Anjani, Noor Halimah

Research Report

Cybersecurity Protection in Indonesia

Policy Brief, No. 9

Provided in Cooperation with:
Center for Indonesian Policy Studies (CIPS), Jakarta

Suggested Citation: Anjani, Noor Halimah (2021) : Cybersecurity Protection in Indonesia, Policy Brief, No. 9, Center for Indonesian Policy Studies (CIPS), Jakarta

This Version is available at:
https://hdl.handle.net/10419/249442

CIPS
Center for Indonesian Policy Studies

POLICY BRIEF

March 2021

shutterstock/Aleksandar Grozdanovski

Policy Brief No. 9

Cybersecurity Protection in Indonesia

by Noor Halimah Anjani

Key Messages

- In 2019, the Indonesian National Cyber and Crypto Agency (BSSN) reported 290 million cases of cyberattacks. That was 25% more than the previous year, when cybercrimes had caused losses of USD 34.2 billion for Indonesia. The Covid-19 pandemic in 2020 triggered a significant increase in phishing attacks, malspams and ransomware attacks, adding to the urgency of establishing a well-functioning infrastructure for cybersecurity in Indonesia.

- Indonesian cybersecurity laws and regulations created fragmented responsibilities across different ministries and they remain ineffective in preventing cyberthreats and cybercrime. A comprehensive regulation on cybersecurity is urgently needed in Indonesia.

- The Indonesian parliament has been discussing an overarching Cybersecurity Bill but the process did not involve the private sector. As a result, the Bill contained provisions that were overly cumbersome and costly for businesses, requiring certifications, accreditations, and approval from BSSN for developing services and products. Local content requirements added further risks to Indonesia's cybersecurity. The Bill was heavily criticized and later withdrawn from the parliamentary agenda in 2020 and 2021.

- A revised Cybersecurity Bill should clearly define and delineate the roles, responsibilities, and authorities of relevant institutions in addressing cybersecurity threats.

- The Indonesian parliament and BSSN should engage in a Public-Private Dialogue (PPD) when deliberating the bill. Engaging in PPD has proven to help sharing relevant information and experiences and producing sensible and workable policies supported by a broad base of stakeholders.

The State of Cybersecurity in Indonesia

In the past decade, the development of information and communication technology (ICT) has positively contributed to global economic growth and has been linked to higher productivity, competitiveness, and citizen engagement (Setiadi, Sucahyo, & Hasibuan, 2012). However, as government agencies, businesses, and society are more than ever connected in cyberspace, new challenges posed by cyberthreats require more attention to develop robust cybersecurity.

Cybersecurity consists of the practice, actions, and measurements that protect the cyber environment and the assets of organizations and users from malicious attacks that aim to undermine the confidentiality, integrity, and availability of information or data (Fischer, 2005; ITU, 2012). Assets include, but are not limited to, connected computing devices, critical infrastructure, servers, networks, and information stored or transmitted in the cyber environment. Considering that interactions in cyberspace depend on the availability, integrity, and confidentiality of information, the protection of information and digital facilities and infrastructure becomes ever more important.

Cyberthreats are actions that may or may not occur but potentially cause serious problems to the computer network or system. Everyone can be affected. Computerized components are part of the government's critical infrastructure and are prone to hackers and become the target of cyberattacks. Minor disruption to the system's performance can lead to significant economic losses (Kovacevic & Nikolic, 2015; Tabansky, 2011). For businesses, intellectual property theft as well as security and data breaches are common threats the companies need to address. Individuals need to be aware of risks concerning data theft and the spread of malicious software and viruses. (Bendovschi, 2015).

The Indonesian National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN) reported 290.3 million cases of cyberattacks in 2019. The number significantly increased compared to the 232.4 million cases during the previous year. Likewise, the Criminal Investigation Agency of the Indonesian National Police (Bareskrim) saw an increase in police reports of cybercrimes. 4,586 police reports were filed on *Patrolisiber*, a Bareskim website for reporting cybercrime, in 2019. An increase from 4,360 reports in 2018 (Patrolisiber, 2020). A cyberattack is an attack on a computer system or computer network to gain unauthorized control or access to the computer system (Maurer & Morgus, 2014; Marshall & Saulawa, 2015). Cybercrimes, on the other hand, are illegal activities that use and target computer systems or networks (ITU, 2012) to cause tangible or intangible losses for those targeted (Wilson, 2008). Not all cyberattacks are legally defined as a crime, but both cyberattacks and cybercrimes are considered cyberthreats.

The damage of cyberattacks and cybercrimes depend on the nature of the victims. For corporate victims, cyberattacks and cybercrimes cause economic losses in the forms of reduced profit, loss in market value, lawsuits, and reputational damage. For individual victims, losses from cyberattacks and cybercrime cause stress and psychological effects, identity theft, and financial harm (Acquisti, Friedman, & Telang, 2006; Agrafiotis et al., 2018; Telang & Watel, 2007;). Microsoft and Frost & Sullivan (2018) reported that, in 2017, cybersecurity incidents caused economic losses of approximately USD 34.2 billion in Indonesia. The calculation includes losses that are: direct – financial losses from productivity loss, fines, and repair costs; indirect – lost opportunities since companies had to rebuild relationships with consumers after a reputational damage; and induced - the cybersecurity incident had an impact on the broader ecosystem and economy and caused a decline in the number of customers and revenues (Microsoft & Frost & Sullivan, 2018).

Changed consumption behaviours due to large-scale social restrictions (*Pembatasan Sosial Berskala Besar* or PSBB) imposed during the Covid-19 pandemic have accelerated Indonesia's digital transformation. The Ministry of Communication and Informatics (MOCI) reported 40% more internet users during the implementation of PSBB between March 2020 to April 2020 (MOCI, 2020). During the pandemic, 70% of Indonesian consumers have tried at least one new digital service, such as online groceries, digital entertainment, online learning, and work from home software, according to a report by the Mobile Marketing Association (2020), an association of companies producing, selling and marketing digital products. The increase in internet traffic has also attracted malevolent actors and led to more cases of cyberattacks in Indonesia. From January to April 2020, approximately there is 88 million cases (BSSN, 2020) involving phishing[1] attempts, malware attacks[2], and information gathering[3]. There is an urgency for robust laws and regulations to ensure the safety and security of cyberspace.

[1] Phishing is an attempt to gain personal and sensitive information such as usernames, passwords, and credit card numbers. The attacker masquerades as a trusted entity, tricks a victim into opening an email, instant message, or text message that contains a malicious link.
[2] Malware attacks use malicious programs or codes to interfere or gain unauthorized access to the normal operations of a computer system. Usually, malware programs have been designed for financial gains.
[3] Information gathered from victims or systems is not sensitive or personal like in phishing attempts. Instead, attackers gather information like phone numbers, pet names or school names, that can be used for guessing passwords or other attacks.

Regulations for Indonesia's Cybersecurity

The legal basis for regulating cybersecurity in Indonesia is the Electronic Information and Transactions Law No. 11/2008 and its revised version Law No.19/2016 (EIT Law). The EIT Law covers several offences, such as distributing illegal content, breach of data protection, unauthorized access to another computer system to gain information, and an illegal and unauthorized interception or wiretapping of other computer systems or electronic systems. The EIT Law provides legal protection for content of electronic systems and electronic transactions. However, the EIT Law does not cover important aspects of cybersecurity, such as information and network infrastructure, and human resources with expertise in cybersecurity.

Based on the EIT Law from 2016, the government issued technical regulations in Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions (GR 71/2019). GR 71/2019 contains updates related to the implementation of cybersecurity in electronic systems and transactions. Apart from several articles related to the offences regulated by the EIT Law, GR 71/2019 contains stronger provisions regarding the protection of personal data and information and website authentication to avoid fake, fraudulent or scam websites. Besides, GR 71/2019 also emphasizes the need for the government to prevent any harm to public interests through the misuse of electronic information and electronic transactions and the need to develop a national cybersecurity strategy. However, GR 71/2019 covers only cybercrimes that are related to electronic transactions, such as the misuse of data, unauthorized electronic signatures, and the spread of malicious viruses and codes. The limited coverage of the EIT Law and GR 71/2019 provide an inadequate response to everchanging cyberthreats, particularly those to the government's critical infrastructure.

To deal with cyberthreats to the national security, the Ministry of Defence (MOD) Regulation No. 82/2014 provides cyber defence guidelines. It is the only regulation that provides a definition of cybersecurity: National cybersecurity comprises all efforts to secure the information and the supporting infrastructure at the national level from cyberattacks. Any words or actions done by any party that threaten national security, national sovereignty, and territorial integrity are considered cyberattacks. Unlike the EIT Law, the regulation covers critical infrastructure of, for example, the financial and transportation systems as objects of cybersecurity. However, the regulation only serves to develop military cyber defence capacities, developed and implemented by the Ministry of Defence for the National Armed Forces (TNI). For non-military cyberthreats, it refers to other regulations, such as the EIT Law.

Attempts to Pass a Cybersecurity Bill

Existing policies and regulations for cybersecurity remain fragmented across different ministries. Due to the lack of an umbrella law for the entire regulatory framework, sectoral responsibilities remain uncoordinated (Aprilianti & Dina, 2021; Rizal & Yani, 2016). There is a risk that this situation causes an inadequate government response to increasing cyberthreats.

Responding specially to increasing cyberthreats to the government's critical infrastructure, the House of Representatives (DPR) and BSSN drafted a bill to serve as the umbrella for all cybersecurity laws and regulations in Indonesia. This Cybersecurity and Cyber Resilience Bill (*Rancangan Undang-Undang Keamanan dan Ketahanan Siber* or Cybersecurity Bill) was initiated by the Legislative Body (*Badan Legislasi*) of the DPR in May 2019 and was supposed to be passed into law in September 2019. It would have made Indonesia the fourth ASEAN member with a cybersecurity law besides Singapore, Malaysia, and Thailand.

As of May 2020[4], the Cybersecurity Bill contained 77 articles, which addressed the implementation of cybersecurity, cybersecurity governance, cybersecurity services, the role of BSSN, cyber diplomacy, and law enforcement. Compared to others laws and regulations, the Cybersecurity Bill covered several important cybersecurity aspects, such as critical infrastructure, the development of cybersecurity technology in Indonesia, and criminal sanctions for violators. The Cybersecurity Bill also aimed to fill the void left by the EIT Law regarding the protection and security of information and network infrastructure, and human cybersecurity resources.

The Cybersecurity Bill mandated BSSN to coordinate efforts for developing a cybersecurity strategy by collaborating with other government institutions, such as the Ministry of Communications and Informatics (MOCI), the State Intelligence Agency (BIN), the Indonesian National Police (POLRI), and the Indonesian National Armed Forces (TNI). However, the Bill did not delineate between authorities and responsibilities of BSSN and other government institutions in protecting cybersecurity. Article 38 stated that BSSN shall filter electronic content and applications containing harmful content to protect the safety of the community when using electronic applications. Filtering content and applications are currently under the mandate of MOCI. Article 38 did not regulate the coordination between BSSN and MOCI to filter content, and there are no detailed criteria regarding what constitutes harmful content.

Aside from not delineating authorities between BSSN and relevant government institutions, business associations have been criticizing Articles 4 and 8 for limiting the involvement of the private sector and its associations in cybersecurity issues (Wibowo, 2019). Article 4 of the Bill stated that cybersecurity will be implemented by state institutions, the central government, local governments, and the society. According to Article 8, society can be involved in the implementation of cybersecurity when protecting electronic systems in their internal organizations or when providing services for cybersecurity. However, the use of the word "society" appears broad and may not be interpreted to specifically include all stakeholders in the private sector.

[4] May 2019 version is available at http://institute.id/wp-content/uploads/2019/09/RUU-Keamanan-dan-Ketahanan-Siber.pdf

Moreover, the Bill did not differentiate between digital infrastructure or applications that require different levels of security. Government Regulation No. 80/2019 on Trading through Electronic System at least addressed differences between government and private applications. Similarly, MOD Regulation 82/2014 has also laid out objects and infrastructure that need to be secured within the cyber defence framework. Far from further developing different security levels within the public or the private sector, a differentiation was not made by the Cybersecurity Bill at all.

In general, cybersecurity rules need to acknowledge the importance of the private sector in disseminating and protecting information, developing methods and operations to control technology, as well as ways to configure the functions of electronic devices (Gallaher, Link, & Rowe, 2008). Therefore, cybersecurity regulations should not generally limit the assessment and enforcement of cybersecurity, but instead include all relevant stakeholders in safeguarding cybersecurity of sensitive objects and infrastructure. Cybersecurity regulations need to differentiate and address the needs of the public and private sectors, identify the specifically required level of cybersecurity, and keep up with technological developments and new arising threats.

As it were, the Cybersecurity Bill lacked input from other government institutions and, in September 2019, the DPR concluded that the Cybersecurity Bill would not be passed into law and the discussion of the Bill started anew. Initially, the DPR had included the Bill in the National Legislative Plan (Prolegnas) 2020, but it was later dropped (DPR, 2020). Without any substantial revisions it was also not included in the Prolegnas 2021. Instead, the DPR added the Cybersecurity Bill to their Medium-term Prolegnas for the legislative period 2020 - 2024.

Closed Policy-Making Process of the Cybersecurity Bill

After discussions of the Bill were initiated in May 2019, the academic research for the Bill was uploaded for public viewing by the DPR in June 2019[5]. While the academic paper was made available to the public, the Cybersecurity Bill itself was never uploaded to the internet. This led to an online petition[6] criticizing the closed policy-making process. The petition called for postponing the Cybersecurity Bill and requested involving the private sector and the academia in the deliberations. The Bill had also not involved relevant government institutions, such as MOCI and National Development Planning Agency (Aprilianti & Dina, 2021).

The closed policy-making process and the exclusion of the private sector resulted in articles that potentially hinder innovation and the development of cybersecurity services and products. Articles of the Bill stipulated certification requirements for businesses that plan to develop cybersecurity services and products for the government procurement process. However, these requirements might have duplicated requirements already stated in other laws and regulations. Article 17 of the Bill required businesses to get BSSN certifications for the products they want to offer for cybersecurity. Articles 19 and 21 required that human cybersecurity resources need to meet BSSN standards and acquire certifications from organizations accredited by BSSN. It remained unclear whether these certifications were the same as those stipulated by the ITE Law under the mandate of MOCI. If they had not been identical, the Bill would have added compliance costs for the private sector and created redundancies of these certifications. This would have disproportionately affected small and medium-sized enterprises with less institutional compliance capacities.

Smaller companies will also be affected by BSSN Regulation No. 8/2020 on Security Systems in the Implementation of Electronic Systems, which was issued in December 2020. It is a technical regulation requested by Article 24 of GR 71/2019. BSSN Regulation No. 8/2020 lays out the need for operators of electronic systems (public and private) to ensure the safety of their information management. The regulations require electronic system operators to employ an individual security expert (local or foreign) or a consulting agency to oversee the implementation of their electronic systems. However, there is no explanation of what qualifications these experts or agencies need according to BSSN standards. The draft of the Cybersecurity Bill followed the same requirement and did not elaborate on the required expertise.

Besides those product certifications, Article 48 of the Cybersecurity Bill mandated BSSN to issue permits for conducting research on, or testing cybersecurity applications. This added further confusion as the article did not determine which activities in research or testing of cybersecurity require a permit from BSSN.

Finally, article 66 of the Cybersecurity Bill required businesses to meet local content requirements, more specifically, a domestic component level (TKDN) of 50%. Since most businesses use foreign hardware and software in their products and services, the required 50% TKDN would have affected the development of cybersecurity products and services in Indonesia.

[5] The academic draft of the Cybersecurity Bill can be accessed at http://dpr.go.id/doksileg/proses1/RJ1-20190617-025848-5506.pdf.
[6] The petition can be accessed at https://www.change.org/p/dewan-perwakilan-rakyat-tolak-ruu-kks-ruu-kks-bermasalah

All mentioned articles appeared to contradict the aim of increasing cyber competitiveness and innovation through cyber utilization that is free, open, and responsible as stated in Article 3 (b) of Cybersecurity Bill. This aim can only be achieved in a meaningful dialogue with all relevant stakeholders from the corporate sector, the academia and the civil society.

Transparency is one of the principles established by Law No. 12/2011 on the Formulation of Law and Regulations in Indonesia. It is being manifested by disseminating the draft law to inform the public and to get input from the public and relevant stakeholders. Besides, the public has the right to provide input orally and in writing in the legislative process. The law also lays out several ways for the public to give input, including public hearing meetings, work visits, socialization, seminars, workshops, and discussions. The closed policy-making process of the Cybersecurity Bill was criticized for not complying with this law.

Policy Recommendations

Including relevant stakeholders in the process of policy-making is an important step. The government can opt for a multi-stakeholder approach through Public-Private Dialogue (PPD) that addresses problematic and challenging policy issues (Shear, Schnidrig, & Kaspar, 2018). Governments that engage in PPD have proven to produce sensible and workable reforms. Simultaneously, a private sector that was engaged in PPD is more likely to support the enforcement of a policy (Bannock, 2005; Herzberg & Wright, 2005).

In cybersecurity, the private sector is not only a victim of cyberattacks but also the responder. Many companies have developed solutions to mitigate cyberattacks that can benefit society. During the Covid-19 pandemic, personal computers and the software being used for work and learning from home have been subjected to such attacks (Bahsi & Karabacak, 2020). Technological companies have adapted to the new situation by improving the security of their products and services. Companies that offer cloud-based services have improved their security to assure their consumer of the safety of their data. Companies that offer video-conferencing software are continuously updating their products with security and privacy improvements.

Cybersecurity is a critical issue and affects not only the government but also the private sector and the society as a whole. Private sector expertise can inform the government about the latest cybersecurity technologies and allows for the robust sharing of knowledge between the government and the private sector. It will benefit the government during the creation and implementation of cybersecurity policy. Ignoring the private sector leads to an inadequate cybersecurity response (Llorente, 2018).

The dialogue between the public and private sectors should focus on developing a national cybersecurity framework. Establishing online platforms to collect input may be practical, especially during the current pandemic. It is vital that this framework serves as an umbrella for existing regulations and inspires the DPR and BSSN to continue focussing on the improvement of the Cybersecurity Bill.

Furthermore, the Cybersecurity Bill needs to clearly define cybersecurity and delineate between the roles, responsibilities, and authorities of relevant government institutions. This will allow BSSN to coordinate all cybersecurity efforts of the relevant government institutions.

References

Acquisti, A., Telang, R., & Friedman A. (2006). Is there a cost to privacy breaches? An event study. *Proceedings of the 3rd International Conferences on Intelligent System.*

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding hot they propagate. *Journal of Cybersecurity,* 4(1). 1-15. Doi: 10.1093/cybsec/tyy006

Aprilianti, I., & Dina, S. (2021). Co-regulating the Indonesian digital economy. *Center for Indonesian Policy Studies*. Retrieved from: https://repository.cips-indonesia.org/publications/332998/co-regulating-the-indonesian-digital-economy

Badan Siber dan Sandi Negara. (2020). Rekap Serangan Siber (Januari – April 2020). Retrieved from: https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Badan Siber dan Sandi Negara. (2020). Indonesia cyber security monitoring report 2019. Retrieved from: https://bssn.go.id/laporan-tahunan-2019-pusopkamsinas-bssn/

Bahsi, H., & Karabacak, B. (2020). Covid-19 pandemic crisis and its implication on Cybersecurity. *Information Security Journal: A Global Perspective*. Retrieved from: https://think.taylorandfrancis.com/special_issues/covid-19-cybersecurity/#?utm_source=CPB&utm_medium=cms&utm_campaign=JPG15743%20

Bannock Consulting Ltd. (2005). Reforming the business enabling environment, mechanism, and processes for Private-Public Sector Dialogue. Retrieved from: http://ppd.cipe.org/global-workshops/workshop-2006/reforming-the-business-enabling-environment-mechanisms- and-processes-for-private-public-sector-dialogue/.

Bendovschi, A. (2015). Cyber-attacks – trends, patterns, and security countermeasures. *Procedia Economics and Finance,* 4. 24-31. Doi: 10.1016/S2212-5671(15)01077-1

Dewan Perwakilan Rakyat. (2020). Program Legislasi Nasional Prioritas. Retrieved from: https://www.dpr.go.id/uu/prolegnas

Frost & Sullivan. (2018). Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar. Retrieved from: https://news.microsoft.com/id- id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi- di-indonesia-sebesar-us34-2-miliar/

Gallaher, M., Link, A., & Rowe, B. (2008). Cyber security: Economic strategies and public policy alternative. Cheltenham, England: Edward Elgar Publishing.

Herzberg, B., & Wright, A. (2005). Competitiveness partnership: Building and Mantaining Public-Private Dialogue to Improve the Investment Climate. A resource drawn from 40 countries experience. *International Finance Corporation (IFC).*

Internet Development Institute. (2019). Tolak RUU KKS! RUU KKS Bermasalah! *Change.org*. Retrieved from:https://www.change.org/p/dewan-perwakilan-rakyat-tolak-ruu-kks-ruu-kks- bermasalahIndonesia Criminal Investigation Agency. (2020). Statistik jumlah Laporan Polisi yang dibuat masyarakat. Retrieved from: https://patrolisiber.id/statistic

International Telecommunication Union. (2012). Understanding cybercrime: phenomena, challenges, and legal response. Retrieved from: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Kementerian Komunikasi dan Informatika. (2020). Penggunaan Internet Naik 40% Saat Bekerja dan Belajar dari Rumah. Retrieved from: https://www.kominfo.go.id/content/detail/25881/penggunaan-internet-naik-40-saat-bekerja-dan-belajar-dari-rumah/0/berita_satker

Kovacevic, A., & Nikolic, D. (2015). Cyber-attacks on critical infrastructure: Review and challenges. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance.* 1-18. Doi: 10.4018/978-1-4666-6324-4.ch001

Llorente, R. (2018). A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity. *LSE IDEAS*.Retrieved from: https://lseideas.medium.com/a-digital-geneva-convention-the-role-of-the-private-sector-in-cybersecurity-cd96ecd70622

Marshall, J., & Saulawa, M. (2015). Cyberattack: the legal response. *International Journal of International Law*, 1 (2) . 1-18. Retrieved from: http://www.ijoil.com/wp-content/uploads/2015/04/CYBER-ATTACKS-ACCEPTED-JOURNAL-1.pdf.

Maurer, T., & Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. *New America Research Report.*

Mobile Marketing Association. (2020). Impact of Covid-19 on Consumer Behaviour in Indonesia. Retrieved from: https://www.mmaglobal.com/indonesia/node/34611

Rizal, M., & Yani, Y. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, 4 (1). 61-78.

Setiadi, F., Sucahyo, Y., & Hasuban, Z. (2012). An overview of the development Indonesia's national cybersecurity. *International Journal of Information Technology & Computer Science*, 6. 106 - 114.

Shears, M., Schnidrig, D., & Kaspar, L. (2018). Multistakeholder Approaches to National Cybersecurity Strategy Development. *Global Partners Digital*. Retrieved from: https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

Tabansky, L. (2011). Critical infrastructure protection against cyber threats. *Military and Strategic Affairs*, 3 (2). 61-78. Retrieved from: https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1326273687.pdf.

Telang, R., & Wattal S. (2007). An empirical analysis of the impact of software vulnerability announcement on firm stock price. *IEEE Transactions on Software Engineering*, 33. , (8). 544 - 557. Doi: 10.1109/TSE.2007.70712

Wibowo, S. (2019). Membongkar borok RUU Keamanan dan Keatahan Siber. *CNNIndonesia*. Retrieved from https://www.cnnindonesia.com/teknologi/20190905204826-186-427990/membongkar-borok-ruu-keamanan-dan-ketahanan-siber

Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress. *Congressional Research Service*.

ABOUT THE AUTHOR

Noor Halimah Anjani specializes on the topics of agriculture and the digital economy in CIPS. Prior to joining CIPS, she worked as a research assistant at Universitas Katolik Parahyangan on women migrant workers and their financial remittances for poverty alleviation. She has published articles on international affairs, such as the Belt and Road Initiative of the Chinese government.

She graduated with a Bachelor's degree in International Relations at Universitas Katolik Parahyangan and she is an alumnus of the CIPS Emerging Policy Leaders Program (EPLP) 2020.

CIPS
Center for Indonesian Policy Studies

The Center for Indonesian Policy Studies (CIPS) is dedicated to providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

As a strictly non-partisan and non-profit think tank, CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allow Indonesia to prosper.

Center for Indonesian Policy Studies

contact@cips-indonesia.org

Jalan Terogong Raya No. 6B Cilandak,
Jakarta Selatan 12430, Indonesia

www.cips-indonesia.org

Our works relies on your support. Visit
www.cips-indonesia.org/donate
to support CIPS.