ISSN 2278-3091
Volume 8, No.1.4, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1781.42019.pdf
https://doi.org/10.30534/ijatcse/2019/1781.42019

# CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries

**Nor Shazwina Mohamed Mizan[1], Muhamad Yusnorizam Ma'arif[2], Nurhizam Safie Mohd Satar[3], Siti Mariam Shahar[4]**

**Research Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia**
[1]p95641@siswa.ukm.edu.my
[2]p89058@siswa.ukm.edu.my
[3]nurhizam@ukm.edu.my
[4]p89063@siswa.ukm.edu.my

## ABSTRACT

This research will provide an overview of the predominant cybersecurity issues in ASEAN countries, current measures adopted by ASEAN countries in tackling cyber security issues and identify challenges that are being faced by ASEAN countries. However, in recent years, cybersecurity has become a critical problem globally, which led ASEAN to step up and take action to address the cybersecurity problem with a sense of urgency. Despite awareness of the importance of a resilient cybersecurity procedure across the region, previous research discovered that measures of protection and other efforts to counter cyber-related incidents amount to a regional and national level. The main objective of this research is to study and analyse previous research that has been conducted by ASEAN members. This research presents an exhaustive review of previous study on cybersecurity issues by using a numerical method. Although the ASEAN region has substantial economic growth, there is limited research on cybersecurity in certain countries of ASEAN. Presently, the fourth industrial revolution (IR 4.0) has advanced technological transformation worldwide. This research aims to support one of the nine pillars of industry 4.0 on the list, namely, cybersecurity. As ASEAN grows in the field of digital connectivity, however, victims of cyber-attacks are bound to rise across the globe. This study has found that generally, studies on cybersecurity focuses on several themes, such as defense against innovative cyber-attacks (DCA), strategies against cybersecurity threats (SCS), government policies and protection against privacy (GPP), protection of computer infrastructures in the government (PCG), and legal and ethical issues on cyberspace (LEC). On top of that, this research highlights the major cyber-attacks faced by certain ASEAN countries as a guide to improve the existing systems. Finally, the results presented can facilitate improvements to be made in cybersecurity implementation in ASEAN countries for future research.

**Key words:** ASEAN, Challenges, Cybersecurity, Issue

## 1. INTRODUCTION

The transformation of the nation towards modernization is rapidly become an Industrial Revolution (IR4.0) this indicated that cybersecurity has become the research subject of choice due to the accelerated growth in digital technology in the modern country globally. The abbreviation for ASEAN is Association of South East Asian Nations. The beginning ASEAN was formed by 5 countries in August 8, 1967 which is Indonesia, Malaysia, Philippines, Singapore, and Thailand in 1967. Brunei Darussalam joined in 1984, and Cambodia, Lao People's Democratic Republic, Myanmar, and Viet Nam joined between 1995 and 1999 which led to total ten member countries, mainly to foster regional peace and security [5]. Thanat Khoman, the former Thai foreign minister and one of founding fathers behind the establishment of ASEAN agreed that the aim was to foster cooperation on various aspects that are educational, cultural, economic and social, technological and others. Furthermore, the purpose was to promote regional stability and peace through the practice of honor and adhering with the laws established and also follow the principles of the United Nations Charter [3]. Information and Communications Technologies (ICT) are now part and parcel of daily life. Everything is at the tip of our fingers with the existence of the internet. This can be proven by the rapid growth in the transformation in digital technology [13]. ICT has become an essential function in business and governments due to the convenience it provides. With the help of advanced computers and the internet, governments are now able to deliver immediate services to their citizens with a higher efficiency level.

ASEAN is well known as the regional expert in economics because of the abundance of resources, raw materials and industries between state members to contribute to the production of the ASEAN economy. The strategic location of Asia is a factor in the economic growth especially in countries such as Singapore, Malaysia Brunei, Indonesia and Philippines, known as ASEAN6. Moreover, there is rapid growth in the market, estimated to be 600 million people as of now. The aforementioned growth as well as the ability to

acquire various natural resources and biodiversity results in a wide range of capabilities to produce for various fields including agriculture, manufacturing, services and exports. Strong Foreign Direct Investment (FDI) with excellent production network, free-trade area progressive investment regime recorded strong regional collaborative achievements [3]. In this case, ASEAN is predicted to become the fourth largest economic by 2030 and is followed by United States (US) next China and the European Union (EU). Singaporean Prime Minister, Lee Hsien Loong, affirmed that fact in his speech at the opening ceremony at 50th ASEAN Economic Ministers Meeting.

In the future, ASEAN might be the main hub for many investors to perform trades such as banking, transportation, e-commerce, telecommunication and shipping as a mode of transport of material and production to further increase the prospects for continuous growth. Daily communication has currently spread over various mediums and channels. The development of decentralised data has impacted civilisation positively. Without any monitoring, government data including classified information can be stolen due to cybercrime [16]. This can be a threat to countries that become the target of terrorist attacks or wars through cyberattacks. Since the beginning of the technological era in IR 4.0, awareness about security when using the internet has already been informed and discussed to reinforce the knowledge from time to time. To achieve this objective, significant work is needed to solve the problem of digital integration across the ASEAN region [34].

## 2. PROBLEM STATEMENT

Until now, regional efforts to adopt a comprehensive cybersecurity strategy have been slow and fragmented. To explore rapid technology and dynamism of industrial revolution 4.0 (4IR) a research via an experimental investigation had to be conducted, which has made it difficult for governments to embrace the acceleration of the 4IR [21]. Modifications in business, education, e-commerce, manufacturing and healthcare are to be unified to a more modern system within the organisational structure or corporation. This may require extensive effort [20] [21]. The issue is that innovation requires a big investment. This has led to the on channelling focus finances to a more profitable sector for the near future without the knowledge that cybersecurity can provide profit on a long-term basis due to rapid growth in cyberspace. Previous studies primarily focusing on certain subjects in cyber security that can be seen in the findings. With the hope of this study could improve direction of security in the future development. Therefore, problem statement for this research is to examine the measures to enhance the current existing system that is being implemented by ASEAN countries. In addition, the study covers the reasons that certain ASEAN countries do not produce enough research in cybersecurity within the country, which have been tied to the increase of cybercrime, scams and threats that can harm the safety to the citizens and disrupt the execution processes by the government. Moreover,
articles on the challenges and issue within the scope of ASEAN countries need to be delved into.

## 3. LITERATURE REVIEW

There have been several studies in the literature that report about cybersecurity in ASEAN countries. These studies mainly focused on cybersecurity issues and challenges, as previously mentioned. Various initiatives have been undertaken to address such issues, such as the Implementation of the Information and Communications Technology Strategic Planning implemented in Malaysia. In July 2011, the Malaysia Administrative Modernization and Management Planning Unit (MAMPU) published on "Public Sector ICT Strategic Plan 2011-2015" and in March 2016, the "Public Sector ICT Strategic Plan 2016-2020". Recognising its importance, MAMPU issued a document entitled, "Public Sector ICT Strategic Plan 2003-2008" in August 2003. It contained the direction and guidelines for the development of Information and Communication Technology Strategic Planning, especially in public sector [29]. There is a huge volume of published studies describe which countries have done the related research, as further explained in the next paragraph.

Based on the report by The Henry M. Jackson School of International Studies at University of Washington, Malaysia lost approximately US$ 900 million to cyber criminals between 2007 until 2012, with an average of 30 user being the victim to cybercrimes daily. It crucial to be aware to these figures will keep rising annually. Moreover, 70 percent of crimes in that country fall under the category of cybercrimes. In Indonesia, cybercrimes costed to governments with US$ 2.7 billion annually. As of 2013, Singapore had the highest per capita losses to cybercrime at US$ 1,158.

There are recent critical cyber-related incidents in ASEAN countries within January 2017 to May 2019. In July 2018, Singapore suffered its worst ever cyberattacks. Hackers broke into SingHealth's IT systems to steal the data of 1.5 million patients and records of the outpatient medication as stated by Prime Minister Lee Hsien Loong in a published article by TODAY. Next, according to the Asia Pacific Risk Centre, the personal data of 850 individuals was stolen from the online database portal of Singapore’s Defense Ministry in 2017. As of October 2018, a total of 45 incidents of ransomware had been reported targeting various sectors in Malaysia, which affected quite a number of servers and computers within the organisations. During Malaysia’s intense data breach episode, there were more than 46 million mobile subscribers’ data reported to be stolen and leaked to the web. In turn, Malaysians may be vulnerable to social engineering attracts and at worst, phones may be cloned as reported by TheStar in October 2017.

The Brunei Computer Emergency response team (BruCert) recorded 2,143 an attacks on cybersecurity in Brunei last year, of which 38 percent was caused by malicious software published by Borneo Bulletin on November 2018. On the Thai website, Toyota Motor Corporation has been the victim of a series of data breaches issued. Thailand was targeted by a cyberattack and some of its customers' data may have been potentially accessed. But the worst attack came in March 2019, when personal information belonging to 3.1 million clients was exposed as a result of a data breach in its sales offices in Japan. The key takeaway of these problems is that the Malaysian government needs to set up a control to reduce cyber-attack activities and increase the success rate of defense to a level that matches other countries [16].

According to Abdul Manap [1], in the digital era, identity can be embedded in mere information that is widely accessible, rather than in "flesh". Criminals will resort to new forms of cyberspace identity theft. This creates further exposure for individuals and a real challenge for law enforcement officials and legislators. The criminal falsely claims to be the victim when apprehended by the police for a crime. [37] had previously reviewed the Intrusion Detection System, which could play an important role in curbing and stopping the misuse that happened in network by irresponsible entities, such as malicious users. The system has two methods for detecting network abuse, namely anomaly-based detection, and signature.

A systematic approach of cybersecurity implementation has to be developed in ASEAN countries in order to compete with first world countries. According to Salamzada [27], some previous works have used a qualitative approach, including conducting an interview to develop a cybersecurity framework or provide suggestions for the improvement of the existing cybersecurity framework. For instance, for VPN technology, data integrity is ensured to always be protected when the user is controlling or transferring the data by connecting another computer using VPN platform. Network architecture provided to recover's site with authentication through VPN technologies. Data integrity is one of the security techniques that can detects if other data been modify during transmission [36].

## 4. METHODOLOGY

This research uses a review paper approach, which is an effective method of conducting a literature review [4]. According to Mark Staples, a systematic review is a technique that can determine, assess and analyse. This involves an overview of literature using online databases, using the keywords based on publication within six years. This research investigates and analyses the cybersecurity issue and challenges, which are related to ASEAN from the years of 2014 until 2019. This helped to identify which countries are actively involved in research on their own cybersecurity safety and was the frequent source of cybersecurity research [28]. Searching techniques to find the relevant online database was executed using keywords such as "cybersecurity AND ASEAN", "cyber-attack", "threat", "issues cyber" and "challenges in ASEAN" to retrieve the result. Relevant information was extract from the retrieved articles and the ensuing discussion centres provided an answer to the research questions [38].

This research involves data from the local universities as secondary data to provide further evidence. To visualise the bigger picture, the data that was gathered from online material resources such as journals, articles, conference proceedings, and book chapters were combined and analysed. From this analysis, the process tracing method will be used whereby data gathered was interpreted using a two-approach method, namely chronologically and thematically. The collection of research has been done from the years of 2014 to 2019.

| **Research Theme Description** | | **Indicator:** |
|---|---|---|
| A | Defense against innovative cyber attacks | DCA |
| B | Strategies against cybersecurity threats | SCS |
| C | Government policies and protection against privacy | GPP |
| D | Protection of computer infrastructures in the government | PCG |
| E | Legal and ethical issues on cyberspace | LEC |

| **Journal/Article Source Country (SC)** | **Indicator:** |
|---|---|
| Singapore | SG |
| Malaysia | MA |
| Brunei Darussalam | BD |
| Indonesia | IN |
| Philippines | PH |
| Thailand | TH |
| Cambodia | CB |
| Myanmar | MY |
| Vietnam | VT |
| Laos | LO |

## 5. FINDINGS

The authors identify 27 journals, articles as well as proceeding papers and highlights the issues and challenges of cybersecurity in ASEAN countries in Table 1 of the collection of data using the specified research theme.

The findings are as displayed in Table 1. All 27 journals/articles and conference proceedings were collected from the Mendeley database, Google Scholar and other databases of journals within the research topic in cybersecurity. Table 1 presents the journals downloaded from the open source database and proprietary journals. The table also simplifies the research theme by an indicator as explained in that table (DCA, SCS, GPP, PCG, and LEC).

**Table 1:** Collection of Data Using Research Theme

| No | Authors | R | SC | Year | Research Theme Indicator | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | A | B | C | D | E |
| 1 | Lowell A. Quisumbing | 15 | PH | 2017 | | ✓ | | | |
| 2 | Candice Tran Dai | 16 | VT | 2015 | | | | ✓ | |
| 3 | Nazura Abdul Manap<br>Anita Abdul Rahim<br>Hossein Taji | 9 | MA | 2015 | | | | ✓ | |
| 4 | Chooi Shi Teoh<br>Ahmad Kamil Mahmood<br>Suhazimah Dzazali | 17 | MA | 2018 | | ✓ | | | |
| 5 | Hashim<br>Mohd Shamir Masrek<br>Mohamad Noorman Yunos Zahri | 18 | MA | 2016 | | | ✓ | | |
| 6 | M.S Razana<br>W. Shafiuddin | 40 | MA | 2016 | | | | ✓ | |
| 7 | Zahri Yunos<br>Rabiah Ahmad<br>Nor Amalina<br>Mohd Sabri | 19 | MA | 2015 | ✓ | | | | |
| 8 | Lean Ping Ong<br>Chien Fatt Chong | 20 | MA | 2014 | | ✓ | | | |
| 9 | Ganesan A/L Supayah<br>Jamaludin Ibrahim | 21 | MA | 2017 | | | | | ✓ |
| 10 | Maslina Daud<br>Rajah Rasiah<br>Mary George<br>David Asirvatham<br>Govindamal Thangiah | 35 | MA | 2018 | | ✓ | | | |
| 11 | Nazli Ismail Nawang | 39 | MA | 2014 | | | | | ✓ |
| 12 | Harry Hung | 22 | SG | 2016 | ✓ | | | | |
| 13 | Ching Yuen Luk | 42 | SG | 2019 | | | | ✓ | |
| 14 | Aufar Muhammad Rizki | 23 | SG | 2018 | | ✓ | | | |
| 15 | Elina Noor | 24 | SG | 2014 | | | | ✓ | |
| 16 | Elina Noor | 41 | SG | 2015 | | | | ✓ | |
| 17 | Goryan Ella Vladimirovna | 25 | BD | 2018 | | | | | \<br>✓ |
| 18 | Sahidan Abdulmana Burhan Saleh | 26 | TH | 2015 | | ✓ | | | |
| 19 | Adam ghazi Tehrani | 27 | TH | 2015 | | | ✓ | | |
| 20 | Ineu Rahmawati | 28 | IN | 2019 | | | | ✓ | |
| 21 | Elsa Faradilla Anak Agung Banyu Perwita | 29 | IN | 2017 | | | | ✓ | |
| 22 | Muhamad Rizal Yanyan M.Yani | 30 | IN | 2017 | | | ✓ | | |
| 23 | Tin Maung Maung Mie Mie Su Thwin | 31 | MY | 2017 | | | | | ✓ |
| 24 | Tin Maung Maung Mie Mie Su Thwin | 32 | MY | 2017 | ✓ | | | | |
| 25 | Lars Gjesvik Niels Nagelhus Schia | 33 | MY | 2018 | | ✓ | | | |
| 26 | Rainer Einzenberger | 43 | MY | 2016 | | ✓ | | | |
| 27 | Aryo C.K Wardana Rodon Pedrason Triyoga Budi Prasetyo | 34 | MY | 2018 | ✓ | | | | |
| 28 | - | - | CA | | | | | | |
| 29 | - | - | LO | | | | | | |

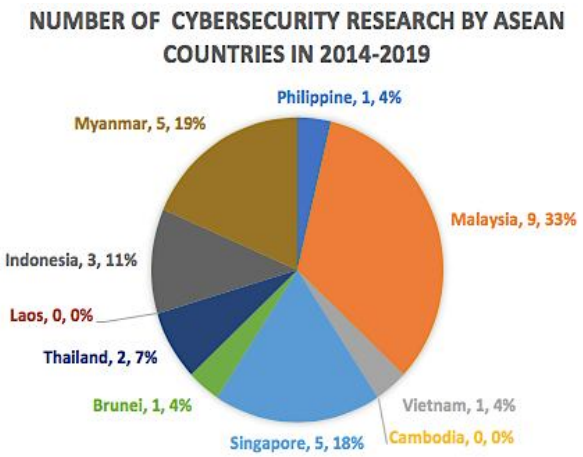


**Figure 1:** Number of Published Cybersecurity Research by ASEAN Countries in 2014-2019

The observation approach of cybersecurity in ASEAN countries can be reviewed by the number of researches done in Figure 1. The findings show that a few countries of ASEAN are not aware of the importance of combating cybercrime in cyberspace in their own countries, such as Cambodia and Laos. From the data in Figure 1, we can see that no research has been carried out from 2014 until 2019 in both countries on cybersecurity issues. However, in terms of the policy, Malaysia, Singapore, and Myanmar have implemented a Notice and Takedown procedure on the forms of legislation and policy. It is illustrated in Figure 1 that there are nine researches completed in Malaysia as well as five in both Singapore and Myanmar between the year 2014 and 2019. Other countries like the Philippines, Vietnam, Brunei, Thailand, and Indonesia have started researching the challenges and issues faced in the field of cybersecurity.

According to Sunkpho, only Indonesia does not have specific cybersecurity law, but they rely on electronic information and the transaction act. On the issue of data protection, countries like Thailand and Indonesia have been given the exception to have general data protection law in place. Thailand and Indonesia do not have a unified law regarding privacy, instead, it is implemented through different laws and decrees. However, both Thailand and Indonesia are in the process of drafting a new general data protection law. Vietnam is the only country that has a comprehensive law that deals with both security and data protection in one single law, namely the Law of Cyber-Information Security (LCIS). One interesting point to note is that Malaysia only applies the Personal Data Protection Act to commercial transactions, excluding data processed by the government [30]. The results of the present study also shed light on the areas of cybersecurity, including Defense against innovative cyber-attacks (DCA), Strategies against cybersecurity threats (SCS), Government policies and protection against privacy (GPP), Protection of computer infrastructures in the government (PCG), and Legal and ethical issues on cyberspace (LEC) as shown in Figure 2.

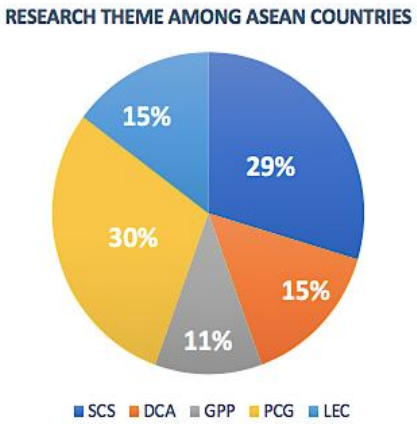


**Figure 2:** Research Theme among ASEAN Countries

Figure 2 illustrates that PCG and SCS are popular research themes among ASEAN countries. Both of them are gathered to have been conducted with eight kinds of research. LEC and DCA are ranked second, with four kinds of research conducted in both research themes. It is apparent from the figure that very few kinds of research on GPP were conducted among ASEAN countries, which is only three researches throughout 2014 to 2019.

## 6. CONCLUSION

This paper presented the results of cybersecurity research done in ASEAN countries in 2014 to 2019. This study has concluded that to overcome the obstacle in cybersecurity, ASEAN requires full cooperation from all its members. These issues and challenges cannot be properly handled and manages independently by individual countries. Therefore, ASEAN needs to seize opportunities and improve cooperation in its persistent effort to reach the goal of cyber-stability for the region. This study has found that generally, research on cybersecurity focuses only on some themes, thus, it needs to be expanded to a wider scope to include a private sector protection policy and protection infrastructure for the public community.

The collection of an evidence from this study shows that research into the field of cybersecurity needs to be improved, given the challenge is great and issues arising out of cyber threats continue to increase. The finding from this study offer a few contributions to current literature. Firstly, this study can be used as a source of literature for the study from 2014 until early 2019 among ASEAN member countries. Secondly, further research could focus on two countries, namely Cambodia and Laos, who have yet to publish any indexed journals. Further investigation and experimentation into cybersecurity issues and challenges are highly recommended. A number of possible future studies using the same experimental set up are apparent. It would be interesting to assess the effects of cybersecurity issues on business and organisational performance in ASEAN or other countries.

**ACKNOWLEDGMENT**

This paper is fully supported by the Institute of Malaysia and International Studies (IKMAS), Universiti Kebangsaaan Malaysia (UKM) through the Projek Arus Perdana 2017 Grant for the title "Enhancing Connectivity Towards ASEAN Integration: A multifaceted Approach" project under the code AP-2017-003/1. Thank you to everyone who contributed his or her ideas and comments in order to complete this paper. Many thanks and gratitude to my supervisor, Dr. Nurhizam Safie Mohd Satar, who has encouraged the writing of this article. I would like to express my greatest appreciation to Dr. Andrew Kam Jia Yi, who is the head of the fund for projects that have created the opportunity to conduct this study.

**REFERENCES**

1. S. Chia. **The ASEAN Economic Community: Progress, Challenges, and Prospects**. 2013. https://doi.org/10.2139/ssrn.2346058
2. L. Haddon. ***Information and Communication Technologies in Everyday Life***. vol. 18, no. 2. Berg, 2004.
3. P. Jayabalan, R. Ibrahim, and A. A. Manaf. **Understanding Cybercrime in Malaysia: An Overview.** *Sains Humanika*, vol. 2, no. 2, 2014.
4. **ASEAN: Conception and Evolution**. in *The 3rd ASEAN Reader*, ISEAS–Yusof Ishak Institute Singapore, 2018, pp. xiii–xviii.
5. E. B. a B. W. World. **Cybersecurity for Industry 4.0 Cybersecurity implications for government, industry and homeland security**. in *Cybersecurity implications for government, industry and homeland security*, 2018.
6. S. A. Omar, F. Hasbolah, and U. M. Zainudin. **The Diffusion of Artificial Intelligence in Governance of Public Listed Companies in Malaysia**. *Int. J. Business, Econ. Law*, vol. 14, no. 2, pp. 1–9, 2017.
7. S. A. Omar and F. Hasbolah. **Awareness and Perception of Accounting Students towards Industrial Revolution 4.0**. in *Proceedings of the 5th International Conference on Accounting Studies (ICAS 2018) 16-17 October 2018, Penang, Malaysia*, 2018.
8. K. Salamzada, Z. Shukur, and M. Abu Bakar. **A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan**. *Asia-Pacific J. Inf. Technol. Multimed.*, 2016. https://doi.org/10.17576/apjitm-2015-0401-01
9. N. Abdul Manap, A. Abdul Rahim, and H. Taji. **Cyberspace Identity Theft: The Conceptual Framework**. *Mediterr. J. Soc. Sci.*, vol. 6, no. 4, pp. 595–605, 2015. https://doi.org/10.5901/mjss.2015.v6n4s3p595
10. Malaysian Administrative Modernisation and Management Planning Unit. **The Malaysian Public Sector ICT Strategic Plan**. *Malaysian Public Sect. ICT Strateg. Plan 2016-2020*, no. August, p. 23, 2016.
11. S. Suhaiza and M. Y. Zawiyah. **Public sector ict strategic planning: framework of monitoring and evaluating process**. *Asia-Pacific J. Inf. Technol. Multimed.*, vol. 6, no. 1, pp. 85–99, 2017.
12. A. Bryman. ***Social research methods Bryman***. 2012.
13. M. Staples and M. Niazi. **Experiences using systematic review guidelines**. *J. Syst. Softw.*, 2007. https://doi.org/10.1016/j.jss.2006.09.046
14. J. Sunkpho, S. Ramjan, and C. Ottamakorn. **Cybersecurity Policy in ASEAN Countries**. *Inf. Inst. Conf.*, no. March, 2018.
15. L. A. Quisumbing. **Global Perspectives on Cyber security Using Latent Dirichlet Allocation Algorithm**. *Int. J. Appl. Eng. Res.*, vol. 12, no. 20, pp. 10310–10323, 2017.
16. C. T. Dai. **Cybersecurity in Vietnam: Formulation and implementation of a new strategy @ La cybersécurité au VIêt Nam: Formulation et mise en œuvre d'une nouvelle stratégie**. *Herodote*, no. 157, pp. 126–140, 2015. https://doi.org/10.3917/her.157.0126
17. C. S. Teoh, A. Kamil Mahmood, and S. Dzazali. **Cyber Security Challenges in Organisations: A Case Study in Malaysia.** *2018 4th Int. Conf. Comput. Inf. Sci. Revolutionising Digit. Landsc. Sustain. Smart Soc. ICCOINS 2018 - Proc.*, pp. 1–6, 2018.
18. M. S. Hashim, M. N. Masrek, and Z. Yunos. **Elements in the cyber security framework for protecting the Critical Information Infrastructure against cyber threats**. *Inf.*, 2016.
19. Z. Yunos, R. Ahmad, and N. A. Mohd Sabri. **A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia** *Inf. Secur. J.*, vol. 24, no. 1–3, pp. 15–23, 2015. https://doi.org/10.1080/19393555.2014.998844
20. L. Ong and C. Chong. **Information Security Awareness: An Application of Psychological Factors A Study in Malaysia**. 2014.
21. G. Supayah and J. Ibrahim. **An Overview of Cyber Security in Malaysia**. *Kuwait Chapter Arab. J. Bus. Manag. Rev.*, vol. 6, no. 4, pp. 12–20, 2017. https://doi.org/10.12816/0036698
22. H. Hung. **Confronting Cybersecurity Challenges through US- Singapore Partnership**. 2016.
23. A. M. Rizki. **Langkah Singapura Dalam Meningkatkan Kesadaran Negara Anggota Asean Untuk Meningkatan Keamanan Siber**. *Pros. Senas POLHI ke-1 Tahun 2018*, 2018.
24. Elina and Noor. **Securing ASEAN ' s Cyber Domain : Need for Partnership in Strategic Cybersecurity**. *S . Rajaratnam Sch. Int. Stud. Singapore*, no. 236, pp. 01–03, 2014.
25. E. V. Gorian. **Singapore's leadership on cybersecurity in ASEAN: intermediate results and future prospects.** *Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса*, 2018.
26. S. Abdulmana and B. Saleh. **Coordinate negative content filtering and threat detection in Thailand on the Internet infrastructure**. *5th Int. Conf. Inf. Commun. Technol. Muslim World*, pp. 6–10, 2015. https://doi.org/10.1109/ICT4M.2014.7020647
27. A. Ghazi-tehrani. T**he Current State of Cybercrime in Thailand : Legal , Technological , and Economic**

**Barriers to Effective Law Enforcement**. *J. Thai Justice Syst. Spec. Ed.*, vol. 1, no. February, pp. 1–28, 2015.
28. I. Rahmawati. **The Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense.** *J. Pertahanan Bela Negara*, 2019.
29. E. Faradilla, A. Agung, and B. Perwita. I**ndonesia Cyber Security Development : The Analysis Of Infrastructure , Regulation And Institutional Building ( 2007-2015 )**. vol. 02, no. 01, pp. 1–5, 2017.
30. M. Rizal and Y. Yani. **Cybersecurity Policy and Its Implementation in Indonesia.** *J. ASEAN Stud.*, 2017.
31. T. M. Maung and M. M. S. Thwin. **Proposed Effective Solution for Cybercrime Investigation in Myanmar.** *Int. J. Eng. Sci.*, vol. 06, no. 01, pp. 01–07, 2017. https://doi.org/10.9790/1813-0601030107
32. T. M. Maung and M. M. S. Thwin. **Proposed Applicable CCFIM Framework for Cybercrime Forensics Investigation in Myanmar**. *15th Int. Conf. Comput. Appl.*, 2017.
33. L. Gjesvik, N. N. Schia, N. W. Paper, and L. Gjesvik. ***Managing a digital revolution Cyber Security Capacity Building in Myanmar***. Norway: Published by the Norwegian Institute of International Affairs, 2018.
34. A. C. K. Wardana, R. Pedrason, T. B. Prasetyo, and U. Pertahanan. **Implementasi digital forensik brunei darussalam dalam membangun keamanan siber implementation of digital forensic brunei darussalam in building cyber security.** vol. 4, pp. 1–22, 2018.
35. M. Daud, M. George, and D. Asirvatham. **Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations?**. *Int. J. Bus. Soc.*, vol. 19, no. 1, pp. 161–180, 2018.
36. Kargar, A. Sistani, R. & Patel. A. M. **Design and Evaluation of a Virtual Private Network Architecture for Collaborating Specialist Users.** 5(1): 15–30. 2016.
37. Kadis, M. R. & Abdullah, A. **Global and Local Clustering Soft Assignment for Intrusion Detection System: A Comparative Study.** Vol 6, No 1. 2017.
38. R, N. H. Abd, Suraya Hamid, L. M. Kiah, S. Shamshirband and S. Furnell. **A Systematic Review of Approaches to Assessing Cybersecurity Awareness.** Kybernetes 44(4):606–22. 2015. https://doi.org/10.1108/K-12-2014-0283
39. N. N Ismail. **Greater freedom in the cyberspace? An analysis of the regulatory regime of the internet in Malaysia.** *South East Asia J. Contemp. Business, Econ. Law*, vol. 5, no. 4, pp. 40–44, 2014.
40. W. S. M.S Razana. **Cybersecurity: Towards Becoming A National Certification Body For Information Security Management Systems Internal Auditors**. *Int. Sch. Sci. Res. Innov. 10(8) 2016*, vol. 10, no. 8, pp. 2907–2910, 2016.
41. Noor E. **Strategic governance of cyber security: implications for East Asia**. *Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance, Tokyo: Japan Center for International Exchange*. 2015.
42. L. C. Yuen. **Strengthening Cybersecurity in Singapore: Challenges, Responses, and the Way Forward.** In Security Frameworks in Contemporary Electronic Government, pp. 96-128. IGI Global, 2019. https://doi.org/10.4018/978-1-5225-5984-9.ch005
43. Einzenberger, R. **" If It's on the Internet It Must Be Right": An Interview With Myanmar ICT for Development Organisation on the Use of the Internet and Social Media in Myanmar**. Austrian *Journal of South-East Asian Studies*, 9(2), pp.301-310. 2016.