Efforts to Strengthen Cyber Defense and Cyber Security of the Indonesian Government in Maintaining National Security

Fadilah Munawaroh[1] Pujo Widodo[2] Yulian Azhari[3]
Peace Studies and Conflict Resolution Program, Faculty of National Security, Universitas Pertahanan Republik Indonesia, Bogor Regency, West Java Province, Indonesia[1,2,3]
Email: fadilah1024@gmail.com[1]

Abstract

The development of science and technology makes the threat to national defense also widen. From threats in the form of physical and non-physical. Increasingly sophisticated technology introduces people to the internet. Internet has become one of the primary needs today. Almost all activities are centralized from the Internet. Socio-economic, political, culture has been affected by the existence of the internet. Relations between communities have become very easy with the internet connected by social media. Out of a total of 270 million Indonesians, more than 170 million are active on social media. Not only that, economic activities, education to health have been facilitated by an online system with the existence of E-commerce and similar applications. This research discusses efforts to strengthen the Indonesian government's cyber defense and cyber security in maintaining national security. Using a descriptive qualitative research method, the author will discuss further the Indonesian government's efforts to strengthen cyber defense and security. One of these efforts has been carried out by issuing Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, the existence of this PP strengthens the protection of personal data and information. Therefore it becomes interesting to be discussed further.

Keywords: Defense, Cyber, National Security, Government

INTRODUCTION

In an era that is increasingly digitized as it is today, the sector in security studies is also affected. Joseph S. Nye (2011) explains that the security sector is not just five, but six sectors. Nye added in his book entitled The Future of Power cyber (cyber) needs to get priority in security studies. He explained that the dimensions of the life of the nation-state including the social order regulated therein would not be separated from the role of cyberspace. So like it or not, the nation state needs to include it as a strategic priority for the country.

Along with technological developments, discourse on cybersecurity and cybercrime has become increasingly diverse, complex, and advanced. The pandemic that has drastically changed the role of technology in people's personal and work lives has made cybersecurity more important than ever. Lohrmann even called 2020 the year of the Cyber Pandemic. Thus, the current discussion on cyber security has begun to shift from cyber security to cyber resilience, namely the ability to anticipate, respond to, and recover from cyber attacks.

In Indonesia, the cyber security and/or cyber resilience landscape is on the way to development. Indonesia's Global Security Index in 2020 ranks 24th globally and 6th in the Asia Pacific region with a score of 94.88. However, in 2021, Sularso from the National Cyber and Crypto Agency (BSSN) stated that Indonesia was included in the top 10 countries with the most sources and targets of cybersecurity anomalies with 190 million attacks originating from and 1 billion attacks targeted at Indonesia. This cyber attack has an impact on society and the government, such as the BPJS data breach case in 2021 which leaked 297 million Indonesian citizens' personal data at an estimated cost of IDR 600 trillion.

Multilevel cyber defense from the scope of individuals, working groups, organizations up to the national scale. Special attention is given to sectors that manage critical infrastructure such as defense and security, energy, transportation, financial systems, and various other public services. Disruptions to electronic systems in these sectors can cause economic losses, lower levels of trust in the government, disruption of public order and others. This risk is a consideration for the need for strong cyber defense within one country. As government agencies, the Ministry of Defense and the Indonesian National Armed Forces have dual interests in cyber defense. First, to secure all electronic systems and information networks in their environment. Second, support the coordination of cyber security in other sectors as needed.

The development of science and technology makes the threat to national defense also widen. From threats in the form of physical and non-physical. Increasingly sophisticated technology introduces people to the internet. Internet has become one of the primary needs today. Almost all activities are centralized from the Internet. Socio-economic, political, culture has been affected by the existence of the internet. Relations between communities have become very easy with the internet connected by social media. Out of a total of 270 million Indonesians, more than 170 million are active on social media. Not only that, economic activities, education to health have been facilitated by an online system with the existence of E-commerce and similar applications. However, in facing the challenges of a very dynamic era, Indonesia has not carefully planned preventive measures for some of the systems that will be affected. In the last 5 years, Indonesia has experienced 7 data leaks from large digital companies which resulted in tens of millions of public data being leaked. This becomes very dangerous because data obtained by irresponsible parties can be traded and misused resulting in Cyber Crime.

The data leaks experienced did not only come from private companies, which also occurred in several government agencies such as the General Elections Commission, BPJS Health, and most recently EHac belonging to the ministry of health. According to the Personal Data Protection Advocacy Coalition (KA-PDP) data leakage occurs because there is still an aspect that is still missing in the current sectoral regulations, namely the obligation of data controllers, to ensure that data processors have implemented technical and organizational efforts to secure personal data that has been processed. . From this we can see that Indonesia's cyber security is still very weak. Even though in the current era of globalization, destroying a country is not only through war but also destroying the system and taking state data.

From a philosophical perspective, in this study researchers will focus on finding information on the efforts made by the government in terms of safeguarding national security data through Cyber Security. This research was conducted by directly reviewing existing policies and evaluating policies and efforts that have been made by the government to find things that must be improved in terms of Cyber Security. And this research can produce recommendations for efforts to strengthen security related to national data whose implementation has been evaluated.

Viewed from the transformative Critical paradigm, the problems that arise from the unpreparedness of the Indonesian Government in facing the challenges of the times should enable the government to evaluate the policies that have been implemented and the efforts that have been made so as to bring about innovation in Cyber Security policies in Indonesia to maintain national data security. Awareness of the existing conflict will transform into a real movement. According to Roxana Radu, Cyber security itself is a set of policies, tools, instruments, risk management in preventing threats from cyberspace. Meanwhile, Madeline Carr explained in her journal entitled Crossed Wires: International Cooperation on Cyber Security that cyber security is a post-state issue. This means that cyber security is a form of threat that cannot be handled using state instruments such as the military. Carr emphasized that threats coming from cyberspace are borderless and invisible but their impact is very much felt.

RESEARCH METHODS

This research uses descriptive qualitative method. Meanwhile according to Lodico, Spaulding, and Voegtle (2006). Qualitative research, also known as interpretive research or field research, is a methodology borrowed from disciplines such as sociology and anthropology and adapted to educational settings. This data collection was carried out using qualitative data collection techniques in qualitative research. In this case, data collection techniques will be carried out in several ways, namely initial observation, literature study and documentation. In data analysis techniques according to Miles M.B and Huberman AM, it consists of several stages, namely the first is data collection, data collection or data collection from interviews, observations, and various documents obtained based on categorization according to the research problem which is then developed. by sharpening the data through further data search. Then the second is data condensation, namely the selection or selection of focus, simplifying and replacing data contained in field notes, interview transcripts, documents and empirical data that have been obtained. the next stage is the presentation of data or data display, the presentation is an arrangement, a collection of information that has been pursed so that a conclusion can be drawn. and the last stage is conclusion drawing or verification or proofing which is evidence of the research conducted. The final conclusion will occur if data collection has been completed, depending on the size and records in the field, storage and improvements that will be used in this final conclusion obtained based on temporary conclusions.

RESEARCH RESULTS AND DISCUSSION

According to Arnold, global cyber security must be built on five areas of work: Legal certainty (cyber crime law); technical and procedural measures (end users and business (direct approach and service providers and software companies); organizational structure (highly developed organizational structure, avoiding overlap); capacity building and user education (public campaigns and open communication of the latest cyber crime threats)); International Cooperation (including reciprocal cooperation in efforts to overcome cyber threats).

The development of information technology has also provided significant changes regarding the concept of security, now the interaction space cannot only be limited physically but also extends to cyberspace. As a consequence, the state must adapt to this development, it is time for the concept of cyber security to be defined as one of the "territories" of the state that maintains its security as the state's obligation to safeguard its territory. Moreover, cyber attacks do not only occur on public institutions, but also attack government institutions. Cyber security addresses the issue of information security for governments, organizations and individual affairs related to technology, and specifically to internet technology.

Cyber attacks are currently a frightening specter for a number of people, especially business owners. It is known that many companies in the world have experienced financial losses of up to $1 trillion in 2020, as a result of the corona virus pandemic where almost all companies have implemented work from home (WFH) policies which have caused digital security to become more sluggish. The projected loss of up to $945 billion, from a new report issued from the Center for Strategic and International Studies (CSIS) and computer security firm McAfee, is almost double the monetary loss from cybercrime which was worth $500 billion in 2018. According to a survey conducted by The Directorate of Cybercrime at the Bareskrim Polri (Dittipidsiber), there are 90 million cases of cyber attacks in Indonesia, and according to the Financial Services Information Sharing and Analysis Center (FS-ISAC), Indonesia is included in the list of countries that are vulnerable to cyber crime attacks. Indonesia itself occupies the 9th position.

The Covid-19 pandemic is a major topic in cybersecurity trends. The hackers took advantage of public unrest as a loophole in launching various attacks, ranging from phishing to ransomware, the data leak case of 91 million users of the online shopping site Tokopedia and the data leak of 1.2 million users of the Bhinneka site. Indonesia was also affected by global cyber security cases such as Coronavirus Ransomware, Covidlock Malware, Border Gateway Protocol hacking, vulnerabilities in Draytek Vigor router products, Remote Code Execution on several product versions of the Windows operating system, Arbitrary Code Execution vulnerabilities on all Google Android operating systems , to the exploitation of the Solar Winds Orion Platform product.

The pandemic period has also become an easy target for hackers who continue to try to break into system security at companies, due to the high use of the internet where almost everyone works from home. Quoted from BSSN, the most attacks received in March 2020, up to 22 cyberattacks using the background of the COVID-19 pandemic issue, these attacks with various types of attacks including Trojan HawkEye Reborn, Blackwater malware, BlackNET RAT, DanaBot Banking Trojan, Spynote RAT, Netwalker ransomware, Cerberus Banking Trojan, Ursnif malware, Adobot Spyware, Trojan Downloader Metasploit, Projectspy Spyware, Anubis Banking Trojan, Adware, Hidden Ad (Android), AhMyth Spyware, Metasploit, Xerxes Bot, and Covid19 Tracker Apps.

According to research conducted by Frost and Sullivan initiated by Microsoft in 2018, cyber crime has caused losses of approximately 478.8 trillion rupiah or as much as 34.2 billion US dollars. This happened before the pandemic. Pratama Persadha, a cyber security expert, has predicted that the global deficit due to cyber attacks will probably reach 84 thousand trillion rupiah or as much as 6 trillion US dollars. These facts show how urgent Indonesia's need for a cyber security strategy is to realize national security in the current era of society 5.0. The development, development and implementation of cyber defense requires a framework that will become a reference so that implementation can occur on an ongoing basis and its performance can be measured at any time. This need is met by developing a framework that includes policies/regulations, institutions, technology and human resources.

The Indonesian government has taken many ways to deal with incoming cyber attacks such as the establishment of the National Cyber and Crypto Agency (BSSN). BSSN was formed based on Presidential Decree No. 53 of 2017. A non-ministerial government institution that is under and responsible to the President. It is a strengthening of the National Crypto Agency coupled with Dit. Information Security, Directorate General of Informatics Applications, Ministry of Communication and Informatics (Perpres No. 53, 2017). BSSN functions in implementing technical policies in the areas of identification, detection, protection, countermeasures, recovery, monitoring, evaluation, control of e-commerce protection, coding, filtering, cyber diplomacy, cyber crisis management center, cyber contact center, information center, mitigation support, recovery countermeasures for cyber vulnerabilities, incidents and/or attacks.

Furthermore, in cybersecurity cooperation through the Indonesia Computer Emergency Response Team (IDCERT), the first CERT team established in Indonesia, in 1998, is an independent community-based technical coordination team to coordinate incident handling involving Indonesian and foreign parties (ID- CERT, 2015). Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). assistance/assistance to improve security and security systems in strategic agencies/institutions (critical infrastructure) in

Indonesia; coordination center (Coordination Center/CC) for domestic and foreign initiatives and as a single point of contact (ID-SIRTII/CC, 2017).

Then the improvement of cyber security technology, several cyber security technical standards have been identified. Indonesian National Standard (SNI) IEC/ISO 27001:2013 requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS) (BSN, 2016). SNI ISO/IEC 27018:2016, Information technology - Security techniques 19 - Practical guidelines for protecting personal information (PII) in a public cloud that acts as a PII processor (BSN, 2016). Trust Positive (Trust+); Workshop on healthy and safe internet use; DNS filtering Newsletter; Ministry of Communication and Informatics program (KOMINFO, 2015). Information Security Index (OUR Index). Evaluation tool for analyzing information security readiness in government agencies based on ISO/IEC 27001:2009 (Director General of Telematics Applications, 2013).

Most recently, the Agency for the Assessment and Application of Technology (BPPT) launched the 2021 Computer Security Incident Response Team (CSIRT) program with the Secure The Future mission in Jakarta, Thursday (3/6/2021). This program is the result of collaboration with the National Cyber and Crypto Agency (BSSN). The use of cyber space must be followed by three things, cyber security, maximizing the use of cyber space to advance national interests at the global level, strengthening the quantity and quality of competitive cyber space at the world level in all layers of cyberspace, both physical layers, logical and social networks.

The formation of the CSIRT is in line with the implementation of the Electronic Based Government System (SPBE), where BPPT and BSSN become a team of experts and a national coordinating team that must organize and make SPBE successful. BPPT together with BSSN, KemenPAN RB, Kemenkominfo continues to strive to build a safe SPBE, through the development of various general and special applications. Of course there will be many points of vulnerability in the system. This is where the role of the CSIRT team is needed in strengthening aspects to create resilience in SPBE. In Indonesia, the basis for cyber security is regulated in the Electronic Information Law Number 11 of 2008 and the revised version Number 19 of 2016. These regulations cover violations such as sharing illegal content, data protection breaches, unauthorized access to electronic systems. The deficiency in the ITE Law is that it does not contain important aspects of cybersecurity, such as information and network infrastructure, and resources with expertise in cybersecurity.

In 2019 the government issued Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, the existence of this PP strengthens the protection of personal data and information. The government's challenges in the current era of society 5.0 in strengthening cyber security include: the insufficient availability of technology experts and security technical experts to design and implement cyber security strategies. The risks that occur due to the cross-border nature of cyber security, which makes a country with a weak cyber security resilience strategy can disrupt the cyber security of other countries. The use of anonymization tools, for example to block chain currencies or encryption, in crimes that use the internet, further complicates policy making.

The emergence of new technologies and systems from time to time requires periodic updating of the monitoring system. The existence of new types of communication service providers who are often domiciled in other countries' jurisdictions and require different treatment compared to traditional telecommunication companies. New forms of cyber crime such as ransomware, identity theft, sexual advances (grooming) and sexual harassment through cyberspace. The need to deal with cyber attacks and other forms of interstate conflict due to the absence of internationally accepted norms and regulations governing state behavior.

Meanwhile, the challenge for the private sector and business is the difficulty in operating across jurisdictions, which means being faced with different laws, penalties and regulatory regimes. Potential for serious defamation as well as civil lawsuits if involved or responsible for a cyber security incident. Pressure to assist governments in enforcing cyber security and fighting cyber crime and terrorism, which can include creating policies and reporting content, shutting down networks, blocking services, even compromising the security of their own products to aid government surveillance. The need to build internal capacity to maintain information and network security. And in the form of incentives to maintain the confidentiality of data that can pose risks and cyber attacks in the name of data privacy and potential defamation.

CONCLUSION

Technological developments that make all threats to the national security of a country increase. Cyber attacks that are currently being faced by many countries in the world have endangered national security. Likewise Indonesia, overcoming uncertain changes requires the Indonesian government to be active in dealing with emerging attacks such as cyber attacks which are currently endangering national security. The leaked Indonesian population data has caused a lot of losses. In dealing with cyber attacks, the Indonesian government has carried out several things, namely the establishment of the National Cyber and Crypto Agency (BSSN) in 2017. Not only that, the Government has also carried out cooperation between cyber institutions to improve Indonesia's cyber security.

The Indonesian government continues to improve cyber security technology to overcome unstoppable cyber attacks. regulated in the Electronic Information Law Number 11 of 2008 and the revised version Number 19 of 2016. These regulations cover violations such as sharing illegal content, data protection violations, unauthorized access to electronic systems. The deficiency in the ITE Law is that it does not contain important aspects of cybersecurity, such as information and network infrastructure, and resources with expertise in cybersecurity. In 2019 the government issued Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, the existence of this PP strengthens the protection of personal data and information.

Recommendations in this study: in implementing the strengthening of Syber Security, Indonesia still needs a lot of improvement. Indonesia needs a legal umbrella that clearly regulates Cyber Security. As academics, it is our legal obligation to encourage the government to immediately pass the Bill on Cyber security and Resilience. The absence of a legal basis for cybersecurity affects the organizational structure that should regulate cybersecurity. In the absence of such legal basis, it becomes impossible to carry out cybersecurity practices on a national scale. This also creates confusion in coordinating responsibilities regarding cybersecurity itself. What can be done again is the increase in human resources. Human resources are one of the most important elements in ensuring the implementation of cyber security, in accordance with established policies. Special knowledge and skills must be owned and maintained in accordance with the development of conditions of security needs. Human resources are manifested in the form of recruitment, coaching and separation programs that refer to applicable regulations. International cooperation is urgently needed, related to the development and strengthening of cyber security capabilities both for infrastructure, infrastructure and in developing HR capabilities in the field of cyber security both bilaterally between the two countries and regionally or internationally. In addition, it is hoped that the increase in information technology and cyber security cooperation will open up opportunities for the development of a new media industry related to information technology in Indonesia as one part of the development of a national strategic industry.

BIBLIOGRAPHY

Carr, Madeline. 2015. Crossed wires: International cooperation on cyber Security dalam interstate journal of international affairs, 2015/2016, issue II

CSIRT, 2021. Indonesia Rugi Lebih Dari 600 trilyun Rupiah Akibat Kebocoran 279 Juta Data Penduduk.

Fikri Kurniawan. 2020. Kerugian Serangan Siber Tahun 2021 Diprediksi RP 84.000 triliun

International Telecommunication Union, 2020. Global Security Index 2020: Measuring commitment to cybersecurity. ITU Publications

IT Governance, n.d. What is cyber resilience | IT Governance UK

Kompas.com. 2019. RI Rugi Rp 478,8 Triliun akibat Serangan Siber, DPR Siapkan RUU

Lohrmann, D., 2020. 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic.

Prof. Dr. Emzir, M.Pd. 2010. Metodologi penelitian kualitatif Analisis data, PT Raja Grafindo Persada, Jakarta

Sularso, G.., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.