Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP)

Pradipta Nindyan Saputra, Arfin Sudirman, Obsatar Sinaga, Wahyu Wardhana, Nurul Hayana

Nowadays, a number of countries are developing alternative approaches to handling their cybersecurity, including Indonesia. Badan Siber dan Sandi Nasional (State Cyber and Cryptography Agency (BSSN)) as an institution appointed by the Indonesian government to be the national cybersecurity coordinator has the responsibility to securing the national critical information infrastructure (IIKN). The IIKN responsible for governmental and private infrastructures including the energy, transportation, finance and banking, information and communication technology, defense and strategic industries, and health sectors. This study tries to investigate how the complex nature of cyberspace, as well as the complexity of public-private relations in securing cyberspace, might be solved through a Public-Private Partnership (PPP) approach. By using qualitative methods based on the main data sources of interviews and supported by books, journals, articles, and internet sources, this study tries to find out whether the PPP on Cybersecurity can be used as an alternative approach in building Indonesia's cybersecurity architecture. It also examines the challenges that arise in the implementation of PPP, especially related to formal agreements and frameworks and informal cooperation between the government and the private sector related to cybersecurity, given the sensitivity of the issue of cybersecurity in Indonesia.

Pradipta Nindyan Saputra, Arfin Sudirman, Obsatar Sinaga, Wahyu Wardhana, Nurul Hayana. Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International and Security Studies* 13, no. 4: 104–120.

Keywords: public-private partnership, cyber security, Indonesia.

Based on the Kapersky Lab report cited by CNN Indonesia and Liputan6, there were more than 50 million cyber threats that attacked Indonesia during 2018. The threat number increasing around 240 percent compared to 2017 (CNN Indonesia, 2019; Liputan6, 2019). According to Kapersky Lab, most of the detected threats came from private users (77.12 percent), while the rest (22.88 percent) of it came from business users. This fact also puts Indonesia as one of a country with the 20th most cyberattacks in the world (CNN Indonesia, 2019; Liputan6, 2019).

This source also explained that the escalation of cyberattacks between 2017 and 2018 came from various potential factors, ranging from the threat of mobile, trojan banking, adware, riskware, and malware (CNN Indonesia, 2019; Liputan6, 2019). Almost in line with this Kapersky Lab report, the BSSN (State Cyber and Cryptography Agency) also reported that from 2018 to May 2019, Indonesia had experienced around 232,447,974 attempts at cyberattacks with 122,435,215 types of malware attacks and 16,939 types of website incidents, including Trojan-activity with an indication of 1.9 million attacks (Badan Siber dan Sandi Negara, 2019b). BSSN reminding that this was a very worrying cause of the attacks that might be initiated by state actors targeting national critical information systems and infrastructures (Badan Siber dan Sandi Negara, 2019b).

In this era where almost all critical infrastructures in all countries have been digitalised, the potential of vulnerability from connected networks increased significantly. In many cases, cyber threats are aimed at the national critical infrastructures to disrupt the economic, political, defense and security sectors of a country (Kementerian Pertahanan Republik Indonesia, 2014: 1; Sutrisno, 2016: 55). Though most of the threats to cyberspace still dominated by non-state actors (hackers, terrorists, and transnational organised crime), it does not rule out the possibility of being organised by one country to invade other countries. Therefore, many countries then pay great attention to the potential impacts arising from cyber threats (Putra et al., 2018; Tréguer, 2015).

The vulnerability in cyberspace and connected networks was addressed by several countries by establishing an advanced cybersecurity mechanisms. Some countries have special agencies to handle cyber problems in the defense and security of their countries (Soewardi, 2013:

33-34). The establishment of any cyber agencies by countries and organisational entities is quite reasonable, considering that several times ahead, the security threats will not only come through conventional ways but also in the form of cyber threats in cyberspace. Some scholars have predicted that the cyber domain will be one of the main focuses that significantly influencing a country's security strategy (Rubens, 2010; Wells, 2016).

The Indonesian government also pays attention to this potential threat. Therefore in 2017, through the Presidential Regulation Number 53 of 2017 (Peraturan Presiden No. 53 tahun 2017) which was later revised by the Presidential Regulation Number 133 of 2017 (Peraturan Presiden No. 133 tahun 2017), the government established Badan Siber dan Sandi Negara (BSSN) (State Cyber and Cryptography Agency). This agency is responsible for the detection and identification, monitoring and control, protection, and prevention and recovery of the National Critical Information Infrastructure (IIKN) (Tumpal, 2019). Apart from being one of the implementations of the national cybersecurity strategy, the establishment of the BSSN is also in line with the mandate of the UN General Assembly Resolution 70/237 of 2015 concerning the creation of a secure cyber ecosystem to protect national and international critical information infrastructure (UN General Assembly, 2015).

Although the Indonesian government has initiated a national cybersecurity strategy and has run short and long-term programs, in its implementation there are still various challenges and obstacles. One of the challenges and obstacles in implementing a national strategy for cybersecurity is the limited resources owned by the government in developing an independent cybersecurity system while on the other hand there is no comprehensive collaboration between the government and the private sectors. Cyber security is an ecosystem where the legal aspects, organisation, implementation, and cooperation must proceed in harmony to obtain effective results.

This is certainly important because as mandated by the Constitution, the responsibility for maintaining state security is a shared responsibility of all elements of society, not just the responsibility of the government. Based on the mandate of the Constitution and reflecting the implementation of national cybersecurity strategies in other countries, one solution to reduce the gap between the government's ability to create a cybersecurity architecture independently is by involving the

private sectors through so-called Public-Private mechanisms Partnership (PPP) (Carr, 2016). Through this approach, how to deal with cybersecurity issues are not only the responsibility of the government but also distributed to the private sectors. In some countries such as the United States and the United Kingdom, PPP is one alternative that has been taken to overcome the problem of cybersecurity. Both of these countries developed a comprehensive understanding of how policymakers (the government) and the private sectors conceptualize their respective roles in managing national cybersecurity, specifically related to roles, responsibilities and authority (Carr, 2016).

This paper tries to find out whether the PPP on Cybersecurity approach can be used as an alternative in building Indonesia's cybersecurity architecture as well as examining the challenges that arise in the implementation of PPP, especially in relation to agreements and formal frameworks also the informal cooperation between government and the private sectors related to cybersecurity, given the sensitivity of the issue of cybersecurity in Indonesia.

Literature Review

The emergence of the Public-Private Partnership (PPP) was initially related to the privatisation of government infrastructure and as a means of attracting private resources for government construction and infrastructure projects (Grimsey & Lewis, 2004). PPP then spreads to the management and provision of public government services based on the infrastructures, such as schools, hospitals, transportation, and even prison (Schneider, 1999). Over the past two decades, these developments have led to extensive international debate about the advantages and disadvantages of PPP (Bovaird, 2004), especially in relation to differing opinions about the extent to which economic efficiency must remain the main standard for assessing the benefits of PPP, or whether there are other values such as fairness, equality, or anything that can be increased or at least maintained in the context of PPP (Hodge & Greve, 2007; Reynaers, 2013)

The next debates revolve about public and private sectors' accountability, including relating to the transparency of their collective agreements outside the formal administrative structure (Forrer, et al, 2010). Although there are many efforts to standardize PPP by international organisations (Commission of the European Communities, 2004; United Nations, 2008), in the end, it must be recognised that differ-

ent political, economic, cultural traditions or social values will affect each countries judgment to PPP (Hurk, et al, 2015). The General PPPs are usually based on explicit or formal agreements, which assigned private sector actors the responsibility to provide public services, new construction projects, and maintaining existing infrastructure. The general PPP also stipulates appropriate division of responsibilities, profit-sharing arrangements, and risk sharing to align the interests of rational actors who tend to be selfish (Sarmento & Renneboog, 2016).

However, general or standard PPP contracts cannot address other potential problems, especially in high-risk projects or those related to long-term partnerships, thus requiring flexibility, learning, and adaptability over time (Hurk & Verhoest, 2016). Some literature shows that trust-based relationships and the use of government and private capacity synergy beyond cost considerations become the most central feature in PPP (Brinkerhoff & Brinkerhoff, 2011). Although often factors of cost and efficiency considerations are the main drivers of PPP formation, risk transfer mechanisms from the government to the private sector are common in many countries. The main benefit of involving the private sector in PPP is related to the fact that the government cannot always and must expend its resources. That then a substantial risk transfer to the private sector will subsequently be partly converted in the form of profits for the private sector (Bossong & Wagner, 2016).

In the context of cybersecurity, the majority of current discussions about security in cyberspace are largely concerned with the need for certain limitations of government action in dealing with decentralised cyberspace and owned or operated by the private sector, both individuals and corporations (Eriksson & Giacomello, 2009). Not surprisingly, questions related to governmental authority and the authority in the cyberspace then emerged to the surface, especially in the context of cybersecurity. A more decentralised cyberspace is under enormous pressure since it then raises structural vulnerability because all actors in cyberspace tend to have broad access in cyberspace (Mueller, et al, 2013). More perpetrators of crime in cyberspace increasingly exploit this vulnerability. This then becomes a kind of call for multidimensional and coordinated governance approaches to improve security in cyberspace (Solms & Niekerk, 2013).

To create good cybersecurity architecture, government and private actors need to be involved with each other (Tropina, 2015). This is reflected in a growing number of policy initiatives and government

declarations that underline the PPP mechanism to enhance or provide cybersecurity. Such partnerships are also an important factor for translating broad or ambiguous cybersecurity conceptions (Min, Chai, & Han, 2015). Furthermore, it seems impossible or realistic to unravel the level of functional interdependence between the government and the private sector in the context of the geographical expansion of security governance networks, especially in the cyber field. On the contrary, what needs to be clarified is how to improve understanding and conceptualization of various forms and types of PPPs in the field of cybersecurity because, for some people, the ideal type of PPP is to focus on providing operational infrastructure, service delivery or policy implementation in a broad sense. Though not only limited to that, PPP will also provide benefits from formal agreements that distribute benefits or benefits, and of course a clear risk distribution (Bossong & Wagner, 2016, p. 2).

Concerning to cybersecurity, the cyber sector does show different characteristics, which can explain the confusion for some people about the possible meaning of PPP in cyberspace. In particular, cybersecurity is at various levels, ranging from infrastructure issues to content management in cyberspace, including the provision of software and others. This is what distinguishes PPP in public infrastructure from PPP in cybersecurity (Bossong & Wagner, 2016).

Perhaps the case of implementing PPP in the European Union and the United States can be considered as an example of a representative, relatively transparent and significant implementation of PPP in cybersecurity (Bossong & Wagner, 2016, p. 2). The EU is noted to have two institutions or centers that can participate in administrative or operational aspects of cybersecurity, namely the European Network Information Security Agency / ENISA (European Network Information Security Agency) and the EC3 Cybercrime Center (EC3 cybercrime center) at EUROPOL. The two institutions have different functions. ENISA builds partnerships to improve the technical reliability and resilience of cyberspace or critical information infrastructure that is in private hands. In contrast, EC3 is looking for more operational exchanges with cybersecurity companies to tackle complex cyber threats and crime, such as botnets, in a more proactive way. Besides, EC3 and its host agency EUROPOL are also trying to expand voluntary mechanisms to control internet content with the private sector, which has recently led to the so-called Internet Referral Unit. The two EU cyber-

security institutions can be considered as variants of the broader PPP pattern for cybersecurity (Bossong & Wagner, 2016, p. 3).

Almost in line with the European Union, the United States also implements PPP in national cybersecurity, specifically to enhance the protection of its national critical information infrastructure. Based on Executive Order 13636, it was determined that the Ministry of Homeland Security, Justice, National Information and Defense voluntarily share information about cyber threats to the private sector. Then, the US Department of Homeland Security plays the role of coordinator in forming consultative groups on cybersecurity, especially in the critical information infrastructure sector with all stakeholders. Finally, under the leadership of the National Institute of Standards and Technology (NIST), a Basic Framework was established to reduce the risk of cyber threats to the critical information infrastructure developed (Min et al., 2015).

What often arises when approaching security issues including cybersecurity through PPP is the classic debate about whether PPP relates to binding regulations and regarding the distribution of obligations versus consideration of economic problems (Héritier, 2001). Even though far beyond that, PPP in the context of security also deals with corporate social responsibility, the openness of coordination methods, also includes speed, flexibility, reach, and support of all parties involved (Graz & Nolke, 2007; Harcourt, 2013). This is because the cyber realm continues to present special challenges in terms of technical complexity, rapid changes, diverse actors and also transnational interdependence so policymaking in a conventional way will tend to experience obstacles if it is not equipped with an alternative mechanism. PPP then emerged as an alternative mechanism for the management of cybersecurity which in some literature grew dynamically as a "cyber co-regulation" between the government and the private sector (Marsden, 2011; Tropina & Cormac, 2015) and also often associated as a multi-governance mechanism stakeholders (Bendiek, 2012; Carr, 2015; Chenou, 2014). Therefore, it cannot only limit the term PPP to a general level but must be understood in the light of the complex characteristics of cybersecurity in order to understand forms of partnerships between government and private in the context of cybersecurity.

Method

At the international level, many countries base their national cybersecurity architecture on a Public-Private Partnership (PPP) approach.

Some examples include the United States (US), Britain, Canada, Finland, Estonia, and Australia (Carr, 2016, p. 45). In a number of studies, this approach has proven successful as a national security cornerstone of these countries. When many countries already have their strong cybersecurity architecture, in fact, there are still many countries that do not yet have a strong cybersecurity architecture, one of which is Indonesia, Indonesia is an important case because they only in 2017 ago had a special cyber body known as ***State Cyber and Cryptography Agency*** (BSSN). During the next two years, there has not been a strong legal corridor underpinning BSSN in building national cybersecurity architecture, so there is still an impression that the role of BSSN has not been maximised and tends to run in place. This is evidenced by the still perched Indonesia as twenty major countries with the highest number of cyberattacks in the world (CNN Indonesia, 2019; Liputan, 2019). Based on this, this article focuses exclusively on Indonesia's cybersecurity strategy, including the potential of PPP, which was later developed as an alternative approach in building national cybersecurity architecture.

A number of informal interviews with representatives from the government and private sectors were conducted over 8 months. Representatives from the Indonesian government sector, who are responsible for national cybersecurity, were asked to comment on how much potential power the government has to manage cybersecurity independently. Then what problems they have observed and identified when the government tried to address the cybersecurity sector independently, including later they were asked to comment on how PPP can be applied on sensitive issues such as cybersecurity, and how effective PPP is in terms of cybersecurity when it is then applied, particularly in the protection of the National Critical Information Infrastructure (IIKN).

Therefore, interviews were also conducted with representatives from the private sector in Indonesia specifically how their perspectives on the distribution of cybersecurity management risks in the PPP corridor, including how they were addressing public-private relations on sensitive issues such as this. Since the sources from the private sector are reluctant to be identified, they are anonymized. The reluctance of key actors to speak openly about this issue is based on the absence of an adequate legal corridor that oversees PPP and then becomes one of the obstacles in researching this issue. Inadequate legal corridors also cause difficulties in seeing details of both formal and informal coop-

eration between the government and private sectors because they are reluctant to open fully.

Discussion

Indonesia Cybersecurity Concern

Cyber threats carry increasingly serious risks to the economy and international security, including Indonesia. This risk has a major impact on the government and private sectors. This makes cybersecurity architecture to safeguard cyber domains increasingly important as the increasing use of cyberspace in Indonesia (Heinl, 2013). Safeguarding this cyber domain certainly requires an increase in the role of the Indonesian government through comprehensive policies (Deibert & Rohozinski, 2010). However, to date, Indonesia's efforts to adopt a comprehensive cyber domain security strategy are rather slow and fragmented. The Government's efforts to protect cyber domains are important so that people can continue to benefit from cyber domains, ranging from information, e-commerce benefits, and other benefits. At the same time to protect the Indonesian people from crime in cyberspace.

At present every individual, group of individuals or transnational actors and even a country can commit crimes in cyberspace (Nye, 2014). Many criminal acts in the cyber domain that have occurred in Indonesia, including the theft of data of customers of PT Bank Mandiri Tbk in 2000 committed by persons from abroad (Purwanto, 2013). To overcome this problem, Bank Mandiri brought security experts from Eastern Europe so that this problem can be quickly resolved. In 2018, hacking of the savings balance of 87 customers of the BRI of Ngadiluwih Bank in Kediri Regency was allegedly committed by foreign syndicates (Kurniawan, 2018). In addition to hacking on bank customers, many hacking of personal data also occurs on social media such as Facebook, Instagram, and twitters. In the previous year, on May 2017, WannaCry malware attacked several hospitals in Jakarta. The attacker tricked the victim to open a rogue malware attachment. Victims are asked for payment to restore their access and data. This hack is believed to have been developed by the US National Security Agency. This attack has infected thousands of computers in nearly 100 countries (Harsono, 2019).

The threat is even more evident even more so with the cancellation of the Draft Law on Security and Cyber Resilience (RUU KKS) (Sari, 2019) which leaves its problems for the cybersecurity ecosystem in In-

donesia. Until the end of 2019, Indonesia did not yet have a cyber-legal basis of law. Quoted from Kompas, Hinsa Siburian, the Head of BSSN, said that the Cyber Security and Resilience Act is very urgent for Indonesia. Therefore, strong rules are needed to protect the community from cyberattacks that can come at any time. Hinsa added the suspicion of hacking in the event of a massive power outage on 4 August 2019 showed that the Law on Security and Cyber Resilience was urgently needed by the state to face attacks on IIKN that affected the lives of many people (Hakim, 2019).

The absence of rules at the level of the law also makes it unclear who is the leading sector to lead and overcome cyberattacks on IIKN because until now there has been no special authority given to BSSN to overcome attacks on IIKN including the deterrence mechanism and also its resolution. BSSN still only relies on Presidential Regulation No. 53 of 2017 and revised by Presidential Regulation No. 133 of 2017 concerning the establishment of BSSN. The points in the two Presidential Regulations are then operationalized by BSSN in the BSSN Regulation and the BSSN Strategic Plan for 2018-2019. One of the weaknesses of regulations that are not in the form of laws is that they are only relatively binding within, without being able to bind other parties who actually must be actively involved based on a strong legal law.

The involvement of other parties in cybersecurity in Indonesia is increasingly needed because the Government has limited ability to protect the activities of the community in cyberspace. Other entities, such as individual groups and the private sector, have similar problems. In addition to the limited ability to deal with threats in the cyberspace there is also some confusion about what must be secured in the context of cybersecurity, because there are so many private and public networks and computers that need to be secured by the government as a security provider. If the Indonesian government needs to secure all cyberinfrastructure, networks, and computers, this effort will be very difficult and require enormous and time-consuming national resources (Wardhana, 2019). This means that the Indonesian government is still an important actor in cybersecurity, but government efforts alone will face difficulties in securing cyberspace when working alone. Whereas on the other hand, the private sector has a number of capabilities in managing the cyber domain because the private sector operates the information network; provides internet services; provides information technology products and other related services. Finally, cooperation

between the state / public-private sector to secure cyberspace is needed, both through domestic and international efforts (Wardhana, 2019).

The process of establishing a cooperation framework in cybersecurity can not be denied requiring time to consider different perceptions about the specific nature of threats and the different interests of each actor in the cyber domain. Therefore, referring to the Comprehensive Study on Cybercrime published by the United Nations Office on Drugs And Crime in 2013, the handling of crime in cyberspace in Indonesia needs to prioritise aspects of crime prevention in cyberspace. Prevention of crime in cyberspace (cybercrime prevention) includes six aspects, namely: criminalization, law enforcement, procedures regarding electronic evidence, state jurisdiction in matters of cybercrime, international cooperation in matters of cybercrime, and the responsibility of service providers in cyberspace (United Nations, 2013).

This collaboration brings together government stakeholders, international institutions, and private actors (Metodieva, 2018). Governments as users and the private sector as service providers must increase information sharing and approval mechanisms in dealing with cyber threats, based on building trust and mutual trust (Raduege, 2013). Indonesia can learn from the European Union, which has imposed strict requirements on online search engine providers. Meanwhile, the US government regulates several private sectors in the cyber business. The government shares limited intelligence to certain private sectors, such as the health and financial sectors to prevent cybercrime (Wardhana, 2019: 107). In short, in dealing with Indonesia's cybersecurity issues, collaboration and partnerships with other actors, especially the private sector are needed.

Public-Private Partnership

The message to involve all parties including the private sector in building national cybersecurity architecture has basically been implied in Presidential Regulation No. 53 of 2017 which was later revised by Presidential Regulation No. 133 of 2017. Article 2 states "BSSN has the task of carrying out cybersecurity effectively and efficiently by utilizing, developing and consolidating all elements related to cybersecurity". Then it is spelled out in article 3 letter "h" related to "the implementation of national, regional and international cooperation in cybersecurity matters" (Peraturan Presiden No. 53 tahun 2017, 2017; Peraturan Presiden No. 133 tahun 2017, 2017).

What is implied in the two Presidential Regulations is then to try to be implemented by BSSN through the 2018-2019 Strategic Plan for the State Cyber and Cryptography Agency (BSSN Strategic Plan). On page six of the Strategic Plan, it is stated that one of the functions of the formation of BSSN is to strengthen cooperation and coordination between Ministries / Non-Ministry Government Agencies and private parties in securing cyber. In particular, it was also mentioned that cooperation, collaboration, and roles between the government and the private sector can occur in the context of securing the National Critical Information Infrastructure (IIKN) and the realm of electronic commerce (Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019, 2019, p. 6).

BSSN then elaborated again the involvement of the private sector in building national cybersecurity architecture in the "seven stages of the themes and challenges of transformation". According to BSSN, to achieve strong national cybersecurity, BSSN must go through seven stages of themes and challenges of transformation. In the fourth stage of the theme, Acceptance and Operational, it is stated that BSSN must be able to create awareness of the need for cybersecurity in Indonesia, including the establishment of synergized and coordinated cybersecurity protocols for all Ministries / Non-Ministry Government Institutions as well as private parties (Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019, 2019, p. 7). This is very important to be implemented to the fullest to ensure that national cybersecurity operations can run smoothly.

That is, referring to Presidential Regulation No. 53 and 133 of 2017 and the 2018-2019 BSSN Strategic Plan, the possibility of implementing PPP in Indonesia's national cybersecurity is not only limited to the theoretical domain, but also at the level of practice in building a national cybersecurity architecture, particularly in the context of securing the National Critical Information Infrastructure (IIKN). This was later reinforced by information obtained from BSSN officials that currently, BSSN refers to the basic framework of the National Institute of Standards and Technology (NIST) in reducing the risk of cyber threats to the National Critical Information Infrastructure. That is, PPP canbe part of the national cybersecurity strategy.

However, the practice of implementing PPP in cybersecurity in the field faces many challenges, one of which is the awareness and acceptance of the Ministry / Institution and the private sector to the BSSN

is still relatively low so that no maximum synergy between the public and private sectors is achieved. The aspect of private sector acceptance of the public sector represented by BSSN is one of the key aspects in optimising the application of PPP in building national cybersecurity architecture. In many cases, the unclear distribution factor of cybersecurity management is often one of the reasons the private sector is reluctant to cooperate and collaborate with the government in dealing with cyber threats. As mentioned in the previous section, theoretically, some literature shows that trust-based relationships beyond cost considerations should be a central feature in PPP (Brinkerhoff & Brinkerhoff, 2011). But of course, it can only be implemented when there are strong and binding laws. Because without clear regulations, the private sector is naturally often reluctant to accept the responsibility and distribution of risks in managing national cybersecurity.

Theoretically, the classic debate about rules that remember versus economic considerations when approaching security issues through PPP is a common occurrence (Héritier, 2001). Even though far beyond general PPP, PPP in the context of security also concerns corporate social responsibility, the openness of coordination methods, also includes speed, flexibility, outreach, and support of all parties involved (Graz & Nolke, 2007; Harcourt, 2013). This is because the cyber realm continues to present special challenges in terms of technical complexity, rapid changes, diverse actors and also transnational interdependence so that policymaking in a conventional way will tend to experience obstacles if it is not equipped with an alternative mechanism such as PPP

The task of the government is to ensure that the implementation of PPP in the cybersecurity ecosystem is guaranteed and protected by strong regulations. This will stimulate the private sector to be more active in the national cybersecurity ecosystem. It cannot be denied that the resources that are often larger and more capable of being owned by the private sector than the government are an added factor for the management of national cybersecurity because the involvement of the private sector will ease the burden of the government in managing cybersecurity. In more detail, BSSN has identified a number of factors that are the basis of why the involvement of the private sector through PPP is very important in building a national cyber architecture. First, the professionalism of private-sector digital management; second, the capability of private companies in cybersecurity; and third, private sec-

tor investment in cybersecurity to ensure the smooth running of its activities.

Conclusion

The Indonesian government needs to increase its cybersecurity awareness in the face of cyber threats. In addition to awareness of Indonesian cybersecurity, Indonesia also needs to develop policies and strategies in the cyber domain. This policy can be based on international best practices and international mechanisms. This security strategy also requires collaboration with the private sector, which is an internet service provider, and at the same time has large resources to take an active role in building the national cybersecurity architecture. Cooperation in cybersecurity mechanisms includes guidelines on sharing information with the private sector. When efforts to establish a cybersecurity law in Indonesia are stuck, international cooperation can be an alternative for the Indonesian government to improve cybersecurity architecture. Furthermore, at the international level, Indonesia needs to be more proactive in international cooperation and enhance cybersecurity cooperation.

Pradipta Nindyan Saputra, Arfin Sudirman, Obsatar Sinaga, Wahyu Wardhana and Nurul Hayana are affiliated with the Department of International Relations, Universitas Padjadjaran, Bandung, Indonesia.

The authors can be contacted at *arfinsudirman@gamil.com*.

References

Badan, S., & Sandi, N. (2019a). Rencana Strategis Badan Siber dan Sandi Negara (BSSN) 2018 - 2019 `. Jakarta.

Badan, S., & Sandi, N. (2019b). Round Table Discussion MPR; BSSN Paparkan Ancaman Perang Siber. Retrieved October 15, 2019, from https://bssn.go.id/round-table-discussion-mpr-bssn-paparkan-ancaman-perang-siber/

Bendiek, A. (2012). European Cyber Security Policy. Berlin.

Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the EU. Crime, Law and Social Change, (Oktober), 1–24. https://doi.org/10.1007/s10611-016-9653-3

Bovaird, T. (2004). Public-Private Partnerships: From Contested Concepts to Prevalent Practice. International Review of Administrative Sciences, 70(2), 199–215. https://doi.org/10.1177/0020852304044250

Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public-Private Partnerships:

Perspectives on Purposes, Publicness, and Good Governance. Public Administration and Development, 31, 2–14. https://doi.org/10.1002/pad.584

Carr, M. (2015). Power Plays in Global Internet Governance. Millenium Journal of International Studies, 43(2), 640–659. https://doi.org/10.1177/0305829814562655

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.

Chenou, J. (2014). From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi- stakeholderism , and the Institutionalisation of Internet Governance in the 1990s From Cyber-Libertarianism to Neoliberalism : Internet Exceptionalism , Multi-stakeholderism , a. Globalisations, (October), 37–41. https://doi.org/10.1080/14747731.2014.887387

CNN Indonesia. (2019). Kaspersky Catat 50 Juta Serangan Siber di Indonesia pada 2018. Retrieved October 15, 2019, from https://www.cnnindonesia.com/teknologi/20190424193414-185-389389/kaspersky-catat-50-juta-serangan-siber-di-indonesia-pada-2018

Commission of the European Communities. Green Paper On Public-Private Partnerships and Community Law On Public Contracts and Concessions (2004).

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. International Political Sociology, 4(1).

Eriksson, J., & Giacomello, G. (2009). Who Controls the Internet ? Beyond the Obstinacy or Obsolescence of the State. International Studies Review, 11, 205–230. https://doi.org/10.1111/j.1468-2486.2008.01841.x

Forrer, J., Kee, J. E., Newcomer, K. E., & Boyer, E. (2010). Public–Private Partnerships and the Public Accountability Question. Public Administration Review, 70(3), 475–484.

Graz, J.-C., & Nolke, A. (2007). Transnational private governance and its limits. London dan New York: Routledge.

Grimsey, D., & Lewis, M. K. (2004). Public Private Partnerships: The Worldwide Revolution in Infrastructure Provision and Project Finance. Cheltenham, UK & Northamton, USA: Edward ElgarPublishing Limited.

Hakim, R. N. (2019). BSSN Sebut RUU Kamtan Siber Mendesak untuk Disahkan, Ini Alasannya. Retrieved October 26, 2019, from https://nasional.kompas.com/read/2019/08/23/17145851/bssn-sebut-ruu-kamtan-siber-mendesak-untuk-disahkan-ini-alasannya

Harcourt, A. (2013). Participatory Gains and Policy Effectiveness : The Open Method of Co-ordination Information Society. Journal of Common Market Studies, 51(4), 667–683. https://doi.org/10.1111/jcms.12022

Harsono, N. (2019). Businesses as risk: Experts Sound Alarm On Cyberthreat. The Jakarta Post.

Heinl, C. H. (2013). Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime (No. 263). Singapore.

Héritier, A. (2001). Market Integration and Social Cohesion : the Politics of Public Services in European Regulation. Journal of European Public Policy, 8(December), 825–852. https://doi.org/10.1080/13501760110083536

Hodge, G. A., & Greve, C. (2007). Public – Private Partnerships: An International Performance Review. Public Administration Review, 67(3), 545–558.

Hurk, M. Van Den, Brogaard, L., Lember, V., Peterson, O. H., & Witz, p. (2015). National Varieties of Public – Private Partnerships (PPPs): A Comparative Analysis of PPP-Supporting Units in 19 European Countries. Journal of Comparative Policy Analysis: Research and Practice, (March), 37–41. https://doi.org/10.1080/13876988.2015.1006814

Hurk, M. Van Den, & Verhoest, K. (2016). The Challenge of Using Standard Contracts in Public – Private Partnerships. Public Management Review, 18, 278–299. https://doi.org/10.1080/14719037.2014.984623

Kementerian Pertahanan Republik Indonesia. Peraturan Menteri Pertahanan Republik Indonesia Nomer. 82 Tahun 2014 Tentang Pedoman Pertahanan Siber, Pub. L. No. 82, 64 (2014). Indonesia.

Kurniawan, D. (2018). Korban Duit Tabungan Raib Bertambah, BRI Kediri Blokir Rekening Nasabah. Retrieved October 26, 2019, from https://www.liputan6.com/regional/read/3371964/korban-duit-tabungan-raib-bertambah-bri-kediri-blokir-rekening-nasabah

Liputan. (2019). 50 Juta Ancaman Siber Diblokir di Indonesia Sepanjang 2018. Retrieved October 15, 2019, from https://www.liputan6.com/tekno/read/3947074/50-juta-ancaman-siber-diblokir-di-indonesia-sepanjang-2018

Marsden, C. T. (2011). Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace. Cambridge: Cambridge University Press.

Metodieva, A. (2018). Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns. Strategic Policy Institute.

Min, K., Chai, S., & Han, M. (2015). An International Comparative Study on Cyber Security Strategy. International Journal of Security and Its Aplications, 9(2), 13–20.

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet Security and Networked Governance in International Relations. International Review of Administrative Sciences, 15, 86–104. https://doi.org/10.1111/misr.12024

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance.

Peraturan Presiden No. 53 Tahun 2017. Perpres Nomor 53 Tahun 2017 (2017). Indonesia.

Peraturan Presiden Nomer 133 Tahun 2017. Perpres No. 133 Tahun 2017 (2017). Indonesia.

Purwanto, D. (2013). Bank Mandiri Teliti Pencurian Data Nasabah Kartu Kredit. Retrieved October 26, 2019, from https://money.kompas.com/read/2013/03/19/16225337/bank.mandiri.teliti.pencurian.data.nasabah.kartu.kredit?page=all

Putra, R. D., Supartono, & D.A.R, D. (2018). Ancaman Siber dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). Jurnal Prodi Perang Asimetris, 4(2), 99–120.

Raduege, H. D. (2013). The Public/Private Cooperation We Need on Cyber Security. Harvard Business Review.

Reynaers, A. (2013). Public Values in Public–Private Partnerships. Public Administration Review, 20(November 2013), 1–10. https://doi.org/10.1111/puar.12137

Rubens, D. (2010). Cyber-Warfare: The Fifth Dimension. London.

Sari, H. P. (2019). RUU Keamanan dan Ketahanan Siber Diputuskan Jadi Inisiatif DPR. Retrieved August 21, 2019, from https://nasional.kompas.

com/read/2019/07/04/13441701/ruu-keamanan-dan-ketahanan-siber-diputuskan-jadi-inisiatif-dpr

Sarmento, J. M., & Renneboog, L. (2016). Anatomy of public-private partnerships: their creation, financing and renegotiations. International Journal of Managing Projects in Business, 9(1), 94–122.

Schneider, A. L. (1999). Public-Private Partnerships in the U . S . Prison System. American Behavioral Scientist, 43(Septeber), 192–208. https://doi.org/10.1177/00027649921955119

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Potensi Pertahanan, 31–35.

Solms, R. Von, & Niekerk, J. Van. (2013). From Information Security to Cyber Security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Sutrisno, B. T. (2016). Urgensi Komando Pertahanan Siber (Cyber Defense Command) Dalam Menghadapi Peperangan Asimetris. Defendonesia, 1(2), 53–60.

Tréguer, F. (2015). Hackers vs States_ Subversion, Repression, and Resistance in the Online Public Sphere. Droit et Société, 1–7.

Tropina, T. (2015). Public–Private Collaboration: Cybercrime, Cybersecurity and National Security. In T. Tropina & C. Callanan (Eds.), Self- and Co-regulation in Cybercrime, Cybersecurity and National Security (pp. 1–41). New York: Springer. https://doi.org/10.1007/978-3-319-16447-2

Tropina, T., & Cormac, C. (2015). Self-and Co-regulation in Cybercrime, Cybersecurity and National Security. Heidelberg: Springer.

Tumpal, R. (2019). Diplomasi Indonesia dalam Upaya Pengelolaan Ruang Siber. Jakarta.

UN General Assembly. Developments in the Field of Information and Telecommunications in The Context of International Security (2015). Retrieved from https://generalassemb.ly/design

United Nations. (2008). Guidebook On Promoting Good Governance in Public-Private Partnerships. New York & Geneva: United Nations.

United Nations. (2013). Comprehensive Study on Cybercrime. Vienna.

Wardhana, W. (2019). Indonesian Cyber Security: A domestic Policy and International Cooperation to Promote Security and Protect Indonesian Society in Cyber Space. In 3rd Indonesia International Defense Science Seminar (p. 105). Jakarta: IIDS.

Wells, L. (2016). Cyberspace as the 5th Domain of Warfare. Singapore.