International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 08 August 2022

DOI: 10.47191/ijsshr/v5-i8-42, Impact factor- 5.871

Page No: 3649-3661

The Effectiveness of Indonesian National Police Strategy in Cybercrime Eradication through ASEAN Ministerial Meeting on Transnational Crime (AMMTC)

Elsafani Daniela Kaburuan[1], Angel Damayanti[2]

[1,2]Universitas Kristen Indonesia

ABSTRACT: Cybercrime has increased along with digital growth in Indonesia in the last decade. There has been a heightened urgency among Indonesian government agencies to eradicate cybercrime. These efforts include a national cybersecurity strategy and taking part in regional cooperation, such as AMMTC. This paper examines the effectiveness of the Indonesian National Police (INP)'s strategy in AMMTC to combat the nation's cybercrime. By looking at the Global Cybersecurity Index (GCI), this article elaborates on whether the INP's approach effectively counters cybercrime in Indonesia. This study utilizes transnational crime, cybercrime, cooperative security, and regional organization concepts. It conducts a qualitative research method with a case study approach as a derivative and an analysis descriptive research type. With primary data in the form of interviews with two sources and secondary data that took various related sources, the research conducts triangulation of data. This study shows that although Indonesia was slower in handling cybercrime cases, the effectiveness of INP's approach on a national and regional scale is starting to look up.

KEYWORDS: Cybercrime, Cybersecurity, Indonesian National Police (INP), ASEAN, AMMTC.

1. INTRODUCTION

Indonesia has a poor history of cyber-security. This is evident from the increasing number of cyber-attack vulnerabilities to cyber incidents that repeatedly occur in businesses and government institutions. The most well-known cybercrime case was probably the Telkomsel website complaining about expensive internet in April 2017. The attack, classified as a hacktivist, allegedly came from the famous hacker group "Anonymous." The Telkomsel page turned into a complaint from the perpetrators about the high price of their data package. The name Telkomsel also changed to Telkomnyet. Even so, the Telkomsel web defacement case did not leave any severe damage. After being hacked, Telkomsel immediately mitigated the problem and apologized to their customers for the operator's negligence (Shantika 2017).

One of the most extreme cybercrime cases has happened to the former Indonesian president, Susilo Bambang Yudhoyono. This issue was first published in a report from The Guardian and ABC on 18 November 2013. The report contains leaked documents from whistleblower Edward Snowden, who wrote that Australian spy agencies had tapped the phone of former Indonesian President Susilo Bambang Yudhoyono (SBY), former deputy presidents Bodieono and Jusuf Kalla, as well as other former senior ministers. In August 2009, Australia's Defense Signals Directorate (DSD) monitored SBY by telephone for five days. The Snowden document also notes that Australia was suspected of snooping on a list of recorded calls by SBY (Patnistik 2013).

In dealing with cybercrime, the Indonesian government has established a cyber security strategy that can be viewed through the Global Cybersecurity Index (GCI). GCI is a metric for measuring Indonesia's commitment as a member country of the International Telecommunication Union (ITU) for its cyber security. This index covers five aspects: legal, organizational structure, international cooperation, capacity building, technical, and procedural (ITU 2020).

Besides, international cooperation allows the formation of various national cyber handling bodies to cooperate with foreign countries (Islami 2017), such as the Indonesia Computer Emergency Response Team (ID-CERT); and the Indonesia Security Incident Response Team on the Internet Infrastructure (ID-SIRTII). There are also formal and non-formal organizations that deal with cyber issues (Arianto and Anggraini 2019), namely the Information and Communication Technology (ICT) Council; Computer Security Incident Response Team (CSIRT); and Indonesia Telecommunication User Group (IDTUG). In capacity building, various programs and guidelines are aimed at educating government agencies about the cyber world and how to protect it. There is also the Indonesian National Standard (SNI), which oversees the Information Security Management System (SMKI), and the Information Security Index, which evaluates information security readiness in government agencies based on ISO/IEC.

By Law No. 2 of 2002, the Indonesian National Police or POLRI is obliged to maintain national security from various threats. Article 2 covers the functions of the POLRI: one of the functions of the State government is preserving public safety and order, law enforcement, protection, shelter, and public service. In addition, the main tasks of the POLRI, as stated in Article 13, also underline the POLRI's obligations to protect Indonesian security, including: (a) maintain public security and order, (b) enforce the law, and (c) provide protection, protection, and (d) service to the community.

From the POLRI side, efforts to deal with national cybercrimes lie in establishing the Directorate of Cyber Crimes (Dittipidsiber) on February 3, 2017, which was previously handled by the Cybercrime Unit Subdirectorate V of the Directorate of Special Economic Crimes (Dittipideksus). The Directorate of Cyber Crime (Dittipidsiber) is a work unit under the Criminal Investigation Unit of the Indonesian National Police and is tasked with enforcing the law against cybercrimes (Direktorat Tindak Pidana Siber Bareskrim Polri 2021).

In addition to the various national strategies that have been taken and determined, Indonesia also takes part in the AMMTC framework for ASEAN members to consult and discuss steps that need to be taken to solve transnational crimes. Indonesia sees AMMTC as a way to strengthen security cooperation and encourage other ASEAN countries to strengthen regulations against cybercrime. Cybercrimes must be handled on two sides, from within and outside the country. From within, the Indonesian government uses and improves existing legal instruments. From the external, Indonesia uses the AMMTC forum to maximize the implementation of existing work programs and update documents on the evolving strategy of the Southeast Asia region. Therefore, this article analyzes Indonesia's role in the AMMTC forum in dealing with cybercrime as measured by the Global Cybersecurity Index (GCI) index.

2. LITERATURE REVIEW

The article "Responding to Cybercrime: Current trends, by Rick Sarre, Laurie Yiu-Chung Lau, and Lennon Y.C. Chang examines how critical the impact of cybercrime is as a global issue that continues to grow. This study shows how criminal activity these days is much easier to do with a computer and causes significant damage. The limitless nature of the internet and the intuitive nature of cybercrime means that countries can be targeted from anywhere, making law enforcement challenging and, in some cases, nearly impossible. This article proposes that the best response to cybercrime is to educate those most vulnerable to become victims and deploy crime prevention tools more frequently. (Sarre, Lau, and Chang 2018)

Even though territorial jurisdiction is the most basic and generally accepted method of exercising jurisdiction, developing decentralized cyberspace changes this paradigm. The second literary discussion of Jean-Baptiste Maillart on "The Limits of Subjective Territorial Jurisdiction in The Context of Cybercrime" questions territorial dilemmas in the digital era. One of the reasons for the inadequacy of personal territorial jurisdiction in the context of cybercrime is its technical nature, precisely because of the technical difficulty in determining where the cybercrime occurred. This literature argument has vital implications, given that cyberspace essentially reduces the significance of the physical location. Traditional legal instruments to existing theories cannot keep up with technological developments and cybercrime. (Jean-Baptiste 2019)

Leo S.F. Lin and John Nomikos, in their article, "Cybercrime in East and Southeast Asia: The Case of Taiwan," follow economic booms in East and Southeast Asia as the internet has been used as a vehicle to commit transnational crimes. Criminals try to exploit the gaps between the legal and judicial systems among countries in the region. This paper examines the threat of cybercrime and uses Taiwan (whose official name is the Republic of China, R.O.C.) as a case study. Taiwan's underground world entered a new stage of development which caused organized crime groups to expand their organization to East and Southeast Asia. This phenomenon has become a regional security threat that requires cross-border cooperation and joint efforts. (Lin and Nomikos 2018)

Sharmaine Marmita, in "The struggle of ASEAN in Cyber Security," suggests a shortage of expertise, public education, and budget allocations for cybersecurity in the Southeast Asia region. This article is sufficient to elaborate on the struggles that are generally fought in cyber security among ASEAN member countries (Marmita 2020). Despite ASEAN's ongoing efforts to develop a solid cybersecurity strategy, progress has been hampered by political, safety, and financial threats, a lack of professionals in these areas, and a lack of understanding of cybersecurity in Southeast Asia. Regional policies of ASEAN member countries are also still limited due to non-intervention considerations regarding a country's right to self-determination. From ASEAN's perspective, inadequate cybersecurity is challenging to maintain. Yet, this article proves that POLRI has successfully deployed a progressive strategy to fight cybercrime in Indonesia.

In *Babak Baru Rejim Keamanan Siber Asia Tenggara Menyosong* ASEAN Connectivity 2025, Indah Novitasari found that under ASEAN Connectivity in 2025, Southeast Asian countries will be encouraged to prioritize information and communication technology connectivity leading to a better cybersecurity regime (Novitasari 2017). However, Novitasari does not consider the high heterogeneity in economic development, which is reflected in the various maturity levels of information and communication technology. ASEAN member countries face multiple challenges in equalizing their cyber capabilities, including limited human and financial resources to subsidize knowledge and communication technology infrastructure and underdeveloped cybersecurity awareness among the population.

3. METHODOLOGY

The complexity of cybercrime requires methodological considerations and research strategies that make qualitative perspectives very effective. The researchers use qualitative methods to unravel and understand the intricacies of cybercrime and its impact and solve this problem regionally and nationally. Qualitative research is also used to describe and analyze the pattern of reciprocal relationships between the Indonesian National Police and the AMMTC. Qualitative research helps researchers understand what to do when analyzing data and allows researchers to produce better, more weighty analyses. The research uses a qualitative method with the type of case study research, which is a derivative of a qualitative approach with a descriptive analysis type of research where the author tries to structurally explain the threat of cybercrime in Indonesia and analyze how the Indonesian National Police as a law enforcement agency handles this problem through AMMTC as an ASEAN regional forum and reviewing the effectiveness of Indonesia's and POLRI's measures through the Global Cybersecurity Index (GCI).

This study's primary data source was interview transcripts with related parties. The secondary data sources used are books, literature, articles, journals, reports, and official documents from the International Convention Section of the International Relations Division of the Indonesian National Police Headquarters by the research conducted. Data collection techniques that will be carried out are primary data with data collection techniques through interviews, and secondary data, namely documentation through library research and online research approaches.

4. CONCEPTS

A. Transnational Crime

As one of the large-scale criminal activities, transnational crime is well-known as a professional criminal group that threatens and disturbs the balance of harmony and public justice. At first, scholars and experts found it difficult to define "transnational crime" as "the terminology is very unstable and at least four terms overlap," including transnational crime, transnational organized crime, international organized crime, and transnational crime (Madsen 2009). However, when international crimes are not included in the problem, this issue becomes apparent, considering that international crimes are activities that threaten global security, such as genocide, war crimes, and crimes against humanity. The most suitable term to frame these issues is "transnational."

The term "transnational crime" was later coined by the Crime and Criminal Justice Branch of the United Nations (UN) in 1974 to identify certain criminal phenomena that transcend international boundaries (United Nations 1994). An Interpol official contributed to the initial informal definition of transnational crime (Bossard 1990), reducing transnational crimes to crimes "whose resolution necessitates the cooperation between two or more countries." United Nations Convention Against Transnational Organized Crime in 2000 defined organized crime, which is now the standard definition, as a structured group of three or more persons, existing for some time and acting in concert to commit one or more severe crimes or offenses established by the Convention, to obtain, directly or indirectly, a financial or other material benefits." (UNODC 2000)

B. Transnational Crime

Cyber law expert Susan Brenner (2012) writes, "cybercrime, like crime, consists of engaging in conduct that a society has outlawed because it threatens social order." Brenner (2004) summarizes several cybercrime laws explicitly developed to deal with cybercrime. These include hacking laws, malware laws, cyber snooping laws, and unauthorized access violations. D.S. Wall (2007) distinguishes cybercrimes including:

1): Computer integrity crimes: "Crimes against the machine,"

2): Computer-assisted crimes (including piracy): "Crimes using the machine,"

3): Computer content crimes (violence, pornography): "Crimes in the machine."

The legal background of cybercrime is fraught with conceptual ambiguity - not least because there are no specific cybercrime offenses in any jurisdiction (Wall 2001). By contrast, laws usually relate to various actions with little apparent coherence. This results in conceptual inconsistencies in how cybercrime is defined in different jurisdictions (Clough 2011) and a little clarity on how far computer/network 'involvement' in crime is needed to become a cybercrime, not just a crime. This definitional decision not only affects the legality/illegality of certain behaviors but has a series of other critical additional outcomes, for example, changes in crime rates, prison rates, police resources, and so on.

C. Cooperative Security

For many analysts involved in the policy process at the end of the Cold War, cooperative security opened up a new security paradigm that was recognized as being able to stand apart from collective defense and security and the notion of competitive security more generally. As Carter, Perry, and Steinbruner (1993) stated, "Cooperative security ... replaces the core of security planning from preparing to counter threats to preventing them from occurring". Michael Moodie (2000) defines cooperative security as "a process whereby countries with common interest work jointly through an agreed mechanism to reduce tensions and suspicion, resolve or mitigate disputes, build confidence, enhance economic development prospects, and maintain stability in their regions."

Indeed, parties involved in cooperative security are not only expected to stop identifying other countries as sources of threats but also to unleash collective capabilities and mechanisms against threats for peaceful purposes. While cooperative security is designed to provide a continuous communication channel even in a conflict, problem-solving is not usually seen as part of cooperative security. Cooperative security (Emmers 2003) "operates through dialogue and seeks to address the climate of international relations rather than specific problems." One of the defining characteristics of cooperative security is the emphasis on building trust and certainty; according to Ralf Emmers (2004), "Cooperative security arrangements aim to develop a "habit of dialogue" among participants and to promote trust-building and enable preventive diplomatic measures."

D. Regional Organization

The term "region" itself is a contentious concept. The basic understanding is that an area that is a grouping of territorial units in geographical proximity is an area that is spatially bound and side by side (Fawcett and Hurell 1995). However, the study of regionalism will undoubtedly touch on the elements of "region" that are often discussed. Apart from being meaningful as a geographical space, the term region also has a political dimension. Joseph Nye (1968) defines an international region as "several countries delimited by geographical relations and degrees of interdependence" and regionalism as "the formation of a grouping of states by region." It can be said that the two elements that characterize the phenomenon of regionalism behind the formation of regional organizations are geographical proximity, and solidarity based on common interests and shared values.

By their nature, regional organizations automatically assume the role of managing regional conflicts. This is not an entirely new phenomenon. Regional organizations are established with the primary objective of maintaining peace and resolving or containing matches to avoid escalating issues. Even in the late 1960s and early 1970s, regional organizations were considered the enabling peace-building blocks, and regions became "islands of peace" (Nye 1971). Before this period, the United Nations recognized the potential role of regional organizations for dispute resolution at the end of the Second World War.

Certain factors such as the intervention of major powers in regional conflicts and lack of competence in dealing with disputes became the main obstacles preventing some regional organizations from carrying out their functions effectively in managing conflicts, especially during the Cold War (Caballero-Anthony 2005). However, significant progress has been seen, demonstrating several regional organizations' success in their respective experiences. One of these organizations is ASEAN. In managing regional conflicts, it should be noted that ASEAN navigated crises cautiously, even during the Cold War.

E. Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI) is a reference that measures countries' commitment to cybersecurity at the global level to raise awareness of this issue's importance and different dimensions (ITU 2020). GCI was born out of a collaborative partnership between the private sector and international organizations to push cyber security issues to the forefront of the national agenda. As a joint project carried out by ABI Research and the International Telecommunication Union, GCI measures the cybersecurity involvement of global countries (ITU 2015). The GCI aims to provide an overview of the position of countries in their cybersecurity engagements at the national level. Since cybersecurity has a wide application field, the level of development or involvement of each country is assessed according to five pillars (ITU 2020), including:

1): Legal measures; are actions based on a legal framework that addresses cybersecurity and cybercrime.
2): Technical measures; are actions based on the existence of technical institutions and frameworks dealing with cybersecurity.
3): Organizational measures; are steps based on the existence of coordination institutions, policies, and strategies for developing cyber security at the national level.
4): Capacity development; measures based on research and development, education and training programs, and certified professional and public sector institutions that promote capacity building.
5): Cooperative measures; are measures based on the existence of partnerships, cooperation frameworks, and information exchange networks.

5. THE INDONESIAN CYBERSPACE CURRENT CONDITION

At the beginning of the COVID-19 pandemic, a survey by the Indonesian Internet Service Providers Association (APJII) in the 2019-Q2 2020 period noted that the number of internet users in Indonesia reached 196.7 million (APJII 2020). The Chairperson of APJII claimed that this increase was due to the increasing distribution of broadband due to the Indonesian government's online learning and work-from-home policies. This figure continues to increase to 202.6 million users, according to the Directorate General of Aptika from Kominfo (Agustini, 2021).

However, internet users' growth invites more cybercriminal groups' attacks. National Cyber and Code Agency or BSSN discovered 1.6 billion cyberattacks in 2021, an almost double increase compared to 495.3 million attacks in 2020 (Vitorio, 2022). The 2021 Cyber Security Monitoring Annual Report from BSSN also detected 1.6 billion traffic anomalies in Indonesia (BSSN 2016). Traffic anomalies are abnormal/unusual internet traffic patterns that infect computer network security. Indonesian police

confirmed that there had been an escalation in cybercrime reports in recent years. This can be seen from the data compiled by the Directorate of Cybercrime, POLRI which shows an increase in cybercrimes from 2016 to 2021.

Table 1. Cybercrimes in Indonesia 2016-2021

No	Year	Total		
		CT (*Crime Total*)	CC (*Crime Clearance*)	%
1	2016	3110	908	29,20%
2	2017	3109	1610	51,79%
3	2018	4360	2273	52,13%
4	2019	4586	2282	49,76%
5	2020	4790	1283	26,78%
6	2021	2842	1504	52,92%

Source: https://twitter.com/CCICPolri, 2022

The data above shows that the total cybercrimes in Indonesia increases to 64.93% and crime clearance (crime cases resolved when the perpetrator was arrested) increases to 70.77% from 2016 to 2020. However, in 2021 the figure decreases to 59.33% for total offense and an increase of 117.23% for crime clearance. It means that efforts to tackle cybercrime during the 2016-2020 period lack of suppress the rise in crime rates. However, in 2021 POLRI brought positive changes to the handling of cybercrimes in the country. Over the past two years, Dttipidsiber and Divhubinter prevailed in handling and preventing cybercrime. Further, the Indonesian government hope that various Cyber Patrol results (Priambodo 2022) and regional cooperation (Sumarno 2022) are to tackle existing crimes and build a qualified protection from the threat of cybercrimes.

Like a magnet attracting various cyber incidents, Indonesia continues to experience successive cybercrime attacks. A member of Commission I of the Indonesian House of Representatives from the PKS faction, Sukamta, expressed his concern about the condition of Indonesia's cybersecurity, which is already in the emergency category. Sukamta underlined the poor infrastructure of Indonesia's cybersecurity so that novice hackers can break into the websites of government institutions (DPR-RI, 2022).

Moreover, cyber security experts from the Communication Information System Security Research Center (CISSRC), Pratama Persadha, assessed that Indonesia's cyber security had reached the red alert level (CNBC 2022). Cyberattacks often hit Indonesia in one month compared to other countries, which on average only experience it once a quarter. Persadha stated that policymakers are "still very new to cyber security and defense." In 2021 alone, Indonesia has seen its government institutions become victims of eight massive cyber incidents, with perpetrators from within and outside the country. The attacks vary, ranging from a data breach, the most common episode, web defacement and ransomware to cyber espionage.

6. POLRI'S EFFORTS IN HANDLING CYBER CRIME

To achieve safe conditions in the cyber world, POLRI formed a particular unit under the authority of the Directorate of Special Economic Crimes (Dittipideksus) by the Head of Indonesian Police Decree No. 53 and 54 of 2002, which was also known as the IT Unit. There was a change in the nomenclature in 2010, where the IT Unit was then changed to the Sub-Directorate of IT and Cyber Crime Dittipideksus Bareskrim POLRI (Irviana and Salomo 2021).

Based on the interview with AKBP Endo Priambodo from Dittipidsiber, this Directorate has two main tasks, investigation and prevention. Initially, the tasks carried out were only law enforcement tasks, namely law enforcement only as a last resort. Dittipidsiber did not have preventive and preemptive functions. However, these essential tasks are no longer sufficient to meet the demands of the times, so the task of prevention is also carried out.

In Dittipidsiber, there are three 3 Sub-Directorates (Subdit), with two Sub-Directors containing investigators (Priambodo 2022). Subdit 1 deals with digital analysis, and Subdit 2 deals with equipment technicalities. Specifically, for Sub-Directorate 3, it is a technical assistance kind of supporting unit, where the task is to maintain existing equipment. A sub-unit also handles domestic and foreign cooperation and social media. These units help the people investigated in Sections 1 and 2, especially with how Dittipidsiber started the investigation.

For Sub-Directorate 3, which handle social media, prevention also carried out by investigating vulnerable accounts. By this, Dittipidsiber can reduce or mitigate potential losses (Priambodo 2022). For example, a provocation in the social media space will result in social/horizontal conflict in the community or persecution. With such prevention task, Head of Dittipidsiber might recommend the Ministry of Communication and Information to take down or suspend the account and the distribution process will stop. There is also a press release that aims to inform the public to be vigilant and to provide an example to potential criminals of what punishments are imposed.

Dittipidsiber conducts cyber patrols, to search the things that might lead to cybercrimes and explore further through profiling and identifying whether the individual committed a cybercrime, as well as analyzing the evidence obtained (Priambodo 2022). If there are suspicious elements, Dittipidsiber will increase its status to an investigation, which can then be submitted to the prosecutor. Dittipidsiber also receives reports from the public as AKBP Endo confirmed that the most frequently found cases include hoaxes, hate speech, defamation, fraud, and online sales. That is why buying goods online should use official e-commerce as the payment process, guaranteeing receipt of goods. In addition, Dittipidsiber also cooperates with various agencies, at home and abroad, to facilitate coordination in investigating organized and transnational cybercrimes.

7. AMMTC: ITS ORIGIN AND PLAN OF ACTIONS

Southeast Asian countries have dealt with transnational crime, which includes not only terrorism but also illegal drugs, human trafficking, smuggling, money laundering, piracy, and, more recently, intellectual property theft and cybercrime. Following this fact, ASEAN ministers signed the ASEAN Declaration on Transnational Crime in 1997 and established the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) annually.

AMMTC assumes the role of the highest policy maker and coordinating body in ASEAN cooperation in transnational crime amid meetings, institutions, and other work programs, including the Senior Official Meeting on Transnational Crime (SOMTC) and the ASEAN Chiefs of National Police (ASEANAPOL) (ASEAN 1999). Since then, the AMMTC has gone through several evolutions, including the expansion to the "Plus Three" format, which was first held in 2004 and seen in other ASEAN meetings, including with ASEAN dialogue partners, such as Japan, South Korea, and China (ASEAN 2004). There are eight areas of transnational crime recognized by ASEAN: arms smuggling, terrorism, money laundering, sea piracy, people smuggling and trafficking in persons, international economic crime, cybercrime, drug trafficking, illicit trafficking of wildlife, and timber (ASEAN Cybercrime Operations Desk 2020).

The first AMMTC Plan of Action was issued in 1999 to fight transnational crime (ASEAN 1999). ASEAN's initial efforts in combating transnational crime focused on drug abuse and drug trafficking, which were prevalent at the time and affected ASEAN's growth and vitality. With globalization, technological advances, and greater mobility of people and resources across national borders, transnational crime is becoming increasingly widespread, diverse, and organized. The Southeast Asia region must be able to face many new forms of organized crime such as terrorism, drug abuse, and trafficking, innovative forms of money laundering, arms smuggling, trafficking in women and children, and piracy.

Recognizing the urgency to tackle transnational crime, the Philippines hosted the ASEAN Ministers of Interior/Home Affairs on Transnational Crime on 20 December 1997 in Manila (ASEAN 2017). The meeting resulted in the Minister's signing of the ASEAN Declaration on Transnational Crime. The document reflects ASEAN's determination to deal with transnational crime and its intention to cooperate with the international community in combating it. The declaration also forms the basic framework for regional cooperation in combating transnational crime. Therefore, the ASEAN Ministers Meeting on Transnational Crime (AMMTC) is held to coordinate the activities of relevant bodies such as the ASEAN Senior Officials on Drug Matters (ASOD) and the ASEAN Chiefs of National Police (ASEANAPOL). The Senior Officials Meeting on Transnational Crime (SOMTC) is held at least once a year to assist Ministers in completing their duties (ASEAN 2017).

The commitment to eradicating transnational crime within the AMMTC and SOMTC is focused on eight areas: counter-terrorism, drug trafficking, human trafficking; arms smuggling; sea piracy; money laundering; international economic crimes; and cybercrime. To date, under SOMTC, five Working Groups have been formed (ASEAN 2020), including:

1). Working Group on Counter Terrorism (WG on CT);
2). Working Group on Trafficking in Persons (WG on TIP);
3). Working Group on Cybercrime (WG on CC);
4). Working Group on Arms Smuggling (WG on AS);
5). Working Group on Illicit Trafficking of Wildlife and Timber (WG on ITWT).

Over time, AMMTC and SOMTC have developed strong ties. They have engaged positively with external ASEAN parties, notably the ASEAN Dialogue Partners, which eventually evolved into AMMTC/SOMTC Plus Dialogue Partner Consulting. In addition, various documents, including joint declarations and memorandums of understanding, have been discussed, signed, and adopted with ASEAN external parties as a collaborative effort to combat transnational crimes or specific areas of a global nature, such as terrorism and trafficking in persons. Furthermore, the ASEAN Plan of Action in Combating Transnational Crime (2016-2025) was formed to follow up on the 2015 Kuala Lumpur Declaration on Combating Transnational Crime mandate and contribute to the realization of the 2025 ASEAN APSC Blueprint (ASEAN 2017). The purpose of this action plan is to continue the close cooperation of ASEAN member countries to prevent and combat transnational crime and enhance ASEAN's capacity effectively.

Regarding the formation of the working group on cybercrime, the ASEAN Working Group on Cybercrime Terms of Reference (ASEAN 2014) mentioned that "The working group provides a platform for the ASEAN member states to collaborate on capacity building, training and sharing of information related to combating cybercrime." The working group in AMMTC has three main

activities: exchange of information, capacity building, and sharing best practices. The exchange of information allows ASEAN member countries to share their cyber cases with various trends and types of crime that continue to develop. Capacity building includes training, workshops, and multiple meetings aimed at increasing the capacity of ASEAN law enforcement officers. Sharing best practices is an exchange of information on the best practices that each country has carried out, then the threats/challenges that will be faced, and how to formulate all activities into a solid force in eradicating cybercrime.

The work program on cybercrime under the SOMTC was compiled in September 2013 at the 9th AMMTC Consultation (ASEAN 2013). ASEAN members and their Dialogue Partners attended it to exchange ideas on cooperation in fighting cybercrime. Since the first meeting in May 2014 in Singapore, the SOMTC Working Group on Cybercrime has been held six times, with the 6th SOMTC on 23 July 2019 in Nay Pyi Taw, Myanmar. SOMTC Working Group on Cybercrime in 2020 was postponed due to COVID-19 (ASEAN 2020) and resumed virtually on September 28, 2021.

8. POLRI'S PERFORMANCE WITHIN THE AMMTC FRAMEWORK AND GCI

The national strategy for eradicating cybercrime aims to determine the effectiveness of the POLRI strategy in combating cybercrime through AMMTC. After conducting interviews with two interviewees (Sumarno 2022), four performances become clear: networking, capacity building, sharing best practices, and prevention. Networking is the most obvious strategy for POLRI to be used in AMMTC, as networking allows POLRI to build relationships with other police forces from ASEAN member countries. Such networking assists POLRI in cases and investigations, such as requesting specific information or accommodation.

Networking includes meeting physically and communicating with other police officers. For example, when conducting investigations related to other countries in ASEAN, forums such as AMMTC bring POLRI and other security forces to provide mutual information to resolve the related issue. Capacity building includes improving POLRI personnel's quality through various training and meetings that Indonesian law enforcement officers can attend. There is also a sharing of best practices that provide enlightenment regarding the results of good cybercrime handling in their respective countries. Sharing best practices can discuss the modus operandi, perpetrators, and various details of a case that are useful for the POLRI in dealing with similar issues.

Finally, there is prevention, which is carried out by increasing awareness about the importance of cybersecurity and instilling better cybersecurity knowledge in Indonesian and ASEAN communities. Conflict mitigation is also included in prevention efforts, where POLRI investigates potential criminal acts and limits their movement and dissemination through information provided by other ASEAN countries.

From the Indonesian government, cybercrime is a problem that should be a concern for domestic and foreign policy, as well as the subject of longstanding multilateral policy commitments. Therefore, this article uses the Global Cybersecurity Index (GCI) from the International Telecommunication to review the cyber security strategy set by the Indonesian government and the Indonesian National Police's performance in response to this strategy, as described below:

Table 2. National Strategy and POLRI's Performance Based on GCI

No	GCI Pillars	National Strategy	POLRI's Performance
1.	Legal measures	1. Policy • Law No. 11 of 2008 concerning Information and Electronic Transaction, which was revised into Law No. 19 of 2016; • Telecommunications Law No. 36 of 1999; • Government Regulation No. 52 of 2000 concerning the Implementation of Telecommunication; • Regulation of the Minister Communication and Information No. 26 of 2007 concerning Security for the Utilization of Internet Protocol-Based Telecommunication Network; • Regulation of the Indonesian Minister of Defense No. 82 of 2014 concerning Guidelines for Cyber Defense, which was revised to	1. Policy In 2021, National Police Chief General Listyo Sigit Prabowo issued SE/2/11/2021 concerning Ethical Cultural Awareness to Create a Clean, Healthy and Productive Digital Space for Indonesia (Nurhanisah, 2021). This circular is an application of the ITE Law. This application regulation was issued to prioritizing preemptive and preventive efforts through virtual police and virtual alerts in monitoring, educating, warning, and preventing the public from potential cybercrimes. The Criminal Investigation Unit/ Dittipidsiber must be able to clearly distinguish between criticism, input, hoaxes, and good name judgments that can be sentenced to determine further steps. Investigators

		become Government Regulation No. 71 of 2019 concerning the Implementation of Electronic System and Transactions. 2. Technical Standard Based on the Regulation of Indonesian Minister Defense No. 82 of 2014, the following items are the technical standards serving as references for cyber defense policies: 1. SNI (Standar Nasional Indonesia) 27001 - Information Security Management System; 2. ISO/IEC 20000 Information Technology Service Management System (ITSM); 3. ISO/IEC 22000 Business Continuity Management (BCM); 4. Control Objectives for Information and related Technology (COBIT); 5. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; 6. TIA-942 Data Center Standards; 7. Open Web Application Security Project (OWASP); 8. Open-source Security Testing Methodology Manual (OSSTMM); 9. Information Systems Security Assessment Framework (ISSAF). 10. National Institute of Standards and Technology (NIST) SP 800.	must have the principle that criminal law is the last resort in law enforcement. 2. Technical Standard SNI 27001 is a standard for measuring an organization's security system. POLRI as a state law enforcement agency must prioritize information security. However, some literature considers that SNI 27001 is still not being complied with (Sugiarto 2021). In addition to SNI 27001, there is also COBIT which is used to evaluate the implementation of information technology governance and take the results as guidelines in planning an organization's information security policy. The use of COBIT standards at Bandung police station shows a low number in the level of technology and information governance capabilities (Jayusman and Abdulghani 2018).
2.	Technical Measures	1. Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), following the issuance of the Regulation of the Minister of Communication and Information Number 26/PER/M.Kominfo/5/2007 concerning Security of the Use of Internet Protocol-Based Telecommunication Networks, ID-SIRTII was formed. The Minister of Communication and Information assigned a team to assist in controlling the security of telecommunication networks based on Internet protocols. The functions and duties of ID-SIRTII are to monitor and detect early and provide warnings in case of disturbances (Mulyadi and Rahayu	As one of the initiators (founders and stakeholders) of ID-SIRTII (BSSN 2022), POLRI has a big part in the formation of ID-SIRTII. To handle domestic cybercrime cases, POLRI has collaborated with ID-SIRTII and ID-CERT (as ID-SIRTII supporting organizations) in the investigation process. In September 2016, POLRI invited ID-SIRTII regarding the prevention of criminal acts from social media during the 2016 DKI Province's election (Alief, 2016). POLRI has also asked ID-SIRTII for assistance in handling POLRI website hackers in 2011 (SumutPos.co 2011). However, ID-SIRTII is closer to collaborating with regional and international cyber institutions such as AP-CERT (Arianto and Anggraini 2019).

		2018). This team coordinates with relevant parties at home and abroad, if necessary, to secure the network. In addition, ID-SIRTII also provides information when threats and disturbances arise, and prepares work plans. 2. Indonesia Communication Emergency Response Team (ID-CERT). Acting as a supporting agency, the Indonesia Communication Emergency Response Team (ID-CERT) is an independent organization that cooperates with the government in special cases to support the development of cyber security in Indonesia. In addition, IDCERT also functions as a supporting institution for government organizations, such as ID-SIRTII (IDCERT, 2013).	
3.	Organizational Measures	1. National Cyber and Crypto Agency (BSSN) The government answered the national cyber security needs by establishing a BSSN which officially operated in January 2018. Based on Presidential Regulation Number 53 of 2017 concerning the Establishment of the National Cyber and Crypto Agency, BSSN became a government organization that specifically handles cyber security issues. The BSSN was formed by the Indonesian government as a transformation of the National Crypto Agency (Lemsaneg) which provides and organizes information security development through cryptography tasks, as well as carrying out functions previously assigned to the Directorate General of Information Security, Ministry of Transportation and Information Technology and the Indonesia Incident Security Response Team on Internet Infrastructure (IDSIRTII). BSSN as an institution responsible for national cyber security in Indonesia must be able to work together with all related elements, both government, private sector, community, academics, and civil society (Mulyadi and Rahayu 2018).	In dealing with cybercrimes, the POLRI Dittipidsiber coordinates and communicates with BSSN regarding crime tracking, cybercrime handling, anticipation, and prevention (Rizki and Gustarina 2021). The POLRI can also request assistance from the BSSN in the context of asset security operations, or seek information about suspected cybercriminals.
4.	Capacity Development	1. Cybersecurity Training, one of the 2022 Digital Talent Scholarship (DTS) programs from the Ministry of Communication and Information of the	1. Increase productivity, skills and competitiveness, professionalism of human resources in information and communication technology.

		Republic of Indonesia. (Tribun Jakarta, 2022) 2. Cyber Security Analyst Training and Certification in 2022. (Digitalent, 2022) 3. Basic Cyber Security Training for Health Sector in April 2022. (Digitalent, 2022) 4. Training in Cyber and Password Security by BSSN in February 2022. (SiarNasional 2022) 5. *Organisation of The Islamic Cooperation-Collaboration of Computer Emergency Response Team* (OIC-CERT) "*Traffic Malware Analysis*" *Technical Workshop* 2021 which was held by BSSN. (IDSIRTII 2021) 6. CSIRT 2021 Technical Guidance, held by Pusopskamsinas BSSN. (IDSIRTII 2021) 7. Webinar *Asia-Pacific Computer Emergency Response Team* (APCERT) *Training* dengan topik "*Stop Using WiFi, It's Dangerous*!" hosted by IDSIRTII in December 2021. (IDSIRTII 2021)	2. Able to apply the principle of information protection, apply the principle of information security for the use of the internet network, to identify attacks on access control. 3. Understand various Information Technology-based security and safety protection solutions in the world of health. 4. Train civil, police, military and state-owned government agencies in cyber security through the Human Resources Development Center. 5. Increase insight and ability in analyzing network traffic (traffic analysis), and assist in the identification process of malware. 6. Support workshops and training related to Incident Response and Handling. 7. Increase knowledge about and increase awareness of the dangers of using public networks.
5.	Cooperative Measures	Indonesia participates in several cyber security activities with the following organizations/forums: • Forum of Incident Response and Security Teams (FIRST) • Asia Pacific Computer Emergency Response Team (AP-CERT) • ASEAN - Japan Expert Cybersecurity Forum • Indonesia - Japan Bilateral Cybersecurity Forum • Internet Governance Forum • ASEAN Network Security Council (ANSAC) Working Group • ASEAN Ministerial Meeting on Transnational Crime (AMMTC) • ASEAN Ministerial Conference on Cybersecurity (AMMC) • World Conference on International Communication.	In various meetings of these organizations and forums, POLRI is often the Indonesian delegation as the national law enforcement officer. As the Indonesian delegation, the Indonesian National Police received various information and knowledge on effective cybercrime prevention and prevention, as well as being able to establish relations from the security aspect with other countries.

Source: From various sources, processed by authors.

The Indonesian government has launched a national cyber security strategy with various programs prioritizing prevention and response. However, regulations under the Legal Measures of GCI show a lack of POLRI performance. Rules set by the Minister of Defense have not been implemented properly, so when viewed through existing technical standards, the level of POLRI's capability is often low. Nonetheless, POLRI has shown good synchronization and cooperation under the Organizational Measures pillar,

together with the BSSN, which provides information regarding perpetrators. Capacity building and cooperative measures are also positive points for the Indonesian National Police, with various capacity-building efforts and cybersecurity organizations and forums in which Indonesia has participated.

Through the five pillars of the GCI, the POLRI's approach to improving the ability to handle cybercrime cases, although limited, has begun to be expanded. Although the implementation of regulations in law enforcement is still lacking, the performance of the Indonesian National Police in organizational measures, capacity building, and cooperative measures remains the work standard for preventing cybercrimes. As a result, by combining regional and national efforts, POLRI can reduce cybercrime rates, as shown in the Cyber Crime data table from Dittipidsiber in 2020 - 2021. The effectiveness of handling cybercrimes by the POLRI can be further enhanced if all legal and regulatory aspects are followed and complied with.

9. CONCLUSIONS

This study explains the importance of guarding against transnational organized crime, especially cybercrime. The danger is reflected in several critical cases in ASEAN and Indonesia based on an in-depth study of the relevant literature. From a theoretical perspective, this study presents a conceptual framework that describes four themes—transnational crime, cybercrime, cooperative security, regional organizations, and the Global Cybersecurity Index—of cybercrime and POLRI's efforts to combat it. Through the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the Indonesian National Police had the opportunity to attend and receive benefits from this regional forum. POLRI's performance in AMMTC consists of four efforts: networking, capacity building, sharing best practices, and prevention.

From a practical perspective, a review of the application of the GCI's five pillars enables the Indonesian government and the Indonesian National Police to measure the effectiveness of cybersecurity, understand the overall key strengths and weaknesses in securing telecommunications and information assets, identify capability gaps in delivering effective cybersecurity, and identify areas priorities that need to be improved. By these indicators, POLRI's performance data for the last five years by Dittipidsiber shows that cybercrime cases decreased from 2020 to 2021. This indicates the effectiveness of the Indonesian National Police in dealing with and preventing cybercrimes in Indonesia. Such a mechanism is the basis for initiating a roadmap for improving Indonesia's cybersecurity. Thus, enabling POLRI to develop the necessary structures further to analyze and deal with dynamic cybercrimes.

REFERENCES

1) Adrienne, McCarthy L., dan Kevin F. Steinmetz. Critical Criminology and Cybercrime. (2020). In Thomas J. Holt dan Adam M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance, 601-621. Switzerland: Palgrave Macmillan.
2) Agustini, Pratiwi. Kominfo Tangani Dugaan Kebocoran Data Aplikasi E-Hac. Aptika Kominfo. September 2, 2021. https://aptika.kominfo.go.id/2021/09/kominfo-tangani-dugaan-kebocoran-data-aplikasi-e-hac/
3) Alief, Bisma. Bareskrim Polri Gandeng Twitter Awasi Akun Penyebar SARA dan Menghasut di Pilgub DKI. Detik.com. September 2016. https://news.detik.com/berita/d-3307475/bareskrim-polri-gandeng-twitter-awasi-akun-penyebar-sara-dan-menghasut-di-pilgub-dkiAPJII. Buletin APJII. APJII, 2020: 74.
4) Arianto, Adi Rio, dan Gesti Anggraini. Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). Jurnal Pertahanan & Bela Negara 9, no. 1, pp. 13-29. (2019).
5) ASEAN Cyberthreat Assessment 2020: Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk (ASEAN Cybercrime Operations Desk, 2020).
6) ASEAN Plan of Action: Combating Transnational Crime (2016-2025) (ASEAN, 20 September 2017).
7) ASEAN Plan of Action to Combat Transnational Crime (ASEAN, 1999).
8) ASEAN Working Group on Cybercrime: Terms of Reference (ASEAN, 2014).
9) Brenner, S. W. Cybercrime Metrics: Old wine in new bottles? Virginia Journal of Law and Technology 9, no. 13, pp. 1-52. (2004).
10) Brenner, S. W. (2012). Cybercrime and the law: Challenges, issues, and outcomes. Boston, MA: Northeastern University Press.
11) BSSN. Sejarah ID-SIRTII. IDSIRTII. (2022). https://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html.
12) BSSN. Buletin Informasi SNI Terbaru. Pusat Informasi dan Dokumentasi Standardisasi Badan Standardisasi Nasional, 2016: 4.
13) Caballero-Anthony, Mely. (2005). Regional Security in Southeast Asia: Beyond the ASEAN Way. Singapore: ISEAS Publications.

14) Carter, Ashton B., Perry James William, dan John D. Steinbruner. (1993). A New Concept of Co-operative Security. Washington, DC: The Brookings Institution.
15) Clough, J. Data theft? Cybercrime and the increasing criminalization of access to data. Criminal Law Forum 22, no. 1, pp. 145–170. (2011). DOI: 10.1007/s10609-011-9133-5
16) CNBC. Banyak Serangan Siber, Ahli Siber: RI Masuk Tahap Red Alert. CNBC. January 24, 2022. https://www.cnbcindonesia.com/tech/20220124144241-37-309936/banyak-serangan-siber-ahli-siber-ri-masuk-tahap-red-alert
17) Digitalent. Kota Jambi - Pelatihan Basic Cyber Security untuk Sektor Kesehatan. Digitalent. 2022. https://digitalent.kominfo.go.id/detail/pelatihan/2416?akademiId=146
18) Digitalent. Pelatihan Thematic Academy Academy (TA) Offline Tahun 2022 bagi Pencari Kerja Gelombang ke-1. Digitalent. 2022. https://digitalent.kominfo.go.id/detail/pelatihan/1912?akademiId=146 \
19) Direktorat Tindak Pidana Siber Bareskrim Polri. Patroli Siber, 2021. https://cybersecurity.sulutprov.go.id/tentang
20) DPR-RI. Sukamta Minta Pemerintah Benahi Keamanan Siber Nasional. DPR-RI. 23 Januari 2022 https://www.dpr.go.id/berita/detail/id/37154/t/Sukamta+Minta+Pemerintah+Benahi+Keamanan+Siber+Nasional
21) Economic and Social Council Resolution: Organised Transnational Crime (United Nations, December 1994)
22) Emmers, Ralf. (2004). Security Cooperation in the Asia-Pacific: Evolution of Concepts and Practices. In See Seng Tan dan Amitav Acharya, Asia-Pacific Security Cooperation: National Interests and Regional Order. Armonk, New York: M.E. Sharpe.
23) Emmers, Ralf. (2003). Cooperative Security and the Balance of Power in ASEAN and the ARF. London and New York: Routledge Curzon.
24) Fawcett, Louise L'Estrange, dan Andrew Hurell. 1995. Regionalism in World Politics: Regional Organization and International Order. New York: Oxford University Press.
25) IDCERT. Profil Indonesia Computer Emergency Response Team. IDCERT. 2013. https://www.cert.or.id/tentang-kami/id/
26) IDSIRTII. Bimbingan Teknis Pembinaan CSIRT. IDSIRTII. 2021. https://idsirtii.or.id/kegiatan/detail_nama/workshop_and_technical_training/98/bimbingan-teknis-pembinaan-csirt.html
27) IDSIRTII. BSSN Menggelar OIC-CERT Traffic Malware Analysis Technical-Workshop 2021. IDSIRTII. 2021. https://idsirtii.or.id/kegiatan/detail_nama/workshop_and_technical_training/105/bssn-menggelar-oic-cert-traffic-malwae-analysis-technical-workshop-2021.html
28) IDSIRTII. IDSIRTII Menjadi Host APCERT Training dengan Tema Keamanan Jaringan Nirkabel. IDSIRTII. 2021. https://idsirtii.or.id/kegiatan/detail_nama/workshop_and_technical_training/107/idsirtii-menjadi-host-apcert-training-dengan-tema-keamanan-jaringan-nirkabel.html
29) Irviana, Claudia N., dan Roy V. Salomo. Analisis Pengembangan Kapasitas Organisasi di Direktorat Tindak Pidana Siber (DITTIPIDSIBER), Badan Reserse Kriminal POLRI (BARESKRIM POLRI). Media Bina Ilmiah, vol. 15, no. 11, pp. 5687-5694, 2021.
30) ITU. Global Cybersecurity Index. ITU. (2020). https://www.itu.int/en/ITUD/Cybersecurity/Pages/global-cybersecurity-index.aspx
31) ITU. Global Cybersecurity Index & Cyberwellness Profiles. ITU Publications, 2015: 1.
32) Jayusman, Yus, dan Tarmin Abdulghani. Evaluasi Tata Kelola Teknologi Informasi Dan Perancangan Kebijakan Sistem Manajemen Keamanan Informasi Berdasarkan Kerangka Kerja Cobit 5 Dan Sni Iso/Iec 27001. Bangkit Indonesia, vol. 2, no.7, 2018.
33) Joint Communique of the First ASEAN Plus Three Ministerial Meeting on Transnational Crime (AMMTC+3) (ASEAN, January 10, 2004).
34) Joint Statement of the Ninth ASEAN Ministerial Meeting on Transnational Crime (ASEAN Secretariat, September 17, 2013).
35) Lin, L.S.F., dan John Nomikos. Cybercrime in East and Southeast Asia: The Case of Taiwan. In Masys, A., Lin, L., Asia-Pacific Security Challenges: Advanced Sciences and Technologies for Security Applications (eds) Springer, Cham, 2018.
36) Madsen, F. G. (2009). Transnational organized crime. London, England: Routledge, 2009.
37) Maillart, Jean-Baptiste. The limits of personal territorial jurisdiction in the context of cybercrime. ERA Forum 19, pp: 375–390, 2019. DOI: 10.1007/s12027-018-0527-2
38) Mantalean, Vitorio. BSSN Sebut Ada 1,6 Miliar Serangan Siber Selama 2021. Kompas. March 7, 2022. https://nasional.kompas.com/read/2022/03/07/20162321/bssn-sebut-ada-16-miliar-serangan-siber-selama-2021
39) Marmita, Sharmaine. The struggle of ASEAN in cyber security. Asia and Africa Today, no. 8, pp. 52-56. 2020. DOI: 10.31857/S032150750010451-8

40) Moodie, M. Cooperative security: Implications for national security and international relations (Cooperative Monitoring Center Occasional Paper No. 14). Livermore, CA: Sandia National Laboratories, 2000.
41) Mulyadi and D. Rahayu, Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN). 2018 6th International Conference on Cyber and IT Service Management (CITSM), pp. 1-6, 2018. DOI: 10.1109/CITSM.2018.8674265.
42) Novitasari, Indah. Babak Baru Rejim Keamanan Siber di Asia Tenggara Menyosong ASEAN Connectivity 2025. Asia Pacific Studies 1, no. 2, pp. 220-233, 2017.
43) Nurhanisah, Yuli. Penerapan dan Penanganan Kasus UU ITE. Indonesia Baik. 2017. https://indonesiabaik.id/infografis/penerapan-dan-penanganan-kasus-uu-ite
44) Nye, Joseph. (1968). International Regionalism: Readings. Boston: Little, Brown.
45) Nye, Joseph. (1971). Peace in Parts. Boston: Little, Brown and Company.
46) Patnistik, Edigius. "Australia Sadap Telepon SBY dan Sejumlah Menteri," retrieved from https://internasional.kompas.com/read/2013/11/18/0950451/Australia.Sadap.Telepon.SBY.dan.Sejumlah.Menteri.Indonesia, November 18, 2013
47) Payne, Brian K. (2020). Defining Cybercrime. In Thomas J. Holt dan Adam M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance. Switzerland: Palgrave Macmillan.
48) Peraturan Menteri Pendidikan Nasional Nomor 27 Tahun 2008 Tentang Standar Akademik dan Kompetensi Konselor, Departemen Pendidikan Nasional, 2008.
49) Priambodo, Endo interviewed by Daniela Kaburuan. Dittipidsiber Interview on Membasmi Kejahatan Siber di Indonesia. Indirect interview. Zoom Meeting, Bogor. April 13, 2022.
50) Rizki, Aththaariq, dan Fauzia Gustarina. SYNERGY OF MULTI-STAKEHOLDERS IN DEFENDING INDONESIA FROM CYBER THREATS. Journal of Social Political Sciences 2, no. 4, pp. 342-353, 2021.
51) Sarre, Rick, Laurie Yiu-Chung Lau, and Lennon Y.C. Chang. Responding to cybercrime: current trends. Police Practice and Research 10, no. 6. 515-518, 2018. DOI: 10.1080/15614263.2018.1507888
52) Shantika, Eka. "Situs Telkomsel Dibajak, Telkomsel Minta Maaf," retrieved from https://www.cnnindonesia.com/teknologi/20170428074646-185-210802/situs-telkomsel-dibajak-telkomsel-minta-maaf, April 28, 2017.
53) SiarNasional. Pusdiklat Badan Siber dan Sandi Negara Bertransformasi Menjadi Pusat Pengembangan SDM. SiarNasional. Februari 2022. https://siarnasional.com/pusdiklat-pengembangan-badan-siber-dan-sandi-negara-bertransformasi-menjadi-pusat-pengembangan-sdm/
54) Sugiarto. Pengembangan Sistem Manajemen Keamanan Informasi Berbasis SNI ISO/IEC 27001:2013: Studi Kasus Data Center Divisi Teknologi Informasi dan Komunikasi Polri = Development of Information Security Management System based on SNI ISO/IEC 27001:2013: A Case Study. Skripsi, Depok: Fakultas Ilmu Komputer Universitas Indonesia, 2019.
55) Sumarno, Wino, interviewed by Elsafani Daniela Kaburuan. POLRI Interview on ASEAN Ministerial Meeting in Transnational Crime (AMMTC). Indirect interview. Zoom Meeting, Bogor. April 11, 2022.
56) SumutPos.co. Polisi Kantongi Hacker Situs POLRI. SumutPos.co. May 2011. https://sumutpos.jawapos.com/nasional/23/05/2011/polisi-kantongi-hacker-situs-polri/
57) Tribun Jakarta. Pelatihan Intensif dan Sertifikasi bidang Cybersecurity untuk Generasi Muda Indonesia. Tribun Jakarta. 2022. https://jakarta.tribunnews.com/2022/03/29/pelatihan-intensif-dan-sertifikasi-bidang-cybersecurity-untuk-generasi-muda-indonesia
58) United Nations Convention against Transnational Organized Crime (UNODC, November 15, 2000)
59) Wall, D. S. (2001). Cybercrimes and the internet. In D. S. Wall, Crime and the Internet. New York: Routledge.
60) Wall, D. S. (2007). Cybercrime. Cambridge, UK: Polity Press.
61) Wiener, Norbert. (1948). Cybernetics: Or control and communication in the animal and the machine. New York: Wile.
62) Yasmin, Muhammad. Perancangan Tata Kelola Keamanan Informasi Menggunakan Framework Cobit 2019 Dan Iso/Iec 27001:2013 (Studi Kasus Ditreskrimsus Polda Xyz). Thesis, STEI Teknik Elektro, 2021.