of concerns about national security and over-dependence. However, Vietnam's telecommunication network is owned by the Ministry of Defence which does not operate according to a market logic, and Vietnam's 5G network as a result is more or less independent of Chinese companies.[80]

While it is a fairly common approach in the region to tackle cyber-dependent incidents (e.g. cyber-attacks on critical infrastructure) at least partially from a cybercrime (rather than geopolitical or national security) perspective, cyber-enabled crimes are placed on a heightened agenda in some countries' approaches to cybersecurity. During the interviews

[77] Tran, B. (2024), Vietnam Strengthens Cyber Capabilities for Political Stability, National Defence, and Socio-economic Development.

[78] AP News (16 October 2019), Vietnam bans animated 'Abominable' over South China Sea map. Available at: https://apnews.com/arts-and-entertainment-movies-general-news-aa84fa2df6d541bd992a46c0761f1742.

[79] Tran, B. (2024).

[80] Tran, B. (23 July 2024), Personal Communication.

conducted for this study, interlocutors from the Philippines reported that 'next to national security, (often domestic) cybercrime is also a usual lens through which threats in cyberspace are perceived'.[81] Additionally, some interviewees indicated that the fact that cybersecurity is often addressed through the lens of cybercrime – an approach that is drastically distinct from the 'like-minded' approach – might originate from a deeper level, namely the training of cybersecurity practitioners which is often only technical.[82] This means that practitioners in the region take an incident-specific and solution-driven approach and are not inclined to put cyber incidents in the wider geopolitical context.

[81] Gomez, M. A. (23 July 2024), Personal Communication.

[82] Domingo, F. (6 September 2024), Personal Communication.

3. Perspectives in the region on public cyber attributions

For the proponent of public attributions of incidents in cyberspace, the underlying logic revolves around addressing the covertness of cyber operations, as accountability remains a vacuous concept if there is no means to identify the culprit of an attack.[83] Apart from increasing awareness which contributes to overall cyber resilience, another important consideration of public cyber attributions is its supposed effectiveness on addressing state-sponsored cyber operations. While cyber-criminals and other non-state actors are unlikely to be influenced by incurred reputation damage, it is assumed that states are bound, to different degrees, by written norms or a tacit understanding of what constitutes responsible state behaviour. Strategically, (public or non-public) cyber attribution can also contribute to the credibility of deterrence. However, public attribution is just the last link in the pipeline of attribution of cyber incidents in cyberspace, and the heightened attention it has received is due to its highly politicised nature.

A brief review of the pipeline of how attribution is conducted, as well as what the alternatives are to public attribution, are necessary for a sufficiently nuanced understanding of the cautious approach in the region regarding cyber attribution. Attribution of cyber incidents begins with technical attribution, typically through technical forensics and intelligence information. This technical attribution aims to answer three questions: (1) whether the incident is malicious, (2) what is the identity of the perpetrators and what are their motives, and (3) what is the gravity of the incident.[84] After that, decisions are taken about if and how the cyber incident should be responded to: an alternative to public attribution is 'private' attribution, by either (1) communicating with the state suspected to be behind the incident, or even (2) conducting responsive operations in cyberspace or in physical space. Within the realm of public attribution, there are a few alternatives to the official public cyber attribution (attribution conducted directly by governmental agencies in a public manner), e.g. unofficial public attribution through press leaks or through cybersecurity firms that may have worked closely with the government during the technical attribution of the incident. As

[83] Zhang, E.S. and Creemers, R. (2023), The Evolution of Chinese Perspectives on Cyber Deterrence and Attribution. LeidenAsiaCentre. p.5.

[84] Levite, A., Lee, J. (2022), Attribution and Characterization of Cyber Attacks. Carnegie Endowment.

pointed out in a LeidenAsiaCentre report from 2023, official public attribution is the only kind of attribution of cyber incidents that is politically contentious between the West and China.

Two unresolved issues concerning official public attribution frequently surfaced during the interviews conducted for this study with experts from the region: first, interlocutors often question the effectiveness of public attribution. As also noted in existing literature written by Western-based authors, public attributions to other state-actors by the US in the last decade has not led to a drop in state-sponsored cyber-attacks on the US and its allies.[85] Second, while various interlocutors of research interviews acknowledge the general considerations of raising cyber-awareness and how public attribution can contribute to overall cyber resilience, questions are also raised about the possible geopolitical motives of public cyber attribution made by the West towards China (which is often at the receiving end of those attributions). It is anyhow worth noting that situations where national governments openly attribute cyber incidents to other state actors are more of an anomaly than common practice. This is of course also due to the difference in cyber forensic capabilities, in which the US and its allies are currently still far ahead.

Official attributions of cyber incidents to state actors in the region remain extremely rare, with very few recent exceptions. In June 2024, the DICT of the Philippines claimed that a Chinese APT conducted cyberattacks against online sites of the Philippine Coast Guard.[86] During the interviews conducted for this study, two interlocutors reported that political considerations seem to have prompted this apparent policy shift, as the current Marcos administration aims to demonstrate (to both their domestic constituencies and international allies) that they are 'stepping up' in tackling cybersecurity issues.[87] However, there are questions about whether the DICT's act of public attribution was coordinated with the Philippines Ministry of Foreign Affairs. It also remains to be seen whether this is an isolated incident and if this policy will persist in future Philippine administrations, in the longer term. More typical is an 'elephant in the room' approach to public cyber attribution, for instance

[85] Levite, A.E. et al. (2022), 'Managing U.S.-China Tensions Over Public Cyber Attribution'. Carnegie Endowment for International Peace & Shanghai Institute for International Studies.

[86] Presidential Communication Office of the Philippines (26 June 2024). Chinese 'APT' behind cyberattacks on PCG – DICT. Available at: https://pco.gov.ph/news_releases/chinese-apt-behind-cyberattacks-on-pcg-dict/.

[87] Gomez, M. A. (23 July 2024). Personal Communication.

Domingo, F. (6 September 2024). Personal Communication.

Singapore's handling of the Singhealth data breach in 2018, where the Cybersecurity Agency of Singapore (CSA) noticed that the cyber-attack was 'the work of a skilled and sophisticated actor bearing the characteristics of APT groups, which are typically state-linked'.[88]

While not attributing cyber incidents to specific nation-states is common practice for ASEAN member states' governments, scholars from the region do not shy away from naming specific state actors in their analyses. In this context, China is usually perceived to be the main source of cyber threats linked to state-sponsored or state-affiliated actors. Scholars from the region characterise China's cyber operation in Southeast Asia as a kind of 'low-impact cyber conflict' or 'grey zone activities'[89], which uses cyber operations as a tool to support its influence in the region while minimising the risk of escalation, as China aims to establish itself as a benign presence both for ASEAN countries and the international community. Scholars in the region have also identified territorial disputes in the South China Sea as a nexus where the cyber dimension of traditional geopolitical conflicts has gained prominence in recent years. These disputes have been the focus of much of the cyber espionage and hacktivism in the region, with the potential risk of escalating conflicts in physical space. As far as attribution is concerned, scholars in the region have also pointed out the complex landscape of cyber threats originating from China, especially the role of state-sympathetic non-state-actors. These actors can either be patriotic hackers who may act autonomously with minimal or no government control,[90] or non-state actors not bound by norms of responsible state behaviour, which are used by state actors to conduct cyber operations while maintaining plausible deniability.[91]

Not antagonising China on an issue that it considers politically sensitive would certainly be a consideration in ASEAN's economic-developmental approach to cybersecurity. Countries in the region are also wary of the West's politicised view of cybersecurity, where public attribution is often viewed as an attempt to broaden its camp, which is largely in line

[88] Ministry of Digital Development and Information (15 January 2019), Government's response to the report of the COI into the cyberattack on SingHealth. Available at: : https://www.mddi.gov.sg/media-centre/speeches/statement-by-minister-on-govt-response-to-report-of-coi-during-parl-sitting/ .

[89] Rahman, M.F.A. (2023), *Advancing Cyber and Information Security Cooperation in ASEAN*. RSiS IDSS Paper. p.3

[90] Tran Dai, C. and Gomez, M.A. (2018), 'Challenges and opportunities for cybernorms in ASEAN', *Journal of Cyber Policy*, 3(2), pp. 217–235. Available at: https://doi.org/10.1080/23738871.2018.1487987

[91] Rahman, M.F.A. (2023). p.5.

with Chinese experts' perspective on the issue.[92] **However, it would be misguided to assume that states in the region do not make official public attributions to China purely out of deference.** The most important underlying issue in many countries in the region (perhaps with Singapore as the only exception) is that they lack sufficient cyber forensic expertise to conduct solid technical attribution. For example, the attribution conducted by the DICT of the Philippines was mostly a statement asserting that a cyber incident had been conducted by a Chinese-linked APT, which is notably different from the cyber attribution reports with evidence substantiated by technical details, commonly published by Western countries.[93] This is also corroborated by interviews conducted for this study. For most countries in the region, this means that they would be unable to make public attribution, should their governments decide to do so. Second, as mentioned above, the fundamental approach to managing cybersecurity in the region is technical, incident-specific, solution-driven, and less placed in a wider geopolitical context. Accordingly, practitioners in the region will be more preoccupied with how to mitigate the damage caused by the specific incident and how to enhance cyber resilience. ASEAN's threat perception in cyberspace mainly focuses on the technical aspects and on cybercrime, rather than on issues of 'national security'. As the effectiveness issue of official public attribution remains unresolved, they have little incentive to resort to this approach.

[92] Jing, L. and Tang, X. (2023), 'An analysis of the asymmetry of cybersecurity governance cooperation between the "Five Eyes Alliance" and ASEAN[" 五眼联盟" 与东盟网络安全治理合作的 不对称性分析]', *Journal of Intelligence*, 42(1), pp. 42–51.

[93] E.g. MIVD. (2024), Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT.

4. Conclusion and Discussion – What should be Europe's role in cybersecurity cooperation with Southeast Asia?

This report describes in outline how ASEAN and its member states perceive and tackle the issue of cybersecurity. A tacit but underlying thread concerns how those perspectives and approaches are different from those held in the West. Based on a review of existing literature primarily by authors from the region, semi-structured interviews conducted with experts from the region, and a brief comparative study of cybersecurity strategy documents published by national governments of ASEAN member states, this report concludes the following.

In general, ASEAN's approach to cybersecurity is based on an economic-developmental logic. Rather than pursuing security as an end in itself, cyber security is considered to be a key enabler of the economic progress and betterment of living standards in the digital economy by enhancing citizens' and businesses' digital trust, specifically regarding ASEAN's digital ambitions in the areas of smart cities network, Industry 4.0, and a digital ecosystem. It should also be highlighted that ASEAN is a grouping that consists exclusively of small and middle powers. As a result of these two factors, countries in the region are primarily concerned to have a cyberspace that is open, secure, interoperable, peaceful, and most importantly, not fragmented along geopolitical lines. This gives these small and middle powers a relatively high level of autonomy and enables non-alignment in cyberspace in the geopolitical sense, and 'technological hedging' in a geo-economic sense in a world where digital solutions are developed by a mere handful of tech-giants, native to different major powers that are growing increasingly hostile towards each other. The current overall ASEAN approach to the US and China is to choose to cooperate in areas that best serve its own interests. China plays a pivotal, if not dominant, role in the development of digital infrastructure in the region due to the fact that solutions provided by Chinese actors are much more available and marketable, which often means that diversification from China is a question of possibility rather than of choice. At the same time, the US and its allies are preferred partners on the issue of security (with Laos and Cambodia as exceptions).

As emphasised several times previously, Southeast Asia is a vastly diverse region with respect to cybersecurity issues, although some shared commonalities (as summarised in the previous paragraph) do exist. Firstly, the region lacks a unified understanding of the scope of 'cybersecurity', which has fundamental implications for the region's threat perception. On

this issue, it should be pointed out that the 'network neutrality' definition that defines cybersecurity purely in technical terms is in itself a normative position. In the Global South including but also beyond Southeast Asia, where such geopolitical contests are less pronounced, the line between 'cybersecurity' and 'information security' is often more blurred. The region's concern about misinformation and disinformation is also genuine, with common concerns of domestic actors of influence operation, and misinformation during the COVID-19 pandemic. Parenthetically, the issue of disinformation is also gaining traction in Europe, with more focus recently and particularly on the phenomenon of Foreign Information Manipulation and Interference (FIMI). Secondly, there is also no consensus on whether cybersecurity should be addressed primarily through the lens of cybercrime or as an issue of national security. On this point, the diversity can be explained by the region's diverse level of digital maturity, political regimes, institutional set-up, and path dependency of past policies.

Public cyber attributions conducted directly by national governments to state actors are extremely rare, with notable recent exceptions in the Philippines. Not attributing to state actors can be explained by at least three factors: (1) Most states in the region, with Singapore as an exception, lack the cyber forensic capabilities to conduct solid technical attribution, substantiated by persuasive evidence backed up by technical details. This means that most countries in the region are simply not in a position to conduct substantiated public attributions, even if they would wish to do so. (2) Public cyber attribution is widely perceived as an ineffective measure to counter threats in cyberspace originating from state actors. Empirically speaking, this claim would also be difficult to reject. Practitioners in cybersecurity in the region, who often have a purely technical training, are inclined to not place cyber incidents in political contexts, and instead come up with incident-specific solutions to mitigate damages caused by the incident. In this framework, a place for public attribution becomes difficult to conceive. (3) Public cyber attribution is viewed as a politically sensitive issue, with the West's conduct of public attribution seen as mainly motivated by geopolitical considerations. As non-alignment is a rudimentary consideration for ASEAN's foreign policy, countries in the region prefer to refrain from positioning themselves on divisive issues. While it is an element in the region's calculus that it should avoid antagonising China which is a key economic partner for the region in cyberspace (more so than the West), it would be misinformed to interpret this as deference to China.

The findings of this report has several ramifications for Europe's future role in the region on the issue of international cybersecurity cooperation.

First, regarding Europe as a security actor in the region: while 'the West' in general is a preferred security partner in the region, European countries and the EU are relatively new to cooperating with the region, compared with the US and its allies such as the Five Eyes Alliance or Japan. ASEAN states generally welcome an increased European presence on non-traditional security issues,[94] including cybersecurity, as it is becoming a major new source of capacity-building. In the wider strategic sense, ASEAN states are particularly keen on enhanced collaboration with Europe to bolster their neutrality and counterbalance the superpowers.[95] In this context, Europe must emphasise that the 'might is right' principle is not the world Europe or Southeast Asia want to live in, accompanied by actions that show its genuine support for a rule-based order. On the other hand, there is a prevailing sentiment that Europe must recalibrate its approach to be more in tune with ASEAN's priorities, in order to enhance their partnership.[96] At least among some countries in the region, there seems to be a shared (neo)colonialist perception of European countries and the EU: essentially, that Europeans 'preach, rather than partner',[97] with normative discourses on various issues including human rights, democracy, and climate change. This inevitably creates a barrier for meaningful cooperation, considering how an enhanced role of the EU in the region might be seen as external interference in ASEAN's political systems.[98] The major ASEAN democracies do not view the EU as providing sufficient economic or security benefits, which leads them to feel that the EU has not earned the right to influence/lecture them on a number of issues (i.e. sustainability).[99] Europe should also be mindful that its foreign policy towards different areas in the world is interconnected, and foreign-policy in one geographical area will likely have 'spill-over' effects on its relations with others. One interlocutor mentioned during the interview conducted for this study that 'the West's position on Gaza damages trust in the

[94] Anonymous interlocutor #4 (24 September 2024), Personal Communication

[95] Djalal, D. (2023), 'A Larger Role from the EU in Southeast Asia: A Perspective from ASEAN', *Sasakawa Peace Foundation USA*, pp. 1–11.

[96] Lee-Makiyama, H. and Wong, J. (2023) *EU-ASEAN: Shared Objectives, Severed Trust*. Policy Brief No. 08/2023. ECIPE.

[97] Anonymous interlocutor #1 (24 September 2024), Personal Communication.

[98] Carnegie Europe et al. (2023), Reimagining EU-ASEAN Relations: Challenges and Opportunities. Carnegie, p.44;

[99] Lee-Makiyama, H. and Wong, J. (2023), *EU-ASEAN: Shared Objectives, Severed Trust*. Policy Brief No. 08/2023. ECIPE.

region', and that 'the crisis in the Middle East influences how some countries in the region view external great powers'.[100] China's role in the Middle East, for example its mediation between Saudi Arabia and Iran, mediation between Palestinian factions, is being appreciated in the region.[101] This is at least most likely true for ASEAN member states with a Muslim majority, such as Malaysia and Indonesia.

Second, regarding practical cooperation on cybersecurity, all interlocutors indicated that countries in the region would welcome an increased European role in capacity-building, in addition to the region's traditional partners - the US's core allies and Japan.[102] Desire for more capacity-building with respect to cybersecurity is a rare instance of consensus in the region. It is in Europe's long-term interest to invest in cyber capacity-building in the region, as the training of the region's cybersecurity practitioner will contribute to the region's cyber-threat perceptions and to a greater alignment in approaches to tackling cybersecurity. In practice, said one interlocutor, Europe should do so in close coordination with its allies to ensure that these activities complement, rather than compete with each other.[103] Besides 'technical' cybersecurity, and with the precondition of sufficiently appreciating the issue's political sensitivity, Europe should also expand its engagement with the region on the issue of tackling misinformation and disinformation. Although there are good points to be made about how cyberspace ought to be open and free with a limited role for states regarding the social interactions taking place therein, insisting that 'information' is not 'cybersecurity' would be an argument that is difficult to relate to for those who are not socialised in the discourse above, especially as the issues of disinformation and FIMI is also gaining traction in Europe. It is important to note that the EU has started dialogues with ASEAN on the issue of misinformation and disinformation.[104] However, it is important to consider the political sensitivity of regulating 'information' and to carefully choose the form of engagement.

[100] Anonymous interlocutors #2 (23 July 2024), Personal Communication.

[101] Yaacob, A. R. (2024). Asian countries: pro-US or pro-China? Studio Asia.

[102] Gomez, M. A. (23 July 2024), Personal Communication.

[103] Domingo, D. (6 September, 2024), Personal Communication.

[104] Delegation of the European Union to the Association of Southeast Asian Nations (ASEAN), (29 January 2024). AICHR-EU Dialogue on Disinformation and Misinformation. Available at: https://www.eeas.europa.eu/delegations/association-southeast-asian-nations-asean/aichr-eu-dialogue-disinformation-and-misinformation_en?s=47.

ASEAN's own regional cooperation on information security could provide an inspiration, where states limit their cooperation to information sharing while refraining from capacity-building.[105]

Third, on China's role in the region's digital economy, it is important to point out that ASEAN's economic-developmental logic of cybersecurity entails that China will remain a prioritised partner for the region. Concerns on over-reliance in the region are emerging, but is for the moment unlikely to incentivise ASEAN to pivot away from cooperation with China in the area of digital infrastructure and economic cooperation for the sake of diversification. To a certain extent, the region's reliance on China may also be due to the fact that alternative digital goods and services offered by the EU, or the US for that matter, are insufficiently competitive. In the long run, the key lies in European industries becoming more active and economically competitive in the region. Governmental efforts based on normative or security arguments, unsubstantiated by economic substance, will otherwise remain largely ineffective.

Fourth, regarding cyber attribution, a change in the region's cautiousness in public cyber attribution is unlikely in the near future. Pursuing collective attribution against China with countries in the region affected by territorial disputes would be counter-productive, so the focus should instead be on providing cyber-capacity-building to the region. At the same time, a significant recent development that seems to be lacking in the discussion in the region so far is an apparent shift in Chinese policy on public attribution: in late 2023 China started to conduct its own official public cyber attribution, in this case against the US.[106] It might be informative for researchers and policy-makers to acknowledge that public cyber attribution is no longer a purely Western phenomenon.

Fifth, this report highlights that the region is highly diverse, and western researchers and policy-makers should refrain from reading the region's approaches to cybersecurity from a regional rather than national angle. Geopolitically, as the Dutch Indo-Pacific strategy correctly points out, 'most of the countries in the region seek to prevent the Indo-Pacific region

[105] Anonymous interlocutor #1 (23 September 2024).

[106] CVERC. (5 September, 2022), Investigation Report on Northwestern Polytechnical University Cyber Attack by NSA (Part 1) [西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）]. Retrieved from: https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm

from becoming a pawn of one of the great powers or spoils in the conflict between them.'[107] This conclusion might be true for ASEAN aggregately, where the geopolitical outlooks of countries in the region are much more complex: Singapore is of course in a privileged position to pursue neutrality, the Philippines enjoys a closer security relation with the US than other ASEAN countries, while Laos and Cambodia are largely dependent on China for historical and geoeconomic reasons. Factors of domestic politics – regime type and the focus on law enforcement agencies – also play a role in how countries approach issues including diversification and threat perceptions in cyberspace. European policy-makers should also not overlook the importance of bilateral ties with individual ASEAN members on specific issues where priorities are more aligned than with ASEAN as a group; yet they should do so with sufficient respect for ASEAN Centrality, which emphasises ASEAN as the core of the region's diplomacy with external powers.

Lastly, the diversity in the region means that this study should be read as a preliminary study on the variable approaches to cybersecurity in the region, and future research should be conducted in an extensively country-specific manner.

[107] Government of the Netherlands (2020), 'Indo-Pacific: Guidelines for strengthening Dutch and EU cooperation with partners in Asia'. Government of the Netherlands. p.1.