# Indonesia's Cyber Security Strategy: Problems and Challenges

Arief Isdiman Saleh[1] and Muhammad Danu Winata[2]

[1]Department of Political Science and Public Policy, Necmettin Erbakan Üniversitesi, Turkiye
[2]Department of Communication, Universitas Negeri Surabaya, Indonesia

ariefisdiman93@gmail.com

**Abstract.**Cyberspace is one among the areas that should be secured by the state, in addition to land, sea and air areas which already included in the national security landscape. Nevertheless, in recent years, among serious threats to the global world comes from cyber threats. Cyber threats potentially attack a country's assets, national interests, and can be carried out at any time. At the same time, internet users continue to increase significantly every year, particularly in Indonesia which reaches more than half of the total population. Majority of them even relies on several activities in the cyber space which require security aspects such as e-commerce, e-banking, etc. Thus, this condition requires good cyber security strategy in order to manage the situation. Therefore, this work is aimed to discusses Indonesian national cyber security strategy in order to analyses problems and challenges towards Indonesian cyber security. Indonesia, in regulating cyber-security has several important regulations. Among of these important regulations are Law on Electronic Transaction and Information (UU ITE), and The Law on The Security of Personal Data (UU PDP). In terms of cyber security in Indonesia, there are several government agencies and NGO's that play important role on cyber security measures in Indonesia. Furthermore, Indonesia also conducts several bilateral, regional, and multilateral cooperation on cyber security in order to solve the problem of cyber security. However, there are several challenges and problems on Indonesia cyber security that hindering Indonesia's ability on cyber-security measures such as overlapping regulations, shortage of human resources, and ignorance and alienation of human and civil rights principles. Meanwhile, the level of internet usage in Indonesia continues to increase with the determination of technology in many aspects of people's lives.

**Keywords:** Indonesia, National Cyber Security, Strategy, Cyber Threats.


A. Mustofa et al. (eds.), *Proceedings of the International Joint Conference on Arts and Humanities 2023 (IJCAH 2023)*, Advances in Social Science, Education and Humanities Research 785,
https://doi.org/10.2991/978-2-38476-152-4_169

## 1 Internet Usage & Cyber Security in Indonesia

Indonesia, is ranked among the countries with the biggest and largest internet users in the world. According to reports issued by InternetWorldStats.com in November [1], Indonesia is among the top 20 countries with the highest internet users. Indonesia, is ranked at 4th place after China, India, and United States of America with the total of internet users of 292,862,868 users per 30 June 2019 [1]. The growth of internet users in Indonesia are tends to be increased every year. According to the reports which was issued by Indonesia Association of Internet Service Provider/Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) in 2018 amounts of internet user in Indonesia is 64,8% of its population in 2018, showing increase of 10,12% than the previous year [2]. This amount might be more increased as several online based start-up businesses and applications are easily being accessed and used by the citizens of Indonesia.

At the same time, the users of social media numbers in Indonesia in recent years are increasing. According to the report which issued by WeAreSocial.com, UK-based company that have its concern on global digital and internet development, the total active numbers of social media users in Indonesia are 150 million or equal with 56% of total Indonesia population. Furthermore, 48% of the active users of social media in Indonesia are accessing it through the mobile platform [3]. Therefore, the development of mobile platform of social media and start-ups in Indonesia increases at the same time with digital and internet development in Indonesia.

The increasing rate of internet users and internet penetration in Indonesia, at one side, is an advantage for e-commerce and other online-based business platform as more of Indonesian population are getting more depending to gadget and internet network. Thus, a number of start-ups and e-commerce platform in Indonesia ranging from travel service to the health service is growing intensively in these recent days. However, along with the big potential of internet users in Indonesia, the threats and risks on Indonesia's cyber security are also getting higher. Indonesia's Cybersecurity Index ranks 24th out of 194 countries and has increased from 41st place in 2018. At the regional level, Indonesia ranks 6th in Asia Pacific and 3rd in ASEAN after Singapore and Malaysia [4].

Therefore, in order to counter the risks and threats to Indonesia's cyber security, effective cyber security strategies are necessary things to be fulfilled by Indonesian stakeholders. Thus, the objective of this paper is to analyze several strategies which are taken by Indonesian stakeholders including several laws and regulations related to the cyberspace and cyber security, several institutions and organizations that having concern on cyber security, and several problems and challenges of cyber security in Indonesia. The discussion on this paper would be divided into 4 parts, are: (1) regulating laws on cyber-security in Indonesia, (2) institutions that have responsibility or concern on cyber-security, (3) international institutions, regulations, and cooperation on cyber space where Indonesia participates in, (4) problems and challenges in Indonesia's cyber security strategy.

## 2 Several Laws Regulating on Cybersecurity in Indonesia

There are several laws in Indonesia that regulates cyberspace and cyber security in Indonesia (see Table 1 below). The early law that regulates cyberspace and cyber security in Indonesia is UU No.36/1999 Tentang Telekomunikasi/ Law No.36/1999 on Telecommunication. According to this law, telecommunication is defined as every activity of broadcasting, delivering and receiving information from any tools of communication [5]. This law does not specifically mention the tools of communication. However, this law generally mentions the medium of telecommunication, including other kinds of electromagnetic tools of communication. This law, actually regulates several new developments in telecommunications system in Indonesia because at the same time when this law was enacted, telecommunication sector was starting to develop intensively [6]. Among several new developments in telecommunication that are enacted at this law is the existence of private telecommunication service provider. According to the Article 8 paragraph 1 of this law, private sectors could become telecommunication service provider along with state- owned telecommunication provider [5]. Thus, private operator, according to this law might operate in Indonesia along with several state-owned operators.

**Table 1.** Several Laws in Indonesia Which Regulate Cyberspace and Activities Within Cyberspace

| No | Law | Year of Issuance | Subjects Regulated |
|---|---|---|---|
| 1 | Law No.36/1999 on Telecommunication [5]. | 1999 | — Devices or mediums used for purpose of telecommunications including electromagnetic devices.<br>— Satellite orbit within the jurisdiction of The Republic of Indonesia.<br>— Telecommunications Service Provider, by issuing permit for private sector to became ISP provider alongside with state provider.<br>— In terms of threats, only mentioning wiretapping activities and sabotage activities which disrupt the telecommunication network. |
| 2 | Law of The Republic Indonesia No.11/2008 on Electronic Informations and Transactions [7] | 2008 | — Clearly mentions several kinds of cybercrime including pornography, hatred speech, gambling, etc. |

| | | | |
|---|---|---|---|
| | | | — Specifically regulate several electronics transactions including e-commerce and e-trade.<br>— |
| 3 | Law of The Republic Indonesia No.19/2016 on Electronic Informations and Transactions [8] | 2016 | — Serving as revision and complementary law of the previous law (Law of The Republic of Indonesia No.11/2008).<br>— Hoaxes, fake, and provocating news transmitter could directly prosecuted.<br>— Simpification of investigation and evidence collecting in the case of cyber-crime by giving permission to perform both in accordance to *KUHP* (Criminal Procedural Law) |
| 5 | Personal Data Protection Law | 2022 | — Protecting personal and individual data from any kind of leakage and misuse in cyberspace. |

The telecommunications service provider, according to this law's 7th article, is specifically divided into 3 kinds, such as: network service operator, telecommunication operator, and special telecommunication operator [5]. However, in order to operate in Indonesia territorial jurisdiction, a written permit should be obtained from related minister. At this context, a written permit should be obtained from Ministry of Communication and Informatics of Republic of Indonesia (*Kementerian Komunikasi dan Informatika Republik Indonesia*) through Directorate-General of Post and Telecommunication Resources and Devices (*Direktorat Jenderal Sumberdaya dan Perangkat Pos dan Telekomunikasi*) [8]. Thus, every telecommunication service provider that operates in Indonesian territory should be abode with this law.

This law, despite does not mention specifically the cyberspace or internet access, also regulates the use of satellite orbit within Indonesian territory. As it had mentioned at this law's 33rd article, the usage of satellite's orbit within Indonesia should be performed under permits and supervision from Indonesian government [5]. Therefore, the usage of internet in Indonesian territory through satellite's orbit as medium of connection is the subject of this law.

In the terms of violation or cyber-related crimes, this law does not mention specifically the kinds of cyber-related crimes and violations. If there are any specific cyber-related crimes related to this law, only actions of wire-tapping on several delivered information at telecommunication network and any kinds of sabotage which could causing disruption or technical problems in telecommunication network [5]. Therefore, this law simply does not specify any kinds of cyber-related crimes and threats except wire-tapping and sabotage against telecommunication networks.

The more specific law that regulates cyber-related activities and crime is Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik/Law of The Republic Indonesia No.11/2008 on Electronic Informations and Transactions. This law regulates the existence of cyberspace in Indonesia more specifically. According to this law, electronic informations are the kind of information which delivered through the medium of internet, telex, telegram, or e-mail in kinds of electronic mail, documents, pictures, and any kind of data delivered through the mediums showed above, whilst electronic transactions are defined as any kind of trade and economic transactions or other legal activities that conducted through the computer, computer networks (intranet/internet), or other electronic devices like cellular phone [7]. Therefore, according to the main definitions on this law, every single of information or data sharing, transactions and other legal activities conducted through the medium of internet network are considered as cyber-related activity.

This law, compared with the previous law shown above, mentions several specific things that did not mentioned at the previous law. For example, this law mentions specifically kinds of cyber-related crime or cyber-related violations. According to article 27,28,29,30, and 31 of this law, several behaviors could be considered as violation to this law or a cyber-related crime, like: creating and sharing pornography contents, online gambling, online or cyber scamming, any defamations or act of bullying using the cyber medium, racist contents creating and sharing, and activities related to hacking, intercepting, and wire-tapping of others computers or networks without any authority to conduct those activities [7]. Therefore, the kinds of cyber-crime that become law objects in Indonesia are clearly mentioned at this law.

However, there are several main weaknesses of this law that might cause the efforts of prevention and law enforcement against cybercrime become ineffective. For example, at this law's chapter 43, there is any form of bureaucratic problem in arresting the culprit of cybercrime or collecting evidence of any cybercrime which requires permission from the chief of local prosecutors. This bureaucratic problem might be an advantage for the culprits of cyber-crime or other cyber-related crime could erase or get rid of the evidence easily thus it might hinder investigation process of any cyber-related crime [8].

In 2016, another law had been enacted as the revision of Law No.11 2008 on Electronic Transactions and Information [7]. The new enacted law is Law No.19 2016 on Electronic Transactions and Information [9]. Compared with the similar law that enacted in 2008, this law serves as complementary of incomplete chapters at previous law. For example, at chapter 31 of the new law, the context of interception or wire-tapping activities by law enforcement institutions are clearly defined. Wire-tapping or interception activities conducted in order to law enforcement, in both laws are permitted under the supervisions of related laws. Nevertheless, the difference of this law with the old laws lies on the widening of responsible agency in the terms of wire-tapping or interception activities for national law enforcement and security interests. It states that other law enforcement agencies or cyber-security related government agencies are permitted to conduct any kind of wire-tapping or interception activities for national security and law enforcement interests [9]. Investigation and arresting processes against the culprit of cyber-crime or other violations of this law are simplified in this law.

According to this law's article 43, any kinds of arresting, evidence collecting, evidence searching, and confiscating against any allegation of cyber-related crime is permitted and should be conducted in accordance with criminal procedural law [9]. Therefore, the procedure of law enforcement against any allegation of cyber-crime conducted by police and other law enforcement institutions become more simplified and make the culprits of cyber-crime or cyber-related violations difficult to erase or disband the evidence.

Any sharing activities of hoaxes, fake news, or another form of news that precipitate fears and hates inside the societies is also ruled at both laws. Both of these laws stated that the creator, transmitter, and distributor of hoaxes and any kind of fake news could be prosecuted and legally sued under the criminal law [10]. Then, on other side, the latter law gives government more authorities to protect Indonesian societies from negative effect of cyber-world abuse. Government, at several necessary moments, might impose blockage or network cutting against any kinds of shared electronic documents and information that violating this law. The main example of blockage imposing conducted by Government of Indonesia, in accordance to this law, is the blockage of Tumblr, a microblogging social media platform in February and March 2018. According to the press release conducted by Minister of Communications and Informatics two years prior to blockage action against Tumblr, the main reason behind the blockage of Tumblr was the abundance of pornography and immoral contents that frequently posted on or through the use of Tumblr [11]. It means that the plans to blockage of Tumblr had been planned a long before. However, due to several complaints from Indonesian netizens and Tumblr itself, the blockage action was taken into actions in the following years. The blockage of Tumblr in Indonesia was officially terminated at December 2018 after Tumblr had shown its commitment to both erase and eliminate any immoral or pornography contents inside Tumblr [12].

In terms of cyber-security strategy, there is no specific laws regulate on national cyber security strategy. Nevertheless, the existing law had regulated several of Indonesian Government's measure to achieve a secure cyberspace in Indonesia and become legal foundation on cyber security in Indonesia. In both Law No.11/2018 and Law No.19/2016, for example, obliges all the providers and operator of electronic and internet system to ensure and have responsibility on security and reliability of internet system [9]. Therefore, although not specifically mentioned, government as a main operator should provide a secure, reliable, and accessible network of internet.

In order to ensure security and reliability of electronic and internet network, other regulations are also enacted. Other regulation that regulates security, accessibility, and reliability of internet and cyber-electronic network is Indonesian Governments Regulations No.82/2012. This law regulates specifically the rules that should be obeyed by internet and cyber network operator in Indonesia along with several surveillance and control functions to ensure security of cyber network in Indonesia. For example, at the use of several software in government institution, this regulation obliges all government institution to ensure that used software in their computers had already registered at the Ministry of Communication and Informatics (Republik Indonesia, 2012). Then, to prevent any kinds of espionage or wiretapping commited by other foreign actors/intelligent, this law obliges the operator position of several strategic electronic

systems and installations should be fulfilled by Indonesian-nationality experts [13]. Then, in order to ensure law enforcement against any form of cyber-crime, every operator might be cooperates cooperatively with the law enforcement agencies in providing any information or evidence on several particular criminal case.

After waiting and delays since its drafting and applications process in 2019, finally in 2022 the Personal Data Protection Act (UU Perlindungan Data Pribadi) was approved. This approval coincides with the increasing number of cases of leakage of residents' personal data. This law functions to guarantee citizens' rights to personal protection and raise public awareness and guarantee recognition and respect for the importance of protecting personal data.

This law is expected to become a strong legal basis for the management and protection of citizens' personal data and government administrators. Protection of personal data is one of human rights which is part of personal protection. This personal protection is stated in Article 28G of the 1945 Constitution. This personal protection or privacy is universal, in the sense that it is recognized by many countries.

Since May 2018, 28 member countries of the European Union (EU) have implemented the General Data Protection Regulation. This figure continues to grow in line with the need to protect citizens' data. In Indonesia, before this law was passed, personal data protection arrangements were spread across several laws and regulations, including Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Information and Electronic Transactions, Law Number 39 of 1999 concerning Human Rights, Law Number 14 of 2008 concerning Public Information Disclosure, and Law Number 23 of 2006 in conjunction with Law Number 24 of 2013.

Industry 4.0 has driven the development of the digital world in Indonesia. Until now, Hootsuite (We are Social) 2022 data shows 204.7 million Indonesians use the internet and 93.5 percent of them are active as social media users. The development of the digital world has also spawned several new cultures and behaviors, from uploading anything to online transactions. This condition has not been followed by public and government awareness to protect personal data. In fact, disclosure of personal data without control is proven to pose many risks of various criminal acts. Bullying, threats, fraud, and account breaches are unavoidable.

## 3 Several Institutions in Charge of Cyber Security in Indonesia

In context of cyber security in Indonesia, there are several actors or institutions that have their concerns to cyber security measures in Indonesia. As the internet users in Indonesia are not only dominated by the governments but also the Indonesian public societies, the institutions that have their responsibilities are specified into two actors: government and public/private actors. As the government of Indonesia takes part in Indonesian cyber network and space as both regulator and operator, the discussion on this chapter will be started from Government institutions which have concerns and responsibilities on cyber security in Indonesia.

The first government institutions that have responsibilities in ensuring security and reliability of cyber network is Ministry of Communications and Informatics of The

Republic of Indonesia. This ministry, has responsibility on running governmental functions in the field of communications and informatics by setting and regulating policies related on communications and informatics, including the cyber space [14]. At the past, these functions were performed by Ministry of Information along with Ministry of Transportation, Post, and Telecommunication of The Republic of Indonesia.

In the terms of cyberspace regulation and surveillance in this ministry, there are 2 directorate-generals within this ministry that have direct responsibilities towards the cyberspace and cyber security in Indonesia. The first directorate general within the ministry that have direct responsibility towards cyberspace, cyber network, and cyber security in Indonesia is Directorate-General of Postal Resource and Informatics Tools. In the terms of cyber network and cyber security, this directorate general has responsibilities and functions on regulating, licensing, standardizating, and performing surveillance towards radio and informatics tools which operate under the jurisdiction of the Republic of Indonesia including the frequency of orbital satellite [15]. Therefore, every existing informatics tools and orbitting satellites might obtaining licence and standardization from this directorate general and under surveillance of this directorate general. Some of telecommunication tools that should obtain standardization from this directorate general including cellular phones, BTS, Personal Computers or Laptops, and analog phones. Besides of these functions, this directorate-general has responsibility on framing/reframing process and frequency band contiguous fixation process on radio frequency band in order to distribute equal cellular and network services inside Indonesian territory [12].

The second directorate general that have responsibilities on cyber networks and cyber security within the ministry is Directorate-General of Informatics Applications [8]. This directorate-general, is one among frontier guard- institutions that has direct responsibilities against any form of misuse of the cyberspace in Indonesia, including the spreading of negative content in internet networks. Even in the terms of Indonesian national cyber-security strategy, this directorate general serves as one of important backbones in national cyber-security strategy by applying several strategies including: building cultures and capacities on information security, managing risk on information security, improving performance of information security, and improving law enforcement capacity in the fields of Electronics Information and Transaction [16]. Therefore, several rules regulating cyberspace and cyber security in Indonesia are mainly both submitted and taken into force by this directorate general, including Law No.11/2008 and Law No.19/2016 on Electronics Information and Transaction.

The main functions of this directorate general are formulating and executing policies in several fields like e-Government, e-Business, and information security that conducted in several working programs and related applications. In the terms of information security, this directorate general has a platform for complaining or reporting negative content in internet under the name of aduankonten.id. This site is opened for every Indonesian citizen or foreign residents residing in Indonesia who wants to complaint or report negative and immoral content in internet networks, especially in social media, websites, and online applications which have indications of spreading negative content (AduanKonten.id, 2020).

Besides of this platform, there is also another supporting system to prevent any transmission or accession towards negative contents in internet under the platform of TRUST+Positif. The TRUST+Positif system is having responsibilities on filtering several sites with negative content like violence, pornography, illegal trading, etc. and sharing to all local ISP's the blacklists of negative content sites (Dirjen APTIKA, 2015b:13). In order to prevent the widespreading of negative content, public participation is also welcomed through complaining and reporting service. Until December 2018, there are at least 547.506 negative content was blocked through two platforms of reporting [17]. The most reported content and sites in these two platforms are pornography, gambling, and any sites that contain any attempts and measure against Intellectual Property Rights contents.

Another government institution that also has concern on cyber security in Indonesia is Indonesia Technology Development and Research Agency (Badan Pengkajian dan Pengembangan Teknologi/BPPT). Indonesia Technology Development and Research Agency (BPPT) participates in Indonesia's cyber security measures through IPTEK-netBPPT, a subordinate institution under coordination of this agency and Ministry of Research and Technology of Republic of Indonesia by providing secure data networks and recovery, wireless network among governmental building across the Indonesian capital, and act as the data center for governmental data [18]. IPTEK-netBPPT, provides internet security service for government sites and public sites through application of the system known as SIMONTIK/ Sistem Monitoring Teknologi Informasi dan Komunikasi in Indonesian or Monitoring System on Information, Technology, and Communication (MSITC). The functions of this system are collecting and analyzing data about cyber attackers penetrations inside the attacked site and enhance any effort to counter cyber-attack against public and governmental sites by optimizing the resources [19].

In the field of national defence, security, and law enforcement, there are 4 government institutions that having responsibilities on cyber-security and cyber-defence in Indonesia. All these government institutions are Indonesia National Police (Kepolisian Negara Republik Indonesia/POLRI), Indonesia National Armed Forces (Tentara Nasional Indonesia/TNI), Ministry of Defence, and Indonesia National Cyber and Enscription Agency (Badan Siber dan Sandi Negara/BSSN). In the terms of cyber-security and law enforcement against any kinds of cyber-crime, Indonesia National Police bears the responsibilities. On the daily basis, the responsibilities on handling and combatting cyber-crime are lied under coordination of Indonesia National Police Headquarters Criminal Investigation Agency (Badan Reserse Kriminal Mabes Polri), particularly The Directorate of Cyber-Crime (Direktorat Tindak Pidana Siber).

According to the official site of Directorate of Cybercrime of Indonesian National Police, there are two kinds of cyber-crime that handled by this directorate. The first cyber-crime is computer-crime which conducted by using computer as the main tools in commiting crime including data manipulation, hacking, system interference and system interference, whilst the second category of cyber-crime is kind of criminal act commited by using computer as a media for commiting criminal act [20]. The criminal acts that fulfill the second criteria are pornography, hate-speech, online-gambling, and online fraud. The Directorate of Cybercrime of Indonesian National Police is also

opened its portal for public to report or complaining any kinds of cyber-crime. In order to prevent any kind of fraud as the result of highlighting e-commerce in current day, the directorate provides a special platform on its site to check the account number and phone number of the recipient in online or e-commerce transaction.

The Ministry of Defence of The Republic of Indonesia [21] and Indonesian National Armed Forces (TNI), at the other place, bears responsibility for Indonesia national cyber defence policy. According to Indonesia Defence White Paper issued in 2015, cyberspace has become 5th domain of warfare arena along with other conventional warfare area such as sea, air, and land warfare arena [21]. Thus, the uses of internet or online-based tools might become effective weapon of warfare through the uses of online propaganda, cyber-espionage, or other kinds of cyber warfare. Therefore, cyber-attacks and online-espionage are considered as security threat towards Indonesian national defences along with other conventional and unconventional contemporary threats like terrorism, radicalism, and separatism [21].

Therefore, among several priorities on Indonesia national defence developments, is the developing of ICT (Information, Communication and Technology) systems in the field of defence is conducted through several measures. Among the main measures conducted by the Indonesian government are: transfer of technology (ToT), research and development cooperation with universities and other institutions of higher education, and cooperation with foreign industries, especially in the development of the usage of satellite technology in the field of national defence (Republik Indonesia, 2015b:42). Then, in the operational level, the developments of cyber defence within the Ministry of Defence is conducted by establishing a Cyber Defence Center with several tasks, including cyber defence operation and conducting quick response measure against any kind of cyber-attacks through the formation of CERT (Computer Emergency Response Team) [22]. Besides of establishing a Cyber Defence Center, Ministry of Defence also empowers and enhance existing cyber-related institutions within its subordination with the functions of supervising, securing, and managing defence IT infrastructure, information system, and enscription system. These tasks are under responsibilities of Ministry of Defence of The Republic of Indonesia Information and Data Center (Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia) [23].

Several tasks of Ministry of Defence of The Republic of Indonesia in the field of cyber security are supported with the establishment of Cyber Unit within Indonesia National Armed Forces. This unit is under direct subordination of Indonesian National Armed Forces Headquarter. The tasks and functions of Cyber Unit of Indonesian National Armed Forces (Satuan Siber TNI) are: (a) protecting Indonesia National Armed Forces vital and critical ICT infrastructure from any unauthorized use or attacks, (b) planning, coordinating, and executing military cyber operations under the framework of IDNAF's cyber-defence tasks, and (c) synchronizing cyber activities and operations in order to supports the IDNAF main tasks [20]. The IDNAF Cyber Unit, is also has the service platform on complaints and reports submission against negative content. Among the negative contents handled by this unit are hoax and other negative contents related to national defence.

The last institution that bears responsibility on cyber-security in Indonesia is Indonesia National Cyber and Encryption Agency (Badan Siber dan Sandi Negara). The Indonesia National Cyber and Encryption Agency is established in 2017 as the extension of the previous national agency in the field of national encryption [24]. The main task of its agency is carrying on cyber security in Indonesia in such effective and efficient way by developing and consolidating all cyber-related elements in Indonesia. In order to performing such task, the main strategy used by Indonesia National Cyber and Security Encryption Agency is multi-stakeholder approach as cyber security in Indonesia involves multi-actor role. This strategy is conducted by performing several steps, are: (a) constructing and building an integrated national cyber operations center, (b) establishing an informal forum on cyber in society, (c) increasing partnership, especially with the private sectors as frequent users and of cyberspace, and (d) supporting and endorsing empowerment measures of cyber communities in Indonesia, including white and grey hackers, social media enthusiasts, and cyber industries community [25].

In addition to the Electronic Transaction Law (UU ITE), cyber security in Indonesia also have been overseen by the Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII), the Indonesia Computer Emergency Response Team (IDCERT), and the Cyber Crime Sub-Directorate (Subdirektorat Kejahatan Siber), Directorate of Economic and Special Crimes (Dittipideksus Bareskrim Polri). Although several policies on cyber security have been regulated through the ITE Law, Indonesia is also facing the problem of the division of authority and which authority is obligated to tackle cybercrime, cyber terrorism, cyber hacktivism and cyber warfare. Thus, the existence of the BSSN (National Cyber and Encyription Agency) as a new institution becomes important for coordinating the tasks of various institutions, especially those dealing with cyber-attacks. Bearing in mind that the impacts of cyber-attack are so broad, not merely an amount of economic loss, but also affect individual rights to the integrity and sovereignty of the state, the development of cyber defense and security is a necessity and even to some extend become obligation in order to maintain national security in Indonesia.

As Indonesia adheres to universal defence system in accordance with the 1945 Indonesian Constitutions, the operations of cyber security in Indonesia should involve the participation of its citizens, not only the governments and operators. It because, according to Chapter 9 at Law No.3/2002, every single of Indonesian citizens should and obliges to participate in every measure of national defence through their enrolment as main component of national defence by joining Armed Forces and Police Force or as supporting element by performing services at each of their respective occupation [26]. Therefore, according to this law, cyber-security and cyber-defence concept in Indonesia is universal and requires all of its citizens to take part in any measures of Indonesian cyber- security and cyber defence.

Besides the governmental actors, public and private actors are also taking part and participate in national cyber security measures in Indonesia. Among them, there are two non- governmental organizations (NGO) that have concern in democratization on

internet in Indonesia and digital rights. Both of the NGO's are ICT-Watch and SAFE-Net (South Asia Freedom of Expression Networks. Each of them has its own prominent programs on cyber- security. ICT-Watch, in terms of cyber-security, has a campaign program known in Indonesian as "Internet Sehat" or Healthy Internet. Healthy Internet or "Internet Sehat" program is a digital literacy program aims to build Indonesian societies awareness, especially teachers and students, on using internet in such a safe and prudence way through providing socializations on digital awareness including publishment of bulletin, books, and documentary film that designated for students and teachers [27]. The most extraordinary things from this digital literacy program is the using of 'zero-rupiah' licence of creative common licence in order to make all content from digital literacy program could be accessed and used by public as education content although the mark of "Internet Sehat" had already registered in Directorate General of Intellectual Rights of Republic of Indonesia [27]. Therefore, with the free and easy access of several contents issued by ICT-Watch through the "Internet Sehat" or Healthy Internet program, the aim of this organization could be reached.

SAFE-Net, at the other place, has also a prominent program that focuses mainly on the freedom of expression and digital rights fulfilling in cyberspace across the Southeast Asia. Although its network of operations covering Southeast Asia, the main concern of this NGO is the digital expression rights in Indonesia, as the establishment background of this organization was the criminalization of several internet users in Indonesia caused by their expression posted in internet after the enactment of Law No.11/2008 on Electronics Information and Transaction (UU 11/2018 Tentang ITE) [28]. According to the annual report that was issued by this NGO at 2018, several violations against digital rights in Indonesia remains take place. Government, according to the annual report, have been become main actor of the violations through several actions ranging from criminalization of several journalists and media owner to internet-blockade policy that imposed in particular region [29]. Other violations of digital rights are also included, like cyber-bullying, cyber-harrassment, and cyber-trafficking. Therefore, the main aim of this organization is surveillance and supervising several government policies, particularly on cyber-security and human rights as the governments of Indonesia at several times ignoring the human rights aspects in enforcing cyber-security strategies.

## 4 International Cooperations and Regulations in The Field of Cyber and Cyber Security Which Are Followed by Indonesia

In the field of cyber-security, Indonesia conducts bilateral, regional, and multilateral cooperation with several international actors. Even, although Indonesia neither became one among non-European Countries that became both parties and signatories of Budapest Convention/International Convention of Cyber Crime nor became one of its observers, several of regulations within the convention are adopted at several law products related to the cyber-crime. For example, in the definition of computer system, both Budapest Convention and Law of The Republic of Indonesia on Electronic Transaction and Information (UU ITE) define computer system as a set of computer

tools that have functions in processing data or information [30] [10]. Nevertheless, Law of The Republic of Indonesia on Electronic Transaction and Information (UU ITE) clearly defines the computer system functions in more specific way, that the definitions of work functions of computer system are extended to saving, spreading, and delivering functions of every electronic information as it had mentioned at Law No.19/2016 on Electronic Transaction and Information's Article 1 paragraph 5 [10].

Another part of Budapest Convention on Cyber Crime that adapted by Indonesia is the substantive criminal law, particularly offences against confidentiality and availability of computer data and systems, computer and content-related offences, and offences of infringement of Intellectual Property Rights [30]. All of these offences adopted by Government of Indonesia inside both Law No.11/2008 and Law No.19/2016 on Electronic Transaction and Information in both laws 7th Chapter of Offences and Prohibited Acts. Nevertheless, in the offence of pornography, Budapest Convention regulates specifically the children pornography as the serious offence whilst at both of Indonesia's Law on Electronics Transaction and Information only defined the offence of pornography in general definitions, that the pornography contents are defined as any contents that violate normal norms in Indonesia whatever the kind of the contents [10].

Despite of unspecific defining of the kinds of pornography, these laws have been became legal background for eradication of children pornography in Indonesia. According to article 27 of these laws, any kinds of producing, replicating, and sharing immoral or pornography content are strictly prohibited [7]. Children pornography, although is not clearly mentioned, also included within the categories of immoral or pornography content that prohibited according to both of Electronics Transaction and Information Law of The Republic of Indonesia [31]. At several case of children pornography in Indonesia, these laws along with related law such as the law of children protection and the law of anti-pornography, are used to prosecute the culprits of children pornography. For example, at the case of "Candy Loly" Facebook group in 2017, Indonesian National Police was imposing multi-layered legal articles against the culrits behind that Facebook group which provides some contents of children pornography. Among the legal articles that were used to prosecute the culprits is Law No.11/2008 and Law No.19/2016 on Electronics Transaction and Information (Suryowati, 22 September 2017).

Indonesia, at multilateral arena, conducts cooperation on cyber-security under several frameworks at several international organizations. Among the cooperation frameworks in the field of cyber-security that joined by Indonesia is International Multilateral Partnership Against Cyber-Threat or abbreviated as IMPACT. The partnership, is conducted by joint collaboration and initiative with the International Telecommunication Union or ITU that was taken into force at 2009 [32]. The ITU-IMPACT initiative, is intended to "pioneering deployment of service and solutions in eradicate and overcome the effects of cyber-threat at the global scale [33]. Indonesia, is among first 50 countries that joined inside the ITU-IMPACT initiative. Another cooperation under the framework of ITU besides the ITU-IMPACT initiative in which Indonesia also participates is Global Cybersecurity Agenda or GCA. This framework of cooperation aims to seeking consensus among countries in the world on addressing

several problems of cybersecurity as the current cybersecurity eradication efforts at some countries, particularly the developing countries sometimes inadequate (ITU, 2007). Indonesia, along with other ITU state members, had joined and has active role on the agenda since the agenda had been launched in 2007 [34].

Besides at multilateral level, Indonesia is also conducting bilateral cooperation in the field of cyber-security with several countries. Among several bilateral cooperation in the field of cyber-security, bilateral cooperation between Indonesia and Australia is one the most important and prominent cooperation in this field. The bilateral cooperation between Indonesia and Australia in the field of cybersecurity cooperation is arranged under Memorandum of Understanding in the cyber cooperation that was signed in August 2018. According to this MoU, the scope of cyber security is arranged under several areas of cooperation including sharing of information, capacity building, and cyber-crime. At the field of cyber-crime, in particular, conducted through training and sharing capabilities in the fields of cyber-forensic and investigation capabilities [35]. This bilateral cooperation, not only involves state actors, but also several NGO's. One among NGO from Indonesia that became partner of Australian Government in the field of cyber-security is ELSAM, an Indonesian-based human rights NGO. The main focus of partnership is empowering human rights enforcement agenda at reformation process of cyber law in Indonesia [36]. Along with several partnership and cooperation, both parties also conducted several forums and dialogs in order to address several problems in the cyberspace. Last forum was held in Jakarta in 2018 which focussed on embodiment of more open, free, and secure internet to enhance economic growth in the current era [37].

At the regional stake, Indonesia has also active roles on several cyber-security cooperation under framework of ASEAN. Among the cooperation in the field of cyber security within ASEAN framework that followed by Indonesia are ASEAN Cyber Capacity Development Project (ACCDP), ASEAN Defence Ministerial Meeting Plus Expert Working Group or ADMM-Plus EWG on cyber security, and other cooperation conducted under the framework of ASEAN Declaration to Prevent and to Combat Cybercrime (ADPCC). At the first cooperation framework, or ACCDP, conducted cooperation within the framework is intended to strengthen the abilities to combat and to cooperate against cyber-crime in Southeast Asia region through several trainings and information sharing [38]. This project was initiated in 2016 by Singapore under cooperation and coordination with INTERPOL.

The other important cooperation within the ASEAN framework which Indonesia involves in is ASEAN Declaration to Prevent and to Combat Cybercrime. The most important point inside the declaration regarding to the cyber-crime and cyber security are strengthening and empowering cooperation among ASEAN member states through exchange of information, experiences, and technical expertise in order to combat cybercrime [39]. This declaration also emphasizes importance of existing regional agency like ASEANAPOL (ASEAN National Polices) in coordinating several cooperation on combating cyber-crime.

## 5 Problems And Challenges in Indonesia Cyber Security Strategy

In spite of the current progress on cyber security strategy, however, there are several existing problem and challenges in Indonesian National Cyber Security Strategy (see Table 2 below). The first problem is the shortage of person, skill, and expertise in the level of technical teams and senior management in order to construct a sophisticated system on cyber-security (Austcyber, 2019). Even at several frontier and important institution, membership of technical team in cyber security remains slight. For example, at Cyber Criminal Directorate of Indonesia National Police, technical teams could only process several cyber-crime cases related to the cases of defamation, hate-speech, or several urgently to be handled cases due to the shortage of human resources or personnel [40]. Therefore, several big figure cybercrime cases like online scamming or trans-national crimes are hard to be resolved.

**Table 2.** Problems and Challenges of Indonesian Cybersecurity Strategies and Its Impacts

| No | Problems and Challenges in Indonesian Cybersecurity Policies | Impacts Caused by Problems and Challenges |
|---|---|---|
| 1 | Shortage of Human Resources (skilled, trained personel, and experts) | Only handful, 'light', and simple cases could be resolved and prosecuted by law like: defamation, pornography, hoaxes, etc. |
| 2 | Shortage of Research and Development in Cybersecurity Supported by Government | – Several skilled and Indonesian experts got recruited by some prominent and advanced company and institutions in cybersecurity. |
| 3 | Overlapping Activities and Actions Between Agencies | – Several government agencies tend to move at their own and even endorsing their own agenda instead of launching joint coordination scheme |
| 4 | Alienation and Ignorance of Human Rights Principles | – Violation of Human Rights, especially the right of freedom of speech. Even several people are sentenced to imprisonment due to the misinterpretation of hate-speech context in one of the law (UU ITE).<br>Example: The case of Prita Mulyasari. |

The shortage of human resource and experts is also become main concern of newly established National Cyber and Encryption Agency. According to the chief of Indonesia National Cyber and Encryption Agency, 30% problem of cyber security in Indonesia is the shortage of human resources and expertise in the fields of cyber security [41]. Actually, Indonesia had possessed resources and experts in the field of cyber security. However, due to the shortage of research and development on cyber security in Indonesia, most of the experts are recruited by several overseas company and institution. Therefore, among the main focuses of Indonesia NCEA is to provide expertise and skill training through research and development in the fields of cyber security.

The next problem and challenge in the field of cyber-security in Indonesia is overlapping coordination among responsible agency in the field of cyber-security. Even at several case, several government agency and institution both promote and endorse themselves as main coordinator or main actor in combating several cyber security problems (Nugraha and Putri, 2016). The establishment or so-called extending functions of Indonesia National Encryption Agency into Indonesia National Cyber and Encryption Agency could not easily prevent the overlapping coordination and functions on eradicating cyber security problems in Indonesia. It because, at the other place, the establishment of Indonesia National Cyber and Encryption Agency even bears potentials to overlap or having clash with other ministry or agencies that had already have program in the field of cyber security. For example, the surveillance, eradication, and content-censoring function of Indonesia National Cyber and Encryption Agency would collide and overlap with the same functions owned by other agencies and ministries, including hate-speech censorship authority under coordination of Ministry of Communication and Informatics and Indonesia National Police's authority to eradicate spreading of hate-speeches and its culprits [42].

In order to prevent the overlapping tasks and functions, Indonesia National Cyber and Encryption Agency had both formulates and launches several strategies to prevent such overlapping in the field of cyber security. Among several strategies conducted by Indonesia National Cyber and Encryption Agency to coordinate efforts and visions on Indonesia cyber security is proactive approach towards related institutions that share the same concern on cyber security issues. The institutions that engaged within the proactive approach are not limited with governmental agencies, but also higher education institutions, research centers, and cyber communities in domestic or international level [43]. However, overlapping tasks and functions in the fields of cyber security remains exist. Several government agencies still conducting surveillance and eradication functions on cyber security for example, the eradication effort of negative contents conducted by Indonesian National Police and Ministry of Communication and Informatics of The Republic of Indonesia. Then, several regulations regulating some aspects of cyber security are remains separated each other and unintegrated thus causing the overlapping in cyber security regulations and actions in Indonesia remains happen [44]. Therefore, the overlapping in cyber security regulations in Indonesia becomes very hard to be terminated.

The other serious problem and challenges in cyber-security in Indonesia is the alienation and ignorance of human rights and democracy aspects in Indonesian cyber law. Current cyber laws that regulate cyber security, sometimes being used to mute citizen's rights to speak their argument or even deliver constructive criticism. The main example of this problem was the case of Mrs. Prita Mulyasari versus a private hospital in Jakarta at 2008. The main cause of this case was Mrs. Prita's complaint and criticism on malpractice or misdiagnose accusation conducted by a private hospital when she was receiving medical treatment at that hospital [45]. She then shared her experience through her mailing list group, but the hospital later known it and thus reported her to the police on the accusation of defamation. Mrs. Prita, then was prosecuted due to her accusation of violating Article 27 of Law No.11/2008 on Electronic Transaction and Information regarding to online defamation [46]. The case then had become more complicated, as the local prosecutor was suddenly postponed the legal prosecution against Mrs. Prita due to the premature application of Article 27 of Law No.11/2008 of Electronic Transaction and Information [47]. This Article along with the law, actually should be taken into force after two years of enactment but on the Mrs. Prita's case it was used against her.

Although finally Mrs. Prita was released from the jail and was imposed house arrest by local prosecutions, the controversy of this case continued. Several Indonesian people, caused by this case, had since became afraid to speak their argument and expression through the cyber platform as they might be the next "Mrs.Prita" [41]. To make the controversy of this case more complicated, the Indonesian Government at that time was considered by several human rights organization getting more aggressive and repressive at the context of defamation. The Indonesian government, at this case, even was considered violating its own constitutional principles that strongly guarantee any kind of freedom of speech [47]. Therefore, the case of Mrs.Prita Mulyasari had created negative precedence against the Law of Electronics Transaction and Information that this law could be used as repressive tools against freedom of speech as one element of democracy.

The ignorance of human rights and democracy aspects in Indonesian cyber law are not limited on the case of Mrs. Prita Mulyasari, but also had reached the highest level of legislation and law-making process. The case that marked the situation is the drafting process of newly planned Indonesian National Cyber Security Law (Indonesian: Undang-undang Keamanan Siber). According to several human rights association, including ELSAM, the newly and currently drafted Cyber Security Law has several serious weaknesses at its drafting process. Several serious weaknesses of being-drafted Cyber Security Law are: (a) the drafting process are conducted in such a hustle way and public participation at the drafting process is very minimum, (b) the potential of 'abuse-of power' and violation of human rights conducted by regulator (the Indonesian Government) are high as this drafted law gives privilege to government to control all aspects of cyberspace in Indonesia, and (c) this law will became the threat to public's right on freedom of speech as The Indonesian National Cyber and Encryption Agency, according to the being-drafted law, has several functions of censoring and imposing blockage against several contents that considered by the agency as the sensitive,

provocative, and dangerous content despite the definitions of such contents is remains undefined clearly [44].

ELSAM is not alone on speaking its objection against the newly drafted National Cyber Security Law. Other Indonesian prominent human rights organization, KontraS/ Komisi Untuk Orang Hilang dan Korban Tindak Kekerasan (Commission for Missing Peoples and Victims of Violence) also speaks its criticism against newly being-drafted National Cyber Security Law. Even at this organization does not only criticize the contain of the drafted law but also the negative excess towards the people's objection against newly drafting law as Indonesian Government through its security apparatus had commited despotic arrest and detention against several figures and activists that speaks their objection against newly being- drafted National Cyber Security Law (Undang-Undang Keamanan Siber Nasional) [48]. Thus, ELSAM, KontraS, and other Indonesian human rights organizations are vociferously urge the government and related agents to postpone the drafting process of National Cyber Security Law due to its potential negative effects against civil and human rights.

## 6 Conclusion

Although Indonesia does not have specific laws governing or ruling cyber security, Indonesia has 4 related laws or regulations on cyberspace that also have concern on cyber security. First Law is Law No.36/1999 on telecommunication that regulates generally the definition, kind, and type of communication. The first law does not specify more about cyber related crime. However, several of violations that also included among kinds of cyber- criminal are mentioned at this law. The second and third law are Law No.11/2008 and Law No.19/2016 on Electronic Transaction and Information. Both laws define specifically the definitions and kinds of electronic transactions and information. These laws have even specify several kinds of cyber-related crime, although the procedures of eradication against the culprits of cyber-crime are become more simplified at the second law.

To complement both laws on regulating cyber-security, the Indonesia government also adds another regulation that known as Indonesian Government Regulation No. 82/2012. At this regulation, Indonesian government regulates more specifically several measures on cyber security including appointment of Indonesian-nationalities expert to have control over strategic cyber installations in order to prevent any kinds of cyber-attack or espionage attack from foreign actors against Indonesia. Then in the terms of cyber defence, according to Indonesian constitution, it conducted by universal system and involves multi-layer of citizens as the universal defence system adhered by Indonesia obliges all of Indonesian citizens to involve themselves in every measure of national defence.

In order to provide more protection on personal data privacy and also as a response to several case of personal data leakage, the Government of The Republic of Indonesia issues the new law regarding personal data protection under the name of Undang-Undang Perlindungan Data Pribadi (The Law of Personal Data Protection). This new law provides legal basic on protection of personal data in cyberspace including leakage

and inappropriate uses of personal data. Regarding to this newly law, similar laws had already enacted and applied in several parts of the world including European Union under the scheme of General Data Protection Regulation

In the terms of actors and institutions on cyber security in Indonesia, there are several government and non-government agencies that have concern and responsibilities on cyber- security issues. Several government agencies that have concern and responsibilities on cyber- security issues are: (a) Ministry of Communications and Informatics (on regulation and surveillance), (b) Indonesia National Technology Center and Development Agency (on technical support), (c) Indonesia National Police (on law enforcement and surveillance), (d) Ministry of Defence and Indonesian National Armed Forces (on defence cyber), (e) Indonesia National Cyber and Encryption Agency (on coordinating and consolidating measures in cybersecurity). Besides the government actors, there are also several non-governmental organizations that have concern on Indonesian cyber security policy including ICT-Watch (on educational function of internet usage) and SAFE-Net (surveillance and advocacy measures against any violation of civil rights in the cyberspace). Nevertheless, as Indonesia adheres to the universal defence principle, every Indonesian citizen bear the same responsibility and duties on protecting and defending the cyberspace.

Indonesia, at international and regional level, conducts several cooperations in the field of cyber-security. At the international level, Indonesia conducts several bilateral cooperations in the field of cyber security, including bilateral cyber cooperation with Australia. Even bilateral cyber cooperation with Australia had created several high-level forum meetings on cyber- related issues conducted at both Indonesia and Australia. At multilateral level, Indonesia became active member of International Telecommunication Union and joined several of its initiatives, including ITU-IMPACT and ITU Global Security Agenda. Cyber cooperation at the regional level, conducted by Indonesia under ASEAN framework through several joint project and initiative including ASEAN Cyber Capacity Development Project (ACCDP) and ASEAN Declaration to Prevent and Combat Cyber Crime. Besides these cooperation, Indonesia also adopts several chapter on Budapest Convention within Indonesia's both Laws of Information and Electronics Transaction, particularly on several definitions and kinds of cyber-crime.Although the current achievement that Indonesia had achieved in the terms of cyber security, there are also several remaining problems and challenges in the field of cyber security in Indonesia. First problem is overlapping coordination on eradicating cyber security problems as there are several agencies that endorse themselves as the main element on eradicating cyber security problems. In spite of several efforts conducted by Indonesia National Cyber and Encryption Agency to coordinate and consolidate cooperation, the overlapping problem could not be resolved yet as several regulations on cyber remains separated. Second problem and also become the main challenges is the shortage of experts and technical human resources in the field of cyber security. Third problem is alienation of civil and human rights aspects on Indonesian cyber laws. Several cases like Mrs.Prita Mulyasari's case and drafting process of drafted Indonesian National Cyber Security Law had indicated that the application of cyber laws in Indonesia sometimes both ignoring and alienating human and civil rights, particularly freedom of speech.

## References


1. Internet World Stats. 2019. Top 20 Countries With The Highest Number Of Internet Users. https://www.internetworldstats.com/top20.html, last accessed 2020/01/25.
2. Asosiasi Jasa Pengguna Internet Indonesia. (2018). Hasil Survei Penetrasi dan Per-ilaku Pengguna Internet Indonesia 2018. https://apjii.or.id/survei, last accessed 2020/01/25.
3. Kemp, Simon. 2019. Digital 2019: Indonesia. https://datareportal.com/reports/digital-2019-indonesia, last accessed 2020/01/25.
4. BSSN RI. 2020. Sejarah Pembentukan BSSN, https://bssn.go.id/sejarah-pembentukan-bssn/, last accessed 2020/01/27.
5. Republik Indonesia. 1999. Undang-Undang No.36Tahun 1999 Tentang Tele-komunikasi. https://jdih.kominfo.go.id/produk_hukum/view/id/564/t/undangundang+nomor+36+tahun+1999+tanggal+8+september+1999, last accessed 2020/01/25.
6. Maskun, Maskun. 2014. Kejahatan Siber (Cyber Crime): Suatu Pengantar. Jakarta: Prenada Media.
7. Republik Indonesia. 2008. Undang-Undang No.11Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, https://www.kpk.go.id/images/pdf/uu%20pip/UU_ITE%20no%2011%20Th%202008.pdf, last accessed 2020/01/25.
8. Dewan Perwakilan Rakyat Republik Indonesia. 2016. Rancangan Undang-Undang ITE No.19 Tahun 2016, http://www.dpr.go.id/doksileg/proses1/RJ1-20161102-050504-9518.pdf, last accessed 2020/01/26.
9. Direktorat Jenderal Sumberdaya Dan Perangkat Pos Dan Informatika. 2018. Laporan Tahunan 2018 Ditjen SDPPI. Jakarta: Ditjen SDPPI.
10. Republik Indonesia. 2016. Undang-Undang No.19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik, https://jdih.bssn.go.id/wp-content/uploads/2017/01/UU2016-19-pub-12192016180910.pdf, last accessed 2020/26/01
11. Kominfo. 2019. Kemenkominfo Cabut Pemblokiran Tumblr. https://kominfo.go.id/content/detail/15768/kemenkominfo-cabut-pemblokiran-tumblr/0/sorotan_media, last accessed 2020/01/26.
12. Rajab, Achmaduddin. 2017. Urgensi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2018 Tentang Informasi Dan Transaksi Elektronik Guna Membangun Etika Bagi Pengguna Media. Jurnal Legislasi Indonesia, 14(4). Pp. 463-472.
13. Republik Indonesia. 2012. Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012, https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012, last accessed 2020/01/26.
14. Kominfo. 2020. Tugas Dan Fungsi. https://www.kominfo.go.id/tugas-dan-fungsi, last accessed 2020/01/27.
15. Dirjen Postel. 2020. Tugas dan Fungsi. https://www.postel.go.id/artikel-tugas-dan-fungsi-1-2231, last accessed 2020/01/25.
16. Direktorat Jenderal Informasi dan Informatika Kemenkominfo RI. 2016. Profil Direktorat Jenderal Aplikasi Informatika. Jakarta: Dirjen Aptika Kemenkominfo.
17. KOMINFO. 2016. Kebijakan Keamanan Dan Pertahanan Siber. https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/, last accessed 2020/01/26.

18. Riza, Hammam and Moedjiono. 2006. Country Paper In Cybersecurity Initiative: Na-tional Cybersecurity Policy & Implementation for Government of Indonesia. Jakarta: ITU.
19. Balai Jaringan Informasi Dan Komunikasi BPPT. 2020. Security BJIK. https://www.ipteknet.go.id/produk/security/, last accessed 2020/01/27.
20. Patroli Siber. 2020. About Us. https://patrolisiber.id/about, last accessed 2020/01/27
21. KEMHAN RI. 2015. Buku Putih Pertahanan Indonesia. 2015. Jakarta, Kementerian Pertahanan: Republik Indonesia
22. KEMHAN RI. 2020. Tugas Pokok dan Fungsi. https://www.kemhan.go.id/bainstranas/tugas-fungsi, last accessed 2020/01/27.
23. Pusat Data Dan Informasi Kemhan RI.2020. Tugas Dan Fungsi Pusdatin. https://www.kemhan.go.id/pusdatin/tugas-fungsi-pusdatin, last accessed 2020/01/27.
24. BSSN RI. 2020. Sejarah Pembentukan BSSN, https://bssn.go.id/sejarah-pembentukan-bssn/, last accessed 2020/01/27
25. Chaerudin,Asep. 2018. Strategi Keamanan Siber Nasional, https://bssn.go.id/wp-content/uploads/2018/08/Strategi-Keamanan-Siber-Nasional-signed.pdf , last accessed 2020/26/01.
26. Republik Indonesia. 2002. Undang-Undang Republik Indonesia No.3 Tahun 2002 Tentang Per-tahanan Negara http://lkbh.uny.ac.id/system/files_force/UU_No3-2002.pdf?download=1, last accessed 2020/01/26.
27. Internet Sehat. 2009. Internet Sehat, Antara ICT-Watch Dan Depkominfo. http://internetsehat.id/2009/02/internet-sehat-antara-ict-watch-dan-depkominfo-notulen-diskusi/, last accessed 2020/01/27.
28. SAFE-Net. 2020. Siapa SAFE-Net. https://internetsehat.id/tentang-kami/, last ac-cessed 2020/01/27
29. SAFE-Net. 2018. Laporan Tahunan SAFE-Net 2018. Denpasar: SAFE-Net.
30. Budapest Convention. 2001. Convention OnCybercrime, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016 80081561, last accessed 2020/01/28.
31. ECPAT. 2011. Pemantauan Global Status Aksi Menentang Eksploitasi Seksual Komersial Anak. Jakarta: ECPAT International
32. ITU-News. 2009, October. Making AnImpact on Global Cyber. https://www.itu.int/net/itunews/issues/2009/08/22.aspx, last accessed 2020/01/28.
33. Touré, Hamadoun I. 2011. Cyber Security Global Status. https://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf, last ac-cessed 2020/01/28.
34. Ardiyanti, Handrini. 2014. Cyber-Security Dan Tantangan Pengembangannya Di In-donesia. Politica, 5 (1). pp 95-110.
35. Department of Foreign Affairs and Trade Australia (DFAT). 2018. Memorandum of Understanding Between The Government Of The Republic Of Indonesia And The Government Of Australia On Cyber Cooperation. https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/mou-indonesia- australia-cyber-cooperation.pdf , last accessed 2020/28/01.
36. Department of Foreign Affairs and Trade Australia (DFAT). 2020. Cyber Cooperation Program: Institute For Policy Research And Advocacy (ELSAM), https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/mou-indonesia-australia-cyber-cooperation.pdf , last accessed 2020/28/01.
37. Department of Foreign Affairs and Trade Australia (DFAT). 2018. Second Indonesia-Australia Cyber Policy Dia-logue: Joint Statements. https://dfat.gov.au/international-

relations/themes/cyber-affairs/Documents/mou-indonesia-australia- cyber-cooperation.pdf, last accessed 2020/28/01.
38. INTERPOL. 2020. ASEAN Cyber Capacity Development Project. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-training-for-police/ASEAN-Cyber-Capacity- Development-Project-ACCDP, last accessed 2020/01/28.
39. ASEAN. 2017. ASEAN Declaration to Prevent and Combat Cybercrime. https://asean.org/wp- content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime, last accessed 2020/01/29.
40. BBC Indonesia. 2018, 12 March. Penanganan Kejahatan Siber Lebih Banyak Untuk Pencemaran Nama Baik, Bagaimana Dengan Kejahatan Lainnya?(Online). Available: https://www.bbc.com/indonesia/trensosial-43368591, last accessed 2020/01/28.
41. Rahman, Arif. 2019, 11 July. Sepertiga Masalah Cyber Di Indonesia Adalah SDM .https://cyberthreat.id/read/1260/Sepertiga-Masalah-Cyber-di-Indonesia-Adalah-SDM, last accessed 2020/29/01.
42. Mantra,IGN. 2020. Tumpang Tindih Tugas Badan Siber Dengan Lembaga Lain. https://kominfo.go.id/content/detail/12355/tumpang-tindih-tugas-badan-siber-dengan-lembaga- lain/0/sorotan_media, last accessed 2020/01/29.
43. BSSN RI. 2018. Rencana Strategis Badan Siber Dan Sandi Negara Tahun 2008-2019. Jakarta: BSSN RI.
44. ELSAM.2019. RUU Keamanan dan Ketahanan Siber Mengancam Kebebasan Sipil. https://elsam.or.id/ruu- keamanan-dan-ketahanan-siber-mengancam-kebebasan-sipil/, last accessed 2020/01/29.
45. Kompas.com. 2009, 3 June. Inilah Curhat Yang Membawa Prita Ke Penjara. https://nasional.kompas.com/read/2009/06/03/1112056/inilah.curhat.yang.membawa.prita. ke.penjara?pag e=all, last accessed 2020/01/29.
46. Rahman, Muhammad Razi. 2009, 4 June. Kasus Prita, Pengadilan Terhadap Kebebasan Berpendapat. https://nasional.kompas.com/read/2009/06/04/20494920/kasus.prita.pengadilan.terhadap.kebebasan.berp endapat?page=all, last accessed 2020/01/29.
47. Wiryawan, Syahrial Martanto et.al. 2016. Pidana Penghinaan adalah Pembatasan Kemerdekaan Berpendapat Yang Inkonstitusional. Jakarta: ELSAM.
48. KontraS. 2019. Catatan Hari HAM Sedunia 2019. https://kontras.org/wp-content/uploads/2019/12/final_cahaham_2019-1.pdf, last accessed 2020/01/29.