ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.2, 2019

Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia

Damar Apri Sudarmadi[1], Arthur Josias Simon Runturambi[2]
damar.apri@bssn.go.id, simonrbi@yahoo.com

Abstract

Cybersecurity governance in Indonesia is still partial and sectoral, resulting in the handling of cybersecurity problems not yet integrated. This makes cyber threats even more real, especially when linked to threats to cybersecurity for government and private institutions. Therefore, cybersecurity management must be carried out in an integrated manner to prevent cyber threats in all aspects of national and state life. In 2017, the National Cyber and Crypto Agency (BSSN) was formed based on the Presidential Regulation on BSSN which states that BSSN is tasked with implementing cyber security effectively and efficiently by utilizing, developing and consolidating all parties related to cybersecurity. The establishment of the BSSN considers that the cybersecurity sector is one of the areas in government that must be strengthened and encouraged in order to realize national security, increase economic growth, ensure the implementation of government policies and programs in the cybersecurity sector. BSSN was formed based on urgent needs in the midst of various challenges and problems related to the implementation of cybersecurity and encryption. BSSN is a government institution that is under and responsible to the President. The formation of BSSN is expected to be able to face problems and challenges in the present and future cyber era. This research is a descriptive type of research using a qualitative approach that seeks to explain the strategy of the National Cyber and Crypto Agency (BSSN) to increase commitment in the field of cybersecurity in dealing with cyber threats in Indonesia.

Keywords: *Strategy, National Cyber and Crypto Agency, Cyber Threat, Cybersecurity, Global Cybersecurity Index.*

[1] Alumni Mahasiswa Kajian Ketahanan Nasional SKSG Universitas Indonesia
[2] Dosen Program Kajian Ketahanan Nasional SKSG Universitas Indonesia dan Kriminolog Universitas Indonesia

1. Pendahuluan

Teknologi Informasi dan Komunikasi (TIK) seperti pedang bermata dua, karena dapat berkontribusi dalam meningkatkan kemajuan peradaban manusia serta dapat juga menjadi sarana yang efektif dalam pelanggaran hukum. Transformasi TIK membuat ancaman siber yang dihadapi suatu negara menjadi lebih kompleks, mengubah pemahaman terhadap kekuatan dan kedaulatan negara, tidak hanya dilihat dari aspek ekonomi dan militer yang dimiliki, tetapi juga dilihat dari aspek kekuatan siber dalam menghadapi ancaman siber. TIK dapat menjadi sumber dari berbagai ancaman dengan aktor (sumber ancaman) yang berasal dari pemerintah, organisasi, kelompok, dan perorangan yang dilakukan dengan unsur kesengajaan maupun tidak dengan maksud untuk mendapatkan keuntungan secara politik, militer, dan ekonomi, maupun dengan tujuan lain. Dalam era siber, jika suatu negara tidak mampu untuk menguasai TIK secara baik dan tepat guna serta terjadi penyalahgunaan TIK, hal tersebut dapat menjadi sumber ancaman bagi keamanan dan ketahanan nasional suatu negara. Keamanan siber memiliki peran penting dalam menjaga keamanan informasi karena menjadi hal yang krusial untuk menjaga data dalam media penyimpanan dan menjamin informasi yang dikirim dalam keadaan aman serta perlindungan sistem informasi terhadap ancaman siber.

Berdasarkan publikasi The Global Cybersecurity Index (GCI) 2017 yang dirilis oleh International Telecommunication Union (ITU), kondisi keamanan siber Indonesia berada dalam tahap pendewasaan (maturing stage) dan termasuk dalam negara dengan kategori keamanan siber yang lemah. GCI merupakan survei yang digunakan untuk mengukur komitmen negara-negara anggota terhadap peningkatan kesadaran di bidang keamanan siber. Nilai GCI adalah indeks gabungan yang menjadi tolok ukur untuk memantau dan membandingkan tingkat komitmen keamanan siber yang diidentifikasi oleh Global Cybersecurity Agenda (GCA) dari ITU dengan 5 (lima) pilar utama yaitu hukum, teknis, organisasi, pengembangan kapasitas dan kerja sama. Tata kelola keamanan siber di Indonesia masih bersifat parsial dan sektoral sehingga menyebabkan penanganan permasalahan keamanan siber belum terintegrasi dan belum terpadu. Hal tersebut menjadikan ancaman siber semakin nyata, terutama bila dikaitkan dengan ancaman ketahanan dan keamanan siber bagi institusi pemerintah maupun swasta. Oleh karena itu, pengelolaan keamanan siber mutlak dilakukan secara terpadu untuk mencegah ancaman siber pada segala aspek kehidupan berbangsa dan bernegara.

Pada tahun 2017, Badan Siber dan Sandi Negara (BSSN) dibentuk berdasarkan Peraturan Presiden tentang BSSN yang menyatakan bahwa BSSN bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan seluruh pihak yang terkait dengan keamanan siber. Pembentukan BSSN mempertimbangkan bahwa bidang keamanan siber menjadi salah satu bidang dalam pemerintahan yang harus diperkuat dan didorong dalam rangka mewujudkan keamanan nasional, meningkatkan pertumbuhan ekonomi, menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber. BSSN dibentuk berdasarkan kebutuhan yang mendesak di tengah berbagai tantangan dan masalah terkait dengan penyelenggaraan keamanan siber dan persandian. BSSN merupakan lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden. Pembentukan BSSN diharapkan mampu menghadapi permasalahan dan tantangan dalam era siber di masa sekarang dan yang akan datang serta guna meningkatkan komitmen bidang keamanan siber dalam menghadapi ancaman siber di Indonesia.

2. Landasan Teoritis

2.1. Strategi

Strategi merupakan rangkaian tindakan manajerial dan keputusan yang menentukan kinerja perusahaan dalam jangka panjang. Ruang lingkup manajemen strategi yaitu pengamatan lingkungan, perumusan strategi (perencanaan strategis atau perencanaan jangka panjang), implementasi strategi dan evaluasi serta pengendalian secara efektif dan efisien. Perumusan strategi merupakan proses yang dilaksanakan oleh para eksekutif senior untuk mengevaluasi keunggulan dan kelemahan yang berkaitan dengan peluang dan ancaman yang ada dalam lingkungan organisasi, kemudian menetapkan strategi yang disesuaikan dengan kompetensi inti organisasi dengan peluang lingkungan. Setiap organisasi mempunyai tipa strategi yang berbeda dalam mencapai tujuan organisasi.

Strategi adalah alat untuk mencapai tujuan atau keunggulan bersaing dengan melihat faktor eksternal dan internal organisasi. Organisasi melakukan tindakan yang dapat menjadikan keuntungan baik untuk organisasi maupun pihak lain yang berada di bawah kendali organisasi. Identifikasi faktor internal yaitu dengan merumuskan keunggulan dan kelemahan yang berasal dari dalam organisasi, sedangkan identifikasi faktor eksternal yaitu dengan merumuskan peluang dan ancaman yang berasal dari luar organisasi. BSSN sebagai organisasi yang mempunyai tugas dan fungsi dalam bidang keamanan siber diharapkan dapat merumuskan strategi dalam menghadapi ancaman dengan mengacu pada 5 (lima) pilar GCI.

2.2. Keamanan Siber

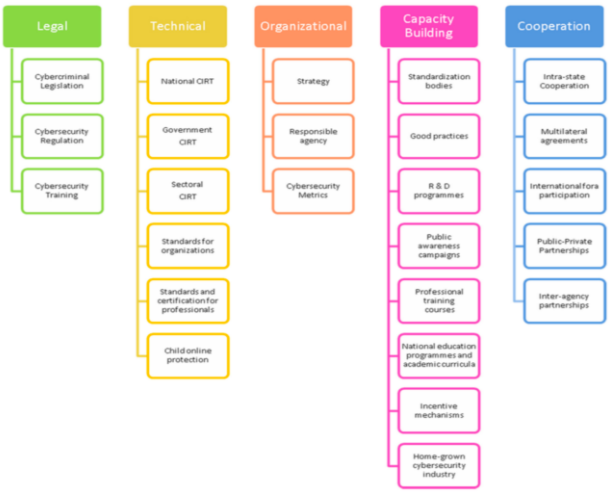
Keamanan siber adalah kumpulan alat, kebijakan, konsep keamanan, pengamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan aset organisasi dan pengguna. Aset organisasi dan pengguna mencakup perangkat komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirim dan/atau disimpan di dunia siber. Keamanan siber berusaha untuk memastikan pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap risiko keamanan di dunia siber. Keamanan siber memiliki peran penting dalam menjaga keamanan informasi karena menjadi hal yang krusial untuk menjaga data dalam media penyimpanan dan menjamin informasi yang dikirim dalam keadaan aman. Keamanan siber adalah perlindungan sistem siber terhadap ancaman siber. Peningkatan perlindungan terhadap informasi dan sistem terhadap akses yang tidak sah (lawan) melalui kerahasiaan, integritas, otentikasi, nir-penyangkalan, dan ketersediaan informasi untuk menghindari serangan siber. Termasuk menyediakan pemulihan sistem informasi dengan menggabungkan kemampuan perlindungan, deteksi, dan reaksi.

Organisasi perlu menyusun rencana komprehensif untuk menangani kebutuhan keamanannya. Organisasi didorong untuk melihat keamanan sebagai proses atau cara berpikir tentang bagaimana melindungi sistem, jaringan, aplikasi, dan sumber daya. Teknik keamanan siber dapat digunakan untuk memastikan ketersediaan, integritas, keaslian, nir-penyangkalan, dan kerahasiaan sistem. Keamanan siber dapat digunakan untuk memastikan privasi pengguna sehingga membangun kepercayaan dari pengguna. Ruang lingkup dunia siber yaitu perangkat lunak yang berjalan pada perangkat komputasi, informasi yang tersimpan (termasuk yang ditransmisikan) pada perangkat atau informasi yang dihasilkan oleh perangkat ini. Instalasi dan bangunan yang menjadi tempat perangkat juga merupakan bagian dari dunia siber.

2.3. *Global Cybersecurity Index* (GCI)

Global Cybersecurity Index (GCI) merupakan hasil survei penelitian yang dilaksanakan oleh International Telecommunication Union (ITU) bersama dengan mitra internasional dari sektor publik dan swasta serta akademisi. ITU merupakan

badan khusus dari Perserikatan Bangsa-Bangsa (PBB) yang menangani bidang TIK. Tujuan dari keamanan siber yaitu mencakup aspek keamanan, ekonomi, sosial yang sejalan dengan kepentingan nasional yaitu bertujuan untuk menjaga keamanan negara. Merujuk laporan yang dihasilkan ITU bersama dengan mitra internasional dari sektor publik dan swasta serta akademisi, telah menetapkan GCI dengan tujuan utama untuk membangun kapasitas di tingkat nasional, regional dan internasional, melalui penilaian keterlibatan negara-negara dalam keamanan siber. GCI merupakan survei yang digunakan untuk mengukur komitmen negara terhadap peningkatan kesadaran keamanan siber. GCI membahas seputar Global Cybersecurity Agenda (GCA) dari ITU dengan 5 (lima) pilar yang dijabarkan dalam 25 indikator, dimana pemeringkatan dan penilaian yang dilakukan oleh ITU dengan menggunakan metodologi pengumpulan data melalui survei daring dan verifikasi data primer dari negara yang merespon, serta data sekunder bagi negara yang tidak memberikan respon terhadap survei daring. Pada tahun 2017, Indonesia berada pada peringkat 70 dari 169 negara, dengan nilai 0,424 dimana rata-rata nilai global 0,357. GCI mempunyai ruang lingkup yang dikategorikan dalam 5 (lima) pilar yaitu hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama.



Gambar 1. Ruang Lingkup GCI: Pilar dan Subpilar (Indikator)

Tujuan utama GCI adalah untuk mengukur jenis, tingkat dan evolusi dari waktu ke waktu komitmen keamanan siber di negara-negara terhadap negara lain; kemajuan dalam komitmen keamanan siber dari semua negara dari perspektif global, kemajuan dalam komitmen keamanan siber dari perspektif regional, pembagian komitmen keamanan siber dan perbedaan antara negara, dan tingkat keterlibatan dalam program dan inisiatif keamanan siber. Tujuan dari GCI sebagai prakarsa untuk membantu negara mengidentifikasi area perbaikan di bidang keamanan siber, serta untuk memotivasi dalam mengambil tindakan guna meningkatkan peringkat keamanan siber, sehingga membantu meningkatkan keseluruhan tingkat komitmen terhadap keamanan siber di seluruh dunia. GCI bertujuan untuk mengilustrasikan praktik di negara lain sehingga negara-negara anggota dapat menerapkan aspek-aspek terpilih yang sesuai dengan lingkungan nasional di negara masing-masing dengan manfaat tambahan yaitu untuk membantu menyelaraskan praktik dan membina budaya keamanan skala global.

3. Metodologi

Penelitian ini merupakan jenis penelitian desktriptif dengan menggunakan pendekatan kualitatif yang berupaya menjelaskan tentang strategi BSSN guna meningkatkan komitmen bidang keamanan siber dalam menghadapi ancaman siber di Indonesia. Pendekatan kualitatif dipilih, karena dalam melakukan penelitian menggunakan suatu alat pengukuran yang tidak berdasarkan penghitungan statistik atau prosedur kuantifikasi lainnya, yang perolehan datanya dari kuesioner dan wawancara yang dilakukan terhadap informan kunci. Dari informasi tersebut, peneliti berupaya untuk mencari makna yang ada di balik fakta. Metode penelitian deskriptif dipilih karena dapat menggambarkan atau melukiskan keadaan subjek atau objek penelitian pada saat sekarang berdasarkan fakta-fakta yang tampak atau sebagaimana adanya, yang kemudian nantinya

akan digunakan untuk menarik suatu kesimpulan.

Peneliti menggambarkan dan menjelaskan data dan informasi yang diperoleh, kemudian melakukan analisis serta menginterpretasikan data dan informasi tersebut. Peneliti menggunakan sumber data primer dan sekunder dalam melaksanakan penelitian. Data primer diperoleh dari sumber langsung melalui wawancara kepada sumber informasi yang dianggap mengetahui dan mampu menjawab pertanyaan yang telah disusun oleh peneliti. Data sekunder yang digunakan yaitu didapat dari referensi buku, jurnal, laporan penelitian atau karya ilmiah lainnya terkait dengan keamanan siber serta dari sumber dokumentasi yang diperoleh dari lembaga, organisasi maupun perorangan, seperti pemberitaan dari media daring dan publikasi resmi dari organisasi tertentu. Teknik analisis data yang digunakan adalah kualitatif, dalam menganalisis data yang diperoleh lebih dilakukan bersamaan dengan pengumpulan data. Peneliti menggunakan teknik analisis data yaitu triangulasi data untuk melakukan pemeriksaan keabsahan atau validitas data, selanjutnya melakukan reduksi data untuk merangkum hasil penelitian yang didapat, kemudian melakukan penarikan kesimpulan.

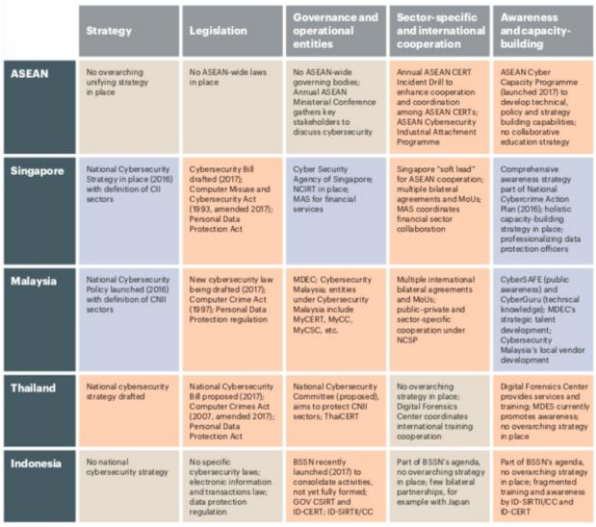
4. Pembahasan

4.1. Profil Organisasi BSSN

Badan Siber dan Sandi Negara (BSSN) resmi dibentuk oleh Presiden pada tahun 2017 yaitu berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Tahun 2017 Nomor 100) sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Tahun 2017 Nomor 277). BSSN mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.

BSSN merupakan lembaga pemerintah yang dipimpin oleh Kepala dan berada di bawah serta bertanggung jawab kepada Presiden. BSSN dibentuk dengan mempertimbangkan bidang keamanan siber merupakan salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional. Pembentukan BSSN merupakan upaya untuk menata Lembaga Sandi Negara (Lemsaneg) menjadi BSSN guna menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber. Dibentuknya BSSN merupakan sebuah kebutuhan yang mendesak di tengah berbagai masalah dan tantangan terkait dengan keamanan siber dan persandian. BSSN merupakan sebuah badan yang merupakan peleburan dari Lemsaneg dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Dit. Kaminfo, Ditjen Aptika, Kominfo). Pembentukan BSSN diharapkan mampu menghadapi permasalahan dan tantangan dalam dunia siber di masa sekarang dan yang akan datang.

Gambar 2. Kondisi 25 Indikator GCI 2017 di Region Asia Pasifik



	Strategy	Legislation	Governance and operational entities	Sector-specific and international cooperation	Awareness and capacity-building
ASEAN	No overarching unifying strategy in place	No ASEAN-wide laws in place	No ASEAN-wide governing bodies; Annual ASEAN Ministerial Conference gathers key stakeholders to discuss cybersecurity	Annual ASEAN CERT Incident Drill to enhance cooperation and coordination among ASEAN CERTs; ASEAN Cybersecurity Industrial Attachment Programme	ASEAN Cyber Capacity Programme (launched 2017) to develop technical, policy and strategy building capabilities; no collaborative education strategy
Singapore	National Cybersecurity Strategy in place (2016) with definition of CII sectors	Cybersecurity Bill drafted (2017); Computer Misuse and Cybersecurity Act (1993, amended 2017); Personal Data Protection Act	Cyber Security Agency of Singapore; NCIRT in place; MAS for financial services	Singapore "soft lead" for ASEAN cooperation; multiple bilateral agreements and MoUs; MAS coordinates financial sector collaboration	Comprehensive awareness strategy part of National Cybercrime Action Plan (2016); holistic capacity-building strategy in place; professionalizing data protection officers
Malaysia	National Cybersecurity Policy launched (2016) with definition of CNII sectors	New cybersecurity law being drafted (2017); Computer Crime Act (1997); Personal Data Protection regulation	MDEC; Cybersecurity Malaysia; entities under Cybersecurity Malaysia include MyCERT, MyCC, MyCSC, etc.	Multiple international bilateral agreements and MoUs; public-private and sector-specific cooperation under NCSP	CyberSAFE (public awareness) and CyberGuru (technical knowledge); MDEC's strategic talent development; Cybersecurity Malaysia's local vendor development
Thailand	National cybersecurity strategy drafted	National Cybersecurity Bill proposed (2017); Computer Crimes Act (2007, amended 2017); Personal Data Protection Act	National Cybersecurity Committee (proposed), aims to protect CNII sectors; ThaiCERT	No overarching strategy in place; Digital Forensics Center coordinates international training cooperation	Digital Forensics Center provides services and training; MDES currently promotes awareness; no overarching strategy in place
Indonesia	No national cybersecurity strategy	No specific cybersecurity laws; electronic information and transactions law; data protection regulation	BSSN recently launched (2017) to consolidate activities, not yet fully formed; GOV CSIRT and ID-CERT; ID-SIRTII/CC	Part of BSSN's agenda, no overarching strategy in place; few bilateral partnerships, for example with Japan	Part of BSSN's agenda, no overarching strategy in place; fragmented training and awareness by ID-SIRTII/CC and ID-CERT

Gambar 3. Kebijakan Keamanan Siber di Negara ASEAN

4.2. Ancaman Siber

Ancaman dapat dimaknai sebagai usaha dan tindakan, baik yang berasal dari dalam maupun luar negeri yang berpotensi membahayakan keselamatan bangsa, kedaulatan negara, dan keutuhan wilayah negara. Konsep ancaman mencakup hal yang selalu berubah berkembang dari waktu ke waktu. Ancaman terhadap kedaulatan negara yang awalnya hanya bersifat konvensional (fisik) mengalami perkembangan multidimensional (fisik dan nonfisik) yang berasal dari dalam maupun luar negeri. Ancaman bersifat multidimensional dapat bersumber dari permasalahan politik, ekonomi, sosial, budaya maupun permasalahan keamanan yang berkaitan dengan kejahatan internasional, misalnya terorisme, narkotika, imigran gelap, bajak laut, pencurian kekayaan alam, dan perusakan lingkungan. Ancaman dikategorikan menjadi 2 (dua) jenis yaitu ancaman militer dan ancaman nonmiliter. Komponen ancaman terdiri atas kemampuan dan niat dari penyerang. Kemampuan terdiri dari 2 (dua) komponen turunan yaitu pengetahuan dan sumber daya, sedangkan niat dapat diukur dari 2 (dua) hal yaitu keinginan dan harapan.

Siber adalah tempat yang sangat dinamis dan kompleks dimana kepentingan dan tindakan pribadi serta ketidaksengajaan secara luas mempengaruhi suatu hubungan dijalin. Siber sebagai suatu kondisi yang keberadaan utamanya dalam dunia virtual diciptakan oleh interaksi mesin-mesin komunikasi, atau yang terkenal dengan nama world wide web (www). Siber yaitu sekumpulan infrastruktur teknologi informasi dan komunikasi, aplikasi, dan peralatan dimana sebuah organisasi, perusahaan, atau misi bergantung, biasanya ditambah penunjang berupa internet, jaringan telekomunikasi, sistem komputer, peralatan pribadi, dan ketika terhubung dengan teknologi informasi, sensor, prosesor, dan mikrokontroler yang tertanam.

Ancaman yang muncul dari dunia siber disebut ancaman siber yaitu potensial insiden siber yang dapat menyebabkan hasil yang tidak diinginkan, yang mengakibatkan kerusakan pada sistem atau organisasi. Ancaman mungkin berasal dari luar atau internal dan mungkin berasal dari individu atau organisasi. Pada dasarnya ancaman siber dapat datang dari mana saja, dalam bentuk apa saja, dapat mengakibatkan gangguan yang berbeda-beda pada objek yang berbeda-beda pula. Ancaman siber pada dasarnya adalah suatu kondisi dalam dunia siber baik disengaja ataupun tidak yang dapat menimbulkan kerusakan, gangguan, kerugian, dan instabilitas pada infrastruktur teknologi informasi dan komunikasi. Salah satu contoh ancaman siber yang tidak disengaja yaitu ketika memperbarui perangkat lunak secara tidak sengaja merusak sistem, sedangkan ancaman siber yang disengaja terdiri atas dua jenis yaitu serangan tertuju (serangan yang terjadi ketika suatu kelompok atau individu secara spesifik menyerang suatu aset siber) dan serangan tidak tertuju (objek serangan tidak ditetapkan atau acak).

Berdasarkan publikasi ITU - National Cybersecurity Strategy Guide, ancaman siber dibedakan berdasarkan karakter, dampak, asal (sumber) dan aktor. Ancaman berdasarkan karakter yaitu ancaman tidak disengaja dan ancaman disengaja. Ancaman tidak disengaja terjadi tanpa niat yang direncanakan (misalnya: kesalahan sistem atau perangkat lunak dan

kerusakan fisik), sedangkan ancaman disengaja dihasilkan dari tindakan kesengajaan terhadap keamanan aset. Ancaman disengaja dilakukan dengan pemeriksaan rutin jaringan komputer menggunakan alat pemantau, hingga serangan yang canggih menggunakan pengetahuan sistem khusus. Ancaman disengaja yang benar-benar terjadi disebut dengan serangan. Ancaman berdasarkan dampak yaitu ancaman aktif dan ancaman pasif. Ancaman aktif adalah ancaman yang mengakibatkan perubahan pada keadaan suatu sistem, seperti modifikasi data dan kerusakan peralatan fisik, sedangkan ancaman pasif tidak mengakibatkan perubahan keadaan pada peralatan. Ancaman pasif bertujuan untuk mengumpulkan informasi dari sebuah sistem tanpa mempengaruhi sumber daya sistem. Teknik ancaman pasif yang umum termasuk menguping, penyadapan dan analisis paket atau inspeksi mendalam.

Definisi sumber ancaman yaitu entitas atau pihak yang ingin melanggar kontrol keamanan informasi atau aset fisik. Sumber ancaman bertujuan untuk mendapatkan keuntungan dari pelanggaran tersebut. Identifikasi sumber ancaman utama yaitu dinas intelijen asing, pegawai yang tidak puas, jurnalis investigatif, organisasi ekstrim, hacktivists, kelompok kriminal terorganisir. Aktor ancaman adalah entitas yang benar-benar melakukan serangan atau jika terjadi kecelakaan akan memanfaatkan kecelakaan tersebut. Misalnya, jika kelompok kejahatan terorganisir berusaha menggalang seorang pegawai, maka kelompok tersebut adalah sumber ancaman dan pegawai tersebut merupakan aktor ancaman. Niat sumber ancaman dan aktor ancaman sering terwujud dalam serangan terutama karena memanfaatkan kelemahan dalam kontrol keamanan. Kelemahan bisa dikarenakan perangkat lunak dan konfigurasi yang buruk. Bahkan kontrol teknis yang baik bisa gagal jika serangan rekayasa sosial dapat memanfaatkan pegawai yang berpengetahuan lemah dalam bidang keamanan.

4.3. Penyelenggaraan Keamanan Siber di Indonesia

Penyelenggaraan keamanan siber di Indonesia mengacu pada 5 (lima) pilar GCI 2017 yaitu aspek hukum, aspek teknis, aspek organisasi, aspek pengembangan kapasitas dan aspek kerja sama. Tujuan dari penilaian berdasarkan GCI 2017 yaitu untuk membangun kapasitas pada level nasional, regional maupun internasional dalam bidang keamanan siber.

1. Aspek Hukum

Aspek hukum diukur berdasarkan keberadaan lembaga hukum dan kerangka kerja yang berhubungan dengan keamanan siber dan kejahatan siber. Aspek hukum terdiri atas 3 (tiga) indikator yaitu keberadaan UU Kejahatan Siber, UU Keamanan Siber, dan penyelenggaraan pelatihan keamanan siber bagi aktor hukum.

Fokus indikator UU Kejahatan Siber yaitu menilai ketersediaan dan kelengkapan keamanan TIK dan perlindungan data privasi, serta berhubungan dengan UU HAM, serta status negara dalam kaitannya dengan perjanjian regional dan internasional yang secara langsung atau tidak langsung terkait dengan keamanan siber. Indonesia mempunyai peraturan dengan substansi yang berkaitan dengan kejahatan siber yaitu UU ITE, meskipun bentuk peraturan tidak secara khusus berdiri sendiri mengatur tentang kejahatan siber.

Fokus indikator UU Keamanan Siber yaitu melihat kapasitas pemerintah dalam merancang dan memberlakukan UU nasional serta mendampingi hukum secara langsung dan tidak langsung yang berkaitan dengan keamanan siber, dengan penekanan khusus pada topik keamanan TIK, privasi dan perlindungan data, dan kejahatan siber. Indonesia meskipun tidak mempunyai peraturan mengenai keamanan siber yang berdiri sendiri, tetapi Indonesia mempunyai beberapa peraturan yang terkait dengan keamanan siber. Peraturan tersebut meliputi topik keamanan TIK, privasi dan perlindungan data dan kejahatan siber.

BSSN diharapkan dapat mendorong penyusunan UU Keamanan Siber di Indonesia.

Fokus indikator pelatihan keamanan siber bagi aktor hukum yaitu diselenggarakannya pelatihan keamanan siber bagi aparat penegak hukum, peradilan dan aktor hukum lain. Indonesia sudah menyelenggarakan pelatihan bagi aktor hukum secara rutin dan berkala, tetapi materi pelatihan belum berkaitan dengan keamanan siber. BSSN diharapkan dapat menginisiasi pelatihan yang diselenggarakan bagi aktor hukum dengan pemberian materi terkait dengan keamanan siber, sehingga aktor hukum mendapat pengetahuan dan informasi terkait dengan perkembangan teknologi keamanan siber serta mengetahui.

2. Aspek Teknis

Aspek teknis diukur berdasarkan keberadaan institusi teknis dan kerangka kerja yang berhubungan dengan keamanan siber. Aspek teknis terdiri atas 6 (enam) indikator yaitu keberadaan 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.

Fokus indikator CERT nasional yaitu adanya organisasi yang diberi mandat dengan tanggung jawab nasional dalam penanganan insiden siber skala nasional. Indonesia mempunyai CERT nasional yaitu BSSN yang diberikan mandat tanggung jawab nasional untuk memantau, mengelola dan menangani insiden siber skala nasional dengan pendekatan multi pemangku kepentingan. BSSN memberikan layanan pada sektor pemerintah, sektor IIKN dan pelaku ekonomi digital.

Fokus indikator CERT pemerintah yaitu adanya CERT yang bertanggung jawab pada sektor pemerintah. Indonesia mempunyai CERT nasional yaitu BSSN yang diberikan mandat tanggung jawab nasional untuk memantau, mengelola dan menangani insiden siber pada sektor pemerintah.

Fokus indikator CERT sektoral yaitu CERT yang bertanggung jawab pada sektor tertentu. Indonesia tidak mempunyai CERT sektoral yang memberikan respon dalam penanganan keamanan komputer atau insiden siber yang mempengaruhi sektor tertentu. BSSN diharapkan dapat bersiap jika ada kebutuhan yang mendesak terkait kebutuhan pembentukan CERT sektoral.

Fokus indikator standar keamanan siber bagi organisasi yaitu adanya kerangka kerja yang disetujui pemerintah dalam penerapan standar keamanan siber dalam sektor pemerintah, IIKN, bahkan sektor swasta. Indonesia tidak mempunyai kerangka kerja dan standar bagi organisasi yang mengacu pada standar mengenai dengan keamanan siber. Namun, Indonesia mempunyai standar yang terkait dengan keamanan siber yaitu SMKI yang tertuang dalam Standar Nasional Indonesia (SNI) ISO/IEC 27001. Penilaian tingkat kesiapan dan kematangan SMKI dengan mengisi alat bantu penilaian yang disebut Indeks KAMI. BSSN diharapkan dapat menyusun standar penyelenggaraan keamanan siber bagi organisasi, sektor pemerintah, IIKN dan pelaku ekonomi digital.

Fokus indikator standar dan sertifikasi bagi profesional bidang keamanan siber yaitu adanya kerangka kerja untuk sertifikasi dan akreditasi para profesional keamanan siber yang diakui secara internasional. Indonesia tidak memiliki kerangka kerja keamanan siber nasional mengenai sertifikasi dan akreditasi lembaga nasional maupun profesional. Namun, profesional di bidang keamanan siber sudah mendapat sertifikasi yang diakui secara internasional dalam bidang keamanan siber. Selain itu, Indonesia sudah mempunyai SKKNI Bidang Komunikasi dan Informasi.

Fokus indikator perlindungan daring terhadap anak yaitu adanya suatu badan hukum yang menjelaskan bahwa setiap kejahatan dapat dilakukan terhadap anak di dunia nyata juga dapat dilakukan di internet maupun di tempat lain dalam jaringan elektronik serta dibutuhkan UU yang mengatur tindakan berorientasi seksual pada anak. Indonesia tidak mempunyai peraturan yang mengatur mengenai

perlindungan daring terhadap anak. Namun, Indonesia mempunyai KPAI yang bertugas dalam bidang perlindungan anak serta mempunyai UU yang berkaitan dengan perlindungan anak yaitu UU Perlindungan Anak dan UU Pornografi, tetapi kedua UU tersebut tidak secara khusus mengatur tentang perlindungan daring terhadap anak. BSSN diharapkan untuk dapat mendorong perumusan perlindungan daring terhadap anak dengan berkoordinasi dengan instansi terkait.

3. Aspek Organisasi

Aspek organisasi diukur berdasarkan keberadaan lembaga koordinasi kebijakan dan strategi untuk pengembangan keamanan siber di tingkat nasional. Aspek organisasi terdiri atas 3 (tiga) indikator yaitu keberadaan strategi keamanan siber nasional; organisasi yang bertanggung jawab dalam bidang keamanan siber; dan metrik pengukuran perkembangan keamanan siber.

Fokus indikator strategi keamanan siber nasional yaitu adanya strategi atau kebijakan keamanan siber nasional yang berkontribusi terhadap keamanan siber. Indonesia tidak mempunyai strategi atau kebijakan keamanan siber nasional. BSSN diharapkan dapat menjadi organisasi titik fokus dalam perumusan strategi keamanan siber nasional.

Fokus indikator organisasi yang bertanggung jawab yaitu adanya organisasi yang bertanggung jawab untuk menyusun dan menerapkan strategi atau kebijakan keamanan siber nasional sekaligus bertindak sebagai CERT nasional. Pemerintah Indonesia pada tahun 2017 membentuk BSSN yang bertanggung jawab dalam bidang keamanan siber, tetapi BSSN masih menyelesaikan permasalahan internalisasi dan harmonisasi organisasi dalam rangka membentuk pondasi organisasi yang kuat. BSSN diharapkan mampu menjadi koordinator dalam penyelenggaraan keamanan siber di Indonesia yang dapat bekerja sama dengan seluruh pemangku kepentingan keamanan siber yaitu sektor pemerintah, IIKN dan pelaku ekonomi digital sesuai dengan mandat Perpres BSSN.

Fokus indikator metrik keamanan siber yaitu adanya benchmarking nasional yang diakui secara resmi digunakan untuk mengukur perkembangan keamanan siber, strategi penilaian risiko, audit keamanan siber, dan alat serta tindakan lain untuk menilai atau mengevaluasi kinerja yang dihasilkan untuk perbaikan di masa mendatang. Indonesia tidak mempunyai metode resmi yang digunakan untuk mengukur pengembangan keamanan siber, strategi penilaian risiko, audit keamanan siber, dan alat serta kegiatan lain untuk menilai atau mengevaluasi kinerja yang dihasilkan untuk perbaikan. BSSN diharapkan dapat menyusun perumusan terkait metrik keamanan siber di Indonesia.

4. Aspek Pengembangan Kapasitas

Aspek pengembangan kapasitas diukur berdasarkan keberadaan penelitian dan pengembangan; program pendidikan dan pelatihan; profesional bersertifikat dan lembaga sektor publik yang mendukung pengembangan kapasitas. Aspek pengembangan kapasitas terdiri atas delapan indikator yaitu keberadaan organisasi standardisasi pada suatu negara; dokumen praktik terbaik berkaitan dengan keamanan siber; program penelitian dan pengembangan; kampanye kesadaran publik; kursus pelatihan profesional; program pendidikan dan kurikulum akademik skala nasional berkaitan dengan keamanan siber; mekanisme insentif yang diberikan dalam bidang keamanan siber; dan industri keamanan siber dalam negeri.

Fokus indikator badan standardisasi yaitu mengukur keberadaan badan standardisasi yang dapat mengembangkan dan mengimplementasikan standar keamanan siber. Indonesia mempunyai Badan Standardisasi Nasional (BSN) yang melaksanakan tugas di bidang standardisasi nasional. Salah satu standar yang terkait dengan keamanan siber yaitu SNI ISO/IEC 27032:2014 dengan judul Teknologi Informasi - Teknik Keamanan - Pedoman Keamanan Siber (ISO/IEC 27032:2012, IDT).

Fokus indikator praktik terbaik keamanan siber yaitu mengukur keberadaan dokumen praktik terbaik terkait dengan keamanan siber. Indonesia tidak mempunyai dokumen praktik terbaik keamanan siber, oleh karena itu BSSN diharapkan dapat menyusun panduan praktik terbaik keamanan siber yang dapat dirujuk dalam penyelenggaraan keamanan siber pada sektor pemerintah, IIKN dan pelaku ekonomi digital.

Fokus indikator program penelitian dan pengembangan yaitu mengukur penyelenggaraan program penelitian dan pengembangan pada bidang keamanan siber. Indonesia tidak mempunyai kebijakan nasional mengenai program penelitian dan pengembangan terkait keamanan siber. BSSN diharapkan dapat berkoordinasi dengan lembaga pemerintah terkait untuk dapat menyelenggarakan program penelitian dan pengembangan pada bidang keamanan siber, sehingga program tersebut dapat diselenggarakan secara terencana dan dapat berkontribusi dalam perkembangan teknologi keamanan siber.

Fokus indikator kampanye kesadaran publik yaitu mengukur penyelenggaraan kampanye kesadaran publik terkait keamanan siber. Beberapa instansi pemerintah menyelenggarakan program kampanye kesadaran publik yaitu Lemsaneg, Ditkaminfo dan ID-SIRTII. BSSN diharapkan untuk mempertahankan dan meningkatkan program kampanye kesadaran publik agar masyarakat memahami perlunya mengamankan komponen dunia siber.

Fokus indikator kursus pelatihan bagi profesional yaitu mengukur penyelenggaraan kursus pelatihan dan pendidikan bagi profesional pada bidang keamanan siber. BSSN diharapkan untuk mempertahankan dan meningkatkan program kursus pelatihan profesional keamanan siber, sehingga kemampuan dan keahlian profesional bidang keamanan siber dapat meningkat sesuai dengan perkembangan TIK dan ancaman siber serta memenuhi kebutuhan organisasi dalam penyelenggaraan keamanan siber di Indonesia.

Fokus indikator program pendidikan dan kurikulum pendidikan nasional yaitu mengukur upaya pemerintah dalam menyelenggarakan mendukung pengembangan program pendidikan dan kurikulum akademik pada bidang keamanan siber. Meskipun status GCI warna merah, Indonesia menginisiasi pengembangan program pendidikan dan kurikulum akademik pada bidang keamanan siber pada level SMK dan perguruan tinggi.

Fokus indikator mekanisme insentif yaitu mengukur penyelenggaraan mekanisme insentif yang dilaksanakan pemerintah dengan tujuan mendorong pengembangan kapasitas di bidang keamanan siber. Indonesia memberikan mekanisme insentif berupa beasiswa kepada masyarakat dan tidak memberikan insentif dalam bidang pengembangan industri dalam negeri terkait keamanan siber. BSSN diharapkan dapat menyelenggarakan program mekanisme insentif dalam bidang keamanan siber secara intensif guna pengembangan kapasitas baik dalam aspek SDM maupun teknologi.

Fokus indikator industri keamanan siber dalam negeri yaitu mengukur penyelenggaraan dukungan pemerintah dalam pengembangan dan peningkatan kualitas teknologi keamanan siber. Di Indonesia, tidak ada program pemberian mekanisme insentif dalam rangka mendorong pasar menciptakan produk dan layanan keamanan siber, karena pemerintah tidak mengalokasi anggaran untuk pengembangan teknologi keamanan siber dalam skala nasional. BSSN diharapkan menyelenggarakan program dalam rangka mendukung pengembangan dan peningkatan kualitas teknologi keamanan siber dalam negeri secara mandiri.

5. Aspek Kerja Sama

Aspek kerja sama diukur berdasarkan keberadaan kemitraan, kerangka kerja kooperatif dan jaringan berbagi informasi. Aspek kerja sama terdiri atas 5 (lima) indikator yaitu kerja sama bilateral; kerja sama

multilateral; partisipasi pada forum internasional; kerja sama pemerintah dengan swasta; dan kerja sama antar instansi pemerintah.

Fokus indikator perjanjian multilateral yaitu mengukur penyelenggaraan program nasional yang diakui secara resmi oleh pemerintah dengan beberapa pemerintah negara lain atau organisasi internasional lainnya. Status GCI yang merah menunjukkan kondisi yang tidak sesuai dengan realita yang terjadi di Indonesia terkait perjanjian multilateral Indonesia dengan organisasi atau entitas atau negara lain. BSSN diharapkan dapat meninjau ulang kondisi tersebut agar dalam penilaian GCI selanjutnya status GCI dapat diperbaiki.

Fokus indikator partisipasi pada forum internasional yaitu mengukur penyelenggaraan partisipasi suatu negara pada forum internasional dalam bidang keamanan siber. Indonesia secara rutin terlibat dalam partisipasi forum internasional yaitu FIRST. Contoh forum internasional yaitu FIRST merupakan forum yang menyatukan berbagai tim respon insiden keamanan komputer dari organisasi pemerintah, komersial, dan pendidikan.

Fokus indikator kerja sama pemerintah dengan swasta yaitu mengukur jumlah kemitraan pemerintah-swasta atau sektor khusus yang diakui secara resmi dalam bidang keamanan siber. BSSN diharapkan dapat menginisiasi kerja sama antara pemerintah dengan pihak swasta dalam pengembangan kapasitas keamanan siber, karena belum ada kerja sama antara pemerintah dengan pihak swasta.

Fokus indikator kerja sama antar instansi pemerintah yaitu mengukur penyelenggaraan kemitraan resmi antara berbagai instansi pemerintah dalam suatu negara dalam bidang keamanan siber. BSSN diharapkan untuk dapat meningkatkan kerja sama antar instansi pemerintah sehingga terjalin koordinasi dan komunikasi yang efektif dalam menghadapi ancaman siber di Indonesia.

4.4. Rekomendasi Strategi BSSN Dalam Menghadapi Ancaman Siber

Dalam rangka perbaikan tata kelola penyelenggaraan keamanan siber dibutuhkan intervensi dari pemerintah, prioritas pemerintah dengan memastikan bahwa keamanan siber dapat meningkatkan ketahanan nasional, keamanan dan kedaulatan negara. BSSN sebagai lembaga pemerintah yang bertanggung jawab dakam bidang keamanan siber diharapkan menjadi organisasi titik fokus dan koordinator dalam penyelenggaraan keamanan siber di Indonesia. Peneliti mengkategorikan berdasarkan 3 (tiga) besaran strategi yaitu (1) Penyusunan kerangka hukum siber; (2) Pengembangan kapasitas keamanan siber; dan (3) Peningkatan kerja sama keamanan siber. Berikut rekomendasi strategi yang dapat digunakan untuk meningkatkan komitmen bidang keamanan siber dalam menghadapi ancaman siber di Indonesia.

1. Penyusunan Kerangka kerja Dunia Siber
   a. Penyusunan Kerangkat Hukum Keamanan Siber

Kerangka hukum yang mengatur tentang keamanan siber di Indonesia belum ada, sehingga diperlukan landasan atau payung hukum dalam penyelenggaraan keamanan siber di Indonesia. Kerangka hukum tersebut dapat menjadi acuan bagi BSSN dalam menyelenggarakan keamanan siber agar sesuai dengan tujuan dan ketentuan peraturan-perundangan yang berlaku serta menghindari penyalahgunaan wewenang oleh pihak-pihak yang berkepentingan. Kerangka hukum keamanan siber bergantung kepada kapasitas pemerintah dalam merancang dan memberlakukan undang-undang nasional serta mendampingi hukum secara langsung maupun tidak langsung yang berkaitan dengan keamanan siber, dengan penekanan khusus pada topik keamanan TIK, perlindungan data dan privasi, serta kejahatan siber.

Berdasarkan pengalaman secara global membuktikan bahwa kerangka kerja hukum dan peraturan terkait keamanan siber lintas sektor

dengan menghadirkan mekanisme pencegahan, mitigasi, yang dipengaruhi ancaman siber. BSSN selaku lembaga pemerintah yang bertanggung jawab dalam bidang keamanan siber diharapkan untuk dapat mendorong penyusunan kerangka hukum keamanan siber, sehingga kerangka hukum yang ditetapkan harus dipatuhi oleh seluruh pemangku kepentingan yang berkaitan dengan penyelenggaraan keamanan siber di Indonesia. Kerangka hukum juga meliputi peraturan dalam penegakan kejahatan yang terjadi dalam dunia siber, karena pelanggaran hukum dalam dunia siber mempunyai mekanisme penindakan yang berbeda dengan yang terjadi di dunia nyata. Oleh karena itu, BSSN diharapkan untuk dapat menyelenggarakan program pelatihan keamanan siber bagi aktor atau aparat penegak hukum yang diselenggarakan secara rutin dan berkala yang bertujuan meningkatkan kemampuan dan memberikan perkembangan pengetahuan terbaru tentang keamanan siber. Tugas yang tidak kalah penting yaitu BSSN diharapkan dapat menginisiasi penyusunan kerangka hukum atau strategi berkaitan dengan perlindungan daring terhadap anak. Indonesia membutuhkan pengembangan kebijakan dalam melindungi anak dari perilaku negatif yang dilakukan dari media daring atau internet, mengingat bahwa kejahatan terhadap anak dapat terjadi tidak hanya di dunia nyata, tetapi juga di dunia siber.

b. Penyusunan Strategi Keamanan Siber Nasional

Indonesia belum mempunyai strategi atau kebijakan tentang keamanan siber nasional yang ditetapkan oleh pemerintah. Strategi atau kebijakan keamanan siber nasional merupakan perencanaan skala nasional berdasarkan visi tertentu untuk mencapai tujuan yang berkontribusi terhadap keamanan siber. Strategi atau kebijakan keamanan siber nasional merupakan bagian dari agenda keamanan siber dalam pemerintahan, karena membantu dalam memprioritaskan keamanan siber terhadap area kebijakan penting lain serta menentukan area tanggung jawab dan mandat dari berbagai aktor pemerintah dan pemangku kepentingan keamanan siber.

Dalam upaya menyusun kebijakan strategi keamanan siber nasional diperlukan kolaborasi multi pemangku kepentingan dalam pembentukan organisasi pusat yang menjadi titik fokus, serta dalam mengidentifikasi peran dan tanggung jawab keamanan siber lintas sektor. Selain itu, apa pun yang dimanifestasikan oleh organisasi titik fokus harus bertanggung jawab dalam mengoordinasikan pengembangan strategi keamanan siber nasional yang komprehensif. BSSN diharapkan dapat menjadi organisasi titik fokus koordinator yang bertanggung jawab dalam menyusun perumusan, penyusunan dan penerapan strategi atau kebijakan keamanan siber nasional dalam penyelenggaraan keamanan siber di Indonesia.

c. Optimalisasi Tugas dan Fungsi BSSN dan CERT

BSSN sebagai organisasi yang bertanggung jawab dalam bidang keamanan siber di Indonesia dan bertindak sebagai CERT nasional. Sampai dengan saat ini, BSSN terus melaksanakan integrasi, koordinasi, harmonisasi instansi pemerintah lain, infrastruktur informasi kritis nasional, sektor swasta, dan masyarakat sipil dalam penyelenggaraan keamanan siber di Indonesia. Optimalisasi BSSN sebagai titik fokus organisasi skala nasional dalam mengatasi permasalahan keamanan siber dan mengoordinasikan pelaksanaan keamanan siber pada tingkat nasional maupun internasional harus terus dilakukan untuk mengurangi kesenjangan dengan negara lain. BSSN juga harus dapat menyusun standar terkait keamanan siber yang dapat digunakan organisasi sebagai acuan atau rujukan dalam penyelenggaraan keamanan siber. Standar yang disusun dapat mengacu pada standar yang berlaku secara internasional, dengan penyesuaian kondisi yang cocok bagi lingkungan di Indonesia. Selain itu, BSSN bertanggung jawab dalam hal peningkatan kapasitas organisasi baik pada sektor pemerintah, IIKN dan sektor swasta

dengan menggunakan metrik atau instrumen pengukuran pengembangan keamanan siber, strategi penilaian risiko, audit keamanan siber.

Fungsi CERT (nasional, pemerintah maupun sektoral) harus terus dimatangkan, karena melihat tantangan ke depan akan terus terjadi peningkatan ancaman siber. Sehingga, optimalisasi tugas dan fungsi CERT perlu dilaksanakan, karena serangan siber dapat terjadi kapan saja dan respon terhadap laporan insiden siber harus selalu diberikan guna memberikan layanan keberlangsungan berjalannya proses bisnis organisasi serta CERT diharapkan dapat menganalisis laporan insiden siber yang dapat bermanfaat bagi komunitas CERT di dalam negeri maupun luar negeri. CERT juga diharapkan dapat selalu berkoordinasi dan berkomunikasi dengan CERT negara lain dalam lingkup regional maupun internasional, sehingga dapat bertukar informasi mengenai insiden siber yang terjadi secara global di dunia.

2. Pengembangan Kapasitas Keamanan Siber

a. Peningkatan Kampanye Kesadaran Publik

BSSN diharapkan untuk dapat mempertahankan bahkan meningkatkan program kampanye kesadaran publik terhadap pentingnya keamanan siber yang selama ini sudah dilaksanakan oleh pemerintah. Kampanye kesadaran publik dapat berupa penyebarluasan informasi kepada berbagai pihak dengan memanfaatkan organisasi, perpustakaan, komunitas, perguruan tinggi dan program pendidikan bagi dewasa, sekolah dan organisasi guru serta orang tua untuk menyampaikan pesan tentang berperilaku dalam dunia siber yang aman secara daring.

Inisiatif pertama harus dilaksanakan peningkatan kesadaran keamanan siber bagi semua pemangku kepentingan nasional di Indonesia dan kemudian mendorong dalam pengembangan kemampuan terkait dengan tata kelola internet dan dunia siber. Dibutuhkan intervensi pemerintah melalui kerangka hukum dan peraturan yang efektif, karena lembaga pemerintah, industri, dan individu harus yakin bahwa data pribadi secara efektif dilindungi dan dalam kondisi aman. Ketika negara mulai meraih manfaat penuh dari TIK, regulasi yang efektif, koordinasi, dan kampanye kesadaran bersama dengan penggunaan solusi keamanan siber, hal tersebut diperlukan untuk melindungi data dan infrastruktur nasional serta untuk memperkuat kapasitas keamanan siber di Indonesia.

b. Penyusunan Program Pendidikan, Penelitian, dan Pengembangan

Indonesia belum mempunyai kebijakan nasional mengenai program penelitian dan pengembangan serta kurikulum akademik dalam bidang keamanan siber termasuk penyusunan panduan berupa praktik terbaik bagi sektor pemerintah maupun swasta. BSSN dituntut untuk dapat menyusun program penelitian dan pengembangan keamanan siber meliputi pengembangan perangkat keras dan lunak, analisis malware, kriptografi, firewall, sistem pencegahan penyusupan dan lain-lain. Penyelenggaraan program dapat bekerja sama dengan instansi pemerintah lain yang bergerak dalam bidang penelitian dan penerapan teknologi maupun dalam bidang ilmu pengetahuan, bahkan dapat bekerja sama dengan sektor industri swasta agar program penelitian dan pengembangan dapat dilaksanakan secara luas dan menyeluruh.

Indonesia belum ada kurikulum akademik berkaitan dengan keamanan siber pada setiap level pendidikan, hanya pada tingkat perguruan tinggi dan beberapa sekolah menengah kejuruan. BSSN diharapkan dapat menginisiasi pendidikan sejak dini berkaitan dengan keamanan siber, program tersebut dilaksanakan selain membantu dalam hal peningkatan kapasitas dan kampanye kesadaran publik keamanan siber, juga memberikan ilmu pengetahuan dan keterampilan terkait keamanan siber. Kampanye kesadaran publik termasuk upaya dalam mempromosikan penyebarluasan informasi untuk menjangkau sebanyak mungkin pihak dengan memanfaatkan lembaga, organisasi, perpustakaan, komunitas,

perguruan tinggi dan program pendidikan bagi dewasa, sekolah dan organisasi guru serta orang tua untuk menyampaikan pesan tentang berperilaku dalam dunia siber yang aman secara daring.

c. Peningkatan Program Pelatihan dan Sertifikasi Keamanan Siber

BSSN diharapkan untuk dapat terus meningkatkan penyelenggaraan program pelatihan maupun sertifikasi dan akreditasi dalam bidang keamanan siber. Program pelatihan dan sertifikasi dapat diikuti oleh para personil maupun profesional yang bekerja pada bidang keamanan siber baik pada instansi pemerintah maupun swasta. Kebutuhan penyelenggaraan pelatihan profesional dalam bidang keamanan siber semakin meningkat mengingat karena perkembangan TIK dan ancaman siber yang semakin meningkat. Program pelatihan dan sertifikasi merupakan salah satu bentuk pengembangan kapasitas bagi SDM bidang keamanan siber dalam upaya peningkatan keamanan siber di Indonesia dalam segi kuantitas maupun kualitas.

d. Penyediaan Mekanisme Insentif Bidang Keamanan Siber

BSSN, diharapkan dapat mendorong kepada pemerintah untuk lebih memperhatikan sektor keamanan siber dengan memberikan program mekanisme insentif dalam bidang keamanan siber guna pengembangan kapasitas baik dalam aspek SDM maupun teknologi. Pemberian insentif untuk pelatihan dan pendidikan pada bidang keamanan siber merupakan salah satu hal penting yang seharusnya dilaksanakan oleh pemerintah. Pelibatan pemangku kepentingan yang terkait dapat memastikan kelangsungan pengembangan pendidikan keamanan siber dengan pembiayaan yang didedikasikan untuk penelitian nasional pada level perguruan tinggi.

Di Indonesia, penyelenggaraan mekanisme insentif diberikan beberapa instansi pemerintah dalam bentuk pemberian beasiswa kepada masyarakat secara luas untuk dapat melanjutkan pendidikan yang berkaitan dengan keamanan siber di beberapa perguruan tinggi baik dalam negeri maupun luar negeri dalam rangka peningkatan kapasitas di bidang keamanan siber. Selain itu penyediaan insentif juga dapat diberikan pada sektor swasta yang bergerak di bidang keamanan siber yang akan mendorong pertumbuhan ekonomi dan teknologi keamanan siber. Mekanisme insentif diberikan pemerintah guna mendorong pengembangan kapasitas di bidang keamanan siber, baik melalui keringanan pajak, hibah, pendanaan, pinjaman, pemberian fasilitas, dan dukungan ekonomi serta keuangan lainnya.

3. Peningkatan Kerja Sama Keamanan Siber

a. Peningkatan Kerja Sama Bilateral dan Multilateral

Pemerintah Indonesia telah menyelenggarakan kerja sama baik secara bilateral dengan negara lain maupun secara multilateral dengan banyak negara lain dan berpastisipasi dalam forum internasional yang dihadiri oleh banyak negara anggota. Kerja sama mengacu pada kemitraan nasional yang diakui secara resmi untuk berbagi informasi keamanan siber atau aset lintas batas oleh pemerintah dengan satu pemerintah asing lainnya, entitas regional atau organisasi internasional dengan bentuk kerja sama berupa pertukaran informasi, keahlian, teknologi, dan sumber daya lainnya. BSSN diharapkan untuk menjadi titik fokus dalam penyelenggaraan kerja sama, tentunya dengan berkoordinasi dengan instansi pemerintah terkait agar penyelenggaraan dapat berjalan dengan harmonis. Pemerintah perlu meningkatan kerja sama dengan banyak pihak yang berkaitan dengan penyelenggaraan keamanan siber mengingat bahwa ancaman siber yang semakin meningkat sehingga membutuhkan koordinasi dan kerja sama dengan berbagai pihak baik dalam lingkup regional maupun internasional dan baik secara bilateral maupun secara multilateral. BSSN juga diharapkan tetap melanjutkan program partisipasi pada forum internasional yang berkaitan dengan keamanan siber sehingga mendorong kerja sama dan koordinasi dalam pencegahan insiden, untuk

merangsang reaksi cepat terhadap insiden siber dan untuk mempromosikan berbagi informasi di antara anggota dan masyarakat luas.

b. Peningkatan Kerja Sama Pemerintah dan Swasta

BSSN diharapkan dapat memulai inisiasi untuk menyelenggarakan kerja sama antara pemerintah dengan sektor swasta terutama dalam berbagi informasi terkait keamanan siber dan aset (manusia, proses, alat). Kerja sama pemerintah dan swasta berupa kemitraan resmi untuk pertukaran informasi, keahlian, teknologi dan sumber daya, baik secara skala nasional maupun internasional. Peningkatan kerja sama juga dapat dilaksanakan dengan pemberian insentif kepada sektor swasta dalam pengembangan kapasitas keamanan siber baik dalam aspek SDM maupun teknologi. Peningkatan kepercayaan terhadap sektor swasta akan mendorong pertumbuhan ekonomi dan perkembangan teknologi keamanan siber. Faktor penghambat kerja sama yaitu kurangnya akreditasi dalam pengadaan pemerintah terkait peralatan di bidang keamanan siber serta kurangnya pengetahuan tentang teknologi dan praktik keamanan siber yang mapan, keterbatasan pemahaman tentang ancaman siber beserta dampaknya serta kurangnya pemahanan dalam hal berinvestasi di bidang keamanan siber.

c. Peningkatan Kerja Sama Internal Instansi Pemerintah

BSSN sebagai koordinator penyelenggaraan keamanan siber di Indonesia diharapkan untuk dapat meningkatkan kemitraan dalam hal berbagi informasi atau aset antara kementerian, lembaga dan instansi pemerintah lainnya. Kerja sama yang dapat mengikat badan-badan pemerintah dari pertahanan, penegak hukum, komunitas intelijen dan sektor IIKN untuk bekerja secara kolaboratif untuk meningkatkan berbagi informasi keamanan siber dengan penekanan pertukaran informasi menggunakan TIK yang terintegrasi antar instansi pemerintah. BSSN berlaku sebagai titik fokus kolaborasi antara pemerintah, industri dan masyarakat sipil pada seluruh level insiden siber. Pusat keamanan siber nasional seharusnya dimandatkan dalam kerangka kerja strategi atau kebijakan keamanan siber nasional yang disahkan oleh pemerintah. Pusat keamanan siber nasional meningkatkan interaksi dan konsultasi serta mempromosikan pendekatan terkoordinasi mengenai keterlibatan pemerintah dengan sektor swasta dan masyarakat.

BSSN diharapkan berkolaborasi dengan pihak terkait pembuatan standar di bidang keamanan siber mengingat bahwa standar keamanan siber merupakan teknik yang umumnya ditetapkan dalam materi yang dipublikasikan dalam usaha melindungi dunia siber yang dimiliki oleh pengguna atau organisasi. Ruang lingkup standar mencakup pengguna, jaringan, perangkat keras dan lunak, proses, informasi dalam penyimpanan atau transit, aplikasi, layanan, dan sistem yang dapat dihubungkan secara langsung maupun tidak langsung dalam jaringan. Tujuan utama yaitu untuk mengurangi risiko, termasuk pencegahan atau mitigasi serangan siber.

5. Kesimpulan

5.1. Penyelenggaraan Keamanan Siber di Indonesia. Berdasarkan 5 (Lima) Pilar GCI

Penyelenggaraan keamanan siber di Indonesia pada aspek hukum yaitu Indonesia sudah mempunyai peraturan dengan substansi yang berkaitan dengan kejahatan siber dan keamanan siber, meskipun bentuk peraturan tidak berdiri sendiri dan secara khusus serta mendalam mengatur tentang kejahatan siber dan keamanan siber. BSSN diharapkan untuk dapat mendorong penyusunan UU keamanan siber, sehingga kebijakan tersebut dapat menjadi acuan bagi BSSN serta seluruh pemangku kepentingan. Indonesia sudah menyelenggarakan pelatihan bagi anggota POLRI secara rutin dan berkala, tetapi belum menyeluruh kepada seluruh aktor hukum di Indonesia.

Penyelenggaraan keamanan siber di Indonesia pada aspek teknis yaitu Indonesia sudah mempunyai CERT nasional yaitu BSSN,

selain itu BSSN juga diberikan mandat tanggung jawab nasional untuk memonitor, mengelola dan menangani insiden siber pada sektor pemerintah. Indonesia tidak mempunyai CERT sektoral, BSSN dapat membentuk CERT sektoral jika kebutuhan terkait CERT sektoral sangat mendesak. Indonesia tidak mempunyai kerangka kerja dan standar bagi organisasi yang berkaitan keamanan siber. Namun, Indonesia mempunyai standar yang terkait dengan keamanan siber yaitu SMKI yang tertuang dalam SNI ISO/IEC 27001. Indonesia meskipun tidak memiliki kerangka kerja keamanan siber nasional mengenai sertifikasi dan akreditasi lembaga nasional maupun profesional. Namun, profesional di bidang keamanan siber sudah mendapat sertifikasi yang diakui secara internasional dalam bidang keamanan siber. Indonesia tidak mempunyai strategi atau peraturan yang mengatur mengenai perlindungan daring terhadap anak. Namun, Indonesia mempunyai KPAI yang bertugas dalam bidang perlindungan anak serta mempunyai UU yang berkaitan dengan perlindungan anak yaitu UU Perlindungan Anak dan UU Pornografi, kedua UU tersebut tidak secara khusus mengatur tentang perlindungan daring terhadap anak.

Penyelenggaraan keamanan siber di Indonesia pada aspek Organisasi yaitu Indonesia tidak mempunyai strategi atau kebijakan keamanan siber nasional. BSSN diharapkan dapat menjadi organisasi titik fokus dalam perumusan dan penyusunan strategi keamanan siber nasional. Indonesia membentuk BSSN, tetapi masih dalam tahap internalisasi dan harmonisasi organisasi dalam rangka membentuk pondasi organisasi yang kuat. BSSN selaku koordinator dalam penyelenggaraan keamanan siber di Indonesia dituntut untuk dapat bekerja sama dengan seluruh pemangku kepentingan yang berkaitan dengan keamanan siber. Indonesia tidak mempunyai referensi diakui secara resmi yang digunakan untuk mengukur pengembangan keamanan siber, strategi penilaian risiko, audit keamanan siber, dan alat serta kegiatan lain untuk menilai atau mengevaluasi kinerja yang dihasilkan untuk perbaikan di masa depan.

Penyelenggaraan keamanan siber di Indonesia pada aspek pengembangan kapasitas yaitu Indonesia mempunyai Badan Standardisasi Nasional (BSN) yang melaksanakan tugas di bidang standardisasi nasional. Salah satu standar yang terkait dengan keamanan siber yaitu SNI ISO/IEC 27032:2014 dengan judul Teknologi Informasi - Teknik Keamanan - Pedoman Keamanan Siber (ISO/IEC 27032:2012, IDT). Indonesia belum mempunyai dokumen best practice (praktik terbaik) berkaitan dengan keamanan siber, oleh karena itu BSSN diharapkan untuk dapat menyusun dokumen praktik terbaik keamanan siber yang dapat dirujuk dalam penyelenggaraan keamanan siber. Indonesia tidak mempunyai kebijakan nasional mengenai program penelitian dan pengembangan keamanan siber. Program penelitian dan pengembangan sudah dilaksanakan oleh Lemsaneg (BSSN), BPPT, dan LIPI, tetapi belum berfokus pada bidang teknologi keamanan siber. Indonesia sudah menyelenggarakan program kampanye kesadaran publik dalam berbagai bentuk bagi masyarakat umum. Indonesia sudah menyelenggarakan program pelatihan bagi profesional keamanan siber. Indonesia sudah menginisiasi pengembangan program pendidikan dan kurikulum akademik pada bidang keamanan siber pada level SMK dan perguruan tinggi. Penyelenggaraan mekanisme insentif diberikan dalam bentuk pemberian beasiswa kepada masyarakat untuk dapat melanjutkan pendidikan yang berkaitan dengan keamanan siber di beberapa universitas baik dalam negeri maupun luar negeri. Indonesia tidak ada program pemberian insentif dalam rangka pasar mendorong pasar dalam menciptakan produk dan layanan keamanan siber. BSSN diharapkan untuk mendorong pemberian insentif dalam rangka mendorong pasar menciptakan produk dan layanan keamanan siber sehingga mendukung

pengembangan dan peningkatan kualitas teknologi keamanan siber.

Penyelenggaraan keamanan siber di Indonesia pada aspek kerja sama yaitu Indonesia sudah menyelenggarakan kerja sama bilateral dengan beberapa organisasi atau negara lain serta Indonesia aktif sebagai anggota PBB. Indonesia juga menyelenggarakan kerja sama multilateral dengan beberapa organisasi atau negara lain dan menjadi anggota dari forum internasional keamanan siber. Indonesia tidak memiliki kemitraan bersama pemerintah-swasta dalam penanganan keamanan siber. Indonesia sudah memenuhi kriteria penilaian pada indikator kerja sama antar instansi pemerintah, karena Indonesia sudah menyelenggarakan kemitraan antar instansi pemerintah. Penyelenggaraan kemitraan resmi antara berbagai instansi pemerintah dalam suatu negara dalam bidang keamanan siber.

5.2. Strategi BSSN Guna Meningkatkan Komitmen Bidang Keamanan Siber dalam Menghadapi Ancaman Siber di Indonesia

BSSN sebagai lembaga pemerintah yang bertanggung jawab pada penyelenggaraan urusan pemerintah bidang keamanan siber di Indonesia, diharapkan untuk dapat meningkatkan komitmen bidang keamanan siber dalam menghadapi ancaman siber di Indonesia dengan melibatkan seluruh pemangku kepentingan keamanan siber, karena pemangku kepentingan berperan dalam pengembangan dan penyempurnaan strategi atau kebijakan pemerintahan. Strategi tersebut yaitu diantaranya percepatan dalam hal penyusunan kerangka hukum dunia siber yang meliputi penyusunan kerangka hukum keamanan siber dan strategi keamanan siber nasional, serta optimalisasi tugas dan fungsi BSSN dan CERT.

Strategi yang dapat dilaksanakan terkait dengan pengembangan kapasitas keamanan siber yaitu penyusunan program pendidikan, penelitian, dan pengembangan terkait teknologi keamanan siber. Peningkatan penyelenggaraan kampanye kesadaran publik sehingga dapat menjangkau ke seluruh lapisan masyarakat. Peningkatan penyelenggaraan program dan sertifikasi keamanan siber bagi publik yang bekerja dalam bidang keamanan siber. Penyediaan mekanisme insentif dalam bidang keamanan siber sehingga dapat meningkatan pengembangan pendidikan keamanan siber dan dapat mendorong pertumbuhan ekonomi dan teknologi keamanan siber.

Peningkatan kerja sama keamanan siber menjadi salah satu strategi yang dapat dilaksanakan yaitu pemerintah Indonesia diharapkan dalam menyelenggarakan kerja sama baik bilateral maupun multilateral terutama terkait bidang keamanan siber dengan negara lain. Kerja sama antara pemerintah dengan pihak swasta diharapkan dapat ditingkatkan guna mendorong pertumbuhan ekonomi dan teknologi keamanan siber. Peningkatan kerja sama internal instansi pemerintah terutama dalam hal berbagi informasi atau aset antara kementerian, lembaga dan instansi pemerintah lainnya. Kerja sama tersebut dapat mengikat badan-badan pemerintah antara lain dalam bidang pertahanan, penegak hukum, komunitas intelijen dan sektor IIKN untuk bekerja secara kolaboratif untuk meningkatkan berbagi informasi keamanan siber dengan penekanan pertukaran informasi menggunakan TIK yang terintegrasi antar instansi pemerintah.

Daftar Pustaka

Buku dan Jurnal

Blaxter, L. Hughes, C. Tight, M. (2006). How to Research. New York: Open University Press.

Bruce J. Biddle. (1979). Role Theory: Expectations, Identities, and Behaviour. New York: Academic Press.

Chandra Wijaya dan Muhammad Rifa'i. (2016). Dasar-Dasar Manajemen. Medan: Perdana Publishing.

Christos Scondars. (2004). Organizational Models for Computer Security Incident

Response Teams (CSIRTs). Pittsburgh: Universitas Carnegie Mellon.

Clauster, J. (2008). An Introduction to Intelligence Research and Analysis. United States of America: Scarecrow Press Inc.

Creswell, J. W. (2003). Research Design-Qualitative, Quantitative, and Mised Methods Approaches. New Delhi: Sage Publication.

Fitriati, Rachma. (2014). Membangun Model Kebijakan Nasional Keamanan Siber dalam Sistem Pertahanan Negara. Bogor: Universitas Pertahanan.

H.B Sutopo, (2002). Metode Penelitian Kualitatif: Dasar Teori dan Penerapannya Dalam Penelitian. Surakarta: Universitas Sebelas Maret Press.

Kearney, A.T., (2018). Cybersecurity in ASEAN: An Urgent Call to Action. Amerika.

Komariah, A. Satori, D. (2011). Metodologi Penelitian Kualitatif. Bandung: Alfabeta.

Lembaga Ketahanan Nasional. (2000). Pendidikan Kewarganegaraan. Jakarta: PT. Gramedia Pustaka Utama.

Norwood, Kerry T., Catwell, Sandra P. (2009). Cybersecurity, Cyberanalysis, and Warning. New York: Nova Science Publisher, Inc.

Prunckun, H, (2015). Scientific Methods of Inquiry for Intelligence Analysis. Rowman & Littlefield.

Refsdal et al. (2015). Cyber-Risk Management. Springer.

Runturambi, A. Josias Simon dan Dadang Sutiadi, 2013. Manajemen Sekuriti: Karakteristik Lokasi dan Desain. Jakarta: Universitas Indonesia.

Schreier, F. (2015). On Cyber Warfare, Working Paper Number 7.

Sugiyono. (2005). Memahami Penelitian Kualitatif. Bandung: Alfabet.

Publikasi

Internasional Telecommunication Union (ITU). (2008). Series X: Data Networks, Open System Communications and Security – Overview of Cybersecurity. ITU-T.

Internasional Telecommunication Union (ITU). (2011). ITU National Cybersecurity Strategy Guide.

International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2012). ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.

Cyber Security Agency of Singapore (CSA). (2016). Singapore's Cybersecurity Strategy. Singapura: Cyber Security Agency of Singapore (CSA).

Ministry of Science, Technology and Innovation of Malaysia (MOSTI). The National Cyber Security Policy. Malaysia: MOSTI.

The Australian Cyber Security Centre (ACSC). (2016). Australia's Cyber Security Strategy – Enabling Innovation, growth & prosperity. Australia: ACSC.

Ministry of Communication and Information Technology – Department of Electronics and Information Technology. (2013). National Cyber Security Policy. India: MCITY.

National Cyber Security Strategy 2016-2021 United Kingdom. (2016).

National Cyber Security Centre (NCSC). (2017). National Cyber Security Centre Overview. Inggris: NCSC.

Ministry of State Security. (2015). The National Cybersecurity Policy Framework (NFPF). Afrika Selatan: Ministry of State Security.

North Atlantic Treaty Organization (NATO). (2016). National Cyber Security Organization: United States. Tallin: NATO.

The Department of Defense of United States (DoD). (2015). The Department of Defense Cyber Strategy. Amerika: DoD.

The Department of State of United States (DoS). (2016). The Department of State Internasional Cyberspace Policy Strategy. Amerika: DoS.

The George Washington University. (2016). Cybersecurity for State and Local Law Enforcement: A Policy Roadmap to Enhance Capabilities. Washington: The George Washington University.

Investment Industry Regulatory Organization of Canada (IIORC). Cybersecurity Best Practices Guide for IIROC Dealer Members. Canada: IIORC.

General Accounting Office. (2004). Cybersecurity for Critical Infrastructure Protection. Amerika: General Accounting Office.

Trusted Information Sharing Network (TISN). (2008). Defence in Depth. Australia: TISN.

Karya Ilmiah

Studer, Evelyne. (2018). Regulating Cybersecurity - What civil liability in case of cyber attacks. Jenewa: University of Geneva.

Ali, Irhamni. (2011). Kejahatan Terhadap Informasi (Cybercrime) Dalam Konteks Perpustakaan Digital. Bogor: Institut Pertanian Bogor.

Erwin, Basuki. (2018). Kontra Intelijen Aksi Spionase Siber Terhadap Anggota Democratic National Committee Menjelang Pemilihan Presiden AS Tahun 2016. Jakarta: Universitas Indonesia.

Maskun. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. Makassar: Universitas Hasanuddin Makassar.

Putra, David dan Datumaya, Arwin. (2016). Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives. Bogor: Universitas Pertahanan.

Rahayu, Ning. (2008). Praktik Penghindaran Pajak (Tax Avoidance) pada Foreign Direct Investment yang Berbentuk Subsidiary Company (PT PMA) di Indonesia (Suatu Kajian Tentang Kebijakan Anti Tax Avoidance.

Triwahyuni, Dewi dan Agustin, Tine. (2016). Strategi Keamanan Cyber Amerika Serikat. Jakarta: Universitas Komputer Indonesia.

Yuliansyah, Moehammad. (2015). Pengaruh Cyber Security Amerika Serikat Menghadapi Ancaman Cyber Warfare. Riau: Universitas Riau.

Yuliardi, Ryscha. Penggunaan Cyberwar Melalui Stuxnet Project Oleh Amerika Serikat Dalam Merespon Perkembangan Proyek Nuklir Iran di Natanz. Surabaya: Universitas Airlangga.

Jurnal

Ardiyanti, Handrini. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. Jakarta: Jurnal Politica.

Budiman, Ahmad. (2017). Optimalisasi Badan Siber dan Sandi Nasional. Jakarta: Pusat Penelitian Badan Keahlian DPR RI.

Hadi, Astar. (2005). Matinya Dunia Cyberspace: Kritik Humanis Mark Slouka Terhadap Jagat Maya. LkiS.

Lippman, Walter. (1943). US Foreign Policy: Shield of The Republic. Boston: Little, Brown.

Rosmawati. (2012). Makalah Pendidikan Kewarganegaraan.

Walker, Seth. (2010). My [Sacred] Space: Discovering Sacred Space in Cyberspace, Summer.

Wolfers, Arnold. (1962). Discord and Collaboration Essays On International Politics. Baltimore: John Hopkins University Press.

World Economic Forum. (2012). Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience.

Burhansyah, Encik Mochammad. (2016). Kerja sama Kepolisian Negara Republik Indonesia (POLRI)-Australian Federal Police (AFP) Sektor Capacity Building Dalam Penanggulangan Tindak Pidana Cyber Crime Di Indonesia Periode 2012-2014. Semarang: Universitas Diponegoro.

Peraturan

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen.

133

Undang-Undang Nomor 24 Tahun 2014 tentang Administrasi Kependudukan.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Tahun 2017 Nomor 100) sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Tahun 2017 Nomor 277).

Media Internet

http://library.binus.ac.id/eColls/eThesisdoc/Bab2HTML/2013201542MCBab2001/page20.html. Tanggal akses 9 Maret 2018

http://nasional.kompas.com/read/2017/11/21/21260801/januari-hingga-juli-2017-indonesia-alami-1773-juta-serangan-siber. Tanggal Tayang 21 November 2017. Tanggal Akses 19 Februari 2018

http://news.liputan6.com/read/2972837/ahli-digital-forensik-sebut-15-situs-pemerintah-diretas-per-hari. Tanggal Tayang 31 Mei 2017. Tanggal Akses 21 Februari 2018

http://www.bbc.com/indonesia/indonesia-40106424. Tanggal Tayang 31 Mei 2017. Tanggal Akses 21 Februari 2018

http://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/. Tanggal tayang 17 Januari 2018. Tanggal akses 9 Februari 2018

https://kominfo.go.id/content/detail/9636/siaran-pers-no-55hmkominfo052017-tentang-himbauan-agar-segera-melakukan-tindakan-pencegahan-terhadap-ancaman-malware-khususnya-ransomware-jenis-wannacry/0/siaran_pers. Tanggal tayang 13 Mei 2017. Tanggal akses 8 Februari 2018

https://www.anonimcyber.com/2017/12/serangan-cyber-yang-menghebohkan-dunia.html. Tanggal tayang 8 Desember 2017. Tanggal akses 7 Februari 2018

http://industri.bisnis.com/read/20171227/105/721489/ini-catatan-penting-seputar-serangan-siber-sepanjang-tahun-2017. Tanggal tayang 27 Desember 2017. Tanggal akses 3 Mei 2018.

https://www.csa.gov.sg/. Tanggal akses 4 April 2018.

https://www.nacsa.gov.my/index.php. Tanggal akses 4 April 2018.

https://www.acsc.gov.au/index.html. Tanggal akses 4 April 2018.

http://meity.gov.in/home. Tanggal akses 4 April 2018.

https://www.ncsc.gov.uk/. Tanggal akses 4 April 2018.

https://www.gov.za/. Tanggal akses 4 April 2018.

https://ccdcoe.org/. Tanggal akses 4 April 2018.

https://www.dhs.gov/. Tanggal akses 4 April 2018.

https://www.defense.gov/. Tanggal akses 4 April 2018.

https://www.state.gov/. Tanggal akses 4 April 2018.
http://computer.expressbpd.com/magazine/dedicated-legislation-for-cyber-security-is-needed-pavan-duggal/13378/. Tanggal tayang 30 Agustus 2015. Tanggal akses 18 Mei 2018.
https://www.jica.go.jp/english/index.html. Tanggal akses 12 Mei 2018.
http://www.aots.jp/hida/en/index.html. Tanggal akses 12 Mei 2018.
http://www.koica.go.kr/english/main.html. Tanggal akses 12 Mei 2018.
https://www.jclec.org/. Tanggal akses 12 Mei 2018.
https://www.first.org/. Tanggal akses 12 Mei 2018.
http://www.impact-alliance.org/home/index.html. Tanggal akses 12 Mei 2018.
https://www.apcert.org/. Tanggal akses 12 Mei 2018.
https://www.intgovforum.org/multilingual/. Tanggal akses 12 Mei 2018.
http://asean.org/. Tanggal akses 12 Mei 2018.