# STRATEGI KEBIJAKAN PENGEMBANGAN SUMBER DAYA MANUSIA SIBER NASIONAL GUNA MENDUKUNG PERTAHANAN NEGARA

## (STUDI KASUS PADA BADAN SIBER DAN SANDI NEGARA 2019)

## *THE POLICY STRATEGY OF NATIONAL CYBERSECURITY HUMAN RESOURCES DEVELOPMENT TO SUPPORT THE NATIONAL DEFENSE (A CASE STUDY AT THE NATIONAL CYBER AND CRYPTO AGENCY 2019)*

Marina Christmartha[1], Rudy A. G. Gultom[2], Sovian Aritonang[3] UNIVERSITAS PERTAHANAN
(marinachristmartha@gmail.com, rudygultom67@gmail.go.id, sonarira@yahoo.com)

**Abstrak –** Perkembangan teknologi yang cepat dan dinamis membuat penanganan dan pengamanannya menjadi semakin kompleks dan lebih sulit. Ketersediaan serta kemampuan SDM siber nasional memainkan peran penting dalam penanganan ancaman perang siber yang semakin besar. Meskipun telah memiliki badan khusus yang menangani masalah keamanan siber yakni Badan Siber dan Sandi Negara (BSSN), kenyataannya bangsa Indonesia masih kurang SDM sibernya, baik dalam segi kuantitas dan kualitasnya. Hal ini menandakan diperlukannya upaya pengembangan SDM siber nasional yang lebih besar lagi. Tujuan penelitian ini ialah untuk mengidentifikasi dan menganalisis faktor lingkungan strategis keamanan siber terhadap eksistensi BSSN sebagai *leading sector* pengembangan keamanan siber nasional serta terhadap hasil perumusan visi, misi, tujuan, strategi, dan kebijakan BSSN saat ini. Metodologi penelitan ini ialah penelitian kualitatif dengan menggunakan desain penelitian studi kasus. Teknik pengumpulan data dilaksanakan melalui wawancara, observasi dan studi literatur yang dianalisis dengan tahapan pengolahan data, pembacaan keseluruhan data, coding data, penentuan tema dan deskripsi pada data *coding*, dan penghubungan tema/deskripsi data. Hasil analisis menunjukkan bahwa faktor Politik, Ekonomi, Sosial, Teknologi, Lingkungan, dan Hukum melatarbelakangi perumusan strategi BSSN dalam melakukan pengembangan SDM siber nasional. Kebijakan pemerintah diperlukan dalam mengatur Rancangan Undang-Undang (RUU) Keamanan Keamanan dan Ketahanan Siber (KSS) agar dapat menyeimbangankan kebutuhan setiap instansi terhadap keamanan sibernya masing-masing. Meningkatkan kerjasama dengan pihak swasta lainnya terlebih dalam hal mencapai pengembangan SDM siber nasional yang lebih maksimal. Disimpulkan bahwa pengembangan SDM keamanan siber memerlukan regulasi yang kuat dan kerjasama dengan pihak swasta dalam membangun dan menggalang kompetensi masyarakat di bidang keamanan siber.

**Kata Kunci:** Implementasi Kebijakan, Pengembangan SDM, Keamanan Siber, Manajemen Pertahanan, Pertahanan Negara

***Abstract*** *– The rapid and dynamic technological developments make the handling of the matter increasingly complex and more sophisticated. The availability and capability of national cyber human resources management play an important role in dealing with the increasing threat of cyber war. Despite of the existence of the National Cyber and Crypto Agency (BSSN) as the special agency that handles cyber security issues, in reality Indonesia is still lacking in its cyber human resources, both in terms of quantity and quality. This indicates the need for greater national cyber human resource*

[1] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan.
[2] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan.
[3] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan.

*development efforts. The purpose of this study is to identify and analyze the strategic environmental factors of cyber security on the existence of BSSN as a leading sector in the development of national cyber security as well as on the results of the formulation of BSSN's vision, mission, objectives, strategies and policies. This research methodology is a qualitative study using a case study research design. Data collection techniques are carried out through interviews, observation and literature studies that are analyzed by the stages of data processing, overall reading of data, coding data, determining themes and descriptions in data coding, and connecting themes / data descriptions. The results of the analysis show that Political, Economic, Social, Technological, Environmental and Legal factors are the background of the BSSN strategy formulation in developing the national cyber human resources. Government policy is needed in regulating the Draft Bill (RUU) on Security and Cyber Security (KSS) in order to be able to balance the needs of each agency with regard to their respective cyber security. Increasing cooperation with other private parties, especially in terms of achieving the development of national cyber human resources more leverage. It was concluded that the development of cyber security HR requires strong regulation and cooperation with the private sector in developing and mobilizing community competencies in the field of cyber security.*

***Keywords:*** *Policy Implementation, Human Resources Development, Cyber Security, Defense Management, National Defense*

## Pendahuluan

Perkembangan zaman telah mengantarkan manusia pada era kemajuan Ilmu Pengetahuan dan Teknologi dengan waktu yang relatif singkat. Inovasi yang diciptakan oleh kecerdasan manusia ditandai dengan kemampuan teknologi dan kapasitas komputer yang telah berevolusi sangat jauh dari pertama ditemukan pada tahun 1936[4]. Berfungsi dalam mempermudah aktivitas manusia dan menjembatani temuan mutakhir lainnya, computer dikembangkan dengan temuan sistem jaringan ARPANET yang menyebabkan pengembangan protokol untuk *internet working*. Selama lebih dari empat puluh tahun berevolusi, sistem jaringan yang semula ARPANET telah diperbaharui menjadi sistem jaringan yang dinamakan Internet. Sepanjang sejarah, internet kian membawa dampak revolusioner baik dalam aspek budaya serta perdagangan. Terdapat hanya 1% informasi yang mengalir melalui jaringan internet pada tahun 1993, meningkat pada tahun 2000 menjadi 51%, dan meningkat melebihi 97% informasi yang dikomunikasikan pada tahun 2007[5]. Kini dengan internet, sistem perdagangan dan ekonomi secara mayoritas dilkukan dengan transaksi online yakni layanan *e-banking, e-commerce, e-trade, e-business*, dan *e-*

[4] Wawan Setiawan, *"Era Digital dan Tantangannya"*, (Sukabumi: Seminar Nasional Pendidikan, 2017),3-4

[5] CNNIndonesia, "Mengenal Sejarah Internet" dalamhttps://www.cnnindonesia.com/teknologi/20190312125646-185-376484/mengenal-sejarah-internet, diakses pada 13 Februari 2020.

*government*[6]. Pada aspek sosial dan budaya, internet juga menghadirkan kemajuan sosial media sebagai alat komunikasi paling cepat dan efesien[7]. Seakan tidak ada lagi batas dan jarak, internet menyatukan dan memungkinkan konektivitas antar manusia di segala penjuru dan tempat.

Jangkauan internet nyatanya tidak hanya membawa perubahan positif, melainkan juga membawa dampak negatif bagi keamanan insani dan negara. Bentuk kriminal digital yang terjadi saat ini disebut sebagai *Cybercrime*.

Menurut Gregory (sebagaimana dikutip dalam Arifah, 2011, p.186), *cybercrime* merupakan perkembangan akan *computer crime* yang terjadi oleh karena adanya lubang- lubang keamanan pada sistem operasi yang menjadi celah bagi *hacker*, *cracker*, dan *script kiddies* untuk meretas komputer di lain tempat.

Tindakan *cybercrime* merupakan sebuah bentuk kejahatan transnasional oleh karena mencakup banyak pelaku yang berasal dari dua negara atau lebih. *Cybercrime* bukan hanya dapat menyerang satu perangkat komputer saja, namun juga mengancam segala bentuk perangkat lunak komputer, seperti situs, *e-mail*, media sosial, serta lainnya yang mengancam keamanan perbankan, instansi pemerintah, militer, dan kepolisian, serta seluruh pihak yang berbasis pada komputer dan internet secara online. Kedaulatan negara juga terancam dengan adanya ancaman *cyber* karena situs-situs pemerintahan dapat saja dirusak dan dijebol sehingga data yang bersifat pribadi dan rahasia negara diketahui oleh pihak lain.

Keberadaan internet di Indonesia yang dimulai sejak tahun 1990-an kini berkembang pesat dengan jumlah pengguna internet yang melebihi 50% populasi penduduk, yakni: 133 juta pengguna internet aktif, 115 juta pengguna media sosial, dan 106 juta pengguna medsos via ponsel[8] (Badan Siber dan Sandi Negara, 2018-2019). Penyelenggara Jasa Internet Indonesia (APJII) tahun 2016 juga menyampaikan

[6] Marco Gercke, *Understanding cybercrime: pheomena, challenges and legal response*, (Geneva: International Telecommunication Union (ITU), 2012), hlm. 32

[7] Agus Subagyo, *Sinergi dalam Menghadapi Ancaman Cyber Warfare,* (Bandung: Universitas Jendreral Achmad Yani, 2018), hlm. 5

[8] Badan Siber dan Sandi Negara, Peta Okupasi Nasional dalam Kerangka Kualifikasi Nasinal Indonesia pada Area Fungsi Keamanan Siber, (Jakarta, BSSN. 2019).

bahwa pengguna internet di Indonesia mempengaruhi potensi ekonomi digital yakni dengan terjadinya peralihan sistem transaksi jual dan beli dari pasar *offline* ke pasar *online*. Akan tetapi, peningkatan ekonomi digital ini juga saat bersamaan meningkatkan risiko ancaman keamanan siber di Indonesia. Oleh karenanya, negara Indonesia terlibat dalam permasalahan *cybercrime* setelah menyumbang 2.4% kejahatan *cyber* di dunia (Anggoro, 2016).

Laporan *Kaspersky Cybersecurity Index* menunjukkan perbandingan keamanan siber antar negara dimana tertulis Indonesia masih belum dapat mengejar ketertinggalannya dengan negara lain tersebut. Data menunjukkan posisi tiap negara berdasarkan skala ancamannya terhadap dunia maya. Untuk lebih jelasnya dapat dilihat pada gambar di bawah ini.

**Implementasi Kebijakan**

Implementasi kebijakan merupakan tindak lanjut dari setiap kebijakan publik yang dibuat dan merupakan wujud nyata dari dari suatu pengarahan yang sah dari suatu kebijakan yang meliputi upaya pengelolaan *input* untuk menghasilkan *output* bagi masyarakat. Didefinisikan bahwa implementasi merupakan proses umum tindakan administratif yang dapat diteliti pada tingkat program tertentu[9].

Ketika tujuan dan sasaran telah ditetapkan, proses implementasi sangat mungking untuk dijalankan. Hal yang penting untuk dilakukan bagi suatu implementasi ialah adanya susunan program yang jelas serta dana yang telah siap dan diperuntukan bagi sasaran yang tepat.

**Manajemen Strategik**

Menurut Fred R. David[10], Manajemen Strategik merupakan suatu cabang ilmu manajemen yang identik dengan seni dalam merumuskan, mengimplementasikan, serta mengevaluasi keputusan – keputusan lintas fungsional yang memampukan sebuah organisasi mencapai tujuannya. Wheelen & Hunger[11] juga menjelaskan bahwa Manajemen Strategik adalah sejumlah keputusan dan tindakan yang mengarah pada penyusunan suatu strategi atau sejumlah strategi yang efektif untuk membantu mencapai sasaran perusahaan.

---

[9] Haedar Akib, I*mplementasi Kebijakan: Apa, Mengapa, dan Bagaimana,* (Makassar: Jurnal Admistrasi Publik, Volume 1 No. 1, 2010), hlm. 32.

[10] Taufiqurokhman, *Mengenal Manajemen Strategik,* (Jakarta: Fakultas Ilmu dan Ilmu Politik Universitas Prof. Dr. Moestopo Beragama, 2018).

[11] Wheelen & Hunger, Strategic Management and Business Policy, (USA: Pearson, 2012)

Berikut ialah tahapan-tahapan yang harus dilalui dalam Manajemen Strategik[12]:

**Analisis lingkungan *(Environmental Scanning)***

Analisis Lingkungan *(Environmental Scanning)* merupakan analisis variabel – variabel dalam lingkungan internal dan lingkungan eksternal. Untuk melihat faktor-faktor strategis secara keseluruhan, maka digunakan analisis PESTLE *(Political, Economic, Social, Technological, Legal, dan Environment)* sebagai teknik dalam manajemen strategis yang digunakan untuk melihat faktor-faktor lingkungan luar/eksternal yang berpengaruh terhadap transformasi BSSN. Faktor-faktor yang dianalisis mencakup bidang politik *(Political)*, ekonomi *(Economic)*, sosial *(Social)*, teknologi *(Technological)*, perundang-undangan *(Legal)* dan lingkungan *(Environment)*.

**a. Analisis Bidang Politik**

Faktor politik meliputi seluruh faktor yang mempengaruhi penguatan dan pelemahan peran BSSN dari kewenangan yang berlaku, kebijakan pemerintah, dukungan pemerintah dan perhatian/keterlibatan BSSN baik formal atau informal di lingkungan pemerintah.

**b. Analisis Bidang Ekonomi**

Faktor ekonomi meliputi semua faktor yang mempengaruhi keamanan siber dan sandi dari sisi perbankan, transaksi ekonomi, keamanan transaksi online, perdagangan elektronik, dan aspek lain yang mempengaruhi.

**c. Analisis Bidang Sosial**

Faktor sosial meliputi semua faktor yang dapat mempengaruhi keamanan siber dan sandi dari sisi tingkat pendidikan masyarakat, tingkat pertumbuhan penduduk, kondisi lingkungan sosial dan lingkungan kerja.

**d. Analisis Bidang Teknologi**

Faktor teknologi meliputi semua hal yang dapat mempengaruhi keamanan siber dan sandi dari sisi penemuan dan pengembangan baru, biaya dan penggunaan teknologi, perubahan dalam ilmu pengetahuan, dan dampak dari perubahan teknologi.

**e. Analisis Bidang Perundangan**

Faktor perundangan berisikan analisis semua faktor yang mempengaruhi keamanan siber dan sandi dari sisi pengaruh hukum seperti perubahan Undang-Undang yang sudah ada atau yang akan disusun dan

[12] Fred R. David, *Manajemen Strategis: Konsep,* (Jakarta, PT. Prenhallindo, 2004:6-7).

disahkan, hak asasi manusia, dan tata kelola.

**f. Analisis Bidang Lingkungan**

Faktor lingkungan berisikan analisis semua faktor yang mempengaruhi keamanan siber dan sandi dari sisi kondisi lingkungan yang dapat diprediksi atau dikendalikan maupun dalam bentuk force majeur (bencana alam).

**Formulasi Strategi *(Strategy Formulation)***

Formulasi strategi *(Strategy formulation)* merupakan pengembangan perencanaan jangka panjang yang meliputi misi, visi, dan tujuan dari perusahaan, pengembangan strategi, dan penetapan kebijakan.

***a.* Visi *(Visions)***

Visi merupakan gambaran keberhasilan yang ingin dicapai, serta memberikan gambaran masa depan. Berikut adalah 6 (enam) kriteria dari sebuah visi yang efektif:

1) Visi yang memberikan gambaran jelas akan masa depan yang ingin dicapai
2) Visi yang mengadopsi kepentingan seluruh bagian dari perusahaan
3) Visi yang realistis dan dapat dicapai
4) Visi yang jelas dan memberi panduan dalam poses pengambilan keputusan
5) Visi yang fleksibel serta memberi keleluasaan bagi perusahaan dalam menetapkan inisiatif dan tanggapan terhadap perubahan lingkungan
6) Visi yang dapat dikomunikasikan

***b.* Misi *(Missions)***

Misi merupakan alasan atau tujuan suatu organisasi berdiri. Misi merupakan langkah awal dari proses pengembangan strategi perusahaan. sebuah misi yang efektif akan sangat membant perusahaan dalam memformulasikan strateginya. Berikut ialah 6 (enam) kriteria sebuah misi yang efektif:

1) Misi yang jelas dan mudah diingat
2) Misi yang menggambarkan keunikan dari sebuah perusahaan
3) Misi yang memberikan fleksibilitas namun tetap konsisten agar tidak kehilangan fokus
4) Misi yang membantu manajemen dalam proses pengambilan keputusan
5) Misi yang menggambarkan budaya dari perusahaan atau organisasi
6) Misi yang menginspirasi seluruh bagian dari organisasi

***c.*** **Tujuan *(Objectives)***

Tujuan merupakan uraian dari visi yang menjadi sasaran jangka menengah yang konkret dan terukur dalam perjalanan mencapai visi, target yang dibuat. Pernyataan tujuan perlu mencerminkan keadaan masa depan yang ingin dicapai perusahaan secara konkret dan terukur. Dengan melihat tingkat pencapaian dari pernyataan tujuan, manajemen bisa menilai seberapa baik organisasi tersebut telah mengarah pada visi yang ingin dicapai.

***d.*** **Strategi *(Strategy)***

Strategi merupakan rencana berskala besar, dengan orientasi masa depan, guna berinteraksi dengan kondisi persaingan untuk mencapai tujuan perusahaan[13]. Jenis strategi dapat dibagi ke dalam 3 (tiga) menurut fungsinya, yakni: 1) Strategi Korporat, 2) Strategi Bisnis, 3) Strategi fungsional.

***e.*** **Kebijakan**

Kebijakan merupakan suatu pedoman dalam menentukan pengambilan keputusan dalam tahap formulasi strategi dengan implementasinya. Kebijakan merupakan acuah dalam menentukan aksi yang mendukung misi, tujuan, dan strategi perusahaan.

***1.*** **Implementasi Strategi *(Strategy Implementation)***

Implementasi strategi merupakan sebuah proses dimana strategi dan kebijakan diarahkan ke dalam tindakan melalui pengembangan program, anggaran dan prosedur[14].

**a. Program**

Program merupakan serangkaian aktivitas atau langkah yang dibutuhkan dalam mencapai sebuah perencanaan. Program merupakan wujud nyata suatu orientasi strategi.

**b. Anggaran**

Anggaran merupakan pernyataan kondisi keuangan yang dibutuhkan dalam perencanaan, control anggaran, serta informasi anggaran yang dapat diketahui secara detail berapa besarnya biaya yang dibutuhkan dari suatu program.

**c. Prosedur**

Prosedur merupakan sistem yang berisikan langkah dan teknik dalam mendeskripsikan secara terperinci mengenai bagaimana tugas khusus

[13] John A. Pearce II & Richard B. Robinson, *Manajemen Strategis: Formulasi, Impementasi, dan Pengendalian,* (Indonesia: Salembag Empat, 2013).

[14] Wheelen & Hunger, *Strategic Management and Business Policy,* (USA: Pearson, 2012, pg.69)

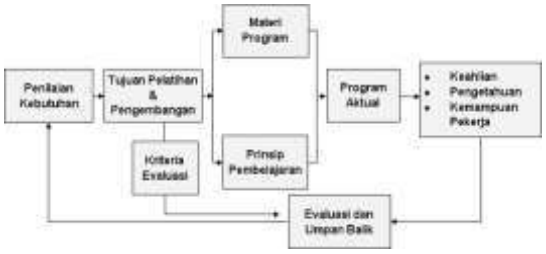
atau pekerjaan dilakukan dengan semestinya.

2. **Evaluasi dan Pengendalian *(Evaluation and Control)***

Proses evaluasi dan pengendalian merupakan suatu proses dimana aktivitas-aktivitas perusahaan, hasil kinerja dimonitor dan kinerja sesungguhnya dibandingkan dengan kinerja yang diinginkan. Elemen ini dapat menunjukkan secara tepat kelemahan-kelemahan dalam implementasi strategi sebelumnya dan mendorong proses keseluruhan untuk dimulai kembali.

**Pengembangan Sumber Daya Manusia**

Langkah-langkah dan pengembangan SDM dapat berjalan sesuai dengan rencana yang ditetapkan akan terlaksana apabila dilakukan melalui langkah-langkah sebagai berikut[15]:




**Gambar 1.** Langkah-langkah Pelatihan dan Pengembangan

Sumber: *Manajemen Sumber Daya Manusia untuk Perusahaan (2015)*

Penilaian kebutuhan adalah suatu diagnosa untuk menentukan masalah yang dihadapi saat ini dan tatangan di masa mendatang yang harus dapat dipenuhi oleh program pelatihan dan pengembangan.

Tujuan Pelatihan dan Pengembangan harus dapat memenuhi kebutuhan yang diinginkan oleh suatu organisasi serta dapat membentuk tingkah laku yang diharapkan serta kondisi-kondisi bagaiamna hal tersebut dapat dicapai.

Materi Program disusun dari estimasi kebutuhan dan tujuan pelatihan. Kebutuhan di sini mungkin dalam bentuk pengajaran keahlian khusus, penyajikan pengetahuan yang diperlukan, atau berusaha untuk memengaruhi sikap.

Prinsip Pembelajaran merupakan suatu kesadaran bahwa pelatihan dan pengembangan akan lebih efektif jika metode pelatihan disesuaikan dengan sikap pembelajaran peserta dan jenis pekerjaan yang dibutuhkan oleh organisasi.

Untuk mencapai tujuan dari program pengembangan dan pelatihan maka metode pengembangan harus dipilih dan disesuaikan dengan kebutuhan dan kemampuan karyawan perusahaan dan dapat dikembangkan oleh perusahaan.

[15] Taliziduhu Ndraha, *Pengantar Teori Pengembangan Sumber Daya Manusia,* (Jakarta: PT RIneka Cipta, 1999).

Pendidikan dalam arti sempit yaitu untuk meningkatkan keahlian dan kecakapan manajer memimpin para bawahannya secara efektif[16]. Sedangkan pelatihan, menurut Gary Dessler[17] adalah metode yang digunakan untuk memberikan karyawan baru atau yang ada saat ini dengan keterampilan yang mereka butuhkan untuk melakukan pekerjaan.

**Konsep Keamanan Siber (Cyber Security)**

*Cyber security* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna[18].

Keamanan siber di Indonesia mengacu pada *Global Cyber Security* yang dibangun di atas lima bidang kerja, yakni: (1) Kepastian Hukum (undang- undang cyber crime); (2) Teknis dan tindakan prosedural; struktur (3) Struktur organisasi yang berkembang dan menghindari tumpang tindih); (4) Capacity building dan pendidikan; dan (5) Pengguna (kampanye publik dan komunikasi terbuka dari ancaman cyber crime.

**Metode Penelitian**

Metode pendekatan kualitatif yang digunakan pada penelitian ini adalah kualitatif deskriptif ini menggunakan pendekatan Manajemen Strategik model Wheelen & Hunger (2012) untuk mengetahui apa dan bagaimana fenomena-fenomena yang terjadi diantara variabel-variabel penelitian dengan pengumpulan data melalui wawancara dan studi pustaka, sedangkan pengolahan data menggunakan metode analisis data kualitatif menggunakan teori John W. Creswell (2014). Peneliti mengumpulkan data primer dan sekunder sebagai materi utama dalam melakukan penelitian. Data primer didapat melalui wawancara, observasi dan dokumentasi di Badan Siber dan Sandi Negara (BSSN) yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang

[16] Malayu Hasibuan, Manajemen Sumber Daya Manusia, (Jakarta: PT. Bumi Aksara, 2000, hlm. 80).

[17] Gary Dessler, *Manajemen Sumber Daya Manusia,* (Jakarta: PT. Indeks, 2006:280)

[18] Handrini Ardiyanti (2014), *Cyber-security dan Tantangan Pengembangannya di Indonesia,* (Junal Politica, V (I), hlm. 95-110.

terkait dengan keamanan siber. Data sekunder diperoleh dari portal terkait seperti portal resmi Kementerian dan Insititusi.

Selanjutnya, data yang diperoleh di uji keabsahannya dengan menggunakan pemeriksaan keabsahan data yang meliputi uji *credibility, transferability, dependability,* dan *confirmability*[19].

**Hasil dan Pembahasan**

Terhadap hasil wawancara utama dengan Badan Siber dan Sandi Negara (BSSN) dengan narasumber pelaksana Deputi Pemantauan dan Pengendalian BSSN yang memiliki kewenangan khusus dalam melaksanakan pengembangan SDM siber nasional, berikut ialah hasil wawancara dan pembahasan yang dikaitkan dengan implemetasi kebijakan pengembangan SDM siber nasional guna mendukung pertahanan negara oleh BSSN.

**Analisis Lingkungan**

Untuk melihat faktor-faktor strategis secara keseluruhan, maka digunakan analisis PESTLE *(Political, Economic, Social, Technological, Legal,* dan *Environment)* sebagai teknik dalam manajemen strategis yang digunakan untuk melihat faktor-faktor lingkungan luar/eksternal yang berpengaruh terhadap transformasi BSSN. Faktor-faktor yang dianalisis mencakup bidang politik *(Political)*, ekonomi *(Economic)*, sosial *(Social)*, teknologi *(Technological)*, perundang-undangan *(Legal)* dan lingkungan *(Environment)*[20].

**1. Analisis Bidang Politik**

Faktor politik meliputi seluruh faktor yang mempengaruhi penguatan dan pelemahan peran BSSN dari kewenangan yang berlaku, kebijakan pemerintah, dukungan pemerintah dan perhatian/keterlibatan BSSN baik formal atau informal di lingkungan pemerintah.

Suhu politik semakin meningkat menjelang Pilkada serentak tahun 2018-2019 menyebabkan terjadinya situasi peredaran berita *hoax*, gambar yang menghasut dan fitnah, pernyataan berbau SARA yang berpotensi membuat perpecahan di masyarakat. Adanya Pilkada Serentak dan Pemilu Nasional 2019 membuat BSSN dalam waktu dekat harus siap untuk turut serta mengamankan proses demokrasi yang berlangsung dan membangun

[19] Sugiyono, *Metodologi Penelitian Kualitatif,* (Yogyakarta, Alfabeda, 2017).

[20] Badan Siber dan Sandi Negara, *Rencana Strategis Badan Siber dan Sandi Negara*, (Jakarta: BSSN, 2018-2019).

kepercayaan *(trust)* dari berbagai pihak kepada BSSN.

Penerbitan Perpres mengenai BSSN memunculkanberbagai aspek perubahan terkait proses transformasi Lembaga Sandi Negara menjadi BSSN. BSSN ke depannya harus melayani kepentingan yang lebih luas, dapat diterima oleh semua pihak baik pemerintah maupun swasta serta dapat menjawab ekspektasi terhadap BSSN yang tinggi yaitu mampu menjamin keamanan siber nasional.

**2. Analisis Bidang Ekonomi**

Keamanan siber di bidang ekonomi adalah hal yang serius. Data *International Telecommunications Union* (ITU) menunjukkan bahwa ancaman dan serangan siber merugikan secara finansial. Menurut Laporan ITU tahun 2017, rata-rata biaya harus ditanggung pengguna internet di Indonesia untuk mengurangi atau mencegah infeksi malware adalah 51 USD. Selain itu, rata-rata besaran kehilangan uang akibat penipuan finansial melalui online mencapai 111 USD. Perdagangan elektronik *(e-commerce)* adalah penyebaran, pembelian, penjualan, pemasaran barang dan jasa melalui sistem elektronik seperti internet atau televisi, world wide web (www), atau jaringan komputer lainnya.

Ada tujuh isu penting yang menghambat berkembangnya industri perdagangan elektronik di Indonesia. Tujuh isu penting tersebut adalah masalah pendidikan dan SDM, masalah pendanaan, masalah logistik, masalah perpajakan, masalah infrastruktur komunikasi, masalah keamanan siber, dan masalah perlindungan konsumen.

**3. Analisis Bidang Sosial**

Jika dilihat dari data *Kaspersky Cybersecurity Index*, terlihat bahwa keamanan siber Indonesia masih tertinggal jauh dibandingkan dengan negara lain. Data dalam laporan tersebut menunjukkan gambaran posisi Negara negara mengenai tingkat bahaya pengguna yang terpapar secara online.

Data dalam laporan *Kaspersky* menunjukkan sebanyak 83 persen masyarakat Indonesia tidak peduli dan tidak percaya bahwa mereka bisa menjadi target kejahatan siber. Ketidakpedulian tersebut berbanding terbalik dengan fakta bahwa 47 persen masyarakat pada dasarnya pernah mengalami beragam ancaman siber, 32 persen telah pernah terserang virus atau serangan malware, dan 15 persen telah pernah diretas akun onlinenya.

Dalam konteks sosial, ancaman siber tidak hanya dilakukan oleh pihak asing, namun juga oleh individu di dalam negeri yang kurang memiliki tanggung jawab dalam berinternet. Akun-akun individu dan organisasi dalam wilayah Indonesia yang melakukan penghinaan atau ujaran kebencian, berita palsu dan sejenisnya dapat membesar menjadi isu keamanan nasional.

**4. Analisis Bidang Teknologi**

Sejumlah factor yangmempengaruhi kualitas dukungan teknologi dalam penguatan BSSN di masa depan diantaranya adalah sumber daya dan infrastruktur. Saat ini, pada aspek sumber daya *(resource)* teknolIndonesia merupakan pasar produk Teknologi Informasi (TI) Internasional. Hal ini dikarenakan produk keamanan TI di Indonesia sebagian besar masih diimpor dari luar negeri. Namun jika dianalisis, sumber daya *(resource)* yang dibutuhkan oleh BSSN bukanlah terkait dengan teknologi saja, namun juga terkait dengan SDM internal. BSSN perlu meningkatkan kompetensi SDM internal terutama kompetensi di bidang sistem kendali industri *(industrial control system)* yang berguna untuk pengamanan siber di industri kritis *(critical industry)*.

**5. Analisis Faktor Lingkungan dan Perundangan**

Dalam transformasi BSSN, lingkungan alam memiliki pengaruh terhadap keamanan siber Indonesia. Contohnya seperti bencana alam yang dapat menghancurkan infrastruktur teknologi informasi. Faktor lain yang menyebabkan mudahnya infrastruktur teknologi informasi hancur oleh bencana alam dikarenakan saat ini belum ada manajemen pemulihan insiden siber akibat bencana alam. Penanganan dan antisipasi yang perlu dilakukan oleh BSSN dalam menghadapi masalah tersebut antara lain membuat *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) pada infrastruktur/teknologi informasi di lingkup pemerintahan, infrastruktur informasi kritikal nasional dan perdagangan ekonomi digital secara komprehensif serta membangun kerjasama dengan instansi dan lembaga terkait pada lingkup nasional dan global ketika terjadi bencana siber.

Persoalan dan tantangan yang dihadapi oleh BSSN juga dapat dianalisis dari perspektif hukum terkait kelembagaan dan peran BSSN. Dalam tataran regulasi keamanan siber, tatanan perundangan yang terkait secara langsung dengan penerapan keamanan

siber di Indonesia belum memadai. Regulasi yang menjadi referensi saat ini masih bersifat sektoral yaitu Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah direvisi menjadi Undang- Undang Republik Indonesia Nomor 19 Tahun 2016. Selain itu, Undang-Undang yang mengatur tentang informasi adalah Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi, dan Undang- Undang Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

Saat ini, Perpres Nomor 53 Tahun 2017 sebagaimana telah diubah terakhir dengan Perpres Nomor 133 Tahun 2017 tentang Badan Siber dan Sandi Negara merupakan wujud konkrit pemerintah untuk beraksi terhadap ancaman siber. Namun masih terdapat masalah terkait yang muncul, seperti contohnya, secara internal masih ada istilah atau definisi yang belum ada satu kesepahaman. Masalah tersebut dapat diselesaikan dengan melakukan perbaikan Peraturan Badan Siber dan Sandi Negara atau Perangkat Peraturan yang lain dan perbaikan tersebut harus bisa menjadi prioritas BSSN secara internal. Penguatan eksistensi BSSN yang dilakukan dengan cara penguatan Undang-undang juga diperlukan dalam menyelesaikan masalah terkait kelembagaan dan peran BSSN dalam perspektif hukum.

**Formulasi Strategi**

Setelah diihat dari faktor-faktor pada lingkungan strategis yang sebelumnya dianalisis dengan analisis PESTLE *(Political, Economic, Social, Technological, Legal, dan Environment)*, berikut ialah Visi dan Misi yang dimiliki oleh BSSN.

1. **Visi dan Misi *(Visions & Missions)***

Visi Misi Badan Siber dan Sandi Negara, maka Visi Badan Siber dan Sandi Negara Tahun 2018-2019 adalah "Menjadi institusi tepercaya dalam menjaga ketahanan dan keamanan siber dan sandi nasional dengan menyinergikan berbagai pemangku kepentingan untuk mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi digital".

BSSN memiliki visi untuk menjadi institusi tepercaya yang mengutamakan profesionalisme, integritas, adaptabilitas, dan kepercayaan dalam mewujudkan keamanan siber dan sandi di Indonesia dengan menunjukkan peran yang strategis dalam

menyinergikan seluruh pemangku kepentingan keamanan siber nasional dan internasional. Dalam hal in, BSSN telah menunjukkan dengan jelas gambaran visi dan misi yang jelas di masa depan dan yang ingin dicapai serta tetap mengadopsi kepentingan seluruh bagian dari perusahaan.

BSSN juga memiliki visi dalam mewujudkan keamanan nasional dengan turut serta menciptakan kondisi siber yang terbebas dari ancaman. BSSSN juga tengah mengupayakan penyelenggaraan perekonomian digital, sehingga masyarakat dengan penuh kepercayaan merasa aman dan nyaman melakukan aktifitas perekonomian secara digital sehingga mampu mempercepat pertumbuhan ekonomi nasional. Visi yang ditetapkan oleh BSSN telah cukup memberi gambaran realistis bagi kemajuan teknologi ke depanna serta bersifat fleksibel karena mengupayakan strategi keamanan siber di era kemajuan teknologi saat ini. Visi tersebut akan semakin jelas apabila dikomunikasikan atau disampaikan secara terbuka kepada masyarakat tentang peran BSSN terkait keamanan siber, agar masyarakat luas juga dapat menyadari akan pentingnya menjaga keamanan siber.

Perihal misi-misi yang dimiliki BSSN, terlihat bahwa BSSN memandang kejelasan suatu misi sebagai hal yang penting. Misi pertama yang dimiliki BSSN ialah menjamin keamanan informasi di sektor pemerintah, infrastruktur informasi kritikal nasional, dan ekonomi digital dalam mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional. BSSN juga berupaya dalam membangun dan tata kelola keamanan siber dan sandi yang komprehensif serta misi kemandirian teknologi keamanan siber dan sandi dengan mendorong tumbuhnya industri dalam negeri di bidang keamanan siber dan sandi.

Terhadap misi membantu manajemen dalam proses pengambilan keputusan, BSSN telah menjelaskan misinya dalam membangun, mengoordinasikan, mengolaborasikan, dan mengoperasionalkan sistem identifikasi, deteksi, mitigasi, manajemen krisis, penanggulangan, dan pemulihan terhadap ancaman, insiden, dan/atau serangan siber dan sandi. Selalin itu BSSN berupaya menyediakan dan mengoptimalkan sumber daya keamanan siber dan sandi

melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan dengan didukung manajemen perkantoran secara transparan dan akuntabel. BSSN juga menggambarkan budaya yang dianut untuk diterapkan dengan menjelaskan misinya membangun budaya keamanan siber melalui penggunaan internet yang aman dan nyaman oleh setiap warga negara Indonesia.

**2. Tujuan *(Objective)***

Berdasarkan hasil penelitian, BSSN memiliki 5 (lima) tujuan khusus yang yang merupakan uraian visi dan misi organisasi. Beberapa tujuannya ialah pertama, tercapainya fondasi struktur, sistem dan budaya organisasi BSSN yang kuat. Saat ini secara sistem dan budaya organisasi BSSN tengah berkembang sejak dibentuknya di tahun 2017. Hasil dari tujuan tersebut tentunya konkret dan apabila belum dapat tercapai tujuan sepenuhnya, masih dalam batas wajar. Meskipun merupakan lembaga baru, sejauh ini BSSN banyak memberikan kontribusi terhadap keamanan nasional di bidang keamanan siber dalam rangka eksistensinya sebagai *leading sector* keamanan siber. Hal tersebut dibuktikan dengan peringkat *Global Cybersecurity Index* (CGI) Indonesia di tahun 2018 yang menempati peringkat ke-41 yang sebelumnya berada di posisi ke-70 secara global.

Tujuan berikutnya yang akan dicapai oleh BSSN ialah tersusunnya kebijakan, sistem dan prosedur berstandar global dalam bidang keamanan siber dan sandi di Indonesia. BSSN saat ini tengah membangun infrastruktur keamanan siber arah terkait keamanan siber di Indonesia. Salah satu infrastruktur keamanan siber yang tengah disusun BSSN ialah *National Security Operation Center (NSOC)* atau Pusat Operasi

Keamanan Siber Nasional[21]. NSOC nantinya akan memegang operasi keamanan siber Indonesia. Keamanan siber nasional meliputi pemantauan keamanan siber nasional, pusat kontak siber, serta tata kelola keamanan informasi dan infrastruktur. NSOC dibentuk sebagai langkah BSSN untuk menjadikan BSSN sebagai Badan Siber Kelas Dunia. BSSN juga meluncurkan tim respon siber sektor pemerintah

[21] CNN Indonesia, "BSSN Ungkap Tantangan Bangun Keamanan Siber dan Awasi Startup". Retrieved from https://www.cnnindonesia.com/teknologi/20191204192016-185-454196/bssn-ungkap-tantangan-bangun-keamanan-siber-dan- awasi-startup, diakses pada 15 Februari 2020.

yang dinamakan *Gov-CSIRT (Government Cyber Security Incident Response Team).*

BSSN juga bertujuan untuk menciptakan sistem manajemen talenta untuk menarik, memelihara dan meretensi SDM siber dan sandi terbaik. Retensi karyawan adalah suatu keharusan yang perlu dilakukan oleh perusahaan guna mempertahankan Sumber Daya Manusia (SDM) terbaik yang dimilikinya. Beberapa upaya BSSN yang dinilai efektif dalam meretensi karyawan yang berpotensi ialah antara lain dengan adanya benefit tunjangan kinerja pegawai di lingkungan BSSN yang telah diatur dalam Peraturan Presiden (Perpres) No.87 Tahun 2018 tentang Tunjangan Kinerja Pegawai di Lingkungan Badan Siber dan Sandi Negara.

**Tabel 1.** Tunjangan Kinerja Pegawai di Lingkungan BSSN

| NO | KELAS JABATAN | TUNJANGAN KINERJA PER KELAS JABATAN |
|---|---|---|
| 1 | 2 | 3 |
| 1. | 17 | Rp. 26.324.000,00 |
| 2. | 16 | Rp. 20.695.000,00 |
| 3. | 15 | Rp. 14.721.000,00 |
| 4. | 14 | Rp. 11.670.000,00 |
| 5. | 13 | Rp. 8.562.000,00 |
| 6. | 12 | Rp. 7.271.000,00 |
| 7. | 11 | Rp. 5.183.000,00 |
| 8. | 10 | Rp. 4.551.000,00 |
| 9. | 9 | Rp. 3.781.000,00 |
| 10. | 8 | Rp. 3.319.000,00 |
| 11. | 7 | Rp. 2.928.000,00 |
| 12. | 6 | Rp. 2.702.000,00 |
| 13. | 5 | Rp. 2.493.000,00 |
| 14. | 4 | Rp. 2.350.000,00 |
| 15. | 3 | Rp. 2.216.000,00 |
| 16. | 2 | Rp. 2.089.000,00 |
| 17. | 1 | Rp. 1.968.000,00 |

Sumber: *Setkab*

Para pegawai pemerintah non pegawai negeri (PPNPN) di lingkungan Badan Siber dan Sandi Negara (BSSN) juga telah dilindungi dengan program Jaminan Kecelakaan Kerja (JKK) dan Jaminan Kematian (JKM) dari BP Jamsostek, Sehingga PPNPN dapat kerja dengan tenang karena manfaat JKK dan JKM BP Jamsostek dapat melindungi tenaga kerja dari berbagai macam risiko

terutama resiko kecelakaan kerja[22]. Sesuai tujuan dibentuknya BSSN, BSSN bertujuan untuk menciptakan kinerja pencegahan, deteksi, mitigasi, dan penanggulangan ancaman keamanan siber dan sandi. Sebagai lembaga yang dibentuk untuk menangani ancaman keamanan siber, BSSN tidak perlu memiliki kewenangan penindakan seperti aparat penegak hukum. BSSN diharapkan menjadi lembaga analisis potensi kerawanan untuk pencegahan serangan pertahanan dan keamanan nasional lewat media siber[23].

Tujuan lainnya yang dimiliki BSSN ialah menjalin kerjasama-kerjasama strategis dengan seluruh pihak untuk membangun keamanan siber dan sandi di Indonesia. Dalam hal ini, terlebih dahulu urgensi peran BSSN diperhatikan, sebagai Lembaga Pemerintah Non Kementerian diharapkan dapat berfungsi sebagai *National Cyber Security Centre* sebagai rujukan utama penanganan keamanan siber dan *clearing house information exchange* sebagai wujud nyata pembangunan ekosistem ranah siber Indonesia dengan segera menginisiasi Peta jalan pedoman penanganan keamanan siber. BSSN juga perlu melakukan penguatan kerjasama antara swasta (melalui ID-CERT), pemerintah (BSSN), masyarakat, dan *stakeholder* internasional (seperti pemilik aplikasi media social yang seringkali dimanfaatkan untuk media kejahatan (twitter, Facebook, dan sebagainya), serta lembaga terkait di dunia international dalam pencegahan maupun penanganan kejahatan siber.

Tujuan yang tak kalah penting dari BSSN ialah dengan membentuk kesadaran, perilaku dan budaya keamanan siber yang baik pada setiap warga negara Indonesia[24].

Hal tersebut dapat terwujud apabila dilakukan peningkatan sosialisasi keamanan informasi (termasuk aspek

[22] Media Indonesia, *"Pegawai Non Pegawai Negeri BSSN Telah Terindungi BP Jamsostek". Retrieved from* https://mediaindonesia.com/read/detail/27413 3-pegawai-non-pegawai-negeri-bssn-telah-terlindung-bp-jamsostek, diakses pada 15 Februari 2020.

[23] Edwin Elnizar, *"Kewenangan Badan Siber dan Sandi Negara Diharap Tidak Offside". Retrieved from* https://www.hukumonline.com/berita/baca/lt5a55768b2da1d/kewenangan-badan-siber- dan-sandi-negara-diharap-tidak-offside/, diakses pada 14 Februari 2020.

[24] Maulia Jayantina Islami, *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index,* (Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo, 2017).

hukum, promosi SKKNI bidang Keamanan Informasi dan Auditor TI) bagi masyarakat dan Sektor yang mengelola data Strategis/ Edukasi Publik juga dapat menumbuhkan kesadaran keamanan, pemahaman kebhinekaan, dan anti terrorisme diterapkan secara sistemastis dimulai dari usia dini dengan memasukkan kurikulum keamanan siber sejak di bangku Sekolah Menengah Pertama.

### 3. Strategi *(Strategy)*

Strategi pemerintah dalam pengembangan SDM keamanan siber diimplementasikan dalam bentuk:

a) Pemenuhan regulasi, kebijakan dan standar terkait SDM siber nasional dalam bentuk peraturan perundang-undangan dan standar-standar kompetensi di bidang Keamanan Siber;
b) Pemberian bimbingan teknis bagi SDM siber nasional;
c) Penyelenggaraan pelatihan-pelatihan di bidang keamanan siber;
d) Melakukan penjajakan untuk akreditasi dan lisensi lembaga sertifikasi profesi bidang keamanan siber;
e) Melakukan pendataan SDM siber nasional sebagai titik tolak pengembangan SDM Siber Nasional.

Menurut analisis fungsi dari strategi BSSN, BSSN telah mengkomunikasikan maksud dalam visi yang ingin dicapai serta bentuk pelaksanaan pengerjaannya, seperti mengenai strategi pemenuhan regulasi, kebijakan dan standar terkait SDM siber nasional dalam bentuk peraturan perundang-undangan dan standar- standar kompetensi di bidang Keamanan Siber. Strategi ini menghubungkan serta mengaitkan kekuatan atau keunggulan organisasi dengan pelang dari lingkungannya. Selain itu, di dalam strateginya, BSSN berupaya menghasilakn dan membangkitkan sumber-sumber daya yang lebih banyak digunakan dari sekarang, yakni dengan upaya strategi pemberian bimbingan teknis bagi SDM siber nasional dan penyelenggaraan pelatihan-pelatihan di bidang keamanan siber. Strategi ini berorientasi pada dihasilkannya identias dan kualitas sumber daya di masa depannya.

Selain itu strategi BSSN dinilai telah tanggap akan keadaan baru di masa depan dengan melakukan proses yang terus menerus dalam menemukan, menciptakan dan menggunakan sumber daya manusia serta mengarahkan

aktivitas pendukungnya yakni dengan melakukan penjajakan untuk akreditasi dan lisensi lembaga sertifikasi profesi bidang keamanan siber. Ditambah lagi dengan aktivitasnya melakukan pendataan SDM siber nasional sebagai titik tolak pengembangan SDM Siber Nasional.

**4. Kebijkaan *(Policies)***

Dalam pengambilan suatu keputusan organsiasi secara keseluruhan, tentunya diperlukan suatu kebijakan yang berfungsi sebagai pedoman luas untuk menghubungkan strategi dan implementasi. Kebijakan tersebut diinterpretasi dan diimplementasi melallui strategi dan tujuan masing-masing divisi yang kemudian dikembangkan dan menjadi pedoman bagi wilayah fungsionalnya untuk diikuti.

Pengembangan kapasitas SDM Siber Nasional menjadi keniscayaan untuk dilaksanakan secara cepat dan terarah, sehingga hal ini menjadi salah satu kebijakan prioritas BSSN di Tahun 2020 dalam mencapai Visi dan Misi BSSN untuk mendukung program pemerintah yang mencanangkan visi 'SDM Unggul, Indonesia Maju'.

Untuk itu, BSSN menetapkan kebijakan pengembangan kapasitas dan kapabilitas SDM siber nasional sebagai acuan utama dengan berpegang pada slogan 'Mewujudkan SDM Keamanan Siber Dan Sandi Yang Terpercaya, Profesional Dan Berdaya Saing'. BSSN saat ini dalam proses pembangunan yang bukan hanya fisik (teknologi) namun juga membangun sumber daya manusianya. BSSN memandang bahwa SDM merupakan kunci dalam menjaga keamanan keamanan siber yang diwujudkan juga melalui pembentukan Sekolah Tinggi Sandi Negara yang sudah dikembangkan menjadi politeknik siber. SDM itu akan dikembangkan dalam Reset and Development (RND) agar teknologi yang dimiliki BSSN tidak ketinggalan.

Meskipun demikian, BSSN saat ini perlu menguatkan payung hukum dan regulasi untuk mendukung pelaksanaan tugas BSSN agar regulasi yang ada tidak tumpah tindih antara pusat dan daerah juga sebagai upaya penguatan eksistensi BSSN sebagai *leading sector* yang dilakukan dengan cara penguatan undang-undang yang diperlukan

**Kesimpulan dan Rekomendasi**

Pada penelitian ini telah dilaksanakan pembahasan implementasi pengembangan SDM siber nasional pada Badan Siber dan Sandi Nasional (BSSN). Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan di atas, maka dapat disimpulkan bahwa:

Hasil analisis lingkungan strategis dengan menggunakan PESTLE menunjukkan bahwa secara faktor politik, penerbitan Perpres memunculkan perubahan Lemsaneg menjadi BSSN dengan tujuan eksistensi BSSN yang semakin luas. Pada faktor ekonomi, keamanan siber yang lemah menjadi faktor penghambat berkembangnya industry perdagangan elektronik di Indonesia.

Dalam lingkup sosial, ancaman siber nasional bukan hanya disebabkan oleh pihak asing, namun juga oleh individu dalam negeri. Pada bidang teknologi, kemampuan SDM internal terutama pada kompetensi di bidang sistem kendali indsutri menjadi faktor bagi BSSN dalam melakukan pengembangan SDM keamanan siber yang lebih cepat. Pada analisis faktor lingkungan, bencana alam sewaktu-waktu dapat menyebabkan mudahnya infrastruktur teknologi informasi hancur karena belum adanya manajemen pemulihan insiden bencana alam. Diperlukan *Business Continuity Plan* (BCP) dan *Disaster Revovery Plan* (DRP) terhadap infrastruktur informasi di lingkup pemerintahan, infrastruktur informasi kritikal nasional, dan perdagangan ekonomi digital secara komprehensif. masih terdapat masalah terkait yang muncul, seperti contohnya, secara internal masih ada istilah atau definisi yang belum ada satu kesepahaman. Masalah tersebut dapat diselesaikan dengan melakukan perbaikan Peraturan Badan Siber dan Sandi Negara atau Perangkat Peraturan yang lain dan perbaikan tersebut harus bisa menjadi prioritas BSSN secara internal.

Proses perumusan visi, misi dan tujuan dilakukan oleh BSSN telah dilakukan secara terbuka dan melibatkan seluruh pemangku kepentingan *stakeholder* sehingga benar-benar dapat menggambarkan cita-cita dari seluruh komponen bangsa Indonesia. Visi, misi, dan tujuan BSSN disosialisasikan dengan cukup baik, terlebih pada lingkungan kementerian dan sedang diupayakan untuk disosialisasikan pada lingkungan masyarakat luas.

Strategi yang dijelaskan oleh BSSN telah jelas namun dibutuhkan penjabaran lebih detail tentang tahapan dan proses strategi tersebut dengan lebih terperinci dan jelas terutama dalam pengembangan SDM siber nasional.

**Rekomendasi**

Berdasarkan hasil penelitian dan pembahasan, serta kesimpulan yang telah di uraikan di atas, maka peneliti merekomendasikan:

1. Kebijakan pemerintah dalam mengatur Rancangan Undang-Undang (RUU) Keamanan Keamanan dan Ketahanan Siber (KSS) agar dapat menyeimbangankan kebutuhan setiap instansi terhadap keamanan sibernya masing- masing.
2. Menganilisis secara lanjut kompetensi para pelaksana pengembangan siber nasional dalam mendukung keberhasilan implementasi pengembangan SDM keamanan siber karena masih dikhawatirkankompetensi pelaksana yang belum seluruhnya cermat dalam melakukan analisis kebutuhan SDM keamanan siber yang tepat. Pemahaman dalam konteks *cyber security* dan *cyber crime* dan peranan tiap instansi juga diperlukan dalam mencegah terjadinya tumpang tindih pelaksanaan fungsi pengembagan SDM siber nasional tersebut.
3. Meningkatkan kerjasama dengan pihak swasta lainnya terlebih dalam hal mencapai pengembangan SDM siber nasional yang lebih maksimal.

**Daftar Pustaka Buku**

Fred R. David, *Manajemen Strategis: Konsep,* (Jakarta, PT. Prenhallindo, 2004:6-7).

Gary Dessler, *Manajemen Sumber Daya Manusia,* (Jakarta: PT. Indeks, 2006:280)

John A. Pearce II & Richard B. Robinson, *Manajemen Strategis: Formulasi, Impementasi, dan Pengendalian,* (Indonesia: Salemba Empat, 2013).

Malayu Hasibuan, Manajemen Sumber Daya Manusia, (Jakarta: PT. Bumi Aksara, 2000, hlm. 80).

Marco Gercke, *Understanding cybercrime: pheomena, challenges and legal response*, (Geneva: International Telecommunication Union (ITU), 2012), hlm. 32.

Maulia Jayantina Islami, *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia*

*Ditinjau Dari Penilaian Global Cybersecurity Index,* (Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo, 2017).

Taliziduhu Ndraha, *Pengantar Teori Pengembangan Sumber Daya Manusia,* (Jakarta: PT RIneka Cipta, 1999).

Wheelen & Hunger, Strategic Management and Business Policy, (USA: Pearson, 2012)

Wheelen & Hunger, *Strategic Management and Business Policy,* (USA: Pearson, 2012, pg.69)

**Jurnal**

Agus Subagyo, *Sinergi dalam Menghadapi Ancaman Cyber Warfare,* (Bandung: Universitas Jendreral Achmad Yani, 2018), hlm. 5

Haedar Akib, I*mplementasi Kebijakan: Apa, Mengapa, dan Bagaimana, (*Makassar: Jurnal Admistrasi Publik, Volume 1 No. 1, 2010), hlm. 32.

Handrini Ardiyanti (2014), *Cyber-security dan Tantangan Pengembangannya di Indonesia,* (Junal Politica, V (I), hlm. 95-110

Wawan Setiawan, *"Era Digital dan Tantangannya",* (Sukabumi: Seminar Nasional Pendidikan, 2017),3-4

**Sumber Elektronik**

Badan Siber dan Sandi Negara, *Peta Okupasi Nasional dalam Kerangka Kualifikasi Nasinal Indonesia pada Area Fungsi Keamanan Siber*, (Jakarta, BSSN. 2019).

Badan Siber dan Sandi Negara, *Rencana Strategis Badan Siber dan Sandi Negara*, (Jakarta: BSSN, 2018-2019).

CNN Indonesia, "Mengenal Sejarah Internet" alamhttps://www.cnnindonesia.com/teknologi/20190312125646-185-376484/mengenal-sejarah-internet, diakses pada 13 Februari 2020.

Edwin Elnizar, *"Kewenangan Badan Siber dan Sandi Negara Diharap Tidak Offside". Retrieved from* https://www.hukumonline.com/berita/baca/lt5a55768b2da1d/kewenangan- badan-siber-dan-sandi-negara-diharap-tidak-offside/, diakses pada 14 Februari 2020.

Media Indonesia, *"Pegawai Non Pegawai Negeri BSSN Telah Terindungi BP Jamsostek". Retrieved from* https://mediaindonesia.com/read/detail/274133-pegawai-non-pegawai-negeri-bssn-telah-terlindung-bp-jamsostek, diakses pada 15 Februari 2020.

Sugiyono, *Metodologi Penelitian Kualitatif,* (Yogyakarta, Alfabeda, 2017).

Taufiqurokhman, *Mengenal Manajemen Strategik,* (Jakarta: Fakultas Ilmu dan Ilmu Politik Universitas Prof. Dr. Moestopo Beragama, 2018).