Jurnal Dinamika Global Vol.7 No. 2, Desember 2022
P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA

Yusep Ginanjar[1]
[1]Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jenderal Achmad Yani
yusep.ginanjar@lecture.unjani.ac.id

Abstract

Cyber security has become a priority issue for all countries in the world since information and communication technology is used in various aspects of life, both in social, economic, legal, organizational, health, education, culture, government, security, defense, and other aspects. In direct proportion to the high level of utilization of information and communication technology, the level of risk and threat of misuse of information and communication technology is also getting higher and more complex. In response to these events, Indonesia then formed the National Cyber and Crypto Agency (BSSN) as a model for national cyber security institutions. This study uses a qualitative method with a descriptive approach. The purpose of this research is to find out how Indonesia's strategy in establishing cyber security in dealing with the threat of cyber crime through the National Cyber and Crypto Agency.

Keywords: *Cyber Security, Cyber Crime, BSSN.*

PENDAHULUAN

Keamanan siber telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lain sebagainya. Berbanding lurus dengan tingginya tingkat pemanfaatan teknologi informasi dan komunikasi tersebut, tingkat risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga semakin tinggi dan semakin kompleks.

Berdasarkan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022, lebih dari 77,02% masyarakat Indonesia menggunakan internet. Artinya ada 210.026.769 jiwa dari total penduduk 272.682.600 penduduk Indonesia yang terkoneksi internet.

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

Peningkatan pengguna internet tejadi di masa pandemi Covid-19 akibat penggunaan teknologi internet untuk menggantikan aktivitas tatap muka. Hal ini juga sejalan dengan data yang dikeluarkan oleh Organization for Economic Co-Operation and Development, dimana terdapat peningkatan akses internet yang terus meningkat dari tahun ke tahun baik oleh rumah tangga maupun individu di seluruh dunia (OECD, 2021).

Indonesia sebagai negara dengan pertumbuhan pengguna internet terbesar keempat di dunia, menghadapi peluang sekaligus ancaman besar dengan perkembangan teknologi digital dan internet baik dari dimensi sosial, politik, dan ekonomi, seperti provokasi politik, hoaks, SARA, ujaran kebencian, ideologi radikalisme, terorisme, hacking, pencurian data, penipuan daring, dan tindak kejahatan lainnya di ruang siber. Hal tersebut harus dapat diantisipasi, dicegah, dan ditangani untuk menjamin keamanan siber (*cyber security*).

Pada Tahun 2020, menurut BSSN (2020), terdapat sekiranya empat saluran *e-commerce* terbesar di Indonesia yang telah menjadi sasaran *data breach* atau kebocoran data entah itu yang disebabkan oleh perusahaan ataupun yang disebabkan oleh pihak individu. Tokopedia, adalah salah satu perusahaan raksasa yang bergerak di bidang distribusi barang dan jasa sudah melaporkan setidaknya terdapat 91 juta data yang bocor di Internet. Pelaku yang belum bisa diidentifikasi dengan nama Shiny Hunters mengaku memiliki data dan hendak menjual data tersebut yang berisikan data pengguna. Disusul Reddoorz sekitar 5.8 juta data, Cermati 2.9 Juta data, dan Kredit Plus 890 ribu data.

Pada kasus terbaru, masyarakat Indonesia dihebohkan dengan bocornya data pendaftar telepon seluler yang dijual bebas di Situs Forum Hacking (Kompas, 2022). Total data yang bocor sebesar 87 GB dijual dengan harga Rp 743 juta (sekitar USD 50.000). Insiden keamanan siber ini melengkapi kasus-kasus yang sebelumnya terjadi seperti kebocoran data PLN, kebocoran aplikasi kesehatan milik Kementerian Kesehatan (E-HAC), kebocoran data BPJS Kesehatan, hingga kebocoran data perbankan (BRI Life). Kasus kebocoran data tersebut dilakukan oleh aktor ancaman yang

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

menamakan dirinya Bjorka, telah membuat Presiden Republik Indonesia membentuk Tim Khusus Pengamanan Data yang melibatkan Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara, Badan Intelijen Negara, dan Kepolisian Negara Republik Indonesia (Rezki Ramadhan dan Chandra Wijaya, 2022).

Dari segi keamanan, salah satu perusahaan keamanan internet internasional yang beroperasi di Indonesia yaitu Eset Indonesia menyatakan bahwa Indonesia mendapat sekitar 1,225 miliar serangan siber setiap harinya, dan dari miliaran data tersebut Eset Indonesia menyebut *Ransomware* masih merupakan serangan tertinggi setiap harinya (Kustin Ayuwiragil, 2017). Tahun 2018 Malware masih tetap merajai serangan siber di Indonesia dan virus *Ransomware* akan terus menjadi momok bagi keamanan dan ketahanan siber untuk setiap perusahaan maupun sektor pemerintahan di Indonesia. Sedangkan di tahun 2019, menurut Gov – CSIRT wilayah satu terdapat kurang lebih 102 (seratus dua) serangan siber yang lebih berfokus kepada *Web Defacement* sebanyak 34 insiden siber, *Phishing* sebanyak 9 insiden siber, *Malware* sebanyak 13 insiden siber, dan kerentanan sebanyak 38 insiden siber. Kebanyakan serangan atau insiden siber yang berlangsung di pemerintahan Indonesia karena kurangnya pemahaman akan kerentanan di dunia siber dan masih menggunakan aplikasi atau instalasi bajakan oleh karenanya masih mudah dimanfaatkan oleh serangan siber di organisasi pemerintah. Di tahun yang sama Gov-CISRT juga berkoordinasi dengan Direktorat Deteksi Ancaman BSSN yang berkolaborasi dengan Honeynet Project menyatakan bahwa total serangan siber adalah sekitar 98.243.8964 yang meliputi Sektor Pemerintah, Akademisi, dan IIKN (BSSN, 2020).

Berdasarkan hal tersebut, keamanan siber Indonesia cukup mengkhawatirkan. Berdasarkan penilaian yang dikeluarkan oleh E-Governance Academy (EGA), nilai proteksi Indonesia adalah 25%. Hal ini berpengaruh pada Indeks Keamanan Siber Nasional Indonesia yang berada di peringkat 83 dan jauh di bawah indeks keamanan siber Malaysia dan Singapura yang berada di peringkat 19 dan 29 (NCSI, 2020).

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

Tabel 1. National Cyber Security Index 2022

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
19	Malaysia	79.22	62.53	16.69
29	Singapore	71.43	80.26	-8.83
83	Indonesia	38.96	46.84	-7.88

Sumber: NCSI, 2022

Dalam rangka merespon berbagai peristiwa tersebut Indonesia kemudian membentuk Badan Siber dan Sandi Negara (BSSN) sebagai model institusi cyber security nasional. 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.

Pada penelitian yang dilakukan oleh Maulia Jayantina Islami (2017) Pemerintah Indonesia telah menginisiasi strategi nasional keamanan siber dan menjalankan program-program jangka pendek maupun panjang, namun dalam implementasinya masih terdapat tantangan dan hambatan. Keamanan siber merupakan sebuah ekosistem dimana aspek legal,

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

organisasi, skill, kerjasama, dan implementasi teknik harus berjalan secara selaras untuk hasil yang efektif. Selanjutnya, pada penelitian yang dilakukan oleh Damar Apri Sudarmadi, Arthur Josias Simon Runturambi (2019) 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.

Berdasarkan fenomena-fenomena yang telah dijelaskan sebelumnya, peneliti tertarik untuk mengkaji lebih jauh mengenai strategi Indonesia membentuk *cyber security* dalam menghadapi ancaman *cyber crime* melalui Badan Siber dan Sandi Negara (BSSN). Adapun tujuan dari penelitian ini adalah untuk mengetahui bagaimana strategi Indonesia dalam membentuk *cyber security* dalam menghadapi ancaman *cyber crime* melalui Badan Siber dan Sandi Negara.

Metode Penelitian

Artikel ini menggunakan pendekatan kualitatif yang mengacu pada makna, konsep, definisi, karakteristik, metafora, simbol, dan deskripsi dari suatu hal. Penelitian kualitatif dilakukan melalui pencarian sebuah jawaban dengan memeriksa berbagai pengaturan sosial dan kelompok atau individu di suatu setting sosial. Dalam hal ini, penelitian kualitatif memahami lingkungan yang diteliti melalui simbol, ritual, struktur sosial, peran sosial, dan sebagainya (B.L. Berg dan H. Lune, 2017:12-15).

Dalam teknik pengumpulan data di sini, penulis hanya menggunakan studi pustaka atau telaah pustaka dengan metode deskriptif dari sumbersumber penelitian sebelumnya maupun data sekunder lainnya. Pustaka-pustaka tersebut berasal dari laporan tahunan maupun kajian yang dilakukan instansi pemerintah dan non-pemerintah, dokumen perjanjian internasional, majalah pemerintah, maupun berita-berita online yang tersedia mengenai keamanan siber.

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

Kerangka Teori

Institutional Theory

Menurut Richard Scott (2004) Institutional theory ditujukan untuk memperdalam struktur sosial yang didasarkan pada proses yang terstruktur, termasuk skema, aturan, norma, dan rutinitas sebagai pedoman otoritatif untuk perilaku sosial. Akar teori ini telah memperkaya studi ilmu-ilmu sosial dan menggabungkan wawasan kreatif mulai dari Marx dan Weber, Cooley dan Mead, hingga Veblen dan Commons. Banyak dari karya ini, muncul pada akhir abad kesembilan belas dan awal abad kedua puluh, seperti munculnya teori neoklasik di bidang ekonomi, behavioralisme dalam ilmu politik, dan positivisme dalam sosiologi pada masa tersebut.

Institusi merupakan aturan permainan dalam masyarakat atau, lebih formalnya, adalah kendala-kendala yang dirancang secara manusiawi yang membentuk interaksi manusia. Tujuan dari institusi adalah untuk menentukan cara permainan dimainkan, pada saat tujuan pemain atau organisasi adalah untuk memenangkan permainan melalui kombinasi keterampilan, strategi, dan koordinasi (D.C North, 1990).

Teori kelembagaan atau institusional menurut Nee dan Swedberg dapat dikonseptualisasikan sebagai sistem dominan yang meliputi elemen informal dan formal yaitu kebiasaan, keyakinan bersama, norma, dan aturan di mana terdapat aktor yang mengarahkan tindakan mereka ketika mereka mengejar kepentingan tertentu. Berdasarkan konsteks tersebut, institusi atau lembagalembaga adalah struktur sosial yang dominan yang menyediakan saluran untuk aksi sosial dan aksi kolektif dengan memfasilitasi dan melakukan penataan kepentingan aktor dan menegakkan hubungan agen utama. Nee dan Swedberg juga menjelaskan bahwa perubahan kelembagaan tidak hanya memperbaharui aturan formal, tetapi membutuhkan penataan kembali kepentingan, norma dan kekuasaan (Victor Nee dan Richard Swedeberg, 2005).

Konsep Strategi

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

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.

Manajemen strategik berkaitan dengan upaya memutuskan persoalan strategi dan perencanaan, dan bagaimana strategi tersebut dilaksanakan dalam praktek. Manajemen strategik dapat dipandang sebagai hal yang mencakup tiga macam elemen utama. Terdapat adanya analisis strategik dimana penyusun strategi (strategis) yang bersangkutan berupaya untuk memahami posisi strategik organisasi yang bersangkutan. Terdapat pula adanya pilihan strategik yang berhubungan dengan perumusan aneka macam arah tindakan, evaluasi, dan pilihan antara mereka. Akhirnya terdapat pula implementasi strategi yang berhubungan dengan merencanakan bagaimana pilihan strategi dapat dilaksanakan (Hunger J. David dan Wheelen Thomas L, 2003:17).

Strategi akan dirumuskan melalui tahapan utama sebagai berikut: 1) Analisis Arah, yaitu untuk menentukan visi-misi-tujuan jangka panjang yang ingin dicapai organisasi. 2) Analisis Situasi, yaitu tahapan untuk membaca situasi dan menentukan Kekuatan-Kelemahan-PeluangAncaman yang akan menjadi dasar perumusan straetegi. 3) Penetapan Strategi, yaitu tahapan untuk identifikasi alternatif dan memilih strategi yang akan dijalankan organisasi.

Selanjutnya, Analisis lingkungan adalah proses dalam manajemen strategi yang bertujuan untuk memantau lingkungan perusahaan. Lingkungan perusahaan disini mencakup semua faktor baik yang berada di

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

dalam maupun di luar perusahaan yang dapat mempengaruhi pencapaian tujuan yang diinginkan (Dirgantoro Crown: 2001;24).

Secara garis besar analisis lingkungan disini akan mencakup analisis mengenai lingkungan eksternal dan lingkungan internal. Lingkungan eksternal akan mencakup lingkungan umum dan lingkungan industri, sedangkan analisis internal akan mencakup analisis mengenai aktivitas perusahaan atau bisa juga analisis mengenai sumber daya, kapabilitas serta kompetensi inti yang dimiliki. Hasil dari analisis lingkungan ini setidaknya akan memberikan gambaran tentang keadaan perusahaan yang biasanya disederhanakan dengan metode SWOT (Strengths, Weaknesses, Opportunities, Threats) yang dimilikinya. Analisis eksternal akan memberikan gambaran tentang peluang dan ancaman (OT) sedangkan analisis lingkungan internal akan memberikan tentang keunggulan dan kelemahan (SW) dari perusahaan.

Konsep *Cyber Security*

Pada dekade kedua abad kedua puluh satu, *prefix* "*cyber*" telah melekat pada konsep-konsep seperti "*cyberculture*", "*cybersex*", dan "*cyberwar*", yang semuanya terkait dengan ranah media digital, virtual reality, dan internet. Dalam budaya populer, awalan dan imbuan berbagai kata terlihat samar-samar, seperti halnya dengan gerakan sastra "cyberpunk". Demikian pula, sejak munculnya internet, kata "network" telah menjadi metafora menonjol dan telah mengambil perhatian di hampir setiap disiplin ilmu kontemporer dan institusi besar. Seperti pada tahun 1948, prefix "*cyber*" ditemukan dalam istilah "*cybernetics*" yang digambarkan sebagai "studi tentang pesan sebagai sarana yang mengendalikan mesin dan masyarakat". Namun, pada dasarnya, tujuan cybernetics adalah untuk mengembangkan bahasa dan teknik menyerang terkait dengan masalah kontrol dan komunikasi pada umumnya dan kemudian menjadi dasar untuk komputasi setelah Perang Dunia II. Seperti halnya istilah "*cyber*", istilah "*network*" sejak pertengahan abad kedua puluh juga telah ada, dan dalam era globalisasi di mana orang di seluruh

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

dunia saling berhubungan melalui infrastruktur transportasi dan komunikasi, network atau jaringan merupakan sebuah material dan realitas metafora (Patrick Jagoda, 2012).

Konsep cybersecurity ini kemudian berkembang di mana menurut Saco dan Deibert ancaman dari cybersecurity juga telah melanggar batas-batas negara sehingga mengancam secara internasional. Hal ini disebabkan oleh, adanya interaksi masyarakat melalui dunia maya yang semakin tinggi akibat kemajuan teknologi dan era informasi. Berbeda halnya pendapat dari Deibert yang menjelaskan bahwa cybersecurity didasari melalui empat wacana terpisah dengan benda rujukan, ancaman, pilihan kebijakan, dan perintah yang berbeda yaitu mencakup keamanan nasional, keamanan negara (terdiri ancaman eksternal terhadap kedaulatan negara serta ancaman internal terhadap keamanan rezim), keamanan swasta, dan keamanan jaringan. Pendapat tersebut didukung oleh Hansen dan Nissenbaum di mana dalam kasus keamanan siber mencakup hubungan antara "jaringan" dan "individu" serta objek referen kolektif manusia sehingga tidak ada wacana tentang keamanan swasta yang merupakan keamanan individu sebagai objek rujukan, melainkan bahwa wacana keamanan individu terkait dengan rujukan sosial dan politik (Hansen, Lene dan Helen Nissenbaum, 2009).

Konsep Diplomasi Siber

Seiring dengan adanya perkembangan zaman, Barrinha dan Renard menyebutkan bahwa diplomasi bukan hanya aktivitas yang melibatkan hubungan antar negara semata, tetapi juga melibatkan sejumlah aktor seperti regional dan international organisation, perusahaan multinasional, *sub-national actors, advocacy networks,* maupun individu yang berpengaruh. Lebih jauh, Barrinha dan Renard juga menyebutkan bahwa konsep diplomasi meluas pada kebijakan baru yang kemudian masuk ke area politik yang belum dipetakan seperti negosiasi iklim hingga meluas ke dalam isu-isu siber (Barinha A. dan Renard T., 2017).

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

Menurut Barrinha dan Renard, diplomasi siber (cyber diplomacy) merupakan diplomasi yang dilakukan di ranah atau domain siber di mana sumber daya diplomatik dan kinerja fungsi diplomatik digunakan untuk mengamankan kepentingan nasional terkait dengan dunia maya yang dilakukan dalam format bilateral maupun multilateral. Dalam hal ini, agenda diplomatik yang menjadi isu utamanya mencakup isu *cyber security, cyber crime, confidence-building, internet freedom*, dan *internet governance*.

Diplomasi siber sendiri telah berkembang pesat dalam mendefinisikan dan merangkum upaya yang terus-menerus dilakukan untuk menyelesaikan jenis konflik baru yang terjadi di dunia maya. Dialog yang dijalankan antar aktor dalam kegiatan diplomasi merupakan salah satu jalan untuk meraih sebuah keuntungan bersama, begitu pula dengan peran utama diplomasi dunia maya yaitu menghasilkan keuntungan melalui dialog tentang masalah keamanan siber (Carmen Elena, 2019).

PEMBAHASAN

Strategi BSSN dalam Membentuk Cyber Security

Keamanan siber telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lain sebagainya. Berbanding lurus dengan tingginya tingkat pemanfaatan teknologi informasi dan komunikasi tersebut, tingkat risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga semakin tinggi dan semakin kompleks.

Menyikapi fenomena tersebut, untuk menciptakan lingkungan siber strategis dan penyelenggaraan sistem elektronik yang aman, andal dan terpercaya; memajukan dan menumbuhkan ekonomi digital dengan meningkatkan daya saing dan inovasi siber; serta membangun kesadaran dan kepekaan terhadap ketahanan dan keamanan nasional dalam ruang siber, pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 membentuk BSSN yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional.

BSSN menyusun Strategi Keamanan Siber Indonesia sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing. Strategi keamanan siber nasional disusun selaras dengan nilai dasar kehidupan berbangsa dan bernegara, yaitu: Kedaulatan, Kemandirian, Keamanan, Kebersamaan, dan Adaptif.

Strategi yang di implementasikan oleh BSSN dalam membentuk 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. Adapun lima pilar GCI tersebut yang akan dijelaskan lebih lanjut, sebagai berikut:

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. BSSN diharapkan dapat mendorong penyusunan UU Keamanan Siber di Indonesia. BSSN juga 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

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

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 (*Computer Emergency Response Team*) nasional; CERT pemerintah; CERT sektoral; standar keamanan siber bagi organisasi; standar dan sertifikasi bagi profesional bidang keamanan siber; dan adanya perlindungan daring bagi anak

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.

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.

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

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

pemerintah dengan swasta; dan kerja sama antar instansi pemerintah.

Berdasarkan acuan GCI diatas, BSSN memiliki arah kebijakan dan strategi nasional untuk mengatasi isu-isu strategis dalam menjaga stabilitas keamanan nasional di ruang siber adalah penguatan keamanan dan ketahanan siber yang diwujudkan dengan strategi berikut:

a. Penguatan pengamanan infrastruktur siber.
b. Pembangunan dan penguatan *Computer Emergency Response Team* (CERT).
c. Pencegahan kejahatan siber dan peningkatan kerjasama internasional bidang siber.
d. Penguatan kapasitas sumber daya manusia keamanan siber.
e. Penyelesaian kejahatan siber clearance rate tindak pidana siber.

Strategi diatas merupakan implementasi dari lima pilar GCI 2017 yang mana strategi tersebut akan diterapkan untuk tahun 2020-2024. Dalam hal ini Indonesia berada dalam tahap pembuatan standarisasi dalam pembentukan Nasional *Cyber Security* sehingga untuk mencapai *cyber security* yang ideal masih memerlukan proses dalam beberapa waktu kedepan. Melalui strategi ini diharapkan BSSN sebagai *leading sector* mampu mengoptimalkan peranannya guna mewujudkan *cyber security* yang ideal bagi Indonesia.

Adapun tujuan strategis Strategi Keamanan Siber Indonesia adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital. Strategi Keamanan Informasi Indonesia ini diharapkan dapat menjadi salah satu fondasi kepercayaan dunia kepada Indonesia dalam berbagai forum keamanan siber internasional. Strategi Keamanan Siber Indonesia merupakan sumbangsih Bangsa Indonesia dalam mendorong terciptanya perdamaian dunia.

Sementara itu dari hasil penelitian terdahulu yang dilakukan oleh Damar Apri Sudarmadi dan Arthur Josias Simon Runturambi, (2019) mengenai strategi yang dapat dilakukan BSSN sebagai berikut:

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

1. Penyusunan Kerangka Kerja *Cyber Security*
    a. Penyusunan perangkat hukum keamanan siber
    b. Penyusunan strategi keamanan siber nasional
    c. Optimalisasi Tugas dan Fungsi BSSN dan CERT
2. Pengembangan Kapasitas Keamanan Siber
    a. Peningkatan kampanye kesadaran publik
    b. Penyusunan program pendidikan, penelitian, dan pengembangan
    c. Peningkatan program pelatihan dan sertifikasi keamanan siber
    d. Penyediaan mekanisme insentif bidang keamanan siber
3. Peningkatan Kerjasama Keamanan Siber
    a. Peningkatan kerja sama bilateral dan multilateral
    b. Peningkatan kerja sama pemerintah dan swasta
    c. Peningkatan kerja sama internal antar instansi pemerintah.

Sementara itu, pada penelitian yang dilakukan oleh Fachrul Febriansyah, Agus Adriyanto, dan Fetri Miftach (2020) mengemukakan bahwa pada hasil penelitianya ditemukan jika penerapan strategi pengamanan SPBE oleh BSSN (Sistem Pemerintahan Berbasis Elektronik) mengalami beberapa hambatan, yaitu regulasi atau kebijakan yang sedang dirancang sehingga strategi belum bisa diimplementasikan. Oleh karena itu, kesimpulan dari penelitian ini adalah penerapan SPBE (Sistem Pemerintahan Berbasis Elektronik) di Indonesia sudah mulai berjalan namun pengamanannya sendiri masih belum siap dikarenakan keterbatasan regulasi dan strategi yang masih belum berjalan.

Dari aspek Teknologi dari GCI, Indonesia saat ini sedang dalam proses menciptakan standar nasional dan alat evaluasi untuk bagaimana keamanan informasi harus dilakukan oleh lembaga pemerintahan dan industri. Salah satu poin menarik dalam strategi ini adalah bagaimana Indonesia mengimplementasikan suatu bentuk filtering Internet lewat program Trust+ dan Nawala filtering. Debat mengenai pemfilteran Indonesia juga menjadi topik yang penting dalam landskap siber Indonesia (Ray

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

Walsh, 2020) dan harus menjadi bagian dari diskusi keamanan siber nasional di Indonesia di masa depan.

Berdasarkan hal tersebut, pentingnya kebijakan dan regulasi terkait dalam penanganan ancaman, pentingnya kebijakan dan regulasi terkait dalam penanganan ancaman *Cyber Crime* dalam membentuk keamanan siber di Indonesia menjadi hal yang sangat penting. hal tersebut dikarenakan pengimplementasian strategi yang telah di rancang untuk membangun *cyber security* yang ideal bagi Indonesia menjadi terhambat. Kepentingan kita untuk membangun *cyber security* yang ideal untuk saat ini diperlukan secepatnya, mengingat kejadian atau kasus-kasus *cyber crime* yang terjadi di Indonesia semakin meresahkan. Menurut GCI (2020) Indonesia menjadi salah satu negara strategis dalam melancarkan aksi *cyber crime*. Indonesia menjadi salah satu negara favorite para hacker dalam melancarkan aksinya, dikarenakan tingkat keamanan yang rendah serta salah satu negara strategis dalam perekonomian dunia.

Analisis Lingkungan Strategis

Perkembangan peranan BSSN dalam membentuk *cyber security* yang ideal bagi Indonesia terus berupaya mempebaiki diri salah satunya degan mengatasi tantangan dan hambatan yang dihadapi oleh organisasi. BSSN perlu diharapkan mampu menjawab isu-isu yang muncul sehingga BSSN mampu mengatasi permasalahan yang terjadi sebagai isu-isu yang strategis. Maka dari itu BSSN menganalisa lingkungan strategis yang dihadapi yang tercantum dalam Rencana Strategis BSSN Tahun 2020-2024 sebagai berikut:

1. Kekuatan
    a. Tersedianya sumber daya manusia yang memiliki kompetensi khusus di bidang keamanan siber dan sandi.
    b. BSSN merupakan instansi pembina jabatan fungsional sandiman.
    c. BSSN memiliki kewenangan untuk melakukan pengaturan ekosistem ekonomi digital dan literasi publik.

d. BSSN memiliki struktur organisasi yang sudah menangani cakupan penguatan keamanan siber dan sandi.
e. BSSN merupakan satu-satunya instansi lembaga pendidikan dan pelatihan pengakreditasi lembaga pemerintah penyelenggara diklat sandi dan siber.

2. Kelemahan
   a. belum optimalnya pemenuhan jumlah sumber daya manusia dibandingkan kebutuhan sumber daya manusia.
   b. belum optimalnya pemetaan jabatan dan penempatan sumber daya manusia.
   c. belum optimalnya sistem pola karier di BSSN.
   d. belum tersedianya standar kompetensi bidang Keamanan Siber yang masih dalam penyusunan.
   e. belum optimalnya pemanfaatan laboratorium untuk penelitian dan pengembangan.
   f. belum tersedianya regulasi dan standar terkait keamanan siber dan sandi secara menyeluruh di BSSN.
3. Peluang Organisasi
   a. Pemanfaatan teknologi era Industri 4.0 seperti big data, artificial intelligence, drone, dan sebagainya untuk peningkatan kinerja organisasi.
   b. Adanya amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik agar BSSN mengelola keamanan sistem pemerintahan berbasis elektronik, menyusun standar keamanan sistem pemerintahan berbasis elektronik Nasional, dan melaksanakan audit keamanan sistem pemerintahan berbasis elektronik.
   c. Adanya amanat pengamanan penyelenggaraan sistem dan transaksi elektronik berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

d. Adanya proyek prioritas strategis nasional penguatan ketahanan dan keamanan siber pada RPJMN Tahun 2020-2024 yang salah satunya peningkatan kapasitas sumber daya manusia keamanan siber dari berbagai sektor seperti K/L/D, IIKN, dan ekonomi digital.
e. Adanya arahan presiden dalam RPJMN Tahun 2020-2024 sebagai strategi dalam pelaksanaan nawacita dan pencapaian sasaran pembangunan nasional, yaitu diantaranya penguatan implementasi manajemen aparatur sipil negara berbasis merit, penyederhanaan birokrasi, dan pengoptimalan manajemen kinerja agar lebih handal, efektif, dan akuntabel.

4. Ancaman Organisasi
   a. ancaman kebocoran data dan informasi diplomasi Indonesia melalui spionase siber.
   b. penerapan ekosistem teknologi jaringan nirkabel (5G) dengan kinerja yang menjanjikan kecepatan data tinggi, pengurangan latensi, penghematan energi, kapasitas sistem yang lebih tinggi, dan konektivitas perangkat secara masif akan menguraikan masalah keamanan siber yang baru.
   c. belum adanya penguatan terhadap pengesahan rancangan undang-undang tentang keamanan dan ketahanan siber.
   d. maraknya ancaman siber melalui hacktivism, kejahatan siber, serangan siber yang berdampak terhadap terhambatnya pertumbuhan ekonomi.
   e. rendahnya pengetahuan masyarakat terkait keamanan siber.
   f. terjadinya perang pikiran melalui berita bohong, cyber bullying, dan ujaran kebencian melalui media sosial.
   g. muncul dan berkembangnya masyarakat 5.0 yang mengadopsi teknologi informasi dan komunikasi (TIK). Hal ini berpotensi munculnya ancaman ketika TIK digunakan untuk kegiatan kejahatan siber.

Jurnal Dinamika Global Vol.7 No. 2, Desember 2022
P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

h. maraknya serangan siber yang semakin berkembang dan massif bahkan terhadap infrastruktur vital.
i. keamanan siber belum menjadi perhatian utama bagi startup sehingga berdampak terhadap perkembangan sektor IIKN. Hal ini berpotensi menimbulkan ancaman keamanan siber.
j. koordinasi antar lembaga penanganan keamanan siber dan sandi yang belum optimal.

Berikut adalah skema dari analisis lingkungan strategis BSSN yang disajikan berdasarkan gambar berikut:

Gambar 1. Hasil Analisis Lingkungan Strategis

P-ISSN 2548-9216 | E-ISSN 2684-9399
https://doi.org/10.36859/jdg.v7i02.1187

Tantangan BSSN dalam Membentuk *Cyber Security* di Indonesia

Adapun tantangan-tantangan yang akan dihadapi oleh BSSN dalam mewujudkan *cyber security* di Indonesia tahun 2020-2024 sebagai berikut:

1. Bergulirnya revolusi industri 4.0 yang menjadi pendukung lahirnya teknologi canggih dan peningkatan penetrasi penggunaan internet di Indonesia. Jika hal tersebut tidak diimbangi dengan peningkatan kesadaran keamanan siber dapat mengeskalasi ancaman keamanan siber yang semakin masif bahkan menyasar infrastruktur vital sehingga mengancam kedaulatan bangsa.
2. Tantangan pengelolaan keamanan siber nasional meliputi pengelolaan sumber daya manusia keamanan siber dan sandi, kebijakan atau regulasi keamanan siber dan sandi termasuk di dalamnya strategi keamanan siber nasional, kerjasama, serta kemandirian teknologi keamanan siber dan sandi dalam rangka mewujudkan kedaulatan siber Indonesia.

Di sisi lain, dalam rangka penyelenggaraan tugas dan fungsi BSSN didentifikasi tantangan yang masih akan dihadapi internal organisasi BSSN meliputi:

a. Aspek kelembagaan yang masih perlu dievaluasi dalam pencapaian sasaran strategis.
b. Aspek Ketatalaksanaan pedoman dan standar operasional prosedur yang belum diterapkan secara menyeluruh.
c. Aspek sumber daya manusia yang kualitasnya perlu ditingkatkan. Dan
d. Aspek sarana dan prasarana yang terbatas serta sistem informasi yang belum terintegrasi sepenuhnya.

KESIMPULAN

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. 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.

Berdasarkan acuan GCI 2017, BSSN memiliki arah kebijakan dan strategi nasional untuk mengatasi isu-isu strategis dalam menjaga stabilitas keamanan nasional di ruang siber adalah penguatan keamanan dan ketahanan siber yang diwujudkan dengan strategi berikut: a. Penguatan pengamanan infrastruktur siber; b. Pembangunan dan penguatan Computer Emergency Response Team (CERT); c. Pencegahan kejahatan siber dan peningkatan kerjasama internasional bidang siber; d. Penguatan kapasitas sumber daya manusia keamanan siber; e. Penyelesaian kejahatan siber clearance rate tindak pidana siber.

Adapun tujuan strategis Strategi Keamanan Siber Indonesia adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital. Strategi Keamanan Informasi Indonesia ini diharapkan dapat menjadi salah satu fondasi kepercayaan dunia kepada Indonesia dalam berbagai forum keamanan siber internasional. Strategi Keamanan Siber Indonesia merupakan sumbangsih Bangsa Indonesia dalam mendorong terciptanya perdamaian dunia.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Profil Internet Indonesia 2022. Page 10 -17.

Badan Siber dan Sandi Negara. Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024.

Bagian Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat, “Laporan Tahunan GOVCSIRT Badan Siber dan Sandi Negara Tahun 2019” *BSSN*, 6 April 2020, diakses 8 November 2022 Pukul 15:34 WiB https://bssn.go.id/gov-csirt-indonesia/

Barrinha A, Renard T. “Cyber-diplomacy: the making of an International society in the digital age”. Global Affairs, (2017).

https://doi.org/10.1080/23340460.201 7.1414924, Retrieved from http://www. tandfonline.com/loi/rgaf20

Berg, B.L. dan H. Lune, Qualitative Research methods for The Social Sciences, ninth edition, England, Essex: Pearson Education Limited, 2017.

Carmen Elena, CÎRNU. "Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy", No. 17 (May-Jun, 2019), http:// www.themarketforideas.com/cyberdiplomacy-addressing-the-gap-in-strategiccyber-policy-a388/.

Damar Apri Sudarmadi, Arthur Josias Simon Runturambi. 2019. Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia
. Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.2

Dirgantoro, Crown. (2001). Manajemen Stratejik: Konsep, Kasus, dan. Implementasi. Jakarta: Grasindo.

Ginanjar, Y. 2019. Hacker sebagai Aktor Non-Negara: Cyber Warfare sebagai Dampak Penyadapan Pejabat Negara Indonesia oleh Intelijen Australia. *Jurnal Dinamika Global,* 4(2), 364-381. https://ejournal.fisip.unjani.ac.id/index.php/jurnal-dinamika-global/article/view/138/113.

Hansen, Lene dan Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School". International Studies Quarterly, Vol. 53, No. 4 (2009).

Hunger, J. David dan Wheelen, Thomas L,(2003). Manajemen Strategis. Andi. Yogyakarta.

Jagoda, Patrick. "Speculative Security". Dalam Derek S. Reveron, Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World (eds). Washington, D.C.: Georgetown University Press, 2012.

Kiki Rezki Ramadhan, Chandra Wijaya. 2022. The Challenges of Personal DataProtection Policyin Indonesia: Lesson learnedfrom the European Union, Singapore, and Malaysia. Technium Social Sciences Journal. Vol.36, 18-28.

Kompas. (2022). Kilas Balik : Lima Kasus Kebocoran Data Pribadi Di Indonesia.
https://www.kompas.com/cekfakta/read/2022/09/06/171100182/kilas-balik-lima-kasus-kebocoran-data-pribadi-di-indonesia-?page=all.
Downloaded in September 2022

Kustin Ayuwiragil, " Indonesia Diserang Hacker Miliaran Kali Tiap Hari " *CNN Indonesia,*8 Desember 2017, diakses 8 November 2022 pukul

12:12 https://www.cnnindonesia.com/teknologi/20171208210751-206-261224/indonesia-diserang-hacker-miliaran-kali-tiaphari/

Maulia Jayantina Islami. 2017. Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. Jurnal Masyarakat Telematika dan Informasi. Vol.8 No.2. Hal:137-144.

Muh. Fachrul Febriansyah, Agus Adriyanto, Fetri Miftach. 2020. Strategi Badan Siber Dan Sandi Nasional Dalam Menghadapi Ancaman Siber Terhadap Sistem Pemerintahan Berbasis Elektronik. Jurnal Peperangan Asimetris. Volume 6 Nomor 2 Tahun 2020.

National Cyber Security Index (NCSI). (2020). https://ncsi.ega.ee/ncsi-index/. Downloaded in September 2022.

Nee, Victor dan Richard Swedberg. "Economic Sociology and New Institutional Economics". Dalam C. M´enard dan M. M. Shirley (eds.), Handbook of New Institutional Economics. Netherland: Springer, 2005.

North, D.C. Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press, 1990.

Organization for Economic Co-operation and Development (OECD). (2021). https://data.oecd.org/ict/internet-access.htm. Downloaded in September 2022.

Ray Walsh. 2020. A guide to internet censorship in Indonesia - And how to unblock websites with an Indonesia VPN. Internet: https://proprivacy.com/guides/indonesia-privacy. Diakses: 29 October 2022.