Journal of Human Security | 2022 | Volume 18 | Issue 1 | Pages 49-53
DOI: 10.12924/johs2022.18010034
ISSN: 1835-3800

Journal of Human Security

Research Article

Cyber criminology and human security: An Analysis of ASEAN Countries Police's Paradigm

Mohammad Fadil Imran

Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia.
Email: mfadilimran@stik-ptik.ac.id
ORCID ID: https://orcid.org/0009-0007-3980-5518

Submitted: 17 July 2021 |In revised form: 3 July 2022 | Accepted: 8 July 2022 | Published: 8 December 2022

Abstract: The paper aimed to analyse the major issues and effects of cybercrime in the ASEAN region based on different jurisdictional settings just as the advanced strategies being exhibited from authorities worldwide in order to control cybercrimes and build cybersecurity systems. The members of ASEAN have developed multidisciplinary crime models which are used to counter cyber-threats and build cyber-resilience models. The models include, criminalisation of cybercrime at a national level, developing and implementing a strategic and coordinated national plan, partnerships between private businesses, universities and international organisations. The main difficulties that ASEAN region's police forces, in their attempt to fight against cybercrime, come across include legal and regulatory complexities, technological and resource restraints, and unequal digital environments. These problems limit the capacity of the police authorities to provide effective cybercrime combating and keep people's security. Suggestions for ASEAN countries generated by the study results include providing legal protection, building capacity of the national cybersecurity, advocating for global cooperation, popularizing cybersecurity awareness, and use of cybercrime prevention measures.

Keywords: Cybercrime, criminalization, ASEAN, crime.

1. Introduction

The recent decades have witnessed a very dramatic development in the technology sphere, which in its turn has profoundly changed the human life in many directions including communication, commerce and entertainment. In this regard, it has become difficult to separate human life from technology [1]. Nevertheless, there are not only benefits which come with the evolution of technologies, but also the forthcoming new issues, such as the risk of cyberattacks and law enforcement [2]. As cyber-infrastructures becoming more common and connected into daily lives, cyber-crimes unfold, becoming a global threat, responsible for the compromising of both individual and government security [3]. For the ASEAN that comprises of ten-member Union where together we have a socio-economic infrastructure engendered in the diverse socio-technological development background, cybercrimes must be addressed in order for security of mankind in the region.

Cybercrime is prevailing persistently by attacking human life including mature humans or even children. In this regard, cybercrime is considered as the fastest growing area [4]. These offences usually result in violations to digital systems and networks by utilizing their weaknesses with the goal of various reasons such as making profit, furthering political aims, destruction of vital infrastructure, etc. Cybercrimes disregard any existing order, functioning without the limitations imposed by physical terrain or boundaries inside national borders, making them really difficult to investigate and prosecute [5]. Consequently, ASEAN law enforcement agencies face multifaceted challenges in cybersecurity protection together with cybercrime deterrence functions that are primarily concerned with the safety and peace for their citizens [6, 7].

In the light of growing cybercrimes pact among ASEAN countries the paradigm of policing paradigm of have evolved to be able to combat against these sophisticated cybercrimes. The traditional law enforcement methods are not sufficient enough to manage the complexity of the cyber-attacks which in turn, calls for a multifactorial type of approach that includes tech expertise and legal guidelines. This is because, the traditional forensic methods that are utilized to investigate the cyber-crimes are not effective [2]. Human security has become prominent in the discussion of cyber security and law enforcement [8]. It is an idea that a person is protected against different dangers, which also includes the ones that appear due to the use of cyberspace.

This paper intends to investigate the paradigm under which law enforcement agencies of ASEAN countries are performing their cybercrime endeavours from the perspective of cyber criminology and human security. The main aim of this study is the structure through which law enforcement agencies of ASEAN countries fight cybercrime. This is done from the perspectives of criminology and human security. Its purpose is to offer the best solutions to enhance the cybersecurity measures. The purpose of the investigation is to examine the existing strategies of regional law enforcement agencies in ASEAN area as well as their efficiency in providing security of people in cyberspace and suggest the better means of crisis reduction during emergency cyber events. Following are the objectives of the

librello

study:

- Analyze the existing strategies and mechanisms of law enforcement agencies' operating in ASEAN countries for the detection of cybercrimes, particularly from the point of view of cyber criminology, and human security.
- Examine the primary issues and the ASEAN region cybercrimes implications, including their effect on an individual and state level human security.
- Research the best practices and exceptional strategies carried out by police authorities around the globe to reduce cybercrimes and build the cybersecurity systems.
- Provide the stakeholders with recommendations and strategies in order to promote comprehensiveness and coordination among the countries in the ASEAN countries when it comes to the response to cybercrimes, while prioritizing the safety and security of human beings in the cyber space.

2. Literature Review

Besides, Cybercrimes goes even deeper into valid issues of human security. They could be individual, corporate and a whole society, depending on the situation [9]. On the individual level, crimes linked to cyber activities are seen to involve victims' identity theft, cyberbullying, and online harassment, which have catastrophic effects on their emotional and psychological well-being [10, 11]. Cybercrime activities break down individuals' confidence on digital devices and subsequently it minimizes the private space of individuals on the internet [12]. Cybercrime capitalizes on digital systems and network imperfections to compromise both human security and security of society round multiple tasks [13]. At the personal level, there might be problems like not-updated cyber-security habits, overlooking online risks, and love for the insecure technologies. This can lead to the rise of cyber-crimes. Furthermore, personal information, which could be social security numbers, financial records, and medical data, plays crucial role in cyber criminals' hunt for chances for cybercrime, scam, and abuse. A community may also be exposed to cyber security risks such as the disruption of vital resources such as payment systems, challenges to institutions, and social instability. Cyber risks can compromise the security, stability and long-term viability of an organization by compromising informational and confidentiality of structural capital, along with its availability and integrity [14]. According to Ghanem, Ghaleb (15), the staggering development of cyber threats have propelled the experts, professionals and specialists within the field of security concerning the development of more dependable system of protection. It also involves the mechanisms of intrusion detection systems (IDS). These mechanisms are equipped for fostering the accurately detected threats resulting in effective outcomes. Cybercrimes that target constituting for communities, kids, elderly people, and minority groups can moment common inequalities in communities as well as social discordance. The nature of crime has experienced an immense metamorphosis given the advancement of the digital age with global law enforcement agencies face new problems and approaches [16]. In the present of the ASEAN context, an area comprising ten of the various economies with uneven levels of economic development and technological infrastructure, the emergence of cybercrimes poses a major infringement of human security. Cybercriminals perpetrating all kinds of digital machinations like online scams and identity theft, cyber espionage and terrorism, capitalize on the weaknesses at the networking and system level, showing a disregard to boundaries and jurisdiction [17]. So, the countries in ASEAN will have more and more complicated cyber challenges and the guarantee of the security and interest of their people in essence should be their main target. Alsharif, Mishra (18) highlighted that the cybersecurity and human vulnerabilities are strongly associated with each other. Their research indicated that a lack of awareness of the three important vulnerabilities associated with the human factors in cybersecurity involves passwords, online hacks, attacks and social engineering. These are the major problems that needs to be addressed and reduced through proper awareness and training. Tarai (19) also revealed that human security means looking at security in a broader way. It considers things like human rights, help people in developing and dealing with issues. Therefore, it can be observed that these issues are inter-connected that needs to be addressed after careful identification. At present, ASEAN countries face cybercrimes from different viewpoints, when those are associated with a danger to individuals, economic stability and the welfare of society in general. However, the research by indicated that ASEAN countries play an important role in the maintenance of cybersecurity through the international security approach [20].

The legislation and regulation concerning cybercrimes in ASEAN member states are characterized by complexities as well as inequalities, the factors that hinder the law enforcers' work efficiency. Each state under membership has their own legislation pertaining to the cyber sector and its own framework of law and regulation, which leads to disparities and jurisdictional delimitation. Furthermore, cyber incidents typically cross national boundaries and the cooperation and coordination among several jurisdictions is required to hunt down the preparatory [21]. Among the main obstacles is the absence of the correspondence between the laws on cybercrimes from one country in the ASEAN region to another. On the one hand, certain countries may have detailed laws pertaining to various types of cyber offences with the reason being that they are up-to-date, while on the other, countries that have outdated or incomplete legislation encounter problems in enforcing cybercrime laws because of the absence of general laws pertaining to the cyber space [22]. Moreover, the fast pace of technological evolution has been the case, in which, the rate at which the technologies are developed have been faster than it takes to make a legal framework around them thus leading to the emergence of gaps in addressing these new cyber threats. The existing laws may not be adequate to target crimes like online harassment, cyber bullying, and piracy, among others [10]. The small geographic size allows for the crimes to be perpetrated from different continents, making it complex for the authoritative bodies to get into the investigation and prosecution. Additionally, the application of anonymizing technologies for instance VPNs or encryption methods bolsters the cause when it comes to tracing and identifying cyber offenses [23]. According to Rais and Songkarn (24), the increased prevalence of cybercrime have become a threat to stability, therefore it is hard for the government to balance the crimes. Regulation and rules on the utilization of this space have to be addressed equally by the member ASEAN states, regional organizations as well as international partners. Initiatives about legal harmonization of cybercrimes, joint cooperation mechanisms, and law enforcement forces development is obligatory in order to effectively counteract the cybercrimes and to provide human safety in the ASEAN region.

In addition, the emergence of digital divide in ASEAN states as a consequence enhances differences in competency level and in access to digital utilities [25]. Some countries could struggle in the field of digital security because of their poor cyber infrastructure and limited knowledge. Moreover, the internationality inherent in the cyber-crimes also requires cooperation and information sharing among police organs on different regions and beyond. To meet the changing crisis of cybercrimes, ASEAN has established legislation and policy response through which the security forces of the region are strengthened to deal with cyber threats and maintain human security [26]. One of the key measures by the ASEAN members is to develop all-encompassing cybercrime laws that penalises and thus keeps people away from cybercrime.

3. Method

Adopting an explorative and descriptive research methodology,

this paper attempts to unravel the paradigm of ASEAN police forces in confronting cybercrimes from the views of cyber criminology and human security basis. Qualitative approach gives the ability to find the intricacies of the cybercrimes affecting ASEAN region, as well as the strategies and effects. Meanwhile, the descriptive analysis is helpful in bringing an overview of the entire subject being discussed. A qualitative angle of the security threats can be used for thorough exploration into the intricate aspects of cyber threats and the repercussions for human security, while a descriptive point of view can be used for all-in-one understanding of the subject matter. While conducting the research, the researcher has conducted a thorough search, reading, reviewing and documentation of relevant literature, articles and statutory instruments published in the year 2022 till date. Systematic investigations of academic and scientific databases, government reports, and legal frameworks on cyber criminology, human security, and legislation charges in ASEAN countries are conducted to read and join the key themes, trends, and perspectives. The section of literature review incorporates different types of sources such as journal articles, book chapters, conference proceedings and official reports, in order to make it practical and the topic clearer. On the other hand, this study emphasizes the real case studies, the reports and the empirical studies to complement its observation of use by the police in the ASEAN countries in compliance to the cybercrimes and to the protection of human security. In general, using a qualitative and descriptive method network of expertise from cyber criminology, human security studies, and legal frameworks is enabled in this study to give a distinctive analysis of the paradigm of ASEAN countries' police forces in reflecting cybercrimes.

4. Results

4.1 Policing Paradigms Employed by ASEAN Countries

With a rising danger of cybercrimes perceived, all ASEAN nations chose to implement multi-dimensional policing models which are aimed at countering cyber threats and building cyber-resilience [20]. An essential part of such frameworks are laws and relevant polices adopted in view of the growing scale of cybercrimes. With laws governing this, the entire framework includes comprehensive cybercrime legislation that outlaws a variety of cyber offences, which include hacking, malware distribution, online fraud, and identity theft. By making legal and enforceable regulations countries of ASEAN can create a legal basis for research, bringing cyber criminals to justice, and that is the main step to create a culture of responsibility in cyberspace [22].

Furthermore, ASEAN countries depend on their national cybersecurity strategic and coordinated action plans in order to provide guidelines for the promotion of cybersecurity governance, capacity building, public awareness, and the establishment of international cooperation [20]. These policies detail the objectives, priorities and the initiatives which are intended to help in strengthening the cybersecurity resiliency, promotion on collaboration among stakeholders and mitigation of the cyber risks so as to protect the human security within the region. To begin with, the nations that make up ASEAN have also done a lot through the use of technological resources and capacity building to grow in the area of cybercrime prosecution [20]. These endeavors will include the setting up of multi-jurisdictional laboratories integrated and capable of using the most advanced tools and techniques in the world for digital evidences analysis and digital crime research [27]. Furthermore, law enforcement officers are expected to additionally take part in the specialized training programs that focus on enhancing the expertise of the officers in the cybercrime ASEAN nations form partnerships with private companies, universities, and international organizations to take advantage of technological skills and assets and to adopt the most successful approaches on the cyberattack problems [28]. Partnerships with the information technology organizations, cybersecurity teams, and learning centers enable the welfare countries as a group to obtain the most advanced technologies, threat intelligence and training to develop the cybersecurity forces to manage the cyber threats.

4.2 Challenges Faced by ASEAN Police Forces

Legal and regulatory complexities turn out to be imposing obstacles in the way of ASEAN police authorities to bring about a satisfactory solution to the issue of cybercrime. A perpetrator of cybercrime can create an impact across the globe, making it complicated to use the current jurisdiction and to punish the criminals who commit across borders. The absence of a uniform law provides for cybercrime across ASEAN countries is another factor negatively affecting law enforcement and prosecution to fight transnational cybercrime [29]. Another part of challenge the ASEAN nation police with cybercrime also includes technological and resource restraints. Lack of funding, useless infrastructure, and insufficient number of such skilled professionals impede the ability to improve cybersecurity measures, to develop the digital forensic capabilities, and to be fully equipped with advanced weapons in the fight against cyber threats [29]. SMEs are greatly prone to get the attacks of cybercrime because of limited financial resources and competencies of cyber security [30, 31]. Apart from that, unequal digital environment between ASEAN countries represents inequality in digital capacity and access to digital resources that hinders the resolution of cyberspace-related problems [32]. Fast pace of tech world makes it essential for police forces in ASEAN to make recurrent investments in new technologies and experts; this is putting ASEAN police forces in the position where they can never get up to speed.

The acute jurisdictional questions and the cross-border collusion put forward daunting obstacles for the ASEAN policemen in going through the process of cybercrimes detection and prosecution. Dual and multi-jurisdictional nature of cyber-crimes excludes the possibility for one country alone to investigate or prosecute such crimes, especially when they involve several countries and/or jurisdictions. Issues with data privacy, sovereignty, and national security that crack open doors to unsubstantiated sharing of intelligence and sensitive information on cybercrime can bring down this initiative [33]. Because of the latter, ASEAN police forces are directly confronting the problems of having solid proof, procurement of the warrants, and extradition of criminals in cross-border cybercrime cases, hence making the fight against cybercrime at the regional level difficult.

4.3 Strategies to tackle Cybercrime

To meet with the increasing threats of cybercrime, the ASEAN countries have designed and applied a spectrum of prevention strategies to counter cybercrime and cyber security maintenance in the region [34]. These tactics involve the preventative campaigns on cybercrimes and awareness crusade, the bettering of the investigation capacities and the forensics professionals in digital domains, and collaboration with private sector stakeholders and the international community. In this vein, cybercrime prevention and awareness campaigns have a significant role in the coverage of the impact of cybercrimes through the education of individuals, enterprises, and community at large on the potential threats and the far-reaching effects of the crimes. Awareness of cybercrimes and cybersecurity is also important in this regard [35].

Campaigns are raising cyber hygiene issues including using strong passwords, keeping software up-to-date, and being cautious of phishing messages and links, which not only raise awareness but also make individuals feel empowered in their online experiences and protect them from cyber threats. Enhanced focus on relevant communes aimed at the specific groups, for example, children, old

people, and SMEs, will help combat the susceptibilities and gradually reduce the damages from cybercrimes in these communities. Elevating the agency's investigative competencies and digital forensics proficiency, among others, will be necessary to ensure the effective handling of cyber-incidents and arrest of cyber criminals, including the prosecution of such crimes [36]. ASEAN countries have spent tremendous resources on the institution of training programs and capacity building projects in the bid to improve the rank of law enforcement officers in their ability to detect and successfully investigate cybercrimes. Specialized technical and laboratory units fitted with up-to-date forensic capabilities including tools and techniques help this public body in the investigation of digital evidence, the tracking of cyber criminals, and the building of sufficiently solid cases for court [37]. Through the full utilization of digital investigation and forensic skills, ASEAN member countries will improve their cybersecurity and law enforcement readiness to protect people from cyber threats and punish cyber criminals.

5. Conclusion

The police paradigms that ASEAN countries form in order to effectively combat cybercrime involve a multi-dimensional and dynamic approach that allows the region to fight cyber threats, and at the same time, to enhance cybersecurity resilience. By bringing legal legislation and policy strategies into action, the ASEAN countries have done their best to make cyber frauds illegal, set up good practices of cybersecurity governance and also cooperate with other nations in fighting against cybercrime. Society, and even cyber criminals, are reaping the benefits of technological advancements, in addition to private efforts aiming at strengthening the capabilities of the law enforcement agencies in their work related to investigating cybercrimes, conducting digital forensics examinations, and responding effectively to the online threats.

The contribution with the private sector partners and international organizations helped spread the awareness about cyber threats, exchange the threat information and make joint initiatives on keeping assets and data secure within the ASEAN countries. ASEAN countries of all kinds need and to cope with the cybercrimes, be more resilient to the cybercrimes, and also to protect the human security in this digital world. Collective efforts and collaboration with other ASEAN countries can be the feasible way for a secure, safe and cyberspace for all stakeholders within the region.

6. Recommendations

Following suggestions are made to the ASEAN countries based on the study's findings:

6.1 Strengthen Legal Frameworks

ASEAN countries should collaborate on establishing a common cybercrime law and upgrading legislation standing to be able to deal with the cyber challenges of the modern time well.

6.2 Enhance Cybersecurity Capacity

The governments should put an emphasis on developing the cybersecurity capacity and should be involved in the provision of training programmes, workshops and exercises for the relevant people including the law enforcement staff members and other stakeholders.

6.3 Promote International Cooperation

The ASEAN member-states is required to boost the existing collaboration platforms and relationships among the region and the international spheres to develop a more resilient common system to address cyber threats.

6.4 Increase Awareness and Education

It would be much better to make cybersecurity awareness and education the focal point of all initiatives of this kind as people, businesses, and even communities will be self-empowered if much effort will be devoted to making security awareness part of people life.

6.5 Implement Cybercrime Prevention Measures

According to ASEAN nations proactive measures against cybercrimes should be implemented, which include cybersecurity strategies development, creation of cyber incident response teams and sponsoring cybersecurity standards and guidelines for organizations.

7. Implications

The scope of the outcomes of the research involves both pragmatic and theoretical importance with regard to cyber criminology and the measures to uphold human security level within ASEAN block. Empirically, the findings coming from a study on the cybercrime landscape, crime governance paradigms, problems faced and the strategies used by ASEAN countries make for a powerful guide for the policymakers, the law enforcement agencies and other stakeholders, all of whom may draft effective policies to battle the cyber threats and safeguard human security. Additionally, the identification of issues like legal obstacles, technical constraints, and capacity variations suggests focusing on tailored measures and measures for capacity development to ensure resilience from cyberattacks in ASEAN countries. Similarly, some other recommendations of filling out legal frameworks, creating public-private partnership, and promoting international cooperation will provide a base for the development of improved cybercrime prevention and reaction effectiveness in the area. Academically, this study may add up a little knowledge in cyber criminology and human security principles that are relevant to the ASEAN nations. In addition, acknowledging the associated challenges and suggestions yields the next-level theories in a way of the factors shaping the efficiency of cybercrime prevention and response mechanisms, which will open the way for further the field of cyber criminology research and development. Briefly, this study has economic and theoretical implications suggest that cyber assault is a priority that should be part of the strategies for human insecurity and adaptability in the digital era. ASEAN region and beyond.

8. Limitations and Future Research

Despite the fact that the conducted research is worthwhile as it provides the detailed information about the policing paradigms and strategies and cybercrimes and institutionalization human security, it still has some limitations which are discussed in the rest of the paper. First, studies are concentrated on ASEAN states which may limit the nationwide effect of the finding in regions with different social, political statues, and cyber-security environment. Furthermore, the use of secondary data sources is inevitable as the data is being collected from primarily secondary sources such as literature reviews and policy documents; which may introduce biases or gaps in the analysis.

The fact that cyber threats change at an unmatched speed with no signs of slowing down in technology may cause part of the investigations to grow out of relevant, and hence inappropriate, at some point. This research could serve as a groundwork to expand the frontiers of cyber criminology and human security in the ASEAN region. Future studies might inspect diverse possibilities to increase

the perception of cyber criminology and human security issues within the ASEAN region. For the first, studies that focused on effective policing aspect and cybercrime intervention would be very useful in finding out successful practice areas for improvement. Thus, compared tests between ASEAN countries and other geographical areas will highlight the difference in policing philosophies, legislation, and cyber security basis. Moreover, emphasizing on long-term research for continuous monitoring of cybercrime escalation, recognition of the new digital landscape and its impact on human security requires the establishment of a culture for deeper comprehension on cyber threats and resilience.

References

[1] Kodongan EMT, Pandie RDY. Technological Developments in the Perspective of Christianity. IJRAEL: International Journal of Religion Education and Law. 2022;1(1):38-45.

[2] Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR, Singh S. A review on cyber crimes on the Internet of Things. Deep Learning for Security and Privacy Preservation in IoT. 2022:83-98.

[3] Saliu HA, Ayodeji GI, Dode R, Oni M, Muhammed H, Sanubi F, et al. Thematic Edition. Studies in Politics and Society. 2022;10(1).

[4] Tuli B, Kumar S, Gautam N. An overview on cyber crime and cyber security. Asian Journal of Engineering and Applied Technology. 2022;11(1):36-45.

[5] Sekati PNM. Assessing the effectiveness of extradition and the enforcement of extra-territorial jurisdiction in addressing trans-national cybercrimes. 2022.

[6] Yoo IT. Cybersecurity Crisscrossing International Development Cooperation: Unraveling the Cyber Capacity Building of East Asian Middle Powers Amid Rising Great Power Conflicts. Korea Observer. 2022;53(3).

[7] Govella K. Governance Challenges in the Maritime, Outer Space, and Cyber Domains and Opportunities for US-Japan Leadership. Governing the Global Commons: Challenges and Opportunities for US-Japan Cooperation, edited by Kristi Govella, The German Marshall Fund of the United States, Policy Paper. 2022.

[8] Triplett WJ. Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy. 2022;2(3):573-86.

[9] Ghazi-Tehrani AK, Pontell HN. Phishing evolves: Analyzing the enduring cybercrime. The New Technology of Financial Crime: Routledge; 2022. p. 35-61.

[10] Okocha DO. Online social networks misuse, cyber-crimes and counter-mechanisms in Nigeria. University of Nigeria Interdisciplinary Journal of Communication Studies. 2022;28(1):62-74.

[11] Gopalakrishnan T, Ravichandran K, Ilango S. Curve Fitting Model Analysis of Cyber Crimes, Cyber Bullying and Online Sexual Exploitation in India. resmilitaris. 2022;12(6):691-701.

[12] Ibrahim H. A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. Wasit Journal of Computer and Mathematics Science. 2022;1(3):76-108.

[13] Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences. 2022.

[14] Ghelani D. Cyber security, cyber threats, implications and future perspectives: A Review. Authorea Preprints. 2022.

[15] Ghanem WAH, Ghaleb SAA, Jantan A, Nasser AB, Saleh SAM, Ngah A, et al. Cyber intrusion detection system based on a multiobjective binary bat algorithm for feature selection and enhanced bat algorithm for parameter optimization in neural networks. IEEE Access. 2022;10:76318-39.

[16] Simoni FL. Police intelligence innovation and transnational organized crime in cyberspace: A South American challenge. 2022.

[17] Spicer J. Is there a link between organised crime and terrorism in the context of shifting power structures in Eurasia? The Russian Case: Macquarie University; 2022.

[18] Alsharif M, Mishra S, AlShehri M. Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science & Engineering. 2022;40(3).

[19] Tarai S. Approaches to human security. IJAR. 2022;8(2):86-90.

[20] Estiyovionita K, Sitamala A. ASEAN's ROLE IN CYBERSECURITY MAINTENANCE AND SECURITY STRATEGY THROUGH AN INTERNATIONAL SECURITY APPROACH. Lampung Journal of International Law. 2022;4(2):81-90.

[21] Blair DC, Roth WB. Cyber Crime and Geostrategic Clash Over the Internet. The Cyber Defense Review. 2022;7(2):15-34.

[22] Tan EE, Ang B. ASEAN Ambiguity on International Law and Norms for Cyberspace. Baltic Yearbook of International Law Online. 2022;20(1):133-62.

[23] Proulx K. Anonymity Online and the Perfect Environment for Cybercrime: Utica University; 2022.

[24] Rais MA, Songkarn P. Hacker and the Treat for National Security: Challenges in Law Enforcement. Indonesian Journal of Counter Terrorism and National Security. 2022;1(1):45-66.

[25] Curtis H, Hogeveen B, Kang J, Le Thu H, Rajagopalan RP, Ray T. Digital Southeast Asia. 2022.

[26] Kaburuan ED, Damayanti A. The Effectiveness of Indonesian National Police Strategy in Cybercrime Eradication through ASEAN Ministerial Meeting on Transnational Crime (AMMTC). International Journal of Social Science And Human Research. 2022;5(8):3649-61.

[27] Casino F, Dasaklis TK, Spathoulas GP, Anagnostopoulos M, Ghosal A, Borocz I, et al. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access. 2022;10:25464-93.

[28] AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo K-KR. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security. 2022;119:102754.

[29] Mishra A, Alzoubi YI, Anwar MJ, Gill AQ. Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security. 2022;120:102820.

[30] Rawindaran N, Jayal A, Prakash E. Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime. Computers. 2022;11(12):174.

[31] Chidukwani A, Zander S, Koutsakis P. A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access. 2022;10:85701-19.

[32] Tran LQT, Nguyen MT. Digital Economy: A Comparative Study in ASEAN. Theory, Methodology, Practice-Review of Business and Management. 2022;18(02):83-92.

[33] Kumar S. CYBER CRIME VIS-A-VIS DATA PRIVACY: DOCTRINAL INVESTIGATION. Galaxy International Interdisciplinary Research Journal. 2022;10(2):167-76.

[34] Yau J. The wild, wild web: explaining variation in ASEAN member-state cyber policy: University of British Columbia; 2022.

[35] Mankotia S, Sharma S. Awareness of Young Internet Users Towards Cyber Security And Cyber Crimes.

[36] Khan AA, Shaikh AA, Laghari AA, Dootio MA, Rind MM, Awan SA. Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. International Journal of Electronic Security and Digital Forensics. 2022;14(2):124-50.

[37] Javed AR, Ahmed W, Alazab M, Jalil Z, Kifayat K, Gadekallu TR. A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. IEEE Access. 2022;10:11065-89.