Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020

Satya Muhammad Sutra*[1], Agus Haryanto[2]
[1,2] Program Studi Hubungan Internasional, Universitas Jenderal Soedirman
Jl. H. R. Boenyamin No. 993, Purwokerto, Jawa Tengah, Indonesia

e-mail: ***[1]satya.sutra@mhs.unsoed.ac.id,** [2]agus.haryanto@unsoed.ac.id

Abstract

This research analyzes the strategy carried out by the National Cyber and Crypto Agency (BSSN) as the national cybersecurity institute. In this research, the author utilizes the Theory of Securitization and The Concept of Cybersecurity. Based on the data obtained, BSSN was formed by the Presidential Regulation on BSSN which state that BSSN is tasked with implementing cybersecurity effectively and efficiently by utilizing, developing, and consolidating all parties related to cybersecurity. BSSN used the Global Cybersecurity Index framework to improve the national cybersecurity capability. The GCI measures the commitment of countries in cybersecurity according to the five pillars: legal measures, technical measures, organizational measures, capacity development, and cooperative measures. The strategy of BSSN is expected to be able to face the problems and challenges in the present and future era.

Keywords— *Cybersecurity, Global Cybersecurity Index, Indonesia, the National Cyber and Crypto Agency*

Abstrak

Penelitian ini menganalisis upaya peningkatan keamanan siber yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) sebagai institusi keamanan siber nasional Indonesia. Dalam menganalisis hal tersebut, penulis menggunakan Teori Sekuritisasi serta Konsep Keamanan Siber. Berdasarkan data yang diperoleh, BSSN dibentuk berdasarkan peraturan presiden dengan tugas untuk melaksanakan keamanan dalam bidang siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, serta mengonsolidasikan berbagai unsur yang berkaitan dengan keamanan siber. Dalam meningkatkan keamanan siber di Indonesia mengacu pada lima aspek pada *Global Cybersecurity Index* yaitu aspek hukum, aspek teknis, aspek organisasi, aspek pengembangan kapasitas, dan aspek kerja sama. *Global Cybersecurity Index* digunakan untuk mengukur komitmen suatu negara terkait kapabilitas keamanan siber di negaranya. Dengan adanya upaya-upaya yang dilakukan BSSN terkait peningkatan keamanan siber diharapkan dapat mengurangi resiko dan ancaman dalam ruang siber di Indonesia.

Kata kunci— Badan Siber dan Sandi Negara, Indeks Keamanan Siber Global, Indonesia, Keamanan Siber

1. Pendahuluan

Perkembangan teknologi dan informasi menjadi salah satu faktor penting yang menyebabkan fenomena globalisasi menjadi berkembang seperti saat ini. Penemuan internet merupakan salah satu

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

hal yang memberikan dampak paling besar dalam perkembangan teknologi informasi. Internet hadir sebagai sebuah bentuk teknologi yang mempermudah arus komunikasi dan informasi bagi para penggunanya. Perkembangan internet telah memberikan berbagai manfaat dalam kehidupan manusia, namun di sisi lain perkembangan internet juga memberi berbagai ancaman dan resiko seperti *cybercrime, cyberterrorism, cyber hacktivism,* dan *cyber warfare*.

Indonesia menjadi negara dengan angka kejahatan teknologi informasi tertinggi kedua di dunia. Hal tersebut dilansir dari kominfo.go.id, disebutkan bahwa Indonesia menduduki peringkat kedua negara dengan tingkat kejahatan teknologi informasi tertinggi di dunia setelah Jepang. Tingginya frekuensi kejahatan siber di Indonesia disebabkan oleh banyaknya pengguna internet yang terus meningkat. Keamanan siber atau *cybersecurity* diperlukan untuk mengantisipasi munculnya kejahatan teknologi informasi tersebut. Keamanan siber merupakan sebuah aktivitas yang dilakukan untuk menjaga pengguna ruang siber dari berbagai ancaman atau serangan yang ada di ruang siber (Prayudi, Budiman, Ardipandato, & Fitri, 2018, hal. 2).

Jumlah kejahatan siber di Indonesia mengalami peningkatan dari tahun 2014 hingga tahun 2019. Berdasarkan penelitian tahun 2020 yang dilakukan oleh Palinggi. et. al, dilaporkan di Indonesia terdapat sebanyak 98 kasus kejahatan siber pada tahun 2014, 305 kasus di tahun 2015, 1207 kasus di tahun 2016, 1763 kasus di tahun 2017, 4000 kasus di tahun 2018 dan 3000 kasus di tahun 2019. Berdasarkan penjelasan di atas, pada tahun 2018 terjadi peningkatan drastis jumlah kasus kejahatan siber di Indonesia yang mencapai 4000 jumlah kasus dari 1763 kasus di tahun 2017. Hal tersebut menunjukkan bahwa keamanan siber di Indonesia masih lemah dan perlu adanya peningkatan (Palinggi, Palelleng, & Allolinggi, 2020, hal. 58).

Keamanan siber menjadi hal penting bagi sebuah negara karena didalamnya mencangkup berbagai aspek yang dapat mempengaruhi keamanan negara. Namun, Indonesia belum memiliki regulasi atau kebijakan resmi dalam undang-undang terkait dengan keamanan siber. Pemerintah Indonesia hanya memiliki regulasi dan kebijakan tentang keamanan informasi dalam UU ITE, yang mana kebijakan tersebut tidak cukup untuk membangun pertahanan negara melalui keamanan siber. Kondisi tersebut terjadi karena dalam UU ITE tidak ada kejelasan terkait penanggulangan ancaman-ancaman (Chotimah, 2019, hal. 116).

Dalam usaha meningkatkan keamanan siber, pemerintah Indonesia kemudian membentuk Badan Siber dan Sandi Negara (BSSN) sebagai institusi keamanan siber nasional. Dibentuknya BSSN sebagai lembaga pemerintah yang bertanggung jawab dalam bidang keamanan siber diharapkan dapat menjadi organisasi utama (koordinator) dalam kaitannya dengan penyelenggaraan keamanan siber di Indonesia. Secara umum, terdapat tiga upaya yang dilakukan oleh BSSN dalam menghadapi ancaman siber yang di Indonesia, yaitu: (1)Penyusunan kerangka kerja dunia siber dengan menyusun kerangka hukum keamanan siber, menyusun strategi keamanan siber nasional, dan mengoptimalkan fungsi dan tugas BSSN; (2)Pengembangan kapabilitas keamanan siber dengan meningkatkan kampanye kesadaran publik terkait isu siber, penyusunan program (pendidikan, penelitian, dan pengembangan) terkait bidang siber dan peningkatan program pelatihan dan sertifikasi keamanan siber; dan (3)Peningkatan kerjasama keamanan siber dengan melakukan kerja sama

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

multilateral maupun bilateral dengan negara lain terkait dengan isu siber, meningkatkan kerja sama antara pemerintah dan swasta dalam bidang siber dan meningkatkan kerja sama internal instansi pemerintah (Sudarmadi & Runturambi, 2019, hal. 163).

Dalam pelaksanaannya BSSN telah melakukan berbagai upaya untuk meningkatkan keamanan siber di Indonesia. Berkaitan dengan hal tersebut, upaya peningkatan keamanan siber yang dilakukan oleh BSSN pada tahun 2017-2020 dipilih terkait dengan pembentukan BSSN itu sendiri dan di tahun tersebut terjadi peningkatan kejahatan siber yang sangat drastis di Indonesia. Padahal BSSN baru saja dibentuk pada akhir tahun 2017 dan sedang gencar meningkatkan keamanan siber Indonesia. Oleh sebab itu, penulis merasa tertarik untuk mengkaji mengenai upaya peningkatan siber apa saja yang dilakukan BSSN pada tahun tersebut.

1.2 Rumusan Masalah

Rumusan masalah yang muncul berkaitan dengan latar belakang diatas adalah, *"Bagaimana upaya peningkatan keamanan siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017-2020?"*

2. Kajian Pustaka dan Kerangka Pemikiran

2.1 Teori Sekuritisasi

Dalam bukunya yang berjudul *Security: A New Framework for Analysis*, Buzzan, Waever, dan Wilde menyebutkan bahwa "*Security is move that takes politics beyond the established rules of the game and frames issues either as a special kind of politics or as above politics*" (Buzzan, Waever, & Wilde, 1998, hal. 23). Berdasarkan pengertian tersebut dapat dipahami bahwa studi keamanan merupakan sebuah langkah yang dilakukan dengan melampaui aturan main untuk melihat suatu isu apakah termasuk dalam ranah politik atau bahkan melampauinya. Sekuritisasi sendiri merupakan bentuk yang lebih ekstrim dari upaya politisasi.

Dalam mengonstruksi sebuah isu, para aktor sekuritisasi dapat menggunakan *speech act*. Penggunaan *speech act* ini dilakukan untuk meyakinkan dan memberi peringatan kepada masyarakat terkait dengan ancaman dari suatu isu. Dengan digunakannya *speech act* tersebut diharapkan dapat mempengaruhi opini publik serta memberikan aktor sekuritisasi kesempatan untuk memobilisasi kekuasaan negara dan membuat peraturan untuk menghentikan ancaman tersebut. *Speech act* merupakan salah satu hal yang dapat menentukan keberhasilan atau kegagalan dari sebuah proses sekuritisasi (Trihartono, Indrastuti, & Nisya, 2020, hal. 5).

Dalam melakukan analisis keamanan melalui pendekatan *speech* act dibutuhkan tiga jenis unit analisis keamanan dalam proses sekuritisasi, yaitu : (1)*Referent Object*, yaitu berbagai hal yang terlihat terancam secara eksistensial dan yang memiliki tuntutan yang sah untuk bertahan hidup; (2)*Securitizing Actor*, merupakan seorang individu maupun kelompok yang mengamankan isu dengan mendeklarasikan bahwa *referent object* secara eksistensial terancam (3)*Functional Actor*, merupakan aktor yang mempengaruhi dinamika suatu sektor dan memiliki peran penting. Namun aktor ini tidak berusaha untuk menjadikan suatu isu atau permasalahan menjadi sebuah isu keamanan (Buzzan, Waever, & Wilde, 1998, hal. 36).

Berdasarkan penjelasan diatas, teori sekuritisasi digunakan karena upaya peningkatan keamanan siber yang dilakukan oleh BSSN sendiri dilakukan untuk mengamankan kepentingan-

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

kepentingan pengguna dari berbagai macam ancaman dalam ruang siber. Dalam hal ini, pengguna ruang siber merupakan *referent object* dari proses sekuritisasi yang dilakukan oleh BSSN (*securitizing actor)* yang menganggap bahwa pengguna ruang siber secara eksistensial terancam oleh adanya ancaman-ancaman dalam ruang siber.

2.2 Konsep Keamanan Siber

Menurut Buzan (1998), terdapat tiga model keamanan yang mengkaji bidang siber yaitu *Hyper securitization*, *Everyday Security Practice*, serta *Technotification* yang menggunakan ahli dalam bidang siber dalam melakukan *Hyper securitization.* Konsep keamanan siber atau *cyber security* sendiri merupakan penerapan dari ketiga bentuk sekuritisasi menurut Buzan tersebut (Hansen & Nissenbaum, 2009, hal. 1171).

Keamanan siber sendiri merupakan sebuah alat, kebijakan, konsep keamanan, perlindungan keamanan, peraturan, pedoman, pendekatan manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang digunakan untuk melindungi pengguna ruang siber dari berbagai ancaman dan resiko yang ada. Keamanan siber menjadi salah satu upaya untuk memastikan bahwa pengguna ruang siber dapat menggunakan teknologi dengan aman dari ancaman siber (Fitri, 2018, hal. 28).

Berkaitan dengan studi kasus pembahasan mengenai upaya peningkatan keamanan siber Indonesia oleh BSSN tahun 2017-2020, konsep keamanan siber menjadi instrumen dasar penjelas. Upaya yang dilakukan oleh BSSN untuk meningkatkan keamanan siber Indonesia dilakukan untuk melindungi pengguna internet serta berbagai aspek yang ada di dalamnya seperti aspek sosial, ekonomi, dan pertahanan. Dengan adanya upaya peningkatan keamanan siber tentu dapat memperkuat pertahanan nasional negara.

3. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif dengan pendekatan deskriptif. Metode kualitatif digunakan untuk menjelaskan mengenai sebuah fenomena dengan sedalam-dalamnya melalui pengumpulan data yang sedalam-dalamnya pula sehingga akan didapatkan detail serta kedalaman dari suatu data yang akan diteliti (Nurdin & Hartati, 2019, hal. 76). Penggunaan metode kualitatif menekankan pada penggunaan metode historis dimana data-data penelitian diambil dari sumber literatur seperti buku, jurnal maupun artikel. Dengan menggunakan metode kualitatif, pembahasan dalam penelitian tersebut akan menekankan pada deskripsi dari permasalahan mengenai upaya peningkatan keamanan siber dilakukan oleh Badan Siber dan Sandi Negara (BSSN) sehingga penelitian yang dilakukan akan lebih dalam dan menyeluruh.

4. Hasil dan Pembahasan

4.1 Dinamika Ruang Siber di Indonesia

Perkembangan teknologi dan informasi menyebabkan munculnya sebuah ruang baru yang bersifat artifisial dan maya yaitu ruang siber atau *cyberspace.* Ruang siber merupakan sebuah ruangan imajiner yang dapat digunakan oleh setiap orang untuk melakukan berbagai kegiatan atau aktivitas sehari-hari melalui cara artifisial. Dalam perkembangan teknologi informasi, internet kemudian muncul sebagai sebuah fenomena dalam kehidupan manusia.

Seiring dengan perkembangan waktu, internet berkembang dengan sangat pesat di seluruh dunia. Indonesia merupakan salah satu negara yang memiliki pengguna internet terbesar di dunia. Jumlah pengguna internet di Indonesia terus

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

mengalami peningkatan dari tahun ke tahun, berdasarkan survei yang dilakukan oleh APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pertumbuhan pengguna internet di Indonesia mengalami peningkatan pesat dari tahun 2017 sampai 2019/ Q2 2020. Pada tahun 2017 terdapat sekitar 143,3 juta pengguna internet di Indonesia; 171,2 juta pengguna di tahun 2018 (APJII, 2018); dan 196,7 juta pengguna di tahun 2019/ Q2 2020 (APJII, 2020).

Banyaknya pengguna internet di Indonesia menyebabkan berbagai macam resiko dan kerentanan muncul dalam ruang siber di Indonesia. Perkembangan teknologi internet dibarengi dengan peningkatan jumlah pengguna internet yang sangat drastis dapat menyebabkan munculnya ancaman siber berupa kejahatan siber maupun serangan siber. Ancaman siber (*cyber thread*) merupakan gangguan atau serangan yang dapat merusak maupun menyebabkan kerugian sehingga dapat mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) suatu sistem informasi.

Ancaman siber terbagi menjadi dua kategori yaitu serangan siber dan kejahatan siber. Serangan siber merupakan upaya yang dilakukan untuk mengganggu atau merusak jaringan yang lebih berfokus pada alur *logic* dari sebuah sistem informasi (Fitri, 2018, hal. 26). Sedangkan kejahatan siber atau *cybercrime* merupakan sebuah tindakan melawan hukum dimana dilakukan melalui perangkat teknologi informasi yang terhubung dengan internet sebagai sarana untuk melakukan berbagai macam kejahatan (Arifah, 2011, hal. 187).

Dalam beberapa tahun, terdapat tiga jenis kejahatan siber dalam sektor publik yang berkembang di Indonesia, yaitu *hacking*, *phishing* dan *malware*. *Hacking* adalah sebuah kegiatan yang dilakukan oleh *hacker* untuk mengakses atau menyusup ke suatu jaringan komputer secara ilegal atau tanpa ijin dari pemilik jaringan tersebut (Kwarto & Angsito, 2018, hal. 102). *Phising* merupakan kejahatan siber yang memiliki sifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Kejahatan ini dilakukan agar korban bersedia untuk memberikan informasi mengenai data diri seperti username dan password ataupun informasi penting lainnya(Wibowo & Fatimah, 2017, hal. 5). *Malware* merupakan sebuah program komputer yang diciptakan untuk membobol atau merusak suatu *software* atau sistem operasi dalam komputer. Salah satu cara yang digunakan untuk menyebarkan malware adalah dengan menyisipkannya ke dalam sebuah aplikasi atau file tertentu (Kwarto & Angsito, 2018, hal. 103).

Dalam perkembangannya, kasus serangan siber di Indonesia mengalami peningkatan yang drastis dalam beberapa tahun terakhir. Berdasarkan laporan tahunan *Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center* atau ID-SIRTII/ CC tahun 2018, terdapat sekitar 232.447.974 jumlah kasus serangan siber ke jaringan yang ada di Indonesia. Ancaman siber terbesar di tahun 2018 adalah ancaman *malware* yang aktivitasnya dilaporkan sebesar 122 juta kasus di Indonesia (ID-SIRTII/ CC, 2018). Kemudian di tahun tahun 2019, menurut laporan tahunan Pusat Operasi Keamanan Siber Nasional BSSN jumlah kasus serangan siber di Indonesia mengalami peningkatan yaitu mencapai angka 290.381.238. Di tahun 2019 ancaman siber terbesar di Indonesia adalah pembocoran data dan serangan siber yang menggunakan *malware* (BSSN, 2019). Selanjutnya, menurut Laporan Tahunan Badan Siber dan Sandi Negara tahun 2020, jumlah serangan siber di Indonesia

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

mencapai angka 316.167.753 kasus (BSSN, 2020).

Banyaknya kasus ancaman siber yang terjadi di Indonesia menunjukkan bahwa kapasitas teknologi dan keahlian di bidang siber yang dimiliki oleh pemerintah Indonesia masih kurang dibandingkan dengan kapasitas yang dimiliki oleh pelaku ancaman siber tersebut. Perkembangan teknologi yang berkembang semakin canggih juga menyebabkan ancaman-ancaman yang ada dalam ruang siber menjadi lebih canggih pula. Hal tersebut menunjukkan bahwa BSSN sebagai institusi keamanan siber nasional perlu untuk selalu meningkatkan kapasitas keamanan siber di Indonesia serta meningkatkan keahlian dari berbagai pihak yang ada didalamnya. Upaya tersebut penting dilakukan untuk mengurangi tingkat ancaman yang ada dalam ruang siber Indonesia.

4.2 Tata Kelola BSSN sebagai Institusi Keamanan Siber Nasional

BSSN dibentuk berdasarkan Perpres No 53 tahun 2017 tentang Badan Siber dan Sandi Negara yang ditandatangani oleh Presiden Joko Widodo pada tanggal 19 Mei 2017. Peraturan tersebut kemudian disempurnakan dan disahkan kembali oleh Presiden Joko Widodo dalam Perpres No 133 Tahun 2017 tentang Badan Siber dan Sandi Negara pada 16 Desember 2017. BSSN merupakan lembaga pemerintah non kementerian yang berada di bawah dan bertanggung jawab kepada Presiden. Dengan dibentuknya BSSN, maka berbagai tugas dan fungsi berkaitan dengan keamanan siber dan persandian dalam Lembaga Sandi Negara, Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika dilaksanakan oleh BSSN (BSSN, 2017).

Pembentukan BSSN sebagai institusi keamanan siber nasional menunjukkan bahwa pemerintah Indonesia telah menganggap bahwa isu dalam ruang siber merupakan hal penting sehingga perlu adanya peningkatan kapabilitas serta pengamanan keamanan siber di Indonesia. Terkait dengan teori sekuritisasi, dalam studi keamanan terdapat tiga tahapan yang dapat menunjukkan bagaimana sebuah isu dapat menjadi sebuah ancaman keamanan. Tahap pertama yaitu non politis (*non-politized*) dimana dalam tahapan ini sebuah isu belum menjadi pembahasan atau perbincangan dalam suatu negara atau wilayah tertentu. Kedua yaitu tahap politis *(politized)* dimana dalam tahap ini sebuah isu sudah menjadi perbincangan, pembahasan, hingga perdebatan pada level pemerintah. Ketiga yaitu tahap ter sekuritisasi (*securitized)* dimana aktor-aktor sekuritisasi yang ada di suatu negara atau wilayah tertentu menyepakati adanya ancaman yang perlu *emergency measures* atau upaya penyelesaian untuk mengatasi hal tersebut.

Terkait dengan tahap pada proses sekuritisasi diatas, pembentukan BSSN pada tahun 2017 menunjukkan bahwa isu terkait dengan ruang siber masuk kedalam tahap ter-sekuritisasi (*securitized*). Dimana pemerintah Indonesia yang berperan sebagai aktor sekuritisasi membentuk BSSN sebagai institusi keamanan siber nasional untuk menyelesaikan berbagai permasalahan yang ada dalam ruang siber Indonesia.

Para aktor sekuritisasi juga menggunakan *speech act* untuk merekonstruksi isu kedalam sebuah masalah keamanan. Dengan penggunaan *speech act* tersebut diharapkan dapat menggiring opini publik serta memberi waktu bagi aktor-aktor sekuritisasi untuk memobilisasi kekuasaan yang mereka miliki untuk membentuk peraturan atau

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

regulasi demi menghentikan ancaman yang ada. Penggunaan *speech act* dapat menentukan keberhasilan atau kegagalan dari sebuah proses sekuritisasi, sehingga perlu adanya pemaksimalan penggunaan pendekatan ini untuk membuat upaya-upaya yang dilakukan oleh aktor sekuritisasi supaya berhasil dengan maksimal (Trihartono, Indrastuti, & Nisya, 2020, hal. 5). Dalam pendekatan *speech act* sendiri, terdapat tiga unit yang berkaitan dengan proses sekuritisasi yaitu *referent object, securitizing actor,* serta *functional actor.*

Terkait dengan penelitian ini, pengguna ruang siber di Indonesia menjadi *referent object* dari berbagai ancaman dan kerentanan dalam ruang siber. Sebagai *referent object,* ancaman siber dapat terjadi dan dialami oleh siapapun tanpa terkecuali, bahkan secara tidak sadar kita maupun orang-orang terdekat juga pernah mengalami ancaman-ancaman tersebut. Pengguna ruang siber di Indonesia yang menjadi *referent object* disini tidak terbatas pada individu saja, namun juga kelompok, organisasi, bahkan sektor pemerintahan yang memiliki akses terkait dengan ruang siber. Oleh karena itu, upaya-upaya perlindungan terhadap ruang siber perlu difokuskan pada keamanan dari *referent object* tersebut.

Dalam proses sekuritisasi selanjutnya, pemerintah Indonesia dan BSSN berperan sebagai *securitizing actor*. BSSN yang dibentuk oleh pemerintah Indonesia sebagai institusi keamanan siber nasional berperan dalam mendeklarasikan pengguna ruang siber sebagai *referent object* yang secara eksistensial terancam oleh berbagai kerentanan yang ada dalam ruang siber. Kedua aktor tersebut berperan dalam menjadikan isu-isu terkait kerentanan dan ancaman dalam ruang siber sebagai sebagai sebuah permasalahan yang mengancam pengguna ruang siber di Indonesia. Ancaman dalam ruang siber yang bersifat tidak terduga menyebabkan pengguna ruang siber di Indonesia dapat mengalami hal tersebut tanpa terkecuali. Sehingga sebagai *securitizing actor* peningkatan kapasitas keamanan siber perlu dilakukan dengan berfokus pada bidang-bidang yang dimanfaatkan oleh pengguna ruang siber Indonesia.

Dalam proses sekuritisasi selanjutnya, muncul *functional actor* sebagai pihak yang terlibat dan memiliki peran penting dalam mempengaruhi dinamika pada sektor siber di Indonesia. *Functional actor* disini merupakan pihak-pihak yang berperan sebagai penentu dari berbagai upaya dan tindakan yang dilakukan oleh BSSN sebagai *securitizing actor* dalam meningkatkan keamanan siber di Indonesia. Namun, aktor ini tidak berusaha untuk menjadikan suatu isu atau permasalahan menjadi sebuah isu keamanan. Terkait dengan hal tersebut, masyarakat Indonesia secara umum dan organisasi-organisasi yang bergerak dalam bidang siber merupakan *functional actor* dalam proses sekuritisasi. Kedua pihak tersebut memiliki pengaruh dalam proses sekuritisasi terkait dengan dinamika pembuatan kebijakan keamanan yang telah dibuat oleh pemerintah Indonesia dan BSSN serta menentukan perkembangan dari proses sekuritisasi terkait dengan bidang siber, tanpa mengambil peran pengguna ruang siber di Indonesia sebagai *referent object* serta pemerintah Indonesia dan BSSN sebagai *securitizing actor*.

4.3 Upaya Peningkatan Keamanan Siber Indonesia Tahun 2017-2020

Berdasarkan teori sekuritisasi dan konsep keamanan siber, Pemerintah Indonesia melalui BSSN berupaya untuk meningkatkan sekuritisasi dan komitmen terkait dengan keamanan siber nasional melalui acuan dari lima pilar yang ada pada

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

Global Cybersecurity Index yaitu aspek hukum (*legal measures*), aspek teknis (*technical measures*), aspek organisasi (*organizational measure*), aspek pengembangan kapasitas (*capacity development*), dan aspek kerja sama *(cooperative measures*) (Islami, 2017, hal. 140). Kelima pilar dalam GCI kemudian menjadi landasan dalam menyusun berbagai upaya dan strategi peningkatan keamanan siber di Indonesia.

4.3.1 Aspek Hukum (*legal measures*)

Aspek hukum atau *legal measures* diukur berdasarkan keberadaan institusi legal serta *framework* yang berkaitan dengan keamanan siber dan kejahatan siber di suatu negara. Terdapat tiga indikator dalam aspek hukum yaitu keberadaan UU Kejahatan Siber, UU Keamanan Siber, dan penyelenggaraan keamanan siber bagi aktor hukum (Sudarmadi & Runturambi, 2019, hal. 163).

Dari ketiga indikator tersebut, dalam rangka pemenuhan aspek hukum terkait penyelenggaraan keamanan siber di Indonesia, pada tahun 2019 Rancangan Undang-Undang (RUU) tentang Keamanan dan Ketahanan Siber telah diinisiasi oleh DPR yang kemudian sudah diserahkan kepada pemerintah. Berkaitan dengan hal tersebut, BSSN sebagai institusi keamanan siber nasional menyelenggarakan diskusi publik dan simposium nasional mengenai RUU tentang Keamanan dan Ketahanan Siber pada 12 Agustus 2019. Kegiatan tersebut dihadiri oleh 300 peserta yang terdiri dari perwakilan kementerian/ lembaga, akademisi, praktisi, ahli/ professional, asosiasi, LSM, komunitas siber nasional, dan media massa yang bergerak di bidang keamanan siber. Selain itu, BSSN pada tahun 2019 juga mengusulkan RUU Persandian dan RUU Rahasia Negara dalam Program Legislasi Nasional Pemerintah 2020-2024 (BSSN, 2019).

4.3.2 Aspek Teknis (*technical measures)*

Aspek teknis diukur berdasarkan keberadaan institusi teknis serta *framework* terkait dengan keamanan siber. Terdapat enam indikator dalam aspek teknis yaitu *Cyber Emergency Response Team* (CERT) Nasional, CERT Pemerintah, CERT Sektoral, Standar keamanan siber bagi organisasi, standar dan sertifikasi bagi profesional bidang keamanan siber, dan adanya perlindungan daring bagi anak (Sudarmadi & Runturambi, 2019, hal. 164).

BSSN sebagai institusi keamanan siber nasional belum sepenuhnya bisa melakukan upaya peningkatan keamanan siber menurut keenam indikator dalam aspek teknis. Indonesia hanya mampu melakukan upaya peningkatan terkait dengan indikator CERT nasional, CERT pemerintah, dan CERT sektoral. CERT merupakan tim koordinasi teknis yang menangani berbagai insiden siber. CERT kemudian disempurnakan menjadi *Computer Security Incident Response Team* (CSIRT) melalui RFC 2350. CERT/ CSIRT dibentuk untuk menyediakan *Point of Contact* (PoC) Tunggal untuk pelaporan insiden siber, membantu penanganan insiden keamanan siber, mencegah insiden keamanan siber terulang kembali, dan berbagai informasi (*lesson learned)*terkait isu siber. BSSN membentuk Gov-CSIRT (*Government Computer Security Incident Response Team*) berdasarkan Keputusan Kepala Badan Siber dan Sandi Negara No. 199 Tahun 2019. Misi Gov-CSIRT yaitu mengkoordinasikan dan mengelaborasikan layanan keamanan siber pada sektor pemerintah dan membangun kapasitas sumber daya keamanan siber pada sektor pemerintah (BSSN, 2019).

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

4.3.3 Aspek organisasi (*organizational measure*)

Aspek organisasi diukur berdasarkan koordinasi antara pembuat kebijakan siber dan strategi keamanan siber yang dikembangkan pada tingkat nasional. Terdapat tiga indikator dalam aspek organisasi yaitu keberadaan strategi keamanan siber nasional, organisasi yang bertanggung jawab dalam bidang siber, dan metrik pengukuran perkembangan keamanan siber (Sudarmadi & Runturambi, 2019, hal. 165).

Berdasarkan penjelasan diatas, Indonesia telah melakukan upaya terkait peningkatan keamanan siber berdasarkan aspek organisasi. Pertama, indikator organisasi yang bertanggung jawab merupakan indikator dimana pemerintah Indonesia telah membentuk Badan Siber dan Sandi Negara (BSSN) sebagai institusi keamanan siber nasional yang didirikan pada 19 Mei 2017. Sebagai CERT/ CSIRT nasional, BSSN hingga saat ini terus berupaya untuk melaksanakan integrasi, koordinasi, harmonisasi dengan berbagai pihak seperti instansi pemerintah lain, sektor swasta, infrastruktur informasi, serta masyarakat sipil terkait penyelenggaraan keamanan siber di Indonesia.

Terkait dengan indikator kedua yaitu keberadaan strategi keamanan siber nasional, Indonesia belum memiliki satupun regulasi atau kebijakan terkait dengan keamanan siber hingga saat ini. Hal tersebut menunjukkan bahwa strategi keamanan siber nasional juga masih dalam tahap peningkatan pemahaman dan pembuatan standarisasi. BSSN sebagai institusi keamanan siber nasional diharapkan dapat menjadi organisasi inti yang bertanggung jawab terkait perumusan strategi keamanan siber nasional. Pada akhir tahun 2020, BSSN telah menyusun draft Strategi Keamanan Siber Nasional (SKSN) dan dalam tahap pengajuan persetujuan kepada Presiden RI. Dengan adanya SKSN diharapkan dapat meningkatkan kapabilitas keamanan siber Indonesia sehingga berbagai permasalahan dalam ruang siber dapat diselesaikan (Kurniawan, 2020).

Selanjutnya indikator metrik pengukuran perkembangan keamanan siber. pada tahun 2020 BSSN bekerjasama dengan berbagai institusi pemerintah daerah untuk menyusun matrik keamanan siber dengan mengoptimalkan sinergi bersama. Matriks keamanan siber dibuat sebagai alat pengukuran dan panduan terkait pencapaian keamanan siber nasional. Matriks tersebut memiliki fungsi untuk mengidentifikasi trend keamanan siber yang sedang berkembang di Indonesia. Upaya sinergitas yang dilakukan oleh BSSN dengan berbagai pemerintahan daerah dilakukan untuk pemberian dukungan anggaran terkait penyelenggaraan pendidikan dan pelatihan keamanan siber, mendukung pembentukan Gov-CSIRT, pemanfaatan fungsi *Security Operation Center*, serta monitoring sistem informasi.

4.3.4 Aspek pengembangan kapasitas (*capacity development*)

Aspek pengembangan kapasitas diukur berdasarkan penelitian dan pengembangan, pendidikan dan program pelatihan, serta tenaga profesional dan aparatur negara yang tersertifikasi. Aspek ini terdiri dari delapan indikator yaitu keberadaan institusi standarisasi di suatu negara, dokumen praktik terbaik terkait keamanan siber, program pelatihan dan pengembangan, kampanye kesadaran publik, kursus pelatihan professional, program pendidikan dan kurikulum akademik nasional terkait keamanan siber, mekanisme intensif dalam keamanan siber, dan industri keamanan siber dalam negeri (Sudarmadi & Runturambi, 2019, hal. 165).

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

Berdasarkan penjelasan di atas, BSSN telah melakukan berbagai upaya untuk meningkatkan aspek pengembangan kapasitas keamanan siber di Indonesia. Terkait dengan kampanye kesadaran publik, BSSN mempunyai sebuah program keamanan data pribadi bernama KLiKS (Kampanye Literasi Keamanan Siber) yang digagas oleh Direktorat Proteksi Ekonomi Digital BSSN (Pusat Studi Forensika Digital, 2018). Sejak dibentuk pada 2018 hingga 2019, KLiKS berhasil dilaksanakan di 12 kota di Indonesia dan dihadiri sekitar 12.000 orang. Pada tahun 2020, BSSN berhasil meluncurkan buku berjudul "KLiKS BSSN Untuk Negeri" yang menceritakan mengenai perjalanan KLiKS di tahun 2019 (BSSN, 2019).

Selain melakukan Kampanye Literasi Keamanan Siber, BSSN juga melakukan berbagai sosialisasi dan edukasi di berbagai lokasi dengan mengundang praktisi, akademisi, peneliti, komunitas, serta berbagai pihak yang berkaitan dengan bidang keamanan siber. Pada tahun 2018, BSSN melakukan sosialisasi dan Workshop di 3 Universitas yang ada di Indonesia yaitu Universitas Syiah Kuala (UNISYAH) Aceh, Swiss German University (SGU) Banten, dan Universitas Islam Indonesia (UII) (BSSN, 2018).

Pada tahun 2019, BSSN melakukan seminar dan workshop di Universitas Indonesia (UI) dan Telkom University (BSSN, 2019). Di tahun yang sama, BSSN juga menggelar Symposium on Critical Information Infrastructure Protection (CIIP-ID) Summit 2019 di Bali untuk melakukan sinergitas dan koordinasi dengan para stakeholder terkait. CIIP-ID merupakan salah satu upaya yang dilakukan oleh BSSN untuk mendapatkan gagasan, ide, pengalaman, strategi, dan *best practice* untuk meningkatkan pengamanan infrastruktur kritikal terkait keamanan siber di Indonesia (Rahman, 2019).

Pada tahun 2020, BSSN bekerjasama dengan Indonesia Honeynet Project (IHP) untuk menyelenggarakan bimbingan teknis (bimtek), webinar dan workshop bagi mitra honeynet, pihak-pihak yang berkepentingan dalam bidang siber dan masyarakat umum. Kegiatan bimtek dilaksanakan pada tanggal 25-26 Februari 2020 di Aston Priority and Simatupang Hotel and Conference Center, Jakarta. Kegiatan ini dihadiri 34 orang dari sektor pemerintah, lima orang sektor IIKN, dan 13 orang akademisi. Kegiatan selanjutnya yang dilakukan oleh BSSN adalah Webinar pusat Malware Nasional (Pusmanas) yang dilaksanakan pada tanggal 14 juli 2020 dan Webinar ISIF Asia yang dilaksanakan pada tanggal 22 Juli 2020 (BSSN, 2020).

4.3.5 Aspek Kerja Sama *(cooperative measures*)

Diukur berdasarkan kerangka kerjasama, partnership, serta *information sharing network* yang dilakukan untuk meningkatkan kapabilitas siber nasional. Terdapat lima indikator dalam aspek kerjasama internasional yaitu kerjasama bilateral, kerjasama multilateral, partisipasi pada forum internasional, kerjasama pemerintah dengan swasta, dan kerjasama antar instansi pemerintah (Sudarmadi & Runturambi, 2019, hal. 166).

Berdasarkan penjelasan diatas, Diplomasi siber merupakan kerjasama yang dilakukan oleh pemerintah Indonesia melalui BSSN dengan negara atau organisasi lain baik secara bilateral dan multilateral. Diplomasi siber Indonesia dalam kerangka kerjasama bilateral diawali dengan membentuk kesepakatan bilateral dengan Kementerian Luar Negeri Kerajaan Belanda pada 3 Juli 2018 terkait kerjasama dalam bidang siber antara kedua negara (Chotimah, 2019, hal. 124).

Pada tahun 2018, pemerintah Indonesia melalui BSSN melakukan

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

penandatangan perjanjian kerjasama dibidang keamanan siber dengan perwakilan dari pemerintahan Britania Raya untuk peningkatan kapasitas di bidang siber kedua negara (BSSN, 2018). Pada 31 Agustus 2018, BSSN sebagai perwakilan Indonesia juga menandatangani perjanjian kerjasama dengan Australia (*Department of Foreign and Affairs*) (Magrisa, 2020, hal. 10). Selanjutnya pada 28 September 2018, BSSN juga melakukan kerjasama dengan Amerika Serikat terkait peningkatan kerjasama dan pembangunan dalam bidang siber (Chotimah, 2019, hal. 124).

Diplomasi siber dalam kerangka kerjasama multilateral juga dilakukan oleh Indonesia dengan diwakili oleh BSSN. BSSN berkontribusi dalam pelaksanaan ASEAN-Japan Cyber Exercise secara online pada 20 Mei 2019 yang dilaksanakan secara serentak di sepuluh negara ASEAN dan Jepang. (Chotimah, 2019, hal. 125). Pada 31 Mei - 2 Juni 2019 BSSN menjadi delegasi Indonesia dalam 18th International Institute for strategic studies (IISS) Shangri La Dialogue di Singapura. Forum tersebut di hadir 30 negara dan mengangkat isu *cyber-capability development*: *deference implication*. Pada tahun yang sama, BSSN juga aktif dalam pertemuan tahuan CERT internasional seperti *FIRST AGM and conference, APCERT AGM and conference, OIC-CERT AGM and conference*. Indonesia juga menjadi narasumber dalam kegiatan *FIRST Symposium di Oman*, *ASEAN CIO Forum* di Bangkok, dan *ASEAN CISO* di Jakarta (BSSN, 2019).

Terkait dengan kerjasama dalam lingkup nasional, BSSN melakukan berbagai kerjasama dengan institusi pemerintah lain maupun pihak swasta. BSSN bekerja sama dengan institusi pemerintahan seperti kementerian, lembaga non kementerian, dan pemerintah daerah terkait bidang keamanan siber. Terkait kerjasama dengan pihak swasta, BSSN melakukan berbagai macam kerjasama dengan pihak-pihak swasta. Seperti pada tahun 2018, BSSN melakukan kerjasama dengan *Course-net* dan amandata. *Course-net* merupakan training center yang memberikan pelatihan dalam bidang keamanan siber. BSSN menjadi pengajar dalam pelatihan tersebut termasuk pelatihan dalam sertifikasi EC-COUNCIL yaitu Certified Network Defender (CND) dan Certified Ethical Hacker (CEH). Sedangkan BSSN dengan amandata berkolaborasi membentuk Soc yang berskala nasional, kerjasama ini dilakukan untuk membangun SDM yang berkelanjutan dan berkompeten dalam bidang siber di Indonesia (BSSN, 2018). Kerjasama antara BSSN dengan *Course–net* berlanjut hingga tahun 2019, kerjasama diperluas tidak hanya CEH, namun EC-Certified Security Analyst (ECSA), Computer Hacking Forensic Investigator (CHFI) (BSSN, 2019).

5. Kesimpulan dan Rekomendasi

Dalam menghadapi konstelasi siber di Indonesia, dibentuklah Badan Siber dan Sandi Negara (BSSN) sebagai institusi keamanan siber nasional pada 19 Mei 2017. Pembentukan BSSN merupakan salah satu upaya yang dilakukan oleh pemerintah Indonesia dalam meningkatkan keamanan siber nasional serta memastikan bahwa pengguna ruang siber dapat menggunakan teknologi dengan aman dari ancaman siber.

Merujuk pada teori sekuritisasi, pembentukan BSSN sebagai institusi keamanan siber nasional menunjukkan bahwa pemerintah Indonesia telah memiliki komitmen yang tinggi sebagai bentuk sekuritisasi terkait dengan peningkatan kapasitas keamanan siber di Indonesia. Hal tersebut dilakukan karena

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

isu siber di Indonesia menjadi sebuah masalah keamanan yang menyebabkan *existential threat* bagi suatu masyarakat atau entitas tertentu. Kondisi tersebut menunjukkan bahwa pengguna ruang siber di Indonesia menjadi *referent object* yang terancam berbagai kerentanan dalam ruang siber. Sedangkan Pemerintah Indonesia dan BSSN berperan sebagai *securitizing actor* dalam proses sekuritisasi selanjutnya. Dalam proses sekuritisasi selanjutnya, *functional actor* muncul sebagai pihak yang berperan sebagai penentu dari berbagai upaya dan tindakan yang dilakukan oleh BSSN sebagai *securitizing actor* dalam meningkatkan keamanan siber di Indonesia.

Pemerintah Indonesia melalui BSSN berupaya untuk meningkatkan sekuritisasi dan komitmen terkait dengan keamanan siber nasional melalui acuan dari lima pilar yang ada pada *Global Cybersecurity Index* yaitu aspek hukum (*legal measures*), aspek teknis (*technical measures*), aspek organisasi (*organizational measure*), aspek pengembangan kapasitas (*capacity development*), dan aspek kerja sama (*cooperative measures*).

Daftar Pustaka

Acuan dari buku:

Buzzan, B., Waever, O., & Wilde, J. d. 1998. *Security: A New Framework for Analysis.* Boulder: Lynne Rienner Publisher.

Fitri, R. 2018. *Membangun Model Kebijakan Nasional Keamanan Siber dalam Sistem Pertahanan Negara.* Jakarta: Universitas Pertahanan Indonesia.

Nurdin, I., & Hartati, S. 2019. *Metodologi Penelitian Sosial.* Surabaya: Sahabat Cendekia

Prayudi, Budiman, A., Ardipandato, A., & Fitri, A. 2018. *Keamanan Siber dan Pembangunan Demokrasi di Indonesia.* Jakarta: Pusat Penelitian Badan Keahlian DPR RI.

Trihartono, A., Indrastuti, S., & Nisya, C. 2020. *Keamanan dan Sekuritisasi dalam Hubungan Internasional.* Depok: Melvana.

Acuan artikel dalam Jurnal:

Arifah, D. A. 2011. "Kasus Cybercrime di Indonesia" dalam *Jurnal Bisnis dan Ekonomi, Vol. 18, No. 2,* 185-195.

Chotimah, H. H. 2019. "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara" dalam *Politicia, Vol. 10 No. 2* , 113-128. doi:10.22212/jp.v10i2.1447

Hansen, L., & Nissenbaum, H. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School" dalam *International Studies Quarterly (53)* , 1155-1175. doi:10.1111/j.1468-2478.2009.00572.x

Palinggi, S., Palelleng, S., & Allolinggi, L. R. 2020. "Peningkatan Rasio Kejahatan Cyber dengan Pola Interaksi Sosio Engineering pada Periode Akhir Era Society 4.0 di Indonesia" dalam *Jurnal Ilmiah Dinamika Sosial Vol. 4 No. 1 ,* 45-63. doi:10.38043/jids.v4il.2314

Islami, M. J. 2017. Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. *Jurnal Masyarakat*

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

Telematika dan Informasi Vol 8 (2) , 137-144. doi:10.17933/mti.v812.108

Kwarto, F., & Angsito, M. 2018. "Pengaruh Cyber Crime Terhadap Cyber Security Compliance di Sektor Keuangan" dalam *Jurnal Akuntansi Bisnis Vol. 11 No. 2* , 99-110. doi: http://dx.doi.org./10.30813/jab.v11i2.1382

Sudarmadi, D. A., & Runturambi, A. J. 2019. "Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia" dalam *Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 2 No. 2,* 157-178. doi: https://doi.org/10.21609/jkskn.v2i2.28

Wibowo, M. H., & Fatimah, N. (2017). "Ancaman Phising Terhadap Pengguna Sosial Media dalam Dunia Cyber Crime" dalam *JOIECT, Vol. 1, No. 1,* 1-5. doi://doi.org/10.29100/v1i1.69.g47

Acuan artikel dalam website:

BSSN, 2017. "Pembentukan Badan Siber dan Sandi Negara (BSSN)" dalam *https://bssn.go.id/pembentukan-badan-siber-dan-sandi-negara-bssn/*

BSSN, 2018. *"BSSN Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber dengan Pemerintahan Inggris Raya" https://bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/*

BSSN, 2019. "Buku (KLiKS BSSN UNTUK NEGERI) Kaleidoskop KLiKS BSSN Tahun 2019" dalam *https://bssn.go.id/buku-kliks-bssn-untuk-negeri-kaleidoskop-kliks-bssn-tahun-2019/*

BSSN, 2019. "PRESS RELEASE: BSSN Gelar Diskusi Publik dan Simposium Nasional RUU Keamanan dan Ketahanan Siber" dalam *https://bssn.go.id/press-release-bssn-gelar-diskusi-publik-dan-simposium-nasional-ruu-keamanan-dan-ketahanan-siber/*

BSSN, 2019. "Press Release: BSSN Launching Gov-CSIRT, Indonesia Kini Punya Tim Respon Insiden Siber" dalam *https://bssn.go.id/press-release-bssn-launching-gov-csirt-indonesia-kini-punya-tim-response-insiden-siber/*

Kurniawan, 2020. "Tingkatkan Keamanan Siber Nasional, BSSN Susun Draft SKSN" dalam *https://m.merdeka.com/peristiwa/tingkatkan-keamanan-siber-nasional-bssn-susun-draft-sksn.html*

Rahman, 2019. "BSSN serap Ide, Gagasan dan Best Practice Pengamanan" cyberthreat.id:*htpps://m.cyberthreat.id/read/2455/BSSN-Serap-Ide-Gahasan-dan-Best-Practice-Pengamanan-IKKN*

Acuan dari tugas akhir, laporan penelitian, skripsi, tesis dan desertasi :

APJII. 2018. *Laporan Survei Penetrasi & Profil Perilaku Pengguna Internet Indonesia.* Jakarta: Polling Indonesia.

APJII. 2020. *Laporan Survey Internet APJII 2019-2020 (Q2).* Jakarta: Indonesia Survey Data Center.

BSSN. 2019. *Indonesia Cyber Security Monitoring Report 2019.* Jakarta:

Global Political Studies Journal
Volume 7 Nomor 1 Edisi April 2023
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v7i1

Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara.

BSSN. 2020. *Honeynet Project BSSN - IHP*. Jakarta: Badan Siber dan Sandi Negara.

ID-SIRTII/CC. 2018. *Indonesia Cyber Security Monitoring Report 2018.* Jakarta: Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center.

Pusat Kajian Anggaran Badan Keahlian DPR, RI. (2021). *Analisis RUU Tentang APBN: Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan.* Jakarta: Pusat Kajian Anggaran Badan Keahlian DPR RI.