UNIVERSITAS PERTAHANAN

URGENSI STRATEGI KEAMANAN SIBER NASIONAL DALAM MENDUKUNG SISTEM PERTAHANAN DAN KEAMANAN RAKYAT SEMESTA : ANALISIS FUNGSI DASAR MANAJEMEN TERHADAP UPAYA TERWUJUDNYA SUMBER DAYA MANUSIA PERTAHANAN SIBER

RUBY ALAMSYAH
NIM 120190101012

Tesis yang Ditulis untuk Memenuhi Sebagian Persyaratan dalam Mendapatkan Gelar Magister Pertahanan

FAKULTAS STRATEGI PERTAHANAN
PROGRAM STUDI STRATEGI PERANG SEMESTA

BOGOR
2020

LEMBAR PERSETUJUAN TESIS

Nama	:	**Ruby Alamsyah**
NIM	:	**120190101012**
Program Studi	:	**Strategi Perang Semesta**
Fakultas	:	**Fakultas Strategi Pertahanan**
Judul Tesis	:	**Urgensi Strategi Keamanan Siber Nasional Dalam Mendukung Sistem Pertahanan Dan Keamanan Rakyat Semesta : Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya Sumber Daya Manusia Pertahanan Siber**

Pembimbing I,	Pembimbing II,
Dr. I Wayan Midhio, M.Phil.	Dr. Agus H.S Reksoprodjo, ST.,DIC.
Letnan Jenderal TNI (Purn)	
Tanggal: 2 Nopember 2020	Tanggal: 27 Oktober 2020

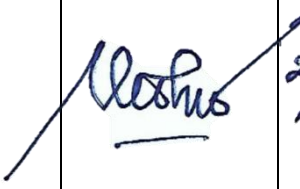
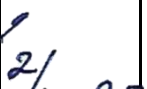
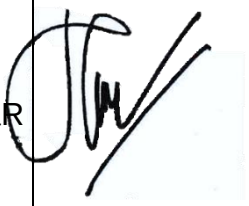
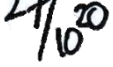
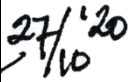
Mengetahui,

Dekan
Fakultas Strategi Pertahanan

Dr. Deni D.A.R, S.Sos., M.Si (Han)
Mayor Jenderal TNI
Tanggal : 10 Nopember 2020

LEMBAR PENGESAHAN TESIS

Nama	:	**Ruby Alamsyah**
NIM	:	**120190101012**
Program Studi	:	**Strategi Perang Semesta**
Fakultas	:	**Fakultas Strategi Pertahanan**
Judul Tesis	:	**Urgensi Strategi Keamanan Siber Nasional Dalam Mendukung Sistem Pertahanan Dan Keamanan Rakyat Semesta : Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya Sumber Daya Manusia Pertahanan Siber**

No	Nama	T.Tangan	Tanggal
1.	Pembimbing I Dr. I Wayan Midhio, M.Phil. Letnan Jenderal TNI (Purn)		
2.	Pembimbing II Dr. Agus H.S. Reksoprodjo, ST.,DIC.		
3.	*Reviewer* I Dr. Hipdizah, S.Adm., M.Si.,CIQnR.,CIQaR Mayor Jenderal TNI (Purn)		
4.	*Reviewer* II Dr. Rizerius Eko H., S.E., S.AP., M.Si. Mayor Jenderal TNI		
5.	*Reviewer* III Dr. Lukman Yudho Prakoso, S.Ip., M.AP. Kolonel Laut (E)		27 Okt 2020

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah diajukan untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang sepengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis diajukan dalam naskah ini dan disebutkan dalam daftar Referensi.

Apabila dikemudian hari terbukti bahwa terdapat plagiat dalam tesis ini, saya bersedia menerima sanksi sesuai ketentuan peraturan/undang-undang yang berlaku.

Bogor, 19 Oktober 2020

Ruby Alamsyah

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Tuhan Yang Maha Esa, atas berkat rahmat dan karunia-Nya, penulisan tesis dengan judul "Urgensi Strategi Keamanan Siber Nasional Dalam Mendukung Sistem Pertahanan Dan Keamanan Rakyat Semesta: Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya Sumber Daya Manusia Pertahanan Siber" dapat diselesaikan. Penyusunan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister pada Program Studi Strategi Perang Semesta Fakultas Universitas Pertahanan.

Penyusunan tesis/disertasi ini dapat diselesaikan berkat bantuan dan dukungan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu, pada kesempatan ini peneliti mengucapkan terima kasih kepada yth:

1. Bapak Mayor Jenderal TNI Dr. Deni D.A.R, S.Sos., M.Si (Han), selaku Dekan Fakultas Strategi Pertahanan, Universitas Pertahanan;

2. Bapak Letnan Jenderal TNI (Purn) Dr. I Wayan Midhio, M.Phil, selaku dosen Pembimbing-1 yang telah berkenan dan penuh kesabaran memberikan bimbingan, ilmu, dan pengetahuan, serta menyediakan waktu, tenaga, dan pikiran demi mengarahkan peneliti dalam menyelesaikan Tesis;

3. Bapak Dr. Agus H.S. Reksoprodjo, ST.,DIC., selaku dosen Pembimbing-2 yang juga berkenan menyediakan tenaga, waktu, dan pikiran untuk memberikan bimbingan kepada peneliti dalam menyelesaikan Tesis ini, khususnya menyangkut aspek *cyberspace* yang masih baru untuk bidang pertahanan negara;

4. Bapak/Ibu selaku tim penguji pada sidang-sidang Tesis, terima kasih.

5. Bapak Kolonel Czi Helda Risman, M.Han, selaku Sekretaris Program Studi SPS yang sejak awal telah banyak membantu dan mengarahkan peneliti dalam hal prosedur penulisan dan lain sebagainya, terima kasih;

6. Para Dosen Magister Pertahanan untuk Program Studi SPS Fakultas Strategi Pertahanan Universitas Pertahanan, terima kasih untuk segala ilmu yang telah diberikan selama peneliti mengikuti perkuliahan;

7. Keluargaku, dalam hal ini isteri dan anaku tercinta, Ibu, Bapak, dan adik-adikku, terima kasih atas kasih sayang, doa, dan *support* yang telah diberikan;

8. Rekan-rekan tercinta Cohort-11 Program Pasca Sarjana Unhan, khususnya untuk Prodi SPS, terima kasih atas suka dan duka yang kita lalui selama perkuliahan, semoga sukses selalu.

Semoga Tuhan Yang Maha Esa membalas kebaikan-kebaikan berbagai pihak atas bantuannya.

Peneliti menyadari bahwa tesis ini masih kurang sempurna, oleh karena itu dengan kerendahan hati mengharapkan kritik dan saran yang konstruktif demi kesempurnaan tesis ini.

Akhirnya, semoga tesis ini dapat memberikan manfaat terhadap pengembangan ilmu pertahanan dan bermanfaat bagi nusa, bangsa, dan negara Indonesia.

Bogor, 19 Oktober 2020

Ruby Alamsyah

ABSTRAK

URGENSI STRATEGI KEAMANAN SIBER NASIONAL DALAM MENDUKUNG SISTEM PERTAHANAN DAN KEAMANAN RAKYAT SEMESTA : ANALISIS FUNGSI DASAR MANAJEMEN TERHADAP UPAYA TERWUJUDNYA SUMBER DAYA MANUSIA PERTAHANAN SIBER

RUBY ALAMSYAH

Bagi negara Indonesia, era teknologi informasi dan komunikasi (TIK) atau digital seperti saat ini, aspek pertahanan dan keamanan menjadi satu kesatuan faktor hakiki dalam mempertahankan kedaulatan, keutuhan wilayah, keamanan dan keselamatan segenap bangsa dan negara dari berbagai bentuk ancaman siber, yang datang dari dalam maupun luar negeri. Dalam membangun keamanan siber, nasional, Strategi Keamanan Siber Nasional (SKSN) akan menjadi pedoman strategis, di mana saat ini masih dalam proses perumusan oleh pemerintah melalui BSSN, sedangkan untuk membangun kemampuan pertahanan siber, maka bidang pertahanan, di samping menempatkan SKSN sebagai hal yang penting di era digital, juga menempuh upaya membangun kompetensi sumber daya manusia (SDM) yang memiliki *knowledge* dan *skill* serta kapasitas dan kapabilitas yang spesifik dalam bidang pertahanan siber untuk kemudian ditransformasikan sebagai bagian dari komponen pertahanan negara dalam kerangka sistem pertahanan dan keamanan rakyat semesta (sishankamrata). Lalu bagaimana kemudian eksistensi SKSN menjadi penting terhadap upaya membangun kompetensi SDM pertahanan siber untuk sishankamrata ? Penelitian ini menggunakan metode kualitatif dengan pendekatan verifikatif fenomenologi, dan dengan analisis fungsi dasar manajemen (POAC) pada tata kelola (manajemen) pembangunan dan peningkatan kompetensi SDM oleh Pushansiber Kemhan, Satsiber TNI, Balitbang SDM Kominfo, dan BSSN, yang menunjang upaya terwujudnya kompetensi SDM pertahanan siber. Hasil penelitian menunjukan gambaran fenomenologi bahwa SKSN menjadi hal yang penting bagi bidang pertahanan dalam kerangka membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

Kata Kunci: Sistem Pertahanan dan Keamanan Rakyat Semesta, Strategi Keamanan Siber Nasional, Kompetensi SDM

ABSTRACT

URGENCY OF NATIONAL CYBER SECURITY STRATEGY IN SUPPORTING THE INDONESIAN UNIVERSAL DEFENSE AND SECURITY SYSTEMS : ANALYSIS BASIC FUNCTION OF MANAGEMENT ON THE EFFORTS THE REALIZATION OF CYBER DEFENSE HUMAN RECOURCES

RUBY ALAMSYAH

*For the Indonesian state, in the era of information and communication technology (ICT) or digital as it is today, the aspects of defense and security have become an essential factor in maintaining the sovereignty, territorial integrity, security and safety of all nations and countries from various forms of cyber threats, which come from domestic and foreign. In building cybersecurity, nationally, the National Cyber Security Strategy (SKSN) will be a strategic guideline, which is currently still in the process of formulating by the government through the BSSN, while to build cyber defense capabilities, the defense sector in addition to put SKSN as an important. In the digital era, we also take efforts to build competency in human resources (HR) who have specific knowledge and skills as well as capacities and capabilities in the field of cyber defense to be transformed as part of the state defense component within the Indonesian universal defense and security systems (*sishankamrata*) framework. Then how then the existence of SKSN becomes important in the effort to build the competence of human resources for cyber defense for* sishankamrata*? This study uses a qualitative method with a phenomenological verivicative approach, and with analysis of basic management functions (POAC) in development governance and improvement of HR competencies by Pushansiber of the Ministry of Defense, Satsiber TNI, Balitbang SDM Kominfo, and BSSN, which support efforts to realize HR competencies cyber defense. The results of the study show a phenomenological picture that SKSN is important for the defense sector in the framework of building cyber defense HR competencies for the benefit of sishankamrata.*

Keywords: The Indonesian Universal Defense and Security Systems, National Cybersecurity Strategy, Human Resources Competence

DAFTAR ISI

Hal

HALAMAN JUDUL i
LEMBAR PERSETUJUAN TESIS ii
LEMBAR PENGESAHAN TESIS iii
PERNYATAAN ORISINALITAS iv
KATA PENGANTAR v
ABSTRAK vii
DAFTAR ISI ix
DAFTAR GAMBAR xii
DAFTAR TABEL xiv

BAB 1 PENDAHULUAN 1

1.1 Latar Belakang 1
1.2 Rumusan Masalah 7
1.3 Tujuan Penelitian 8
1.4 Manfaat Penelitian 8
1.4.1 Manfaat Teoritik 8
1.4.2 Manfaat Praktis 9

BAB 2 TINJAUAN PUSTAKA 10

2.1 Landasan Teori 10
2.1.1 Teori Pertahanan Negara (Hanneg) 11
2.1.2 Teori Strategi 14
2.1.3 Teori Manajemen 20
2.2 Landasan Konseptual 23
2.2.1 Pengertian Urgensi 23
2.2.2 Keamanan (*Security*) 23
2.2.3 Ancaman 26
2.2.4 Kompetensi 30
2.3 Penelitian Terdahulu Yang Relevan 32
2.4 Kerangka Berpikir 35

BAB 3 METODE PENELITIAN 37

3.1 Metode dan Desain Penelitian 37

3.1.1 Metode Penelitian 37
3.1.2 Desain Penelitian 39
3.2 Tempat dan Waktu Penelitian 40
3.2.1 Tempat Penelitian 40
3.2.2 Waktu Penelitian 40
3.3 Subyek dan Obyek Penelitian 41
3.3.1 Subyek Penelitian 41
3.3.2 Obyek Penelitian 42
3.4 Teknik Pengumpulan Data 43
3.4.1 Penelitian Lapangan 43
3.4.1.1 Wawancara 43
3.4.1.2 Observasi 44
3.4.1.3 Dokumentasi 44
3.4.2 Penelitian Kepustakaan (*Library Research*) 44
3.5 Pemeriksaan Keabsahan Data 44
3.6 Teknik Analisis Data 45
3.6.1 Pengumpulan Data (*Data Collection*) 46
3.6.2 Kondensasi Data (*Data Condensation*) 46
3.6.3 Penyajian Data (*Data Display*) 47
3.6.4 Kesimpulan (*Conclussion: Description/Verifying)* 47
3.7 Faktor-Faktor Kualitatif Yang Diteliti dan Operasional Teori George R. Terry 47
3.7.1 SKSN Sebagai Faktor-1 (F_1) 48
3.7.2 Sishankamrata Sebagai Faktor-2 (F_2) 50
3.7.3 Operasional Teori Manajemen George R.Terry Terhadap Faktor-1 (F_1) dan Faktor-2 (F_2) 51

BAB 4 HASIL PENELITAN DAN PEMBAHASAN 53

4.1 Gambaran Umum Obyek Penelitian 53
4.2 Hasil Penelitian 61
4.2.1 Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata 61
4.2.2 Faktor-Faktor Yang Mendukung dan Menghambat SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata 77
4.2.3 Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan Sishankamrata 85

4.3 Pembahasan 92
4.3.1 Analisis Prinsip POAC Berkenaan Dengan Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata 93
4.3.2 Analisis Prinsip POAC Pada Faktor-Faktor Yang Mendukung Dan Menghambat SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata 100
4.3.3 Analisis Prinsip POAC Pada Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan Sishankamrata 109
4.3.4 Eksistensi Urgensi SKSN Dalam Upaya Peningkatan Kompetensi SDM Pertahanan Siber, Terhadap Teori Strategi dan Hanneg, Maupun Konseptual Ancaman dan Keamanan 115
4.3.5 Matrik Deskripsi Fungsi Kompetensi SDM Pertahanan Siber Dengan Tolok Ukur Pada Kompetensi SDM TIK dan SDM Keamanan Siber 118

BAB 5 KESIMPULAN DAN REKOMENDASI 120

5.1 Kesimpulan 120
5.2 Rekomendasi 121

DAFTAR PUSTAKA 124

LAMPIRAN – LAMPIRAN 133

Lampiran 1 (Surat Perintah Penelitian) 133
Lampiran 2 (Surat Permohonan Penelitian) 135
Lampiran 3 (Surat Keterangan Penelitian) 139
Lampiran 4 (Panduan Pertanyaan Wawancara) 144
Lampiran 5 (Dokumen Pendukung Data Penelitian) 152
Lampiran 6 (Display Hasil Kondensasi Data Penelitian) 187
Lampiran 7 (Dokumentasi Kegiatan Wawancara) 197

RIWAYAT HIDUP PENELITI 200

DAFTAR GAMBAR

		Hal
Gambar 2.1	Diagram Sistem Pertahanan Negara …….	12
Gambar 2.2	*National Cybersecurity Strategy Model* ……..……..	16
Gambar 2.3	*The Pillars of Cybersecurity* …..……..	17
Gambar 2.4	Kerangka Berpikir Penelitian ……	36
Gambar 3.1	Proses Analisis Data Kualitatif Model Interaktif …….	46
Gambar 3.2	Diagram Operasional Teori Manajemen George R. Terry Terhadap Faktor Kualitatif Penelitian ……. ...…	52
Gambar 4.1	Proses Tata Kelola SDM TIK ke SDM Pertahanan Siber	59
Gambar 4.2	Kunjungan Kerja Kepala BSSN di Pushansiber Kemhan	63
Gambar 4.3	Kunjungan Kerja Wamenhan RI ke Pushansiber Kemhan	64
Gambar 4.4	Kajian Kebutuhan Kompetensi SDM Pertahanan Siber Berkorelasi Dengan Jenjang karir …….	65
Gambar 4.5	Nota Kesepahaman (MoU) Antara TNI dan BSSN …….	67
Gambar 4.6	Pembukaan Latihan Bersama *Cobra Gold Exercise* 2018	68
Gambar 4.7	Program Digital Talent Scholarship (DTS) Kominfo ……	69
Gambar 4.8	Pelatihan dan Sertifikasi Kompetensi Bidang TIK Berbasis SKKNI Gelombang-1 Tahun 2020 Secara *Online* ……..…….	70
Gambar 4.9	Tiga Sasaran Strategis Pengembangan SDM dan Kesiapan Masyarakat ……	71
Gambar 4.10	Forum Komunikasi Bakohumas Bahas Keamanan *Cyber* Untuk Pertahanan Negara ……..	74
Gambar 4.11	Esensi Kompetensi SDM Keamanan Siber di Indonesia	75
Gambar 4.12	Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber	77
Gambar 4.13	Pushansiber KEMHAN Hadiri *Cybersecurity Drill Test* BSSN Untuk Sektor Pemerintah …….	78

Gambar 4.14	Pushansiber Kemhan Hadiri FGD Kajian Strategi Organisasi BSSN Dalam Mengkonsolidasi Unsur Keamanan Siber ……...	79
Gambar 4.15	Pushansiber Kemhan Menerima Kunjungan BSSN Terkait Koordinasi Identifikasi Sektor IIKN ……	80
Gambar 4.16	Tim Siber TNI Melaksanakan Latihan ISTX ……..	81
Gambar 4.17	Perolehan *Score Cybersecurity Drill Test* ……..	86
Gambar 4.18	Kegiatan Latma *Cobra Gold Exercise* 2019 …….	87
Gambar 4.19	Kegiatan *Cyber* Jawara Tahun 2015 ……..	88
Gambar 4.20	Program DTS Kominfo Tahun 2020 ……	89
Gambar 4.21	Sosialisasi Bimtek G-CIO Kominfo Tahun 2017 ……	90
Gambar 4.22	BSSN *Cybersecurity Drill Test* (Sektor Pemerintah) …..	91

DAFTAR TABEL

		Hal
Tabel 2.1	Hasil Penelitian Terdahulu Yang Relevan …….	34
Tabel 3.1	Daftar Instansi Tempat Penelitian ……..……	40
Tabel 3.2	Jadwal Waktu Penelitian ……..……	41
Tabel 3.3	Daftar Subyek Penelitian ……..……	41
Tabel 3.4	Uraian Fungsi dan Indikator Faktor – 1 (F_1) ……..……...	49
Tabel 3.5	Uraian Fungsi dan Indikator Faktor – 2 (F_2) ……..……..	50
Tabel 4.1	Matrik Implementasi POAC Pada F_1 Yang Relevan Dengan Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber …….....	95
Tabel 4.2	Matrik Implementasi POAC Pada F_2 Yang Relevan Dengan Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber ……..……	96
Tabel 4.3	Matrik Implementasi POAC Pada F_1 dan F_2 Terkait Faktor-Faktor Pendukung dan Penghambat SKSN Terhadap Upaya Membangun SDM Pertahanan Siber ……	102
Tabel 4.4	Matrik Implementasi POAC Pada F_1 dan F_2 Terkait Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber ……..……	110
Tabel 4.5	Matrik Deskripsi Area Fungsi Kompetensi SDM Pertahanan Siber Bertolok Ukur Pada Kompetensi SDM TIK dan SDM Keamanan Siber ……..……	118

BAB 1
PENDAHULUAN

1.1 Latar Belakang.

Indonesia sebagai negara merdeka dan berdaulat menempatkan aspek pertahanan dan keamanan sebagai satu kesatuan faktor yang sangat hakiki dalam menjamin keberlangsungan hidup berbangsa bernegara. Tanpa kapasitas dan kapabilitas dalam bidang pertahanan dan keamanan, negara tidak mungkin mampu untuk kewajiban mempertahankan kedaulatan, keutuhan wilayah, keamanan dan keselamatan bangsa dan negara dari berbagai ancaman yang datang dari dalam maupun luar negeri. Semangat tersebut sejalan dengan cita-cita Proklamasi Kemerdekaan Indonesia tanggal 17 Agustus 1945, di mana bangsa Indonesia telah bertekad bulat untuk membela serta mempertahankan dan menegakkan kemerdekaan serta kedaulatan bangsa dan Negara Kesatuan Republik Indonesia (NKRI) berdasar Pancasila dan UUD Negara Republik Indonesia Tahun 1945.

Perkembangan kemajuan Teknologi Informasi dan Komunikasi (TIK) di era digital saat ini, aspek upaya menjaga kedaulatan, keutuhan wilayah, keamanan, dan keselamatan bangsa negara dari ancaman baru berbasis *cyberspace* (ruang siber atau dunia maya), atau lazim juga disebut dengan *cyber threat* (ancaman siber), telah membawa dampak pada perubahan paradigma, konsep, dan strategi pada aspek pertahanan dan keamanan Indonesia yang secara fundamental operasionalnya tidak lagi terbatas pada ranah (domain) fisik, namun telah merambah ke ranah non-fisik. Ancaman siber atau ancaman yang terjadi di dan/atau melalui ruang siber tersebut, merupakan ancaman berdimensi teknologi yang karakteristiknya jauh lebih kompleks, canggih, penetratif, efektif, dan destruktif.

Ruang siber merupakan wujud kemajuan dan perkembangan ilmu pengetahuan di bidang TIK, yang dengan sifat dinamisnya akan terus dan terus berkembang. Ruang siber juga merupakan wujud ekosistem yang terbentuk setidaknya oleh tiga faktor penting yang saling berkorelasi, yaitu: SDM (*people*), proses (*process*), dan teknologi (*technology*). Bila dijabarkan lagi, di dalamnya meliputi antara lain: teknologi sistem informasi, basis data, jaringan telekomunikasi data (*internet*), aplikasi, sistem komputer, dan perangkat prosesor berikut pengendali, termasuk operator (*brainware*), maupun manajemen (tata kelola) sistem elektronik, serta teknologi kecerdasan buatan atau *artificial intelligence* (AI).

Infrastruktur TIK telah dimanfaatkan di berbagai negara pada sektor-sektor penting (strategis) untuk kehidupan umat manusia. Dan seiring dengan hal tersebut, muncul bentuk-bentuk ancaman baru di ruang siber, yang menjadikan infrastruktur TIK di berbagai sektor strategis tersebut kemudian menjadi sangat *critical* (vital/kritikal), sehingga harus selalu dijaga dan dipelihara kamanannya. Karena vitalnya infrastruktur TIK tersebut, maka padanya didudukkan sebagai suatu infrastruktur informasi kritikal (*critical information infrastructures*), yang apabila terjadi ancaman dan gangguan terhadapnya, maka akan berdampak serius terhadap kepentingan nasional suatu negara. Ancaman siber sangat dinamis, tidak cukup menempatkannya sebagai ancaman aktual (ancaman yang sudah ada), namun padanya terdapat karakteristik sebagai ancaman potensial, terutama ketika eskalasinya terus dan terus meningkat, dan bermuara pada suatu titik tertentu terjadinya insiden serangan siber (sebagai bentuk bencana yang tidak pernah diperkirakan sebelumnya), lalu berkembang luas sehingga menjadi konflik dahsyat berskala masif, yang kemudian dipersepsikan sebagai perang atau peperangan siber (*cyber war* / *warfare*).

Aktivitas ancaman maupun serangan siber yang pernah terjadi terhadap Indonesia, antara lain: dengan Portugis pada tahun 1999 (terkait

isu konflik Timor Timur); dengan Malaysia dari tahun 2007 sampai sekarang (perseteruan antar *hacker* kedua negara yang bermotif politik, budaya, saling ejek, dan lain sebagainya); terjadinya insiden kebocoran dokumen rahasia oleh *Wikileaks* yang merugikan Indonesia (tahun 2010); aksi-aksi sadap komunikasi digital Indonesia oleh intel asing; kebocoran info dan data akibat lemahnya perhatian dan rendahnya pengetahuan keamanan informasi dan komunikasi; berbagai tindak pidana siber maupun kegiatan terorisme yang memanfaatkan *internet* sebagai media komunikasi dan kegiatan belajar; kejahatan bidang telekomunikasi; kejahatan siber (*fraud scam, spam, phishing skimming)* sejak tahun 1997 sampai sekarang (sebagaimana dikutip dari artikel Kementerian Pertahanan, 2013). Barangkali tidak harus sebagai negara target, namun Indonesia juga setidaknya sudah menjadi negara terdampak dan bahkan memiliki risiko tinggi akibat sebaran *malware* stuxnet global yang target utama sebenarnya adalah fasilitas pengayaan nuklir di Natanz (Iran) yang mengalami bencana di tahun 2010. Dari 100% sebaran *malware* tersebut, negara Iran menempati urutan sebaran pertama tertinggi sebesar 52,2%, disusul Indonesia dan India yang masing-masing sebesar 17,4% dan 11,3% (ESET – Microsoft Windows, 2010). Artinya sejak tahun 2010 faktor risiko keamanan siber Indonesia meningkat.

Semenjak 2003, instansi Kepolisian RI (Polri) juga mencatat sejumlah kasus, seperti: *cyber crime carding (CC fraud), card skimming, hacking, craking, internet banking fraud*, *malware, cyber* pornografi, *online gambling*, *transnational crime* (narkoba, mafia, teroris, pencucian uang, perdagangan manusia, pasar gelap*)*; sehingga pada tahun 2002, Indonesia menduduki peringkat kedua kejahatan TIK setelah Ukraina, terutama *online fraud* (bahasan Tim kerja Pertahanan Siber Kemhan RI, 2013). Hal tersebut diperkuat oleh laporan tahunan *Akamai Internasional* bahwa pada tahun 2013 negara Indonesia menduduki posisi puncak setelah negara China sebagai negara dengan lalu lintas serangan siber tertinggi. Indonesia

adalah 1,3% pangsa pasar pengguna *Internet* dunia yang menyumbang 38% dari total serangan siber di dunia (Akamai International, 2013).

Sistem Pertahanan Negara (sishanneg) atau Sistem Pertahanan dan Keamanan Rakyat Semesta (sishankamrata) adalah sistem pertahanan negara (hanneg) di Indonesia yang bersifat semesta, yang melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, dipersiapkan pemerintah secara dini, diselenggarakan secara total, terpadu, terarah, berkesinambungan, dan berkelanjutan demi tegaknhya kedaulatan, keutuhan wilayah NKRI, serta terlindunginya keselamatan segenap bangsa dari berbagai ancaman (UU No.34/2004 tentang TNI, Pasal 1 ayat 6). Pada dasarnya penyelenggaraan hanneg adalah untuk mencegah dan mengatasi ancaman (militer dan non militer) yang nyata maupun belum nyata, dari dalam dan luar negeri. Sifat kesemestaan dalam sishankamrata dimaknai sebagai wujud perang semesta itu sendiri di mana pengelolaanhya melalui suatu konsep yang disebut sebagai strategi perang semesta. Kekuatan hanneg yang diperlukan dalam penyelenggaraan strategi perang semesta untuk menghadapi berbagai bentuk ancaman, meliputi seluruh komponen hanneg, yaitu: kekuatan pertahanan militer (meliputi komponen utama, cadangan, dan pendukung), maupun kekuatan pertahanan nirmiliter (meliputi unsur-unsur utama dan unsur-unsur lain kekuatan bangsa).

Indonesia telah memanfaatkan perkembangan dan kemajuan TIK di berbagai bidang (sektor) kehidupan, baik sektor pemerintah, swasta, dan masyarakat. Seluruh infrastruktur TIK (*cyberspace*) yang ada pada sektor-sektor tersebut merupakan wujud sumber daya milik nasional yang meliputi sumber daya manusia (SDM), sarana prasarana, maupun infrastruktur TIK (*cyberspace*) sebagai sumber daya buatan (SDB). Terhadap ancaman baru berdimensi teknologi, maka mutlak dihadapi oleh seluruh komponen kekuatan hanneg, dalam hal ini segenap sumber daya nasional meliputi

orang (*people*), proses (*process*), dan teknologi (*technology*) dengan kapasitas dan kapabilitas dalam bidang TIK (*cyberspace*).

Saat ini sumber daya nasional bidang TIK di Indonesia sudah mulai ada dan dibangun sejak lebih dari satu dekade, dan seluruhya tersebar di berbagai komponen bangsa (termasuk bidang pemerintahan). Untuk membangun kepentingan nasional di ranah siber, maka tahun 2017 dibentuklah Badan Siber dan Sandi Negara (BSSN) berdasarkan Peraturan Presiden (Perpres) Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) yang selanjutnya disempurnakan melalui Perpres Nomor 133 tahun 2017 tentang Perubahan atas Perpres Nomor 53 tahun 2017 pada tanggal 16 Desember 2017. BSSN bertanggung jawab dalam bidang keamanan siber nasional dengan fungsi penentuan kebijakan keamanan siber melalui peran kerjasama antar sektor pemerintah, swasta, dan masyarakat. Sebagai lembaga pemerintah, BSSN turut mengemban tanggung jawab dalam hal penyiapan dan pengelolaan keamanan siber nasional meliputi faktor-faktor: *people*, *process*, dan *technology*, dalam suatu Strategi Keamanan Siber Nasional (SKSN).

Eksistensi SKSN sangat penting dan strategis, khususnya tehadap upaya membangun kapasitas dan kapabilitas sishankamrata melalui terwujudnya keamanan dan pertahanan siber secara nasional. Untuk membangun kemampuan pertahanan siber dalam kerangka kerja sishankamrata (aspek strategi perang semesta), harus dipersiapkan secara dini oleh pemerintah melalui mekanisme PSDN untuk hanneg. Bila dihadapkan kepada ancaman baru era digital (ancaman siber), maka kerangka kerja operasional SKSN maupun sishankamrata, keduanya memiliki faktor-faktor maupun prinsip-prinsip yang relatif sama, meski terdapat sedikit perbedaan dalam hal nomenklatur maupun teknis penyelenggaraannya, di mana dalam perspekstif SKSN nomenklaturnya disebut sebagai keamanan siber, sedangkan dalam perspektif

sishankamrata (hanneg) nomenklaturnya disebut sebagai pertahanan siber. Terlepas dari hal tersebut, keberhasilan dalam membangun kemampuan pertahanan siber untuk kepentingan sishankamrata (aspek strategi perang semesta), selain membutuhkan sumber daya bidang TIK nasional maupun SDM yang memiliki kompetensi (*knowledge* dan *skill* serta kapsitas dan kapabilitas yang profesional, terlatih, berkompetensi, dan berkualifikasi) dalam bidang pertahanan siber, juga akan bergantung kepada eksistensi SKSN. Dengan kata lain eksistensi SKSN sangat mempengaruhi keberhasilan strategi perang semesta dalam menghadapi bentuk ancaman baru berdimensi teknologi (ancaman siber).

Pada kenyataannya masih terdapat tantangan dan/atau permasalahan dalam hal bagaimana sumber daya TIK nasional ditata kelola (manajemen) sekaligus didudukkan sebagai suatu hal yang penting bagi kepentingan sishankamrata. Upaya membangun kemampuan baru hanneg untuk menghadapi ancaman siber, masih menjadi tantangan dan/atau masalah, dan dari berbagai perspektif maupun faktor menunjukkan bahwa Indonesia belum sepenuhnya siap/mampu menangani ancaman siber. Membangun kemampuan baru hanneg bidang pertahanan siber, sangat bergantung kepada bagaimana keberhasilan tata kelola penyiapan seluruh komponen hanneg dalam sishankamrata yang meliputi SDM, wilayah, sarana prasarana dan sumber daya nasional lainnya, yang satu sama lain tidak mungkin terpisahkan. Meski demikian, dengan tidak bermaksud mengesampingkan pentingnya untuk menganalisa aspek fungsi dasar manajemen SKSN terhadap segenap elemen dalam sishankamrata tersebut, maka dalam penelitian ini, analisis hanya fokus pada aspek SDM, dengan pertimbangan: a) SDM merupakan pilar pertama dan paling utama dari tiga pilar keamanan siber, yaitu *people* (misal: pendidikan, latihan, kompetensi, kualifikasi, *skill* dan sebagainya), selanjutnya pilar *process* (misal: organisasi, doktrin, kebijakan dan sebagainya), dan pilar *technology* (seluruh infrastruktur informasi kritikal, dan dengan catatan bahwa teknologi

tidak mungkin terselenggara tanpa pilar *people* dan *process*); b) masih rendahnya kompetensi SDM Indonesia, baik dalam bidang TIK, keamanan siber, dan pertahanan siber (*knowledge*, *skill*, profesional, terdidik, terlatih, berkompetensi, dan berkualifikasi); dan c) penelitian ini akan menjadi awal dari penelitian-peneitian serupa berikutnya dengan fokus pada faktor/aspek lain komponen sishankamrata dalam kerangka pembangunan kemampuan pertahanan siber.

Lalu apakah konsep SKSN hasil rumusan BSSN mampu mendukung upaya terwujudnya kompetensi SDM pertahanan siber guna mendukung kepentingan kerangka kerja sishankamrata (peningkatan kompetensi SDM keamanan siber sebagai komponen kekuatan hanneg yang diproyeksikan untuk tujuan perang semesta) ? Dari hal-hal tersebut (secara deduktif), peneliti melakukan penelitian tentang urgensi SKSN dalam mendukung sishankamrata, dengan fokus pada analisis fungsi dasar manajemen terhadap upaya terwujudnya kompetensi SDM pertahanan siber.

1.2 Rumusan Masalah.

Pada bagian ini, sebagai fokus penelitian adalah: “Bagaimana eksistensi SKSN menjadi urgensi terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata ?”. Sedangkan sub fokus penelitian, sebagai berikut:

1.2.1 Bagaimana peran dan fungsi SKSN terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata ?

1.2.2 Faktor-faktor apa saja yang mendukung dan menghambat SKSN terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata ?

1.2.3 Bagaimana praktik-praktik keamanan siber yang aplikatif sesuai konsep SKSN yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata ?

1.3 Tujuan Penelitian.

1.3.1 Menganalisis implementasi peran dan fungsi SKSN terhadap upaya membangun SDM pertahanan siber untuk kepentingan sishankamrata. Yang dimaksud adalah signifikansi eksistensi peran dan fungsi SKSN Indonesia melalui misalnya ketersediaan *roadmap* atau program pembangunan SDM TIK nasional yang pengelolaannya mendukung upaya terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

1.3.2 Menganalisis faktor-faktor yang mendukung dan menghambat pengelolaan SDM keamanan siber dalam SKSN terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

1.3.3 Menganalisis wujud praktik-praktik keamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN) yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

1.4 Manfaat Penelitian.

1.4.1 Manfaat Teoritik. Hasil penelitian dapat dimanfaatkan pada studi pengembangan keilmuan sosial di bidang pertahanan, sub bidang strategi pertahanan berkenaan dengan tantangan dan ancaman baru di era digital. Dalam hal tersebut, khususnya demi terwujudnya kompetensi SDM pertahanan siber yang ditunjang eksistensi kerangka kerja SKSN dalam hal

pengelolaan SDM keamanan siber nasional, untuk kepentingan sishankamrata.

1.4.2 Manfaat Praktis. Hasil penelitian dapat dimanfaatkan pihak-pihak terkait dalam mendorong aktualisasi SKSN di Indonesia dalam mendukung sishankamrata, khususnya terhadap upaya membangun (terwujudnya) kompetensi SDM pertahanan siber sebagai bagian dari komponen kekuatan hanneg yang diproyeksikan dalam perang semesta.

BAB 2
TINJAUAN PUSTAKA

Menurut Creswell (2013:40), tinjauan pustaka memiliki tujuan untuk memberi informasi pada pembaca mengenai hasil-hasil penelitian lain yang erat kaitannya dengan penelitian yang sedang dilakukan, mengaitkan penelitian dengan berbagai literatur, serta mengisi bagian-bagian (celah-celah) dalam penelitian sebelumnya (Cooper, 1984; Marshal dan Rossman, 2006). Pada bagian ini, peneliti mencantumkan referensi dan konten yang berisikan uraian penting dari berbagai konsep, teori, ketentuan/aturan hukum, standar-standar baku, dan doktrin maupun pandangan-pandangan para pakar/ahli dari berbagai kalangan yang relevan dan berpengaruh, agar dalam proses kegiatan penelitian ini lebih memperoleh klarifikasi–klarifikasi secara ilmiah sekaligus justifikasi (pembenaran) berdasarkan referensi teoritis, konseptual, dan ketentuan hukum yang berlaku.

2.1 Landasan Teori.

Menurut Moleong (2014:14), berpandangan bahwa teori dalam penelitian kualitatif dibatasi pada pengertian: suatu pernyataan sistematis berkaitan erat dengan seperangkat proposisi dari data yang diuji secara empiris. Lebih jauh Moleong menyatakan bahwa dalam uraian dasar teori (Bogdan & Biklen, 1982) digunaka istilah paradigma, yang diartikan sebagai kumpulan longgar tentang asumsi logis yang dianut bersama, konsep, atau proposisi yang memandu cara berpikir dan cara penelitian.

Menurut William Wiersma (1986) tentang teori bahwa: "*A theory is a generalization or series of generalization by which we attempt to explain some phenomena in a systematic manner*". Teori adalah generalisasi atau kumpulan generalisasi yang dapat digunakan untuk menjelaskan berbagai fenomena secara sisternatik. Bahwa setiap penelitian senantiasa

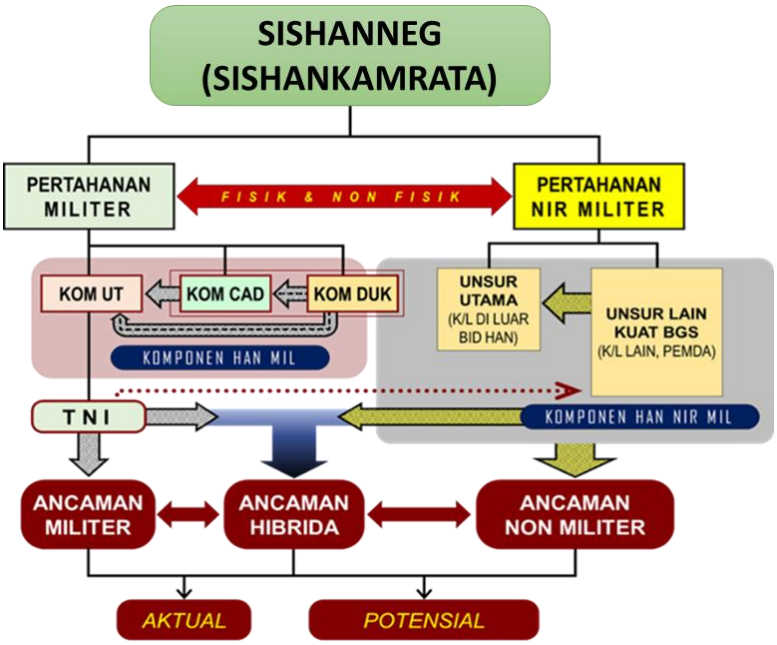
menggunakan teori, hal tersebut sebagaimana diutarakan Neuman (2003) yang menyatakan bahwa "*Researchers use theory differently in various types of research, but some type of theory is present in most social research*". Selain itu Kerlinger (1978) juga rnengernukakan bahwa "*Theory is a set of interrelated construct (concepts), definitions. and proposition that present a systematic view a phenomena by specifying relations among variables, with purpose of explaining and predicting the phenomena*"; bahwa teori adalah seperangkat konstruk (konsep), definisi, dan proposisi yang berfungsi untuk melihat fenornena secara sistematik, melalui spesifikasi hubungan antar variabel, sehingga berguna untuk menjelaskan dan meramalkan fenomena.

2.1.1 Teori Pertahanan Negara (Hanneg).

Hanneg menurut UU RI Nomor 3 tahun 2002 merupakan fungsi pemerintah sekaligus usaha mewujudkan satu kesatuan hanneg untuk tercapainya tujuan nasional (melindungi segenap bangsa dan seluruh tumpah darah, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia berdasarkan kemerdekaan, perdamaian, dan keadilan sosial). Pada pasal 1 juga dinyatakan bahwa hanneg diselenggarakan untuk mempertahankan kedaulatan, keutuhan wilayah, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Uraian tersebut di atas dapat diasumsikan sebagai suatu konsep teori hanneg yang dianut Indonesia.

Usaha hanneg ditempuh melalui upaya-upaya pembangunan, pemeliharaan, pengembangan, dan penggunaan kekuatan hanneg menurut prinsip demokrasi, hak asasi manusia (HAM), kesejahteraan, lingkungan hidup, hukum nasional dan internasional serta kebiasaan internasional, dan hidup berdampingan secara damai. Warga negara

dilibatkan dalam hanneg sesuai peran dan fungsi maupun hak dan kewajibannya melalui upaya bela negara sebagai aktualisasi rasa cinta tanah air yang berorientasi pada cita-cita demi mewujudkan kepentingan nasional.



Gambar 2.1 Diagram Sistem Pertahanan Negara

Sumber: diolah peneliti

Fungsi hanneg adalah terwujudnya pertahanan wilayah NKRI sebagai satu kesatuan pertahanan meliputi fungsi-fungsi penangkalan, penindakan, dan pemulihan (kaldaklih). Penangkalan merupakan usaha segenap kekuatan nasional dengan efek psikologis guna cegah dan tiadakan setiap ancaman dari luar dan dalam negeri, fisik dan nonfisik, melalui upaya kemampuan terintegrasi sesuai fungsi hanneg. Fungsi penindakan, adalah wujud pengerahan kekuatan pertahanan dalam rangka menghadapi berbagai bentuk ancaman sesuai mekanisme sishankamrata (dapat disebut juga sebagai wujud strategi perang semesta). Di dalam menghadapi ancaman militer, melalui pengerahan kekuatan militer

(perang), sedangkan menghadapi ancaman nonmiliter, melalui pengerahan kekuatan nirmiliter. Fungsi Pemulihan, adalah usaha hanneg yang dilaksanakan oleh kekuatan militer dan nirmiliter secara terintegrasi guna memulihkan kembali situasi dan kondisi keamanan yang terganggu akibat perang, pemberontakan (separatis), konflik vertikal/ horizontal, kerusuhan, teroris, bencana atau diakibatkan oleh ancaman nonmiliter lain.

Kesemestaan dalam sishankamrata bersifat strategis karena menempatkan warga negara Indonesia sebagai subyek penting hanneg sesuai peran masing-masing (Doktrin Hanneg, 2015). Kesemestaan juga dimaknai sebagai satu kesatuan pertahanan menyeluruh oleh integrasi dua sumber daya kekuatan pertahanan, yaitu militer dan nirmiliter, sehingga kekuatan dan kemampuan hanneg Indonesia lebih kuat, disegani, dan berdaya tangkal tinggi. Jelaslah bahwa proyeksi wujud aktualisasi kesemestaan adalah perang semesta, sebagai mandala sekaligus palagan peperangan dan pertempuran total menghadapi segala bentuk ancaman. Dalam sishankamrata, terdapat sumber daya hanneg yaitu komponen pendukung dan komponen cadangan yang berperan mendukung efektiitas dan efisiensi pelaksanaan tugas-tugas kekuatan militer maupun nirmiliter. Keduanya merupakan sumber daya nasional yang ditranformasikan melalui upaya pengelolaan sumber daya nasional untuk hanneg (UU Nomor 23 tahun 2019).

Pada dokumen kebijakan hanneg tahun 2020 (Keputusan Menhan Nomor: Kep/104/M/I/2020 tanggal 20 Januari 2020), hanneg diselenggarakan pemerintah yang dipersiapkan secara dini dalam sishankamrata melalui usaha pengelolaan sumber daya nasional yang meliputi segenap SDM, SDA, SDB, serta sarana prasarana nasional, di segenap wilayah NKRI sebagai satu kesatuan pertahanan dalam menanggulangi ancaman. PSDN untuk hanneg telah diundangkan dalam UU Nomor 23 tahun 2019. Hal tersebut turut memperkuat eksistensi bahwa

sumber daya nasional bidang TIK (*cyberspace*) yang ada di sektor-sektor strategis nasonal yang juga tersusun oleh pilar-pilar keamanan siber, yaitu: *people*, *process*, dan *technology*, berikut kapasitas dan kapabilitas bidang keamanan siber, merupakan komponen sumber daya nasional yang akan dikelola dan ditransformasikan dalam mendukung sishankamrata (konteks perang semesta) untuk menghadapi berbagai acaman baru di era digital.

2.1.2 Teori Strategi.

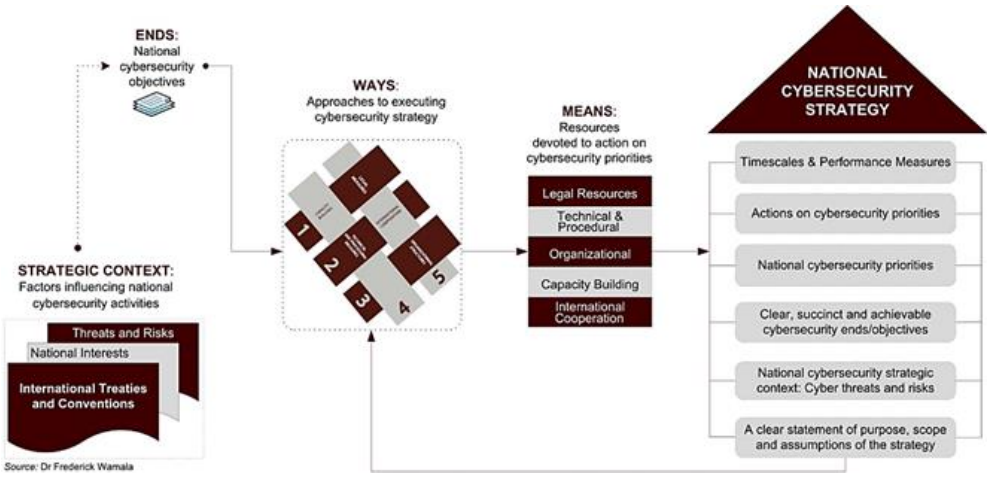
Strategi penting dalam suatu organisasi dan/atau siapapun untuk bagaimana agar sasaran/tujuan tercapai efektif dan efisien memanfaatkan segenap sumber daya yang ada. Strategi yang baik, terencana, dan diperhitungkan, maka segala ancaman, gangguan, hambatan, dan tantangan di dalam setiap upaya pencapaian sasaran dan tujuan, mampu tertangani dan tersolusikan dengan baik. Teori strategi banyak digunakan dan diterapkan dalam bidang-bidang militer (pertahanan), keamanan, pemerintahan, dan bisnis.

Kolonel Arthur F. Lykke (1997), merumuskan teori strategi sebagai "… *that strategy at any level consists of ends or objectives, ways or concepts, and means or resources…*", bahwa suatu strategi pada tingkat manapun, adalah penjabaran dari tujuan/sasaran (*ends*) yang ingin dicapai, cara/konsep (*ways*) yang digunakan mencapai tujuan, serta sarana prasarana maupun sumberdaya (*means*) yang digunakan untuk mencapai tujuan. Lykke membagi elemen-elemen dalam suatu formulasi strategi sebagai *ends*, *means*, dan *ways* yang kemudian dirumuskan atau diformulasikan sebagai "*Strategi = E + W + M"*. Sebenarnya Arthur F. Lykke mengadopsi formulasi tersebut dari Jenderal Maxwell D. Taylor (*US Joint Chief of Staff*) saat berkunjung ke US *Army War College* pada tahun 1981 yang juga menyatakan bahwa strategi sebagai suatu bentuk seni dan ilmu dalam mempekerjakan angkatan bersenjata suatu negara untuk

mengamankan tujuan kebijakan nasional dengan menerapkan kekuatan atau ancaman dari kekuatan. Jenderal Maxwell D. Taylor menandai bahwa strategi terdiri dari tujuan, cara, dan sarana. Ia mengekspresikan konsep tersebut sebagai sebagai sebuah persamaan, yaitu: STRATEGI sama dengan TUJUAN (tujuan yang ingin dicapai) ditambah CARA (tindakan) ditambah SARANA (instrumen yang dengannya beberapa tujuan dapat dicapai). Konsep umum ini dapat digunakan sebagai dasar untuk perumusan segala jenis srategi militer, politik, ekonomi, dan sebagainya (termasuk tentunya aspek keamanan), tergantung pada elemen kekuatan nasional yang digunakan.

Teori strategi dalam kaitannya dengan hanneg di Indonesia, merujuk pada Buku Putih Pertahanan Indonesia (BPPI) tahun 2015, meliputi “apa yang dipertahankan (*ends* atau tujuan dan sasaran), bagaimana cara mempertahankan (*ways* atau cara mencapai sasaran), serta dengan apa mempertahankan (*means* atau sumber daya yang digunakan)”. Dalam konteks topik penelitian, serta merujuk pada kebijakan hanneg tahun 2020, terdapat 4 (empat) sasaran strategis hanneg yang ingin dicapai, yaitu: a) terjaga kedaulatan dan keutuhan Wilayah NKRI, serta terlindunginya keselamatan bangsa dari berbagai ancaman; b) terbangunnya sishankamrata secara terintegrasi dan modern; c) terwujudnya PSDN untuk hanneg; serta d) terselenggaranya pengelolaan wilayah pertahanan.

Teori strategi dalam konteks strategi keamanan siber, bahwa sampai saat ini di Indonesia belum secara spesifik menentukan SKSN, namun demikian telah ada ketentuan maupun konsep (rumusan) yang mungkin dapat diasumsikan relevan sebagai suatu SKSN, yaitu: *pertama*: Model SKSN Rumusan *International Telecommunication Union* (ITU); *kedua*: Konsep SKSN menurut PP No.71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE); dan *ketiga*: Konsep SKSN 2020-2024 rumusan BSSN.



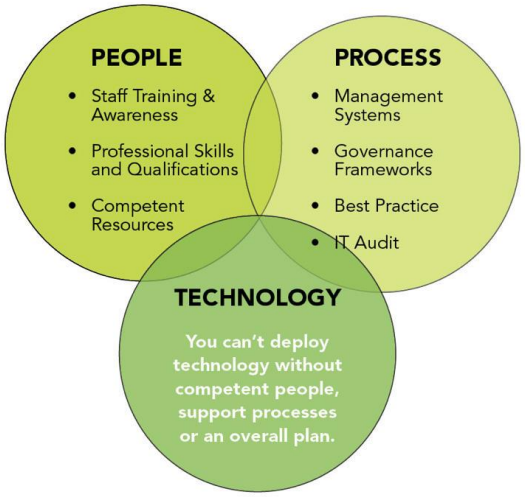
Gambar 2.2 *National Cybersecurity Strategy Model*

Sumber: *ITU National Cybersecurity Strategy Guide* (2011, p.35)

Dalam konteks global, *International Telecommunication Union* (ITU) telah menyusun model SKSN. ITU telah menerbitkan panduan tentang *National Cybersecurity Strategy Guide* di tahun 2011. Di era digital saat ini, panduan tersebut jadi acuan di berbagai negara di dunia dalam merancang SKSN yang baru, yang ada, maupun meningkatkan yang sudah ada, agar kemudian mampu mendukung kepentingan nasionalnya melalui konsep strategi keamanan siber yang handal sekaligus mampu kolaboratif secara global. ITU juga menempatkan kerangka kerja internasional *Global Security Agenda* (GCA) sebagai jantung utama pada model SKSN yang dirancang sesuai paradigma strategi *Ends-Ways-Means*.

Model pada gambar 2.2, merupakan kombinasi vital yang mengedepankan kolaborasi antara pakar strategi keamanan siber dengan para pemangku kepentingan siber yang bertanggung jawab atas kebijakan nasional. Model tersebut menunjukan konteks strategis yang terdapat dalam rumusan SKSN, sebagai faktor-faktor yang mempengaruhi aktivitas keamanan siber nasional, seperti adanya ancaman dan risiko, serta kepentingan nasional, maupun adanya kesepakatan dan konvensi-

konvensi internasional. Untuk aspek *ends* (*national cybersecurity objectives*) adalah sasaran atau tujuan keamanan siber nasional yang relevan dengan kepentingan tujuan nasional. Untuk aspek *ways* (*approaches to executing cybersecurity strategy*) atau pendekatan strategi keamanan siber, merujuk pada kerangka kerja internasional GCA yang meliputi 5 (lima) pilar strategis, yaitu: *legal measures* (tindakan legal), *technical and procedural measures* (tindakan teknis dan prosedural), *organizational structures* (struktur organisasi), *capacity building* (pengembangan kapasitas), dan *international cooperation* (kerjasama internasional). Sedangkan untuk aspek *means* (*resources devoted to action on cybersecurity priorities*), dalam hal ini merupakan sumber daya yang ditujukan untuk tindakan pada prioritas keamanan siber, meliputi: *legal resources* (sumber daya hukum), *technical and procedural* (teknis dan prosedural), organizational (organisasi), *capacity building* (pengembangan kapasitas), dan *international cooperation* (kerjasama internasional). Sehingga rumusan *ends+ways+means* tersebut diperoleh konsep model SKSN yang relevan.



Gambar 2.3 *The Pillars* of *Cybersecurity*

Sumber: *vulpoint.com* / Jean Sebastian Opdebeeck (2018)

Dalam PP No.71/2019 tentang PSTE, konsep SKSN tidak dijabarkan secara spesifik, namun bila mencermati klausul-klausul yang ada, secara implisit hanya mencakup pengaturan tentang aspek keamanan informasi sebagai kewajiban bagi penyelenggara sistem elektronik maupun sebagai peran dari pemerintah. Hal tersebut diperkuat oleh Permenkominfo RI No.4/2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI) yang mengatur kewajiban bagi penyelenggara sistem elekronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko, sehingga secara fundamental, kewajiban tentang keamanan informasi telah sudah memenuhi syarat maupun prinsip-prinsip keamanan siber yang dibangun oleh 3 (tiga) pilar, yaitu: *people* (manusia), *process* (proses), *technology* (teknologi).

Dalam PP No.71/2019 tersebut, yang dimaksud dengan keamanan informasi sebagai peran pemerintah, meliputi: pengaturan standar keamanan informasi, perlindungan infrastruktur informasi kritikal (vital), pengaturan manajemen risiko, pengaturan SDM dalam penyelenggaraan perlindungan sistem elektronik, dan lain sebagainya. Bila dikaitkan dengan SKSN, maka secara implisit pada Pasal 94 ayat (1) menyebutkan “peran pemerintah untuk melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum sebagaimana dimaksud dalam pasal 90 huruf b”, peran pemerintah tersebut kemudian dipertegas pada huruf a, yaitu “penetapan strategi keamanan siber nasional yang merupakan bagian dari strategi keamanan nasional, termasuk pembangunan budaya keamanan siber”.

Sejalan dengan mandat Pasal 94 Ayat (1) huruf a PP No.71/2019 tentang PSTE, lembaga BSSN (dalam konteks pemerintah) telah menyampaikan suatu Pengantar Strategi Keamanan Siber Indonesia (SKSI) pada laman (halaman muka) *website* resmi BSSN. Di dalam

pengantar tersebut tercantum visi SKSI yaitu: “Membangun dan Menjaga Keamanan Siber Nasional dengan Mensinergikan Berbagai Pemangku Kepentingan Untuk Ikut Serta Mewujudkan Keamanan Nasional dan Meningkatkan Pertumbuhan Ekonomi Nasional”, serta 5 (lima) sasaran atau tujuan strategis SKSI, yaitu: tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber, dan keamanan siber pada ekonomi digital. Rangkaian kalimat terakhir dalam pengantar ini sepertinya merupakan aspek *ends*, sementara untuk aspek *ways* dan *means* tidak secara eksplisit dicantumkan.

BSSN juga telah menyusun konsep SKSN 2020-2024 yang rumusannya merujuk pada konsep SKSN model ITU, (catatan: konsep telah menjadi terbitan internal BSSN, namun belum dipublikasikan), sebagai berikut: a) parameter *ends* dalam rumusan ini sepertinya mengadopsi ketentuan pasal 94 ayat (1) huruf a PP No.71/2019 tentang PSTE, sehingga yang menjadi sasaran atau tujuan SKSN ini “untuk melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum”; b) parameter *means* dalam rumusan ini adalah mengadopsi *means* SKSN model ITU, dalam hal ini 5 (lima) kategori sumber daya, yaitu: hukum, teknis dan prosedural, organisasi, pembangunan kapasitas, dan kerjasama internasional; dan c) parameter *ways* dalam rumusan ini adalah pilar-pilar SKSN (lima pilar), yaitu: *pilar kesatu*, Ketahanan Siber Indonesia (*Cyber Resilience*); *pilar kedua*: Kepastian Hukum Ruang Siber (*Cyberspace Law Harmonization and Enforcement*); *pilar ketiga*: Kemampuan Teknologi siber (*Cyber Technology Capacity*); *pilar keempat*: Dukungan Pertumbuhan Ekonomi Digital (*Digital Economy Growth Support*); *pilar kelima*: Kerjasama Internasional dan Nasional (*International and National Engagement*).

Tampak jelas bahwa SKSN diproyeksikan sebagai konsep strategi nasional bidang keamanan siber guna melindungi kepentingan nasional

dari ancaman siber melalui upaya-upaya tertentu (sebagai contoh: upaya terwujudnya kelembagaan, upaya operasional pertahanan/keamanan/ ketahanan siber maupun upaya operasional kontijensi keamanan siber nasional, upaya terwujudnya berbagai lembaga diklat kompetensi SDM bidang TIK dan keamanan siber, dsb), serta menggunakan seluruh sarana prasarana serta segenap sumber daya yang ada. Dengan demikian tujuan SKSN juga menjadi tujuan sishankamrata, dan oleh karena itu juga, maka dinamika aspek-aspek operasional dalam SKSN (dalam hal ini operasi keamanan siber), tentulah akan selaras dengan dinamika aspek-aspek operasional dalam sishankamrata (dinamika operasi pertahanan siber sebagai bagian dari strategi perang semesta guna menghadapi ancaman berdimensi teknologi). Kedua aspek strategis, baik SKSN maupun Strategi Perang Semesta tersebut, memiliki faktor-faktor yang saling terkorelasi erat, sehingga eksistensi SKSN menjadi sesuatu yang urgensi bagi kepentingan sishankamrata.

2.1.3 Teori Manajemen.

Hasibuan, 2000 (Torang, 2013:165) berpandangan bahwa manajemen merupakan ilmu sekaligus seni dalam mengatur proses pemanfaatan SDM dan sumber-sumber lain secara efektif efesien guna mencapai tujuan tertentu. Sejalan hal tersebut, Miller (Torang, 2013:166) berpandangan manajemen sebagai proses untuk memimpin sekaligus memperlancar kegiatan SDM yang terorganisir dalam kelompok untuk mencapai tujuannya.

George R. Terry berpandangan bahwa manajemen adalah pencapaian dari berbagai tujuan yang sudah ditetapkan melalui/bersama-sama usaha orang lain. Manajemen penting terhadap setiap aktivitas dalam mencapai tujuan. Manajemen berorientasi pada proses yang memerlukan SDM, *knowledge* dan *skill* supaya aktivitas tindakan lebih efektif dalam

pencapaian hasil. Organisasi akan gagal bila mengabaikan fungsi manajemen. Peneliti bepandangan bahwa manajemen atau tata kelola, merupakan ilmu untuk mengatur proses kegiatan dalam rangka mencapai tujuan sesuai rencana. George R. Terry membagi manajemen ke dalam empat fungsi dasar (*four principles of management*), yaitu: *Planning* (Perencanaan), *Organizing* (Pengorganisasian), *Actuating* (Pelaksanaan) dan *Controlling* (Pengendalian), atau keseluruhannya disingkat POAC.

Fungsi perencanaan, adalah proses fungsi dasar manajemen dalam rangka menetapkan tujuan dan langkah-langkah yang harus dilakukan agar tercapai tujuan. Aspek perencanaan berfungsi memberikan informasi dalam koordinasi seluruh pekerjaan secara efektif dan akurat. Perencanaan yang baik mutlak berdasarkan sasaran, sederhana, punya standar dan fleksibel, seimbang memanfaatkan segala sumber daya yang dimiliki.

Fungsi pengorganisasian, merupakan fungsi penataan berbagai kegiatan yang dibutuhkan guna mencapai target, termasuk ddalamnya adalah menempatkan SDM dalam kegiatan, penyiapan sarana prasarana yang sesuai untuk keperluan kerja, serta pendelegasian wewenang pada setiap orang sesuai bidang pelaksana kegiatan. Dari ha tersebut, maka muncul beberapa azas pengorganisasian, yaitu: tujuan, pembagian kerja, penempatan tenaga kerja, wewenang dan tanggung jawab, dan pelimpahan wewenang.

Fungsi pelaksanaan merupakan usaha atau ikhtiar dalam mengaktualisasikan atau menjalankan kegiatan yang telah direncanakan dan diorganisasikan sehingga tercapai tujuan sebagaimana telah ditetapkan. Agar fungsi pelaksanaan mampu berjalan dengan baik, maka dibutuhkan *leadership* yang baik yang didukung juga oleh peran serta aktif seluruh SDM dalam organisasinya. Beberapa faktor penting dalam fungsi

pelaksanaan adalah: *kepemimpinan,* sikap dan moril, komunikasi, insentif*,* supervisi, serta disiplin.

Fungsi pengawasan atau pengedalian merupakan salah satu fungsi dasar dalam manajemen untuk mengawasi apakah dinamika kegiatan dari organisasi sudah/tidak sesuai dengan rencana. Selain itu juga untuk mengawasi penggunaan segala sumber daya organisasi mampu terpakai efektif dan efisien tanpa menyimpang dari rencana. Proses pengawasan meliputi: menentukan standar pengawasa, ukuran pelaksanaan, bandingkan pelaksanaan dengan standar, cari dan temukan bila terdapat perbedaan, dan perbaiki penyimpangan.

Dalam penelitian ini, teori manajemen dari George R. Terry (fungsi dasar manajemen POAC) dimanfaatkan peneliti sebagai alat bantu analisis data-data terkait bagaimana peningkatan kompetensi SDM TIK nasional menjadi SDM keamanan siber dan SDM pertahanan siber, yang kemudian dapat dimanfaatkan untuk kepentingan sishankamrata. Dengan kata lain hal tersebut fokus pada bagaimana tata kelola peningkatan kompetensi SDM keamanan siber (menurut konsep SKSN hasil rumusan BSSN) mampu mendukung upaya bidang pertahanan dalam mewujudkan kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Tentu dinamika pengelolaan dalam membangun kompetensi SDM terdapat faktor-faktor yang mendukung maupun menghambat, dan peneliti meyakini adanya afiliasi (hubungan) dalam hal tata kelola peningkatan kompetensi SDM pertahanan siber yang *intake*-nya bersumber dari *output* dan *outcome* hasil pengelolaan SDM TIK maupun SDM keamanan siber nasional. Peneliti juga kemudian meyakini bahwa upaya mewujudkan kompetensi SDM pertahanan siber akan bergantung pada pengelolaan SDM keamanan siber dalam konsep SKSN.

2.2 Landasan Konseptual.

Pada bagian ini diuraikan tentang pengertian, konsep, dan aturan/hukum yang relevan guna memahami kompleksitas topik meliputi: pengertian urgensi, keamanan, dan ancaman.

2.2.1 Pengertian Urgensi.

Tidak mudah menemukan pengertian urgensi yang bersumber dari para ahli. Namun demikian, kata urgensi apabila ditinjau dari bahasa latin yaitu "*urgere*" sebagai kata kerja yang mempunyai arti "mendorong", bila ditinjau dari bahasa Inggris (bersumber dari *Oxford Learner's Dictionaries*) *online* yaitu "*urgent*" sebagai kata sifat (*adjective*) bermakna sebagai sesuatu yang perlu ditangani atau terjadi segera (sinonim: menekan), dan dalam Kamus Besar Bahasa Indonesia (KBBI) *online* yaitu "urgensi" sebagai kata benda (nomina) yang bermakna keharusan yang mendesak; hal sangat penting. Kata Urgensi terbentuk dari kata dasar "urgen" yang diberi akhiran "i" sehingga bermakna sebagai sesuatu hal yang menjadi bagian yang paling utama atau unsur yang penting. Dengan demikian, dalam penelitian ini, penggunaan kata urgensi dapat dimaknai/dimengerti sebagai sesuatu yang merujuk kepada hal-hal yang bersifat mendorong sekaligus memaksa terhadap sesuatu yang penting untuk diselesaikan atau ditindaklanjuti. Sehingga terhadap topik dan masalah dalam penelitian ini, peneliti berpendapat bahwa konsep SKSN sebagai sesuatu hal yang penting dan mendesak untuk segera diselesaikan atau ditindaklanjuti.

2.2.2 Keamanan (*Security*).

Secara etimologis, konseptual keamanan atau *security* bersumber dari bahasa latin "*securus: (se+cura)*" bermakna bebas dari bahaya, bebas dari rasa takut (*free from danger*, *free from fear*). Sedangkan menurut KBBI

online, didefinisikan sebagai situasi aman tenteram. Dari *wikipedia*, didefinisikan sebagai situasi bebas bahaya. Definisi tersebut dapat dipergunakan dalam hubungannya dengan bentuk-bentuk kejahatan, musibah, dan lain sebagainya. Keamanan menjadi topik luas termasuk keamananan nasional dari ancaman terorisme, keamanan komputer dari *hacker* atau *cracker*, keamanan rumah dari pencuri maupun penyusup, keamanan finansial dari krisi ekonomi, serta banyak lainnya. Berbagai konteks bidang keamanan yang relevan untuk diuraikan meliputi, antara lain: keamanan nasional, keamanan dalam negeri, keamanan siber, keamanan siber nasional (*national cyber security*), keamanan informasi, dan keamanan siber dalam konteks/perspektif hanneg.

Keamanan dalam konteks Keamanan Nasional, merujuk pada *draft* RUU Keamanan Nasional (hasil rapat tanggal 16 Oktober 2012), merupakan kondisi dinamis bangsa dan NKRI yang menjamin keselamatan, kedamaian, dan kesejahteraan warga negara, masyarakat, dan bangsa, terlindunginya kedaulatan dan keutuhan wilayah negara, serta keberlangsungan pembangunan nasional dari segala ancaman; sedangkan untuk Keamanan Dalam Negeri, sebagaimana merujuk pada UU RI No.2/2002, terbagi menjadi dua, yaitu kamtibmas dan kamdagri.

Keamanan dalam konteks Keamanan Siber (*Cybersecurity*), merujuk pada dokumen *International Telecomunication Union* (ITU) berkode ITU-T X.1205 tentang *Overview of Cybersecurity*, disebutkan: "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.*

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity (which may include authenticity and non-repudiation), Confidentiality". Bahwa keamanan siber adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi aset pemangku kepentingan siber. Aset organisasi dan pengguna, termasuk perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan segenap informasi yang ditransaksi dalam lingkungan siber. Keamanan siber berupaya memastikan terwujudnya pemeliharaan keamanan aset organisasi dan properti pengguna dari risiko keamanan siber. Secara umum, tujuan keamanan siber mencakup: ketersediaan, integritas, dan kerahasiaan.

Keamanan dalam konteks Keamanan Informasi, sebagaimana merujuk pada Permenkominfo RI No.4/2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI), yang dimaknai sebagai terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi. Di lain pihak, keamanan siber dalam konteks (perspektif) hanneg, adalah sebagaimana merujuk pada Permenhan RI No.82/2014 tentang Pedoman Pertahanan Siber, yang definisinya adalah segala upaya dalam rangka terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi (berikut sarana prasarana pendukung di tingkat nasional) secara lintas sektor. Keamanan siber dalam komteks hanneg dinyatakan sebagai Pertahanan Siber (*cyber defense*) yang kemudian dapat dimaknai sebagai upaya penanggulangan ancaman serangan siber yang mengganggu penyelenggaraan hanneg. Dari hal tersebut, apabila pengertian/pemahaman tentang keamanan siber dan keamanan informasi disederhanakan, menjadi sebagai berikut: a) keamanan siber adalah penggunaan berbagai teknologi dan proses untuk

melindungi *networking*, komputer, program, maupun data dari serangan, kerusakan, atau akses tidak sah; dan b) keamanan informasi adalah melindungi informasi dari akses, penggunaan, gangguan, modifikasi, atau perusakan tanpa izin tanpa memandang bagaimana informasi itu disimpan secara elektronik atau fisik. Bagaimana dengan pertahanan siber ? Apakah ada kaitannya dengan keamanan siber ? Bila merujuk pada artikel *online* Direktorat Jenderal Aplikasi dan Informatika (Ditjen Aptika) Kemenkominfo (2016), disebutkan bahwa keamanan siber maupun pertahanan siber memiliki setidaknya satu keterkaitan erat, yaitu bahwa keduanya diterapkan untuk menjaga dan mempertahankan *confidentiality*, *integrity*, dan *availability* informasi elektronik atau sistem elektronik. Di satu sisi, keamanan siber dapat berupa salah satu bentuk dari pertahanan siber. Di sisi lain, pertahanan siber dapat berupa pertahanan aktif maupun pertahanan pasif. Pertahanan pasif dapat tercakup dalam ruang lingkup keamanan siber. Keamanan siber maupun pertahanan siber dapat diselenggarakan baik secara individu, kolektif, maupun oleh negara (pemerintah), tergantung ruang lingkupnya masing-masing. Keamanan siber maupun pertahanan siber oleh negara adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi penting bagi negara, keamanan nasional, maupun terlindunginya sistem elektronik strategis (vital) bagi keberlangsungan layanan publik maupun negara.

2.2.3 Ancaman.

Secara umum, ancaman atau *threat* dipahami sebagai suatu usaha (kegiatan) oleh individu/kelompok tertentu yang berpotensi membahayakan keselamatan individu/kelompok lain. Tidak satupun negara di dunia yang benar-benar bebas dari ancaman sepanjang perjalanan hidup bangsa dan negaranya. Ancaman bisa menjadi *issue* yang meresahkan masyarakat suatu negara. Dulu kala hingga kini, banyak contoh peristiwa ancaman bagi keselamatan masyarakat di berbagai negara.

Ancaman (*Threat*) menurut *Oxford Dictionary* adalah "*a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done*", atau pernyataan niat untuk menimbulkan rasa sakit, cedera, kerusakan, atau tindakan bermusuhan lainnya pada seseorang sebagai balasan atas sesuatu yang dilakukan atau tidak dilakukan.

Ancaman menurut UU No.34/2002 tentang TNI, diartikan sebagai setiap upaya dan kegiatan, baik dari dalam maupun luar negeri yang dinilai mengancam (membahayakan) kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa. Di dalamnya juga tercantum definisi tentang ancaman militer sebagai ancaman oleh militer suatu negara kepada negara lain. Selain itu, ancaman bersenjata yang diartikan sebagai ancaman dengan kekuatan bersenjata.

Ancaman menurut UU RI No.17/2011 tentang Intelijen Negara, adalah setiap upaya, pekerjaan, kegiatan, dan tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah NKRI, dan kepentingan nasional di berbagai aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan.

Ancaman dalam konteks Hanneg (merujuk pada dokumen Kebijakan Hanneg Tahun 2020), dapat berupa ancaman aktual maupun ancaman potensial, sebagai dampak dari perkembangan lingkungan strategis global, regional, dan nasional, yang begitu, kompleks dan multidimensional (bersumber dari permasalahan ideologi, politik, ekonomi, sosial budaya, dan masalah-masalah keamanan terkait kejahatan internasional, seperti: terorisme, imigran gelap, narkotika, pencurian kekayaan alam, bajak laut, dan kerusakan lingkungan).

Dalam konteks hanneg dikenal ancaman aktual dan potensial. Ancaman aktual merupakan ancaman militer, nonmiliter dan hibrida, yang berkembang dan cenderung terus berlanjut dalam beberapa tahun ke depan, dari dalam maupun luar negeri yang berimplikasi pada kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa. Ancaman aktual antara lain: pelanggaran wilayah perbatasan/intervensi asing, separatisme dan pemberontakan bersenjata, perompakan, pembajakan dan penyanderaan WNI, terorisme dan radikalisme, ancaman siber, ancaman intelijen (*spionage*), *psy war*, senjata biologis, *natural disaster*, pencurian kekayaan alam, wabah dan penyakit, narkoba, termasuk ekses daro revolusi industri 4.0 dan revolusi masyarakat 5.0. Ancaman potensial merupakan ancaman yang belum terjadi, yang sewaktu-waktu dapat terjadi dan pada situasi tertentu menjadi ancaman aktual, antara lain: berupa perang konvensional/konflik terbuka (invasi asing), senjata nuklir, krisis ekonomi, pandemi, dan imigran asing.

Di dalam Doktrin Hanneg 2015 (Permenhan RI No.38 tahun 2015) terdapat penjelasan khusus tentang ancaman yang sebagai akibat dari kemajuan TIK (ancaman baru di era digital atau ancaman siber), ancaman tersebut disebut sebagai ancaman berdimensi teknologi. Terminologi tersebut juga tercantum dalam buku Pedoman Strategis Pertahanan Nirmiliter (Permenhan RI Nomor 19 tahun 2016) di mana ancaman siber merupakan ancaman nonmiliter berdimensi teknologi.

Menurut UU RI No.11/2008 tentang Informasi dan Transaksi Elektronik (ITE) maupun UU RI No.19/2016 tentang Perubahan atas UU No.11/2008 tentang ITE, tidak terdapat definisi spesifik mengenai ancaman siber di dalamnya. Kedua UU tersebut memang mengatur tentang ITE (teknologi informasi secara umum), dan keduanya fokus terhadap yurisdiksi yang diberlakukan kepada setiap orang yang melakukan perbuatan hukum

sebagaimana yang diatur di dalam kedua UU dimaksud, baik berada di dalam maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di dalam dan/atau di luar wilayah hukum Indonesia, dan merugikan kepentingan Indonesia. Dengan kata lain, terdapat ancaman hukuman pidana terhadap pelaku yang melanggar perbuatan yang dilarang menurut UU ITE.

Mencermati esensi perbuatan dilarang dalam UU ITE, dapatlah kiranya konseptual ancaman siber dalam konteks ITE ini dipersepsikan sebagai sifat formil dan sifat materiil dari suatu tindak pidana, sebagai berikut: a) ancaman siber dipersepsikan sebagai bentuk tindakan/kegiatan melawan hukum melalui perbuatan yang dilarang menurut undang-undang ITE. Hal ini relevan dengan sifat formil dari tindak pidana, dan hal tersebut tercermin dari adanya ancaman hukuman terhadap pelaku perbuatan yang melanggar ketentuan/aturan ini; dan b) ancaman siber dipersepsikan sebagai bentuk tindakan/kegiatan yang menimbulkan suatu akibat (dampak) dari melakukan perbuatan yang dilarang menurut undang-undang ITE. Hal ini relevan dengan sifat materiil tindak pidana, dan sebagai contoh dapat diambil substansinya pada Pasal 33 UU No.11/2008 (tentang ITE) dinyatakan bahwa “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya”, kemudian dampak kerugian yang ditimbulkan dari adanya tindakan/kegiatan sebagaimana tercantum pada pasal 33 telah difasilitasi dalam pasal 49 dari UU yang sama.

Ancaman siber menurut *draft* RUU Keamanan dan Ketahanan Siber (KKS). Bahwa sejak terbentuknya BSSN, pemerintah berada dalam proses menyusun *draft* RUU KKS untuk dapat dicantumkan dalam program legislasi nasonal (prolegnas) sekaligus dibahas dan diputuskan oleh DPR. Terlepas dari masih berjalannya proses tersebut, terdapat rumusan definisi

mengenai ancaman siber dan beberapa terminologi lain yang relevan, sebagai berikut: a) adalah segala upaya, tindakan, dan/atau kegiatan, baik dari dalam maupun luar negeri, yang dinilai dan/atau dibuktikan, dapat melemahkan, merugikan, dan/atau menghancurkan kepentingan siber Indonesia; b) KKS adalah kondisi dinamis siber pada seluruh aspek kehidupan nasional yang terintegrasi, aman, dan tangguh serta mampu mengembangkan kekuatan siber Indonesia dalam menghadapi segala ancaman siber terhadap kepentingan nasional Indonesia; c) kepentingan siber Indonesia adalah keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah, dan kepentingan nasional ipoleksosbudhankam di ruang siber; d) insiden siber adalah ancaman siber yang mengakibatkan sistem elektronik tidak berfungsi sebagaimana mestinya; dan e) serangan siber adalah ancaman siber yang mengakibatkan objek keamanan siber tidak berfungsi, sebagian atau seluruhnya, dan/atau bersifat sementara atau permanen. Dari uraian tersebut, dapat disimpulkan bahwa ancaman siber adalah ancaman dalam bentuk tindakan, upaya dan/atau kegiatan yang dilakukan dengan memanfaatkan TIK berbasis *cyberspace*, dari dalam maupun luar negeri, yang dinilai dan/atau dibuktikan mampu melemahkan, merugikan, dan/atau menghancurkan kepentingan nasional Indonesia.

2.2.4 Kompetensi.

Secara estimologi, kompetensi dimaknai sebagai kemampuan yang dibutuhkan untuk melakukan atau melaksanakan pekerjaan yang dilandasi oleh pengetahuan, keterampilan dan sikap kerja . Menurut kamus bahasa Indonesia (KBI), kompetensi didefinisikannya sebagai kewenangan (kekuasaan) untuk menentukan (memutuskan suatu). Spencer and Spencer (1993:9) mendefinisikan sebagai karakteristik yang mendasari seseorang dan berkaitan dengan efektivitas kinerja individu dalam pekerjaannya. Menurut Suparno (2001:27), adalah kecakapan yang memadai untuk melakukan suatu tugas, atau memiliki keterampilan dan

kecakapan yang disyaratkan. Dan menurut Stephen Robbin (2007:38), merupakan *ability* (kemampuan) atau kapasitas seseorang mengerjakan berbagai tugas dalam suatu pekerjaan, di mana *ability* ditentukan oleh faktor intelektual dan fisik. Dengan demikian, kompetensi dapat dimaknai sebagai kemampuan dari seseorang yang dapat terobservasi mencakup atas pengetahuan, keterampilan dan sikap kerja dalam menyelesaikan suatu pekerjaan atau tugas sesuai dengan standar performa yang ditetapkan.

Secara umum, kompetensi dapat juga dipahami sebagai kombinasi dari keterampilan (*skill*), atribut personal, dan pengetahuan (*knowledge*) yang tampak pada perilaku menjalankan tugas-tugas (job behavior). Menurut Spencer (1993:10) terdapat 5 (lima) karakteristik kompetensi, yaitu: a) *knowledge* (pengetahuan, wujud kompetensi yang kompleks), yaitu segala informasi yang dimiliki seseorang untuk bidang tertentu; b) *skills* (keterampilan/keahlian), merupakan kemampuan untuk melaksanakan suatu tugas tertentu secara mental dan fisik; c) *motives* (motivasi) merupakan sesuatu di mana manusia secara konsisten berfikir sehingga melakukan tindakan; d) *traits* (watak) adalah kepribadian yang membuat manusia perilaku atau merespon sesuatu dengan cara tertentu (misal: tahan atau tabah menerima tekanan, kontrol dan percaya diri; dan e) *Self concept* (jati diri) merupakan sikap dan nilai-nilai yang dimiliki. Kompetensi dapat ditingkatkan dan dioptimalkan melalui berbagai kegiatan pendidikan dan pelatihan (diklat) sesuai bidang kepentingan organisasi.

Diklat dapat didefinisikan sebagai usaha yang terencana dari suatu organisasi guna peningkatan pengetahuan, keterampilan dan kemampuan. Pendidikan dapat didefinisikan antara lain sebagai sebuah aktifitas yang memiliki maksud atau tujuan tertentu yang diarahkan untuk mengembangkan potensi yang dimiliki manusia baik sebagai manusia ataupun sebagai masyarakat dengan sepenuhnya, Nurkholis (2013:54).

Menurut Hasibuan (2009:54), pendidikan merupakan suatu proses untuk meningkatkan keahlian teoritis, konseptual, dan moral SDM. SDM yang memperoleh kesempatan diklat terprogram, kompetensinya meningkat dan cenderung lebih terampil dan profesional dibanding SDM dalam diklat tidak terprogram. Sehingga diklat terprogram semakin penting dalam menunjang peningkatan kompetensi seiring tuntutan peran, tugas dan fungsi, sebagai akibat dari tantangan perubahan situasi dan kondisi kerja, maupun kemajuan teknologi yang dihadapi organisasi.

2.3 Penelitian Terdahulu Yang Relevan.

Dalam tinjauan pustaka ini, peneliti menyertakan garis besar catatan berikut hasil-hasil penelitian terdahulu yang relevan, sebagai berikut:

Handrini Ardiyanti (2014) dalam penelitian yang berjudul "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia", menyatakan bahwa sebenarnya Indonesia berada dalam keadaan darurat *cyber-security* dengan melihat kenyataan bahwa tingkat kejahatan dunia maya (*cyber crime*) memprihatinkan. Tidak sama dengan penanganan kejahatan lain, *cyber-crime* perlu pemikiran komprehensif dalam menanganinya. Penelitian tersebut bertujuan untuk memperoleh gambaran tentang kebijakan *cyber-security* di Indonesia sekaligus memetakan prospek pengembangan *cyber-security* di Indonesia dan tantangannya. Penelitian menggunakan metode pendekatan kualitatif dengan melakukan kajian-kajian berbagai sumber literatur seperti jurnal, *report*, buku, maupun artikel terkait. Hasil penelitian secara singkat menyatakan *cyber-security* ke depan sebaiknya dibangun atas lima bidang, yaitu: kepastian hukum (undang-undang siber); teknis dan prosedural; struktur orgaisasi; *capacity building* dan pendidikan; dan kerjasama internasional.

Agus Subagyo (2015) dalam penelitian berjudul “Sinergi Dalam Menghadapi Ancaman *Cyber Warfare*”. Bahwa era globalisasi, hakekat ancaman salah satunya adalah ancaman siber. Era digital telah melahirkan kejahatan siber yang potensial menimbulkan perang siber. Indonesia memerlukan tentara siber untuk menghadapi ancaman tersebut. Kemhan RI harus jadi *leading sector* proses perumusan kebijakan pertahanan siber menghadapi ancaman perang siber. Sinergitas antar pemangku kepentingan siber menjadi kunci sukses. Penelitian bertujuan untuk memberikan gambaran bahwa penting untuk membangun sinergitas dalam menghadapi ancaman *cyber warfare*, serta perlunya Kemhan bertindak dalam mengambil langkah-langkah terciptanya sinergitas menghadapi *cyber warfare*. Penelitian menggunakan metode kualitatif bersifat deskriptif naratif, yang secara subyektif menggambarkan dan menguraikan hal apa adanya berdasar pengalaman peneliti terhadap data-data dan definisi maupun makna dari berbagai sumber artikel, jurnal, buku yang relevan. Hasil penelitian menunjukan sinergitas adalah keniscayaan dan mutlak. Kemhan harus menjadi pelopor sinergitas perlawanan terhadap ancaman *cyber warfare*. Mekanisme komunikasi, koordinasi, *networking*, dan teknis kerja sama harus dipacu Kemhan melalui pembentukan komunitas pertahanan siber (*cyber defence community*) guna penangkalan, pendeteksian, dan pencegahan dini dari ancaman *cyber warfare*.

Maulia Jayantina Islami (2017) dalam penelitian berjudul “Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian *Global Cybersecurity Index*”. Bahwa teknologi tidak cukup mengatasi *issue* keamanan informasi. *Cybersecurity* bagian dari ekosistem, di mana hukum, organisasi, kemampuan, kerjasama, dan teknis bekerja selaras agar efektif (ITU, 2017). Tujuan penelitian untuk memberikan gambaran tentang strategi pemerintah hadapi tantangan keamanan siber berikut potensi peningkatan strategi di masa depan menurut aspek *people*, *process*, dan *technology* (PPT). Penelitian menggunakan metode kualitatif

berbasis *non-numeric* data berupa tulisan dan gambar. Interpretasi data dari *literature review*, dan kajian bersumber dari literatur seperti jurnal, *report*, buku, maupun artikel yang *reliable*. Hasil penelitian menunjukan pemerintah menginisiasi strategi keamanan siber nasional dengan menjalankan program-program jangka pendek dan panjang, meski masih terdapat tantangan dan hambatan aspek SDM, prosedur dan kebijakan yang perlu koordinasi seluruh elemen terkait.

I Wayan Midhio, Yono Reksoprodjo, dan Hamzah Zaelani (2018) dalam penelitian yang berjudul "Pembangunan Kapasitas *Cyber Security* di Negara ASEAN: Analisis Komparatif Terhadap Brunei dan Indonesia". Bahwa dampak negatif *cyberspace* memaksa setiap negara berupaya penuh membangun kapasitas *cybersecurity* nasional. Penelitian menggunakan metode kualitatif dengan pendekatan deskriptif. Hasil penelitian menunjukan perbandingan pembangunan kapasitas *cybersecurity* antara Brunei Darussalam dan Indonesia sehingga menjadi masukan dalam pengembangan kapasitas *cybersecurity* Indonesia kedepan. Dalam penelitian ini, esensi penting yang relevan adalah bahwa strategi keamanan siber merupakan kerangka kerja tindakan prosedural dalam pembangunan kapasitas *cybersecurity* di Indonesia, selain itu pengelolaan permasalahan *cybersecurity* di Indonesia masih bersifat sektoral oleh masing-masing lembaga.

Tabel 2.1 Hasil Penelitian Terdahulu Yang Relevan

PENELITI	JUDUL	PERSAMAAN	PERBEDAAN
Handrini Ardiyanti (2014)	Cyber-Security dan Tantangan Pengembangannya di Indonesia	Relevan pada konteks: • Kebijakan Cybersecurity di Indonesia • Pentingnya Pengembangan Strategi *Cybersecurity* di Indonesia	• Penelitian Handrini Ardiyanti Tidak Menyinggung Aspek Hanneg/Sishankamrata • Penelitian ini Menempatkan Aspek *Cybersecurity* relevan sebagai dan/atau merupakan wujud Pertahanan Siber dalam kerangkas Sishankamrata

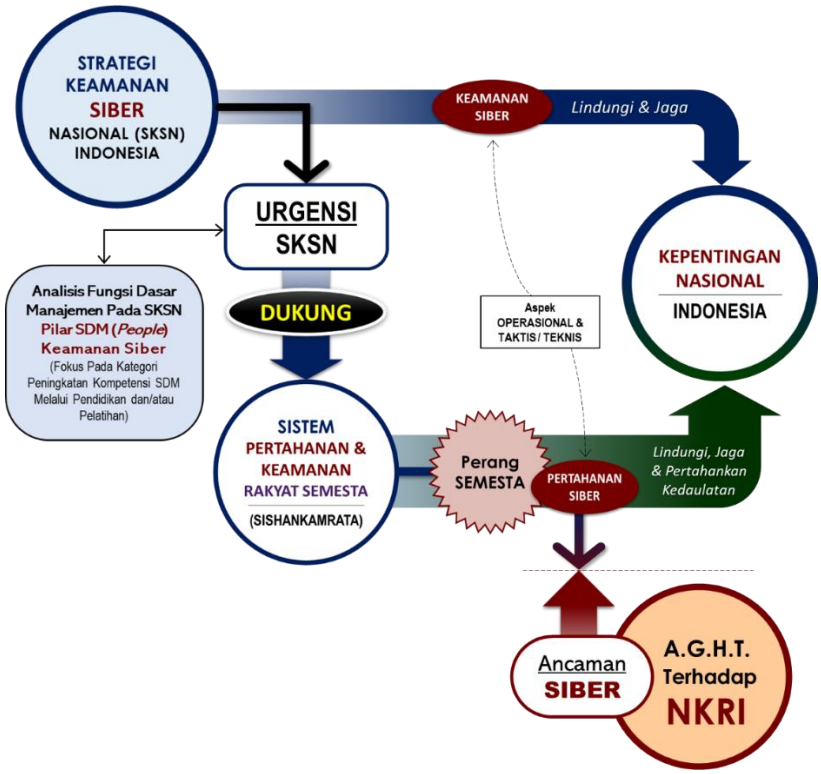
PENELITI	JUDUL	PERSAMAAN	PERBEDAAN
Agus Subagyo (2015)	Sinergi Dalam Menghadapi Ancaman *Cyber Warfare*	Relevan pada konteks: • Ancaman *Cyber Warfare* • Bagaimana Upaya HANNEG Indonesia Terhadap Ancaman *Cyber Warfare*	• Penelitian Agus Subagyo Relatif Tidak Menyinggung Aspek Strategi • Penelitian ini Menempatkan Aspek Strategi Keamanan Siber sebagai urgensi untuk mendukung Sishankamrata.
Maulia Jayantina Islami (2017)	Tantangan Dalam Implementasi Strategi Keamanan Siber Naisonal Indonesia Ditinjau Dari Penilaian GCI	Relevan dalam konteks: • Strategi Pemerintah Tadapi Tantangan Keamanan Siber • Peluang Peningkaan Strategi Keamanan Siber • Tantangan SDM Keamanan Siber • Pilar-Pilar Keamanan Siber: *People*, *Process*, & *Technology*	• Penelitian Maulia Jayantina Relatif Tidak Menyinggung Ancaman Siber maupun Strategi keamanan Siber terhadap konteks Sishankamrata. • Penelitian ini Menempatkan Aspek Strategi sebagai urgensi untuk kepentingan Sishankamrata
I Wayan Midhio, Yono Reksoprodjo, dan Hamzah Zaelani (2018)	Pembangunan Kapasitas Cyber Security di Negara ASEAN: Analisis Komparatif Terhadap Brunei dan Indonesia	Relevan dalam konteks: • Strategi Keamanan Siber sebagai kerangka kerja tindakan prosedural dalam pembangunan kapasitas *cybersecurity* di Indonesia. • Di Indonesia permasalahan *cybersecurity* masih ditanggulangi oleh masing-masing lembaga.	• Penelitian I Wayan Midhio, Yono Reksoprodjo, dan Hamzah Zaelani mengkomparasikan pembangunan kapasitas *cybersecurity* antara negara Brunei dan Indonesia. • Penelitian ini menempatkan aspek strategi *cybersecurity* sebagai urgensi di Indonesia dalam mendukung Sishankamrata.

Sumber: diolah peneliti.

2.4 Kerangka Berpikir.

Uma Sekaran (1992) dalam Sugiyono (2011) berpandangan bahwa kerangka berpikir adalah model konseptual tentang bagaimana teori berhubungan dengan beragam faktor yang telah diidentifikasi sebagai hal yang penting, dengan demikian dapat dikatakan bahwa kerangka berpikir ialah sebuah pemahaman yang melandasi pemahaman-pemahaman yang lainnya, sebuah pemahaman yang paling mendasar dan menjadi pondasi bagi setiap pemikiran atau suatu bentuk proses dari keseluruhan dari

penelitian yang akan dilakukan. Secara umum, kerangka berpikir dalam penelitian ini sebagaimana diilustrasikan dalam Gambar 2.4 (Kerangka Berpikir Penelitian).



Gambar 2.4 Kerangka Berpikir Penelitian

Sumber: diolah peneliti

BAB 3
METODE PENELITIAN

3.1 Metode dan Desain Penelitian.

3.1.1 Metode Penelitian.

SKSN dan Sishankamrata, keduanya merupakan wujud aktualisasi situasi sosial (*social situation*), yang dalam hal perumusan maupun penetapannya merupakan otoritas pemerintah, sehingga untuk penelitian ini, peneliti menggunakan metode kualitatif dan dengan pendekatan verifikatif fenomenologi.

Afrizal (2017:13) berpandangan bahwa metode penelitian kualitatif merupakan metode penelitian ilmu-ilmu sosial yang mengumpulkan dan menganalisis data kualitatif berupa kata-kata (lisan dan tulisan) dan perbuatan manusia, di mana peneliti tidak berusaha menghitung atau mengkuantifikasikan data kualitatif yang diperoleh dan dengan demikian tidak menganalisis angka-angka.

Moleong (2014:16) menyatakan bahwa: “Penelitian kualitatif adalah penelitian yang bermaksud memahami fenomena tentang apa yang dialami subjek penelitian, misal: perilaku, persepsi, motivasi, tindakan, dan lain sebagainya, secara menyeluruh (holistik) dengan cara menggambarkannya dengan bahasa dan kata-kata pada suatu konteks khusus yang alamiah memanfaatkan berbagai metode alamiah”.

Menurut Iskandar (2008:187) penelitian kualitatif berpegang kepada paradigma naturalistik dan fenomenologi, karena senantiasa dilakukan dalam *setting* alamiah terhadap suatu fenomena. Selain itu, penelitian kualitatif juga menggunakan beberapa teknik pengumpulan data untuk menggambarkan suatu fenomena.

Creswell (2013:20) memperkenalkan beberapa strategi atau pendekatan penelitian kualitatif yang salah satunya adalah fenomenologi sebagai strategi penelitian di dalamnya peneliti melakukan identifikasi terhadap hakikat pengalaman manusia mengenai fenomena tertentu. Memahami berbagai pengalaman hidup manusia membuat filsafat fenomenologi menjadi metode penelitian yang prosedurnya mewajibkan peneliti mengkaji berbagai subjek dengan terlibat langsung dan relatif lama di dalamnya demi mengembangkan *pattern* dan hubungan-hubungan makna (Moustakas, 1994).

Bungin (2012:70), mengemukakan bahwa metode penelitian kualitatif verifikatif sebagai usaha pendekatan induktif terhadap segenap proses penelitian. Format desain penelitiannya berbeda total dengan format verifikatif kualitatif. Format ini cenderung mengkonstruksikan format penelitian dan strategi mendapatkan data lapangan, sehingga model format penelitiannya induktif. Namun dalam memperlakukan teori, format ini lebih fleksibel pada teori, pengetahuan tentang data, dan tidak mengharuskan peneliti tutup mata. Metode ini punya keunggulan dalam mengungkapkan makna di balik data yang terlihat. Di samping itu juga memiliki kelebihan menafsirkan makna yang tersembunyi di dalam realitas. Penelitian ini bertitik tolak pada fenomenologi serta mendukung *post-positivisme*. Bungin (2012:71) mengungkap tiga faktor penyebab pendekatan dalam penelitian ini cocok untuk metode kualitatif, antara lain: a) secara ontologis, *post-positivisme* memiliki sifat *critical realism* yang memandang realitas sosial ada dalam kenyataan sebagaimana hukum alam, namun mustahil bila realitas sosial mampu dilihat dengan benar oleh manusia; b) secara metodologis, metode eksperimental teknik observasi belum cukup mendapatkan “kebenaran data”, namun harus menggunakan metode triangulasi, yaitu menggunakan berbagai sumber data, peneliti, dan teori;

dan c) secara epistemologis, hubungan pengamat (peneliti) dengan objek penelitian (realitas sosial) tak terpisahkan, sebagaimana positivisme.

Penggunaan metode kualitatif dengan pendekatan verifikatif fenomenologi menjadi pilihan peneliti karena sangat relevan diterapkan untuk topik penelitian ini. Untuk menggali makna feomena realitas sosial pada topik urgensi eksistensi SKSN terhadap upaya membangun kompetensi SDM pertahanan siber dalam mendukung sishankamrata, tentu memerlukan suatu pendekatan langsung peneliti dengan obyek penelitian sepanjang dinamika pengamatan. Karena data yang didapat, secara utuh akan merepresentasikan suatu gambaran tentang detail-detail yang sulit dideskripsikan oleh data-data kuantitatif.

3.1.2 Desain Penelitian.

Menurut Moh. Nazir (2014:70) desain penelitian digambarkan sebagai keseluruhan proses yang dibutuhkan dalam perencanaan maupun pelaksanaan kegiatan penelitian, mulai dari tahap persiapan hingga menyusun laporan. Gambaran lain yang lebih argumentatif diperoleh melalui *internet* pada situs http://pasca.undiksha.ac.id/, di mana desain penelitian didefinisikan sebagai strategi pilihan peneliti dalam mengintegrasikan komponen-komponen penelitian secara sistematis dan logis dalam pembahasan maupun analisis fokus penelitian. Gambaran keduanya menyinggung tentang integrasi seluruh komponen penelitian, yang berarti desain penelitian merupakan wujud komprehensif dari rencana penelitian. Kata komprehensif mencakup semua komponen penelitian seperti: pertanyaan penelitian, jenis data, metode, hingga analisis yang akan dilakukan. Merujuk pada kedua deskripsi tersebut, pada penelitian ini, desain yang dibangun peneliti adalah desain dengan teknik analisis data kualitatif model interaktif (*interactive model*), Miles and Huberman

(2014:15). Model tersebut, dikolaborasikan peneliti dengan teori manajemen George R. Terry (fungsi dasar manajemen POAC).

3.2 Tempat dan Waktu Penelitian.

3.2.1 Tempat Penelitian.

Penelitian dilaksanakan di wilayah Jakarta dan sekitarnya pada institusi-institusi yang terkait dengan bidang pertahanan negara maupun keamanan siber, baik di lingkungan pemerintah dan non pemerintah (*private sector*), yaitu:

Tabel 3.1 Daftar Instansi Tempat Penelitian

No	Aspek	Instansi	Bidang Jabatan
1.	Pertahanan	Kementerian Pertahanan RI	Pusat Pertahanan Siber
		Tentara Nasional Indonesia	Satuan Siber TNI
2.	Komunikasi dan Informatika	Kementerian Komunikasi dan Informatika	Badan Penelitian dan Pengembangan SDM Kementerian Kominfo
3.	Keamanan Siber Nasional	BSSN	Direktorat Pengendalian SDM

Sumber: diolah peneliti.

3.2.2 Waktu Penelitian.

Periode waktu penelitian terhadap obyek penelitian adalah mulai kurun waktu tahun 2014 s.d 2020 (± 6 tahun) merujuk pada ketika pemerintah mulai menginisiasi konsep membangun keamanan siber nasional hingga sekarang. Sedangkan rencana waktu penelitian, bila dimulai sejak penyusunan *draft* proposal tesis adalah hampir selama 4 (empat) bulan atau sesuai yang diberikan oleh lembaga UNHAN

Tabel 3.2 Jadwal Waktu Penelitian

No	Kegiatan	Tahun 2020															
		Juli				Agustus				September				Oktober			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1.	Penyusunan Draft Proposal																
2.	Pengajuan Proposal																
3.	Pengumpulan Data																
4.	Analisis Data																
5.	Penyusunan Tesis																
6.	Penyampaian Tesis																

Sumber: diolah peneliti.

3.3 Subyek dan Obyek Penelitian.

3.3.1 Subyek Penelitian.

Subyek penelitian (informan) dalam penelitian ini menggunakan prosedur *purposive* sebagai salah satu strategi menentukan informan yang berhubungan erat dengan masalah penelitian tertentu, Bungin (2011:107). Sedang menurut Husaini dan Purnomo (2009:45) *purposive* adalah pemilihan informan secara khusus berdasarkan tujuan penelitianya. Dengan demikian subyek penelitian adalah responden yang dalam hal ini berasal dari kalangan pejabat, staf, pakar, dan narasumber yang berkaitan erat dengan masalah penelitian ini, sebagai berikut:

Tabel 3.3 Daftar Subyek Penelitian

No	Bidang / Sektor	Responden / Informan
1.	Pertahanan dan TNI	Kepala Pusat Pertahanan Siber Kemhan, yang dalam hal ini didelegaskan kepada pejabat Kepala Bidang Jaminan Keamanan, Pushansiber Kemhan, yaitu: Kolonel Sus Tri Satya.
		Komandan Satuan Siber Mabes TNI, dalam hal ini didelegasikan kepada pejabat Asisten Operasi Satsiber TNI, yaitu: Kolonel Laut (E) Eko Wing W., S.T., beserta Staf

No	Bidang / Sektor	Responden / Informan
2.	Komunikasi dan Informatika	Kepala Pusat Badan Penelitian dan Pengembangan SDM Kemkominfo, yang dalam hal ini didelegasikan kepada pejabat Kepala Pusat Penelitian dan Pengembangan Sumber Daya Perangkat, dan Penyelenggaraan Pos dan Informatika (Puslitbang SDPPPI) Kominfo, yaitu Bapak Bonnie M. Thamrin Wahid Manan beserta staf.
3.	Keamanan Siber Nasional	Kepala BSSN, yang dalam hal ini didelegasikan kepada pejabat Deputi IV Bidang Pemantauan dan Pengendalian, BSSN, yaitu Mayjen TNI (Mar) Dr. Suharyanto, S.E., M.M. yang secara teknis oleh staf di lingkungan Direktorat Pengendalian SDM beserta staf, yaitu Bapak Anas Hilal dan Bapak Rian Irawan.

Sumber: diolah peneliti.

3.3.2 Obyek Penelitian.

Objek penelitian adalah sesuatu yang menjadi perhatian dalam sebuah penelitian karena objek penelitian merupakan sasaran yang hendak dicapai untuk mendapatkan jawaban maupun solusi dari permasalahan yang terjadi. Menurut Sugiyono (2012:144) pengertian objek penelitian adalah sasaran ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu tentang suatu hal obyektif, valid, dan *realiable* tentang suatu hal (dalam hal ini faktor kualitatif tertentu).

Obyek dalam penelitian ini adalah fokus pada aspek tata kelola membangun SDM keamanan siber nasional (menurut/sesuai konsep SKSN rumusan BSSN), guna mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Fokus tersebut kemudian dijabarkan dalam sub-sub topik rumusan masalah yang meliputi: a) mendeskripsikan implementasi peran dan fungsi SKSN terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata; b) menganalisis faktor-faktor yang mendukung dan yang

menghambat tata kelola (manajemen) kompetensi SDM keamanan siber dalam SKSN, terhadap upaya membangun SDM pertahanan siber untuk kepentingan sishankamrata; dan c) mendeskripsikan praktik-praktik keamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN Indonesia) yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

3.4 Teknik Pengumpulan Data.

Pengumpulan data adalah prosedur yang sistematik dan standar untuk memperoleh data yang diperlukan. Teknik pengumpulan data yang dilakukan penulis untuk mendapatkan data dalam penelitian ini adalah:

3.4.1 Penelitian Lapangan (*Field Research*).

Penelitian lapangan ini merupakan teknik pengumpulan data untuk mendapat data primer yang berhubungan dengan masalah yang diteliti. Peneliti menggunakan teknik ini dengan pengumpulan data, sebagai berikut:

3.4.1.1 Wawancara. Sebagai teknik pengumpulan data penelitian di mana peneliti berkomunikasi secara langsung dengan subyek penelitian sesuai Tabel 3.3 (Daftar Subyek Penelitian) mengenai masalah yang diteliti sekaligus mengumpulkan data-data yang relevan dari wawancara. Teknik yang digunakan tidak terstruktur, di mana dalam pengumpulan data, peneliti tidak menggunakan pedoman wawancara terstruktur, sistematis, dan lengkap. Pedoman yang digunakan hanya berupa garis-garis besar panduan pertanyaan terkait permasalahan yang akan ditanyakan. Wawancara juga dilakukan secara mendalam.

3.4.1.2 Observasi. Teknik penelitian langsung terhadap obyek penelitian untuk memperoleh data primer secara langsung dari responden (informan) dari setiap subyek penelitian. Data hasil observasi, selanjutnya dianalisis sehingga diperoleh gambaran dan verifikasi yang jelas mengenai permasalahan yang diteliti.

3.4.1.3 Dokumentasi. Pengumpulan data dilakukan dengan menelaah sekaligus menverivikasi data dan informasi dari berbagai dokumen yang berkaitan dengan obyek penelitian yang diperoleh baik dari setiap subyek penelitian maupun sumber-sumber resmi lainnya.

3.4.2 Penelitian Kepustakaan (*Library Research*). Penelitian yang dilakukan dengan cara mempelajari, meneliti, mengkaji serta menelaah literatur berupa buku-buku (*text book*), jurnal, peraturan perundang-undangan, majalah, surat kabar, artikel, dan penelitian-penelitian sebelumnya yang memiliki hubungan dengan masalah yang diteliti. Hal ini bertujuan untuk memperoleh sebanyak mungkin referensi maupun tambahan teori yang diharapkan mendukung dalam pengumpulan dan pengolahan (analisis) data penelitian.

3.5 Pemeriksaan Keabsahan Data.

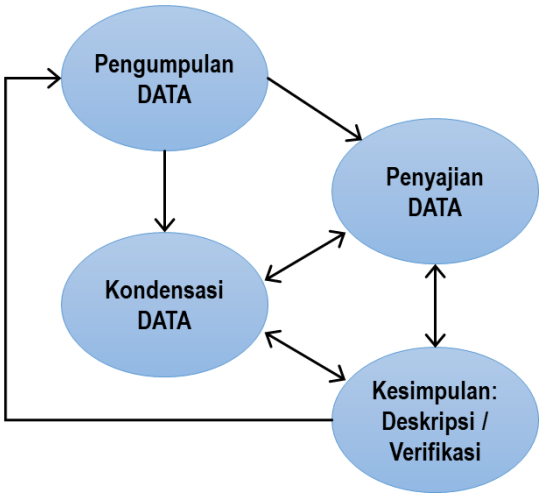
Pemeriksaan keabsahan data dilakukan hanya dengan menggunakan teknik triangulasi yaitu mengecek kebenaran data atau informasi yang diperoleh peneliti dari berbagai sudut pandang yang berbeda dengan cara mengurangi sebanyak mungkin bias yang terjadi pada saat pengumpulan dan analisis data. Teknik triangulasi sumber dan metode, yaitu dengan membandingkan dan mengecek balik derajat kepercayaan suatu informasi yang diperoleh melalui waktu dan alat yang berbeda dalam penelitian.

Triangulasi sumber berarti membandingkan dan mengecek balik derajat kepercayaan suatu informasi yang diperoleh melalui waktu dan alat yang berbeda, Patton dalam Moleong (2014:330). Hal itu dapat dicapai dengan jalan: membandingkan data hasil pengamatan dengan data hasil wawancara yang di dapat di tempat penelitian, membandingkan keadaan dengan perspektif informan pada faktor kualitatif pertama dengan informan dari faktor kualitatif kedua, dan membandingkan hasil wawancara dengan isi suatu dokumen yang berkaitan dengan upaya membangun kapasitas dan kapabilitas SDM keamanan dan pertahanan siber. Sedangkan triangulasi metode yakni melakukan pengecekan terhadap penggunaan metode pengumpulan data, apakah informasi hasil wawancara sama dengan hasil observasi, atau apakah hasil observasi sesuai dengan informasi pada pelaksanaan wawancara di berbagai tempat penelitian.

3.6 Teknik Analisis Data.

Sugiyono (2020:131) mengemukakan bahwa, analisis data adalah proses mencari dan menyusun secara sistematis data yang diperoleh dari hasil wawancara, catatan lapangan, dan dokumentasi, dengan cara mengorganisasikan data ke dalam kategori, menjabarkan ke dalam unit-unit, melakukan sintesa, menyusun ke dalam pola, memilih mana yang penting dan yang akan dipelajari, dan membuat kesimpulan sehingga mudah difahami oleh diri sendiri maupun orang lain.

Penelitian ini adalah penelitian kualitatif dengan pendekatan verifikatif fenomenologi. Teknik analisa data yang digunakan adalah analisis data kualitatif model interaktif (Miles and Huberman: 2014). Secara umum, komponen-komponen proses dalam model analisis data kualitatif ini mencakup: pengumpulan data (*data collection*), kondensasi data (*data condensation*), penyajian data (*data display*), dan deskripsi/gambaran kesimpulan atau verifikasi (*conclusion drawing/verification*).



Gambar 3.1 Proses Analisis Data Kualitatif Model Interaktif

Sumber: *Miles and Huberman*, (2014, p.20)

3.6.1 Pengumpulan Data (*Data Collection*). Langkah ini adalah yang pertama sebagai tahap yang sangat menentukan proses dan hasil penelitian. Kesalahan dalam pengumpulan data, akan berakibat langsung terhadap proses dan hasil suatu penelitian. Dalam penelitian kualitatif, peneliti sebagai instrumen kunci dalam pengumpulan data yang dilakukan secara langsung dengan observasi dan wawancara, dan studi kepustakaan maupun dokumentasi. Peneliti berharap memiliki waktu yang cukup agar data yang terkumpul semakin banyak dan bervariasi.

3.6.2 Kondensasi Data (*Data Condensation*). Langkah kedua adalah kondensasi data yang terjadi terus menerus sepanjang proses penelitian kualitatif. Bahkan sebelum data benar-benar dikumpulkan, kondensasi data antisipatif terjadi ketika peneliti memutuskan (seringkali tanpa kesadaran penuh) kerangka kerja konseptual, kasus mana, pertanyaan penelitian mana, dan pendekatan pengumpulan data mana yang harus dipilih. Ketika pengumpulan data berlangsung, selanjutnya dilakukan penulisan ringkasan

hasil wawancara, mengkode sesuai olah data, mengembangkan tema, menghasilkan kategori, dan menulis memo analitik.

3.6.3 Penyajian Data (*Data Display*). Langkah ketiga adalah penyajian data guna memudahkan peneliti melihat gambaran secara keseluruhan berkenaan dengan obyek penelitian. Batasan yang diberikan dalam penyajian data adalah sekumpulan informasi yang tersusun dan memberi kemungkinan adanya penarikan kesimpulan dan pengambilan tindakan. Dalam penelitian ini, penyajian data diwujudkan dalam bentuk uraian, dan gambar-gambar. Namun demikian, yang dominan digunakan untuk penyajian data dalam penelitian ini adalah dengan teks naratif.

3.6.4 Kesimpulan (*Conclussion: Description/Verifying*). Langkah keempat adalah penarikan kesimpulan dan verifikasi. Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan berubah bila tidak ditemukan bukti-bukti yang kuat yang mendukung pada taap pengumpulan data berikutnya. Tetapi apabila kesimpulan yang dikemukakan pada tahap awal, didukung oleh bukti-bukti yang valid dan konsisten saat peneliti kembali ke lapangan mengumpulkan data, maka kesimpulan yang dikemukakan merupakan kesimpulan yang kredibel.

3.7 Faktor-Faktor Kualitatif Yang Diteliti Dan Operasional Teori George R. Terry.

Faktor kualitatif penelitian merupakan hal yang diteliti dalam penelitian kualitatif ini, sehingga diasumsikan oleh peneliti sebagai suatu atribut, sifat atau nilai dari orang, obyek atau kegiatan yang mempunyai kategori atau peran atau fungsi tertentu yang ditetapkan peneliti untuk dipelajari dan kemudian ditarik kesimpulannya. Dalam penelitian kualitatif, yang bersifat holistik dan lebih menekankan pada proses, maka dalam melihat hubungan antara faktor kualitatif pada obyek yang diteliti lebih

bersifat interaktif, yaitu bisa saling mempengaruhi (*reciprocal*/interaktif). Berdasarkan pemahaman tersebut, dan untuk memudahkan analisa, maka dalam penelitian ini terdapat 2 (dua) faktor kualitatif dan beberapa sub faktor kualitatif yang oleh peneliti dikelompokkan sebagai berikut:

3.7.1 SKSN Sebagai Faktor – 1 (F_1).

Sebagai tolok ukur sementara, dalam penelitian ini konsep SKSN yang dipergunakan adalah hasil rumusan BSSN, yaitu SKSN 2020 – 2024 sebagai faktor kualitatif pertama yang kemudian disebut sebagai Faktor 1 (F_1). Dalam hal elemen cara (*ways*) untuk SKSN mencapai sasaran strategis, terdapat 5 (lima) pilar, di mana setiap pilar dijabarkan kedalam fungsi dan indikator penting, antara lain: kategori, aksi, dan/atau keluaran (*output*) berikut indikator capaian masing-masing pilar. Menurut peneliti, hal tersebut juga merupakan faktor-faktor fungsional yang sedemikian rupa sehingga konsep strategis (dalam SKSN) dapat terlaksana sesuai/menurut cara (*ways*) kelima pilar tersebut. Dengan demikian Pilar 1 s/d 5 SKSN tersebut menjadi Sub Faktor 1 s/d 5 atau bila dijabarkan menjadi: Pilar-1 sebagai sub faktor 1.1 ($F_{1.1}$), Pilar-2 sebagai sub faktor 1.2 ($F_{1.2}$), Pilar-3 sebagai sub faktor 1.3 ($F_{1.3}$), Pilar-4 sebagai sub faktor 1.4 ($F_{1.4}$), dan Pilar-5 sebagai sub faktor 1.5 ($F_{1.5}$). Namun demikian, dalam penelitian ini tidak seluruh pilar digunakan, peneliti telah memilih yaitu: sub faktor Pilar-1 ($F_{1.1}$), Pilar-2 ($F_{1.2}$), dan Pilar-5 ($F_{1.5}$) sebagai faktor-faktor kualitatif yang diteliti. Seluruh faktor kemudian diasosiasikan (dihubungkan) peneliti berdasarkan uraian deskripsi fungsi maupun indikator dari masing-masing sub faktor terhadap pilar *people* dalam *cybersecurity* yang sekaligus difungsikan sebagai titik simpul (*node*) di dalam proses analisis data yang memiliki hubungan fungsi dasar manajemen (POAC) dengan *node* Faktor – 2 (F_2).

Tabel 3.4 Uraian Fungsi dan Indikator Faktor – 1 (F_1)

FAKTOR KUALITATIF	SUB FAKTOR	FUNGSI dan INDIKATOR Merujuk Pada Konsep SKSN 202-2024 (Rumusan BSSN)		PILAR *Cyber Security*
	Pilar SKSN (*ways*)	**Kategori**	**Aksi dan/atau Keluaran**	
Faktor 1 → **F_1** **Strategi Keamanan Siber Nasional (SKSN)** Konsep: Membangun dan Menjaga Keamanan Siber Nasional dengan Mensinergikan Berbagai Pemangku Kepentingan Untuk Ikut Serta Mewujudkan Keamanan Nasional dan Meningkatkan Pertumbuhan Ekonomi Nasional Merujuk pada Pengantar Strategi Keamanan Siber Indonesia BSSN https://bssn.go.id/strategi-keamanan-siber-nasional/. Wujud Operasional: **Keamanan Siber** Pilar Keamaan Siber: ***People* = SDM** ***Process* = Proses** ***Technology* = Teknologi**	Pilar Kesatu / P_1 (Ketahanan Siber Indonesia) Sebagai Sub Faktor **$F_{1.1}$**	Penyiapan Konsep Teknokratik dan/atau Aturan	• Arsitektur Keamanan • Standar & Kriteria Keamanan • Diseminasi	Teknologi
		Peningkatan Kompetensi SDM	• Pendidikan dan/atau Pelatihan • Pengujian Kompetensi • Penyelenggaraan Konsultasi	Manusia
		Pembangunan dan/atau Penyelenggaraan Sarpras	• *National Security Operational Center* • *Security Operational Center*	Teknologi
		Penguatan Koordinasi & Kolaborasi	• *National CERT/CSIRT* • *CERT/CSIRT* • *National Threat Analisys Center* • *Program Voluntary Vulnerability Disclosure (Bug Hunting)*	Proses
		Manajemen	Kegiatan Monitoring & Evaluasi	Proses
	Pilar Kedua / P_2 (Kepastian Hukum Ruang Sber) Sebagai Sub Faktor **$F_{1.2}$**	Penyiapan Konsep Teknokratik dan/atau Aturan	• UU Keamanan & Ketahanan Siber • UU Perlindungan Data Pribadi	Proses
		Peningkatan Kompetensi SDM	Pendidikan dan/atau Pelatihan	Manusia
	Pilar Ketiga / P_3			
	Pilar Keempat / P_4			
	Pilar Kelima / P_5 (Kerjasama Internasional & Nasional) Sebagai Sub Faktor **$F_{1.5}$**	Peningkatan Kompetensi SDM	Pendidikan dan/atau Pelatihan	Manusia
		Penguatan Koordinasi & Kolaborasi	Penyelenggaraan Latihan Bersama Secara Berkelanjutan (*Cyber Defense Exercice*)	Proses
			Kegiatan Berbagi Informasi (Diseminasi Edukasi Keamanan Siber & Forum Petemuan Tingkat Internasional)	Proses
			• MoU Pendidikan Bagi ASN, TNI/Polri, & Pemangku Kepentingan • MoU Penguatan Komitmen Keamanan Siber & Internet sbg Sumnda Bersama	Proses

Sumber: diolah peneliti.

3.7.2 Sishankamrata Sebagai Faktor – 2 (F_2).

Sishankamrata merupakan sistem pertahanan negara di Indonesia yang aktualisasinya dalam bentuk perang semesta. Penyelenggaraan perang semesta dilakukan melalui suatu bentuk tata kelola (manajemen) strategis yang disebut sebagai strategi perang semesta, karena di dalamnya melibatkan komponen/elemen seluruh warga negara Indonesia (WNI), wilayah, serta segenap sumber daya dan sarana prasarana nasional lainnya. Gelar perang semesta untuk menghadapi ancaman siber sebagai ancaman berdimensi teknologi, wujud operasionalnya adalah pertahanan siber. Sehingga untuk penjabaran komponen WNI dalam faktor kualitatif sishankamrata menjadi sub faktor kualitatif SDM pertahanan siber, oleh peneliti dengan merujuk pada Pedoman Pertahanan Siber (Kemhan/TNI) dan Doktrin Hanneg 2015. Seluruh faktor/sub faktor tersebut kemudian diasosiasikan terhadap pilar *people* dalam *cybersecurity* yang setiap elemennya difungsikan sebagai titik simpul (*node*) di dalam proses analisis data yang memiliki hubungan fungsi dasar manajemen (POAC) dengan *node* Faktor – 1 (F_1).

Tabel 3.5 Uraian Fungsi dan Indikator Faktor – 2 (F_2)

FAKTOR KUALITATIF	SUB FAKTOR	FUNGSI dan INDIKATOR Merujuk Pada Pedoman Pertahanan Siber (Kemhan/TNI) & Doktrin HANNEG 2015		PILAR *Cyber Security*
	Komponen/Unsur SISHANKAMRATA	Kategori	Aksi dan/atau Keluaran	
Faktor 2 → **F_2** **Sistem Pertahanan dan Keamanan Rakyat Semesta (SISHANKAMRATA)** Konsep: Sihankamrata merupakan bentuk hanneg yang dikembangkan dengan melibatkan seluruh warga negara, wilayah, serta segenap sumber daya dan sarana prasarana	**Seluruh Warga Negara Indonesia (WNI)** Sebagai Sub Faktor **$F_{2.1}$**	Sumber Daya Manusia (SDM)	Ketersediaan SDM Yang Kompeten Sebagai Aset Utama Sekaligus Faktor Sentral	Manusia
			Pengembangan SDM (Rekrutmen, Penggunaan & Pembinaan, & Penugasan Khusus)	
			Pembinaan Latihan & Peningkatan Kemampuan/Keterampilan SDM	
	Wilayah NKRI			
	Segenap Sumber Daya & Sarana Prasarana Nasional Lainnya	Kebijakan / Regulasi	• Kebijakan Dasar • Kebijakan Srategis • Kebijakan Operasional • Kebijakan Manajemen Pengamanan Informasi, • Standar Acuan (Pedoman),	Proses

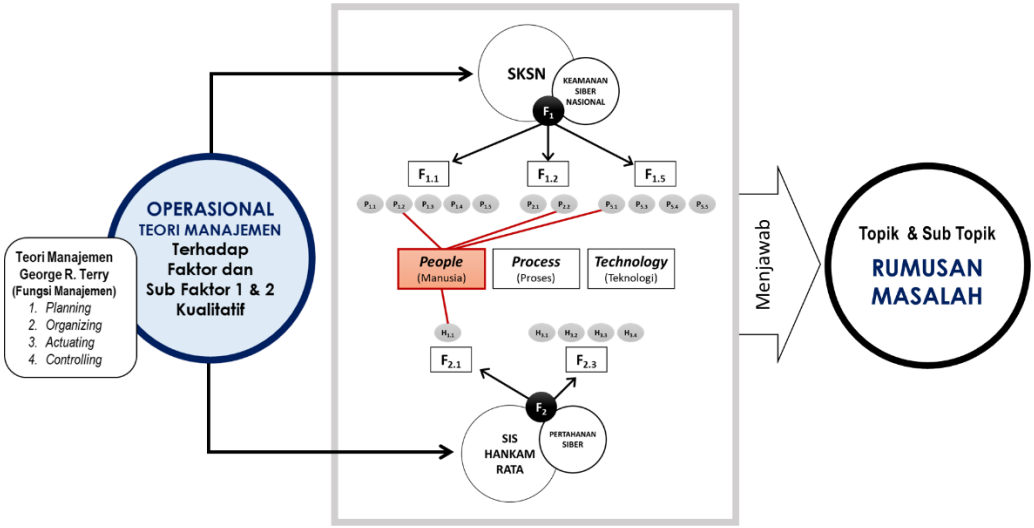
FAKTOR KUALITATIF	SUB FAKTOR	FUNGSI dan INDIKATOR Merujuk Pada Pedoman Pertahanan Siber (Kemhan/TNI) & Doktrin HANNEG 2015		PILAR *Cyber Security*
	Komponen/Unsur SISHANKAMRATA	**Kategori**	**Aksi dan/atau Keluaran**	
nasional, yang dipersiapkan secara dini oleh Pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah NKRI, dan keselamatan segenap bangsa dari segala ancaman (termasuk dhi ancaman siber). Penjabaran Pasal 30 Ayat (2) UU NRI 1945 Wujud Operasional: **Pertahanan Siber** Pilar Pertahanan Siber: **Sesuai Dengan Pilar Keamanan Siber**	Sebagai Sub Faktor $F_{2.3}$		• Kebijakan Pengorganisasian	
		Kelembagaan / Organisasi	Tugas dan Fungsi, Wewenang, Struktur, dan Bentuk Kelembagaan	Proses
		Teknologi / Infrastruktur	• Sarana Prasarana Gedung, NOC, Laboratorium dan Fasilitas Pendukung Lain • Pusat Data & Pemulihan (DRC) • Jaringan Komunikasi Data • Aplikasi (Sistem Informasi) Administratif dan Khusus • *Hardware* & *Software* Spesifik Pertahanan Siber • Rancangan Teknis & Infrastruktur Pertahanan Siber (Sebagai *Critical Information Infrastructures*)	Teknologi
		Kegiatan Operasional Pertahanan Siber	• Operasional Pertahanan Siber • Operasional Pengamanan Informasi • Penerapan Standar Nasional / Internasional Untuk Pertahanan Siber • Kegiatan Pendidikan dan Latihan Pertahanan Siber Pada Skala Nasional / Internasional	Proses

Sumber: diolah peneliti.

3.7.3 Operasional Teori Manajemen Geroge R. Terry Terhadap Faktor – 1 (F_1) dan Faktor – 2 (F_2).

Bila diilustrasikan hubungan operasional teori manajemen George R. Terry terhadap Faktor 1 dan 2 beserta Sub Faktor masing-masing faktor kualitatif dalam penelitian ini, diperoleh gambaran sebagaimana pada gambar 3.2 Meskipun seluruh faktor dan uraiannya dicantumkan dalam gambaran tersebut, namun tidak kemudian mengurangi/menghilangkan fokus penelitian sebagaimana tercantum sebagai topik dan sub topik rumusan masalah yang esensinya adalah terkait urgensi SKSN Indonesia terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Sehingga dalam proses operasionalisasi teori

manajemen George R Terry hanya akan fokus pada faktor dan sub-sub faktor yang relevan untuk kategori SDM dan/atau peningkatan kompetensi SDM, dengan indikator aksi/keluaran yang hanya relevan dengan praktik-praktik kegiatan pendidikan dan latihan yang menunjang upaya membangun/meningkatkan kompetensi SDM pertahanan siber. (Catatan: pada gambar di bawah ini tergambar sebagai bidang yang terhubung dengan garis-garis berwarna merah).



Gambar 3.2 Diagram Operasional Teori Manajemen George R. Terry Terhadap Faktor Kualitatif Penelitian

Sumber: diolah peneliti

BAB 4
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Gambaran Umum Obyek Penelitian.

Merujuk pada rumusan BSSN, SKSN diproyeksikan memiliki fungsi sebagai kerangka kerja pembangunan dan pengembangan di bidang keamanan siber yang menunjukan tujuan nasional yang hendak diwujudkan, pilar, dan inisiatif yang diprioritaskan, tahapan, waktu, dan indikator pelaksanaan, serta uraian mengenai peranan dari segenap pemangku kepentingan yang terkait. SKSN juga diproyeksikan sebagai pedoman bagi menteri dan pimpinan lembaga di bidang keamanan siber dalam menetapkan kebijakan nasional dan sektoral yang terkait dengan SKSN yang dituangkan dalam dokumen rencana strategis di bidang tugas masing-masing sebagai bagian dari Rencana Pembangunan Jangka Menengah Nasional (RPJMN). Berkenaan dengan SKSN sebagai pedoman, hal tersebut menunjukan adanya korelasi erat dengan peran, tugas, dan fungsi organisasi dari masing-masing subyek penelitian dalam penelitian ini, yaitu:

Pertama: Pushansiber Kemhan RI bertugas melaksanakan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber. Dan dalam melaksanakan tugas, Pushansiber Kemhan menyelenggarakan fungsi-fungsi: a) penyusunan kebijakan teknis, program dan anggaran di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber; b) pelaksanaan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber; c) pemantauan, evaluasi, pengendalian dan pelaporan di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber; d) pembentukan CERT (*Computer Emergency Response Team*) dalam rangka merespon serangan siber,

serta pemantauan dan evaluasi dalam setiap pelaksanaan tugas CERT; dan e) pengelolaan ketatausahaan dan kerumahtanggaan Pusat.

Kedua: Satsiber TNI bertugas menyelenggarakan kegiatan dan Operasi Siber di lingkungan TNI dalam rangka mendukung tugas pokok TNI. Satsiber TNI menyelenggarakan fungsi (secara garis besar): a) perencanaan kegiatan dan Operasi Siber TNI dalam rangka penangkalan, penindakan, pemulihan dan dukungan operasi; b) perencanaan adminlog kegiatan dan Operasi Siber TNI dalam rangka penangkalan, penindakan, pemulihan dan dukungan operasi; c) penangkalan siber, meliputi monitoring, deteksi, observasi serta mitigasi dan *cyber awareness* untuk melindungi infrastruktur kritis TNI dari berbagai dimensi ancaman siber; d) penindakan siber, meliputi eksploitasi dan Pusprop guna memperoleh keunggulan siber dalam operasi; e) pemulihan siber, yaitu pemulihan insiden siber sebagai dampak dari berbagai bentuk serangan siber meliputi forensik, pemeliharaan dan instalasi serta *Military Computer Emergency Response Team* (Mil-CERT); dan f) bantuan siber, meliputi pembangunan sistem dan dukungan operasi, baik dari aspek teknis maupun nonteknis yang menyangkut operasi dan kegiatan siber. Selain fungsi utama tersebut, terdapat beberapa fungsi umum, salah satunya adalah penyelenggaraan fungsi personel untuk mendukung tugas Satsiber TNI.

Ketiga: Balitbang SDM mempunyai tugas menyelenggarakan litbang bidang TIK serta pengembangan SDM TIK. Balibang SDM menyelenggarakan fungsi: a) perumusan kebijakan teknis di bidang litbang TIK serta pengembangan SDM TIK; b) pelaksanaan litbang di bidang TIK serta pengembangan SDM TIK; c) pelaksanaan evaluasi dan pelaporan di bidang litbang TIK serta pengembangan SDM TIK; d) pelaksanaan administrasi Balitbang SDM; dan e) pelaksanaan fungsi lain yang diberikan oleh Menteri.

Keempat: BSSN mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur terkait keamanan siber. BSSN menyelenggarakan fungsi (garis besar), antara lain: a) menyusun, melaksanakan, memantau, dan mengevaluasi kebijakan teknis, di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi *e-commerce*, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber; b) pengoordinasian kegiatan fungsional dalam pelaksanaan tugas BSSN dan sebagai wadah koordinasi bagi semua pemangku kepentingan; c) pelaksanaan pembinaan dan pemberian dukungan administrasi kepada seluruh unit organisasi di lingkungan BSSN; d) pengawasan atas pelaksanaan tugas BSSN; e) pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN; dan f) pelaksanaan kerjasama nasional, regional, dan internasional dalam urusan keamanan siber.

Dalam perspekstif bidang hanneg, eksistensi SKSN diyakini akan menjadi hal yang sangat penting terhadap upaya mewujudkan SDM pertahanan siber untuk kepentingan sishankamrata. Di dalam konsep SKSN yang sampai saat ini substansinya masih terus disempurnakan oleh BSSN, tercantum bagaimana strategi pemerintah dalam upaya membangun kompetensi SDM nasional untuk bidang keamanan siber (atau pertahanan siber dalam perspektif hanneg), hasil strategi dan upaya pemerintah dalam membangun kompetensi SDM keamanan siber nasional tersebut nantinya menjadi bagian dari sumber daya nasional yang akan dikelola (ditransformasikan) sebagai komponen-komponen kekuatan hanneg.

Dalam konteks membangun SDM nasional di era digital, tampak adanya perbedaan kompetensi dan terminologi, yaitu: a) istilah SDM TIK menurut Kementerian Kominfo; b) istilah SDM keamanan siber menurut BSSN; dan c) istilah SDM pertahanan siber menurut bidang pertahanan (Kemhan dan TNI). Secara umum, perbedaan tersebut dapat dijelaskan sebagai berikut: *pertama*, untuk istilah SDM TIK, merupakan wujud kompetensi *knowledge* (pengetahuan) *dan* skill (keterampilan) SDM nasional dalam bidang TIK yang diperlukan untuk mengawaki sarana dan prasarana serta infrastruktur TIK yang ada di berbagai sektor strategis, antara lain: pemerintahan, perbankan, kesehatan, energi, transportasi, pertanian, ekonomi, pertahanan, keamanan, dan lain sebagainya. SDM TIK nasional dibangun pemerintah untuk *outcome* yang mengacu pada upaya pembangunan TIK nasional yang telah, sedang, dan akan dilaksanakan pemerintah berdasarkan *roadmap* Pembangunan TIK Nasional yang fokus pada pembangunan infrastruktur TIK dengan menitikberatkan pada pembangunan SDM TIK, peningkatan layanan TIK, dan pengembangan TIK yang pada intinya bertujuan untuk memiliki nilai tambah bagi pertumbuhan ekonomi dan meneguhkan kedaulatan bangsa; *kedua*, untuk SDM keamanan siber, yaitu merupakan wujud kompetensi SDM TIK nasional yang kemudian ditingkatkan dan dikembangkan untuk memiliki *knowledge* dan *skill*, serta kapasitas dan kapabilitas dalam bidang keamanan siber nasional (sebagaimana dinyatakan dalam pengantar SKSN, tujuan strategisnya adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital); dan *ketiga*, untuk SDM pertahanan siber, yaitu merupakan wujud peningkatan kompetensi SDM TIK nasional menjadi SDM keamanan siber yang kemudian ditingkatkan lagi kompetensinya sehingga memiliki *knowledge dan skill* serta kapasitas dan kapabilitas bidang pertahanan siber dalam menghadapi dan menanggulangi ancaman siber yang mengganggu kedaulatan negara maupun kepentingan nasional.

Meski ada perbedaan kompetensi dan terminologi, namun terdapat hal yang tidak mungkin dipungkiri bahwa pada ketiga kompetensi SDM tersebut terdapat aspek *knowledge* dan *skill*, serta kapasitas dan kapabilitas yang hakekatnya sama-sama dalam satu bidang, yaitu: komunikasi dan informatika atau siber. Meski secara hakiki sama, namun seolah menjadi berbeda ketika SDM tersebut oleh masing-masing bidang (pertahanan siber, keamanan siber, serta komunikasi dan informatika) dibangun kompetensinya sesuai kebutuhan dan/atau untuk tujuan bidang dari masing-masing organisasi tersebut.

Perbedaan kompetensi tersebut tidak mengesampingkan kenyataan bahwa upaya pemerintah dalam membangun kompetensi SDM TIK nasional tidak cukup sekedar memenuhi kebutuhan akan ketersediaan SDM TIK sesuai tuntutan *roadmap* pembangunan TIK nasional yang fokus pada pembangunan infrastruktur TIK, namun dalam perkembangannya diperlukan kompetensi SDM bidang pertahanan dan keamanan (dengan meningkatkan dan mengembangkan *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM TIK nasional), khususnya untuk mampu menghadapi berbagai bentuk ancaman siber di era digital. Untuk itu diperlukan upaya strategis pemerintah dalam hal menata kelola (manajemen) SDM TIK nasional agar siap menghadapi ancaman siber.

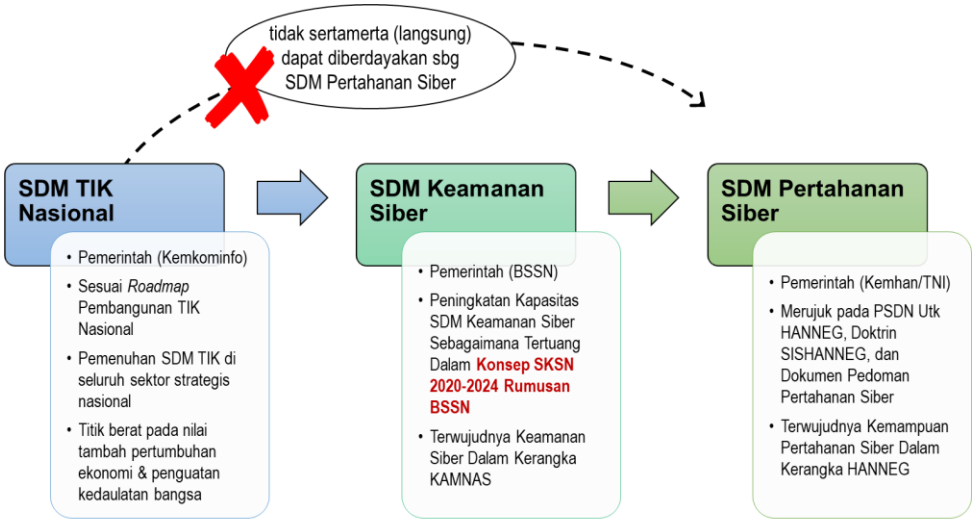
Bukanlah hal yang mudah bagi pemerintah untuk membangun SDM TIK nasional yang juga harus memiliki kompetensi dalam bidang keamanan siber maupun pertahanan siber. Perlu upaya-upaya dan langkah-langkah strategis pemerintah dengan tujuan agar infrastruktur TIK nasional yang dibangun tersebut aman dan tahan dari berbagai ancaman siber. Salah satu upaya strategis pemerintah yang telah, sedang, dan akan dilaksanakan oleh BSSN adalah tersusunnya konsep SKSN yang di dalamnya memuat antara lain strategi nasional dalam rangka membangun kompetensi SDM

keamanan siber nasional. Strategi dalam konsep SKSN tersebut tentu menjabarkan langkah-langkah strategis yang harus ditempuh pemerintah dalam menata kelola membangun SDM keamanan siber, yang pada waktunya nanti oleh bidang pertahanan akan ditransformasikan sebagai SDM pertahanan siber untuk mendukung kepentingan sishankamrata.

Menurut pandangan peneliti, terwujudnya SDM pertahanan siber untuk kepentingan sishankamrata merupakan hasil dari suatu proses panjang tata kelola (manajemen) pembangunan kompetensi SDM TIK nasional yang berkesinambungan. Proses tersebut bersifat strategis, karena kompetensi SDM TIK nasional yang dibangun pemerintah berdasarkan kerangka kerja *roadmap* pembangunan TIK nasional, dan tidak seketika itu juga langsung dapat digunakan atau diberdayakan oleh bidang pertahanan sebagai SDM pertahanan siber. Mengapa demikian ? karena kompetensi SDM TIK nasional tersebut masih jauh dari atau belum memenuhi tuntutan kebutuhan kriteria kompetensi SDM pertahanan siber yang mensyaratkan *knowledge dan skill* serta kapasitas dan kapabilitas SDM yang dalam hal ini obyektifnya adalah mampu untuk menghadapi berbagai macam ancaman siber demi melindungi kepentingan nasional dan mempertahankan kedaulatan NKRI.

Dalam membangun kompetensi SDM dengan kemampuan pertahanan siber, di samping memiliki kompetensi sebagai SDM TIK, di dalamnya juga terdapat upaya untuk membangun *knowledge dan skill* serta kapasitas dan kapabilitas SDM keamanan siber yang spesifik, misalnya untuk *knowledge*, antara lain secara umum menguasai konsep dan teoritis tentang jaringan komputer dan komunikasi, keamanan informasi, dan intelijen; sedangkan untuk *skill* antara lain memiliki kemampuan dalam rekayasa keamanan jaringan komputer dan komunikasi dengan menggunakan metodologi tertentu, rekayasa keamanan informasi, merencanakan dan merancang pengelolaan keamanan siber, serta

mengoperasikan fitur keamanan perangkat jaringan yang meliputi sistem operasi, perangkat lunak dan perangkat keras. Seluruhnya masih perlu proses dan tata kelola (manajemen) lebih lanjut yang juga spesifik agar kompetensi SDM TIK nasional yang ditingkatkan menjadi SDM keamanan siber, mampu memenuhi kriteria kompetensi sebagai SDM pertahanan siber. Dan hal tersebut diyakini oleh bidang pertahanan hanya dapat dipenuhi (diakomodir) nantinya melalui SKSN. Tata kelola peningkatan kompetensi SDM keamanan siber dalam konsep SKSN tersebut telah memenuhi prinsip pilar *people* keamanan siber yang sebagian besar kriteria kompetensi SDM-nya relevan dengan tuntutan kriteria SDM pertahanan siber. Melalui proses tata kelola kompetensi SDM dalam konsep SKSN, maka kompetensi SDM keamanan siber akan ditingkatkan menjadi SDM pertahanan siber oleh bidang pertahanan, sekaligus dikelola untuk kemudian ditrasformasikan menjadi SDM pertahanan siber sebagaimana prinsip-prinsip pengelolaan sumber daya nasional (PSDN) untuk Hanneg.



Gambar 4.1 Proses Tata Kelola SDM TIK Ke SDM Pertahanan Siber

Sumber: diolah peneliti

Sebagaimana tampak dalam gambar 4.1 bahwa SDM TIK nasional sebenarnya merupakan awal (*basic*) dari proses membangun kompetensi SDM keamanan siber maupun pertahanan siber. Kebutuhan SDM untuk kompetensi keamanan siber maupun pertahanan siber sangat membutuhkan *knowledge dan skill* serta kapasitas dan kapabilitas bidang TIK. Penggunaan SDM dengan kompetensi keamanan siber dan pertahanan siber, sangat mensyaratkan (menuntut) adanya kriteria kompetensi SDM yang lebih daripada sekedar kompetensi SDM TIK, yaitu SDM TIK dengan kriteria *knowledge* dan *skil* serta kapasitas dan kapabilitas bidang keamanan siber maupun bidang pertahanan siber yang mampu untuk menyelenggarakan dan melaksanakan tugas, peran, dan fungsi khusus, yaitu untuk menghadapi dan menanggulangi berbagai bentuk ancaman siber terhadap kepentingan nasional secara semesta atau bersifat kontijensi nasional. Tata kelola untuk kompetensi SDM seperti itu tentulah bersifat spesifik, termasuk dalam hal ini untuk kapasitas SDM pertahanan siber yang tentunya sangat bergantung kepada terwujudnya SDM keamanan siber yang menjadi tanggung jawab BSSN.

Idealnya tata kelola (manajemen) yang dilakukan oleh pemerintah dalam membangun kompetensi SDM TIK nasional, SDM keamanan siber, dan SDM pertahanan siber, harus memiliki tata kelola (manajemen) kompetensi SDM yang komprehensif, integratif, dan berkesinambungan semenjak awal dibangunnya kompetensi SDM TIK nasional hingga diperlukan untuk memenuhi kebutuhan SDM dengan kompetensi keamanan siber maupun pertahanan siber. Namun demikian, gambaran umum obyek penelitian di lapangan menunjukan kondisi dinamika tata kelola (manajemen) dalam pembangunan kompetensi SDM yang relatif satu dengan lainnya masih belum komprehensif, belum integratif, dan belum berkesinambungan. Dampak signifikan dari kondisi tersebut khususnya pada bidang pertahanan, dalam hal ini terhadap upaya mewujudkan kompetensi SDM pertahanan siber yang sangat bergantung

pada kompetensi SDM TIK nasional maupun kompetensi SDM keamanan siber.

Ketergantungan dalam mewujudkan SDM pertahanan siber terhadap *output* dan *outcome* hasil tata kelola kompetensi SDM TIK nasional maupun SDM keamanan siber, menjadikan keduanya tersebut menjadi vital dan penting untuk bidang pertahanan. Tata kelola membangun SDM keamanan siber nasional yang dirumuskan BSSN dalam konsep SKSN 2020-2024, tampaknya menjadi wujud peran dan fungsi SKSN dalam mengakomodir sebagian besar tuntutan kriteria kompetensi SDM pertahanan siber.

4.2 Hasil Penelitian.

Sebagaimana telah dikemukakan pada bagian awal, maka fokus penelitian ini adalah terhadap bagaimana eksistensi SKSN di Indonesia penting terhadap upaya membangun kemampuan SDM pertahanan siber untuk sishankamrata. Hasil penelitian mengacu kepada uraian sub fokus-sub fokus penelitian yang seluruh datanya diperoleh peneliti melalui wawancara dengan setiap informan (narasumber) subyek penelitian, kemudian data-data hasil wawancara dikondensasi dan dijamin keabsahannya terhadap/berdasarkan sumber-sumber referensi lainnya antara lain: dokumen, artikel, jurnal, peraturan dan regulasi yang relevan.

4.2.1 Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata.

Pada sub fokus ini, hasil penelitian diperoleh atau berupa perspektif dan pandangan umum (sebagai gambaran dan/atau deskripsi) bersumber dari subyek-subyek penelitian, terkait peran dan fungsi SKSN (dalam hal ini strategi peningkatan kompetensi SDM keamanan siber dalam konsep

SKSN 2020-2024 rumusan BSSN yang nantinya akan diimplementasikan oleh BSSN dan para pemangku kepentingan siber nasional), terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Yang dimaksud dengan peran dan fungsi SKSN tersebut adalah signifikansi eksistensi peran dan fungsi SKSN Indonesia terhadap misalnya tersedianya *roadmap* atau program pembangunan SDM TIK nasional yang pengelolaannya selain sesuai dengan konsep SKSN, juga mendukung upaya terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

Sejak terbentuknya BSSN di tahun 2017, di mana kemudian badan ini menginisiasi penyusunan konsep SKSN 2020-2024, ironisnya eksistensi konsep tersebut masih belum sepenuhnya diketahui oleh hampir seluruh pemangku kepentingan siber di Indonesia. Secara internal BSSN telah menerbitkan konsep SKSN 2020-2024, meski belum dipublikasikan, karena belum ditetapkan sebagai suatu bentuk aturan nasional, dan malahan sampai dengan saat ini BSSN masih melakukan perbaikan dan penyempurnaan terhadap konsep-konsep strategis di dalamnya.

4.3.4.1 Pushansiber Kemhan RI.

Pushansiber Kemhan belum mengetahui tentang adanya SKSN maupun konsep SKSN 2020-2024 rumusan BSSN. Namun demikian berpendapat bahwa di era digital seperti saat ini, apabila SKSN tersebut terwujud, maka eksistensinya (dalam hal ini peran dan fungsi SKSN) akan menjadi vital dan penting tidak hanya sekedar untuk membangun kompetensi SDM keamanan siber nasional saja, namun juga akan sangat mendukung bidang pertahanan dalam upaya membangun kapasitas SDM pertahanan siber (wawancara di Pushansiber Kemhan, pada 3 September 2020).

Pushansiber Kemhan belum menyusun/memiliki semacam *roadmap* dan atau program kerja yang spesifik berkenaan dengan pembangunan kompetensi SDM untuk pertahanan siber. Adapun pemenuhan SDM baru sebatas memenuhi kebutuhan di lingkungan Kemhan (Pusdatin dan Pushansiber), yang *intake* SDM-nya bersumber baik dari internal (Kemhan dan TNI), maupun dari eksternal (bersifat kontrak kerja) yang setiap tahun jumlahnya terbatas, dan itupun masih belum mampu memenuhi kompetensi SDM yang dipersyaratkan (wawancara di Pushansiber Kemhan, pada 3 September 2020).

Gambar 4.2 Kunjungan Kerja Kepala BSSN di Pushansiber Kemhan

Sumber: kemhan.go.id/bainstrahan (2019)

Di era digital dengan berbagai tatangan ancaman siber, Kemhan menempatkan kompetensi SDM pertahanan siber sebagai yang paling vital dan penting. Hal tersebut sejalan dengan apa yang dikemukakan Wakil Menteri Pertahanan (Wamenhan) RI, Bapak Sakti Wahyu Trenggono pada kunjungan kerjanya ke Pushansiber Kemhan pada hari Jumat tanggal 13 Nopember 2019 lalu. Wamenhan RI menyatakan bahwa "*ada 3 (tiga) kemampuan yang harus dimiliki dalam membangun teknologi pertahanan siber, tetapi yang lebih penting dari itu semua adalah SDM-nya. Jadi ketika saya pergi ke Korea, Cina, lalu ke Belanda, teknologi itu fungsinya sekitar 40% saja, tetapi 60% nya dari orang-orangnya*". Hal yang disampaikan

Wamenhan RI tersebut, semakin menegaskan bahwa kompetensi SDM pertahanan siber penting untuk diwujudkan, dan itu memerlukan *effort* berikut tata kelola (manajemen) yang baik dan spesifik dalam hal perencanaan, pengorganisasian, pelaksanaan, dan pengendalian.

Gambar 4.3 Kunjungan Kerja Wamenhan RI ke Pushansiber

Sumber: kemhan.go.id/bainstrahan (2019)

Secara umum, konsep (rumusan) kompetensi SDM pertahanan siber sebagaimana tercantum pedoman pertahanan siber, antara lain: a) memiliki cybersecurity awarnes; b) memiliki pengetahuan dan keterampilan dalam hal: information *security and risk management*, *access control systems and methodology*, *cryptography*, *physical security*, *telecommunications and network security*, *security architecture and models*, *business continuity planning and disaster recovery plan*, *applications security*, *operations security*, *legal*, *regulations*, *compliance and investigations*, dan implementasi SNI 27001; c) memiliki pengetahuan dan keterampilan penanganan insiden sekurang-kurangnya meliputi: *digital forensic*, *incident response*, *operation system*, dan *data communication networking*; d) pengetahuan dan keterampilan melakukan *penetration test* sekurang kurangnya meliputi: *information security in general*, *using penetration testing tools*, *IT examination and reporting*, dan *web based application developing*; e) *system assurance*; f) pengetahuan dan ketrampilan sistem meliputi: *network security*, *operating systems security*, *systems*

infrastructure and database, *security*, *digital control system*, dan *system development*; dan g) pengetahuan dan kemampuan merehabilitasi dan rekonstruksi kerusakan yang terjadi pada jaringan TIK dan muatannya. Hal lain yang sangat spesifk adalah seluruh *knowledge* dan *skill* tersebut di atas kemudian diaktualisasikan sebagai kompetensi pertahanan siber.

Gambar 4.4 Kajian Kebutuhan Kompetensi SDM Pertahanan Siber Berkorelasi Dengan Jenjang Karier

Sumber: Pedoman Pertahanan Siber (2014, p.35)

Pada intinya kompetensi SDM pertahanan siber yang diharapkan adalah memiliki *knowledge* dan *skill* serta kapasitas dan kapabilitas yang spesifik untuk bidang pertahanan siber. Menurut pandangan peneliti, kompetensi tersebut juga bergantung kepada *output* dan *outcome* dari pembangunan kompetensi SDM TIK nasional maupun kompetensi SDM keamanan siber nasional, sebagai *basic* (awal) bidang pertahanan membangun kompetensi SDM pertahanan siber. Meskipun sampai saat ini bidang pertahanan belum merumuskan *roadmap* kompetensi SDM pertahanan siber, namun sebagai acuan atau standar adalah merujuk pada Permenhan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI (wawancara di Pushansiber Kemhan, pada 3 September 2020). Sebagai gambaran, hal yang paling spesifik dari wujud kompetensi

SDM pertahan siber adalah adanya *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM dengan kemampuan melakukan operasional pertahanan siber terhadap berbagai bentuk ancaman siber yang mengganggu kepentingan hanneg dan kedaulatan NKRI. Kemampuan tersebut merupakan aktualisasi fungsi hanneg yang secara garis besar meliputi penangkalan siber, penindakan siber, penanggulangan siber, dan perbantuan siber. *Knowledge* dan *skill* serta kapasitas dan kapabilitas tersebut bersumber dari kompetensi SDM TIK nasional dan SDM keamanan siber nasional yang dikelola untuk ditrasformasikan menjadi SDM pertahanan siber menurut UU No.23/2019 tentang PSDN untuk Hanneg.

4.3.4.2 Satsiber TNI.

Demikian halnnya Satsiber TNI, sejak lembaga BSSN terbentuk, masih belum mengetahui tentang apa itu SKSN maupun konsep SKSN 2020-2024 hasil rumusan BSSN (wawancara di Satsiber TNI, pada 10 September 2020). Namun demikian, bahwa kiranya MoU (Nota Kesepahaman) antara Satsiber TNI dengan BSSN (dengan Nomor: Kerma/44/XI/2018 dan Nomor: PERJ.337/KBSSN/KH.02.01/11/2018 tertanggal 8 November 2018), yang mengatur rencana kerja sama tentang Penguatan Keamanan Siber dan Persandian di Lingkungan TNI, di mana satu dari 6 (enam) ruang lingkupnya adalah terkait dengan peningkatan dan pengembangan SDM. Dan melalui MoU ini, sebagaimana tercantum dalam konsep SKSN, maka BSSN akan mengimplementasikan peran penting dalam upaya membangun SDM keamanan siber nasional yang pada saatnya nanti ditransformasikan sebagai SDM dengan kompetensi pertahanan siber untuk kepentingan sishankamrata.

TNI juga masih belum memiliki atau merumuskan *roadmap* terkait rencana kerja pembangunan kompetensi SDM bidang pertahanan siber

(wawancara di Satsiber TNI, pada 10 September 2020). Meskipun demikian, Satsiber TNI tetap berupaya dalam membangun kompetensi SDM pertahanan siber, dengan mengikutsertakan SDM Satsiber TNI pada berbagai program dan kegiatan yang dilaksanakan oleh pihak lain, baik dalam bentuk seminar maupun pelatihan-pelatihan, baik di dalam negeri maupun luar negeri, misalnya dengan Thailand pada Latihan *Cobra Gold Exercise* tahun 2018 dan tahun 2019, dan dengan AS dalam hal ini *Hawaiian National Guard* atau HING pada kegiatan Latihan *Information System and Technology Exchange* (ISTX) tahun 2019.

Gambar 4.5 Nota Kesepahaman (MoU) Antara TNI dan BSSN

Sumber: facebook.com/badansiberdansandinegara (2018)

Meski Satsiber TNI belum mengetahui eksistensi SKSN, namun sependapat bahwa di era digital seperti saat ini, eksistansi atau peran dan fungsi SKSN penting bagi Indonesia. Dan bila dihadapkan kepada upaya membangun SDM keamanan siber nasional, maka eksistensi SKSN juga menjadi penting khususnya terhadap upaya bidang pertahanan dalam mendukung kelancaran tata kelola TNI dalam membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata (wawancara di Satsiber TNI, pada 10 September 2020).

Gambar 4.6 Pembukaan Latma *Cobra Gold Exercice* 2018

Sumber: tni.mil.id/ Puspen TNI (2018)

Standar dan kriteria kompetensi SDM pertahanan siber yang diharapkan mampu dibangun oleh Satsiber TNI, masih mengacu kepada Permenhan Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI (wawancara di Satsiber TNI, pada 10 September 2020). Meskipun pada prinsipnya selaras dengan Pushansiber Kemhan, namun terdapat aspek yang sangat fundamental dalam kompetensi SDM pertahanan siber yang sangat dibutuhkan oleh jajaran TNI, yaitu ketika pertahanan siber diaktualisasi dalam suatu *theatre* sishankamrata dalam bentuk gelar operasi militer, di mana alut sista TNI yang berbasis TIK harus dipertahankan (misal: *Network Centric Warfare*) dan/atau alut sista TNI yang berbasis TIK dioperasionalkan (sebagai *cyber weapon*) untuk tujuan melakukan serangan-serangan siber terhadap ancaman siber lawan. Hal tersebut tentu menunjukan bahwa SDM pertahanan siber memiliki spesifikasi kompetensi yang penuh dengan aspek dan dinamika dalam bidang hanneg.

4.3.4.3 Balitbang SDM Kemenkominfo RI.

Balitbang SDM Kemenkominfo RI telah mendelegasikan permintaan penelitian ini kepada Puslitbang SDPPI. Pada dasarnya Kominfo

memahami tentang SKSN, namun sejak BSSN terbentuk belum mengetahui tentang adanya konsep SKSN 2020-2024 yang telah dirumuskan BSSN (wawancara *online*, pada 8 September 2020). Berkenaan dengan SKSN, maka Balitbang SDM Kominfo adalah sebagaimana merujuk pada PP No.71/2019 tentang PSTE, pasal 94 ayat (1) huruf a, di mana penetapan strategi keamanan siber nasional yang merupakan bagian dari strategi keamanan nasional, termasuk pembangunan budaya keamanan siber, merupakan peran pemerintah. Adapun dengan konsep SKSN rumusan BSSN, itu diluar sepengetahuan Kominfo meskipun BSSN dalam hal tersebut juga merupakan bagian dari institusi pemerintahan. Dalam konteks kompetensi SDM keamanan siber maupun kompetensi SDM pertahanan siber, maka terminologi yang digunakan oleh Kementerian Kominfo (dalam hal ini Balitbang SDM Kominfo) adalah SDM bidang Teknologi Informasi dan Komunikasi (TIK).

Gambar 4.7 Program *Digital Talent Scholarship* (DTS) Kominfo

Sumber: kumparan.com/kumparantech (2019)

Balitbang SDM Kominfo dalam melaksanakan tugas dan fungsi membangun SDM TIK nasional merujuk pada *roadmap* Pembangunan TIK Nasional yang fokus pada pembangunan infrastruktur TIK dengan menitikberatkan pada pembangunan SDM TIK, peningkatan layanan TIK dan pengembangan TIK yang memiliki nilai tambah bagi pertumbuhan ekonomi dan meneguhkan kedaulatan bangsa (wawancara *online*, pada 8

September 2020). Dari hal tersebut maka tampak dalam perspektif Kominfo, pembangunan kompetensi SDM bidang TIK masih menitikberatkan kepada sektor ekonomi di mana pembangunan kompetensi SDM bidang TIK nasional cenderung diproyeksikan untuk siap bersaing di dunia industri. Salah satu program rutin yang sampai saat ini masih diselenggarakan oleh Kominfo adalah program *Digital Talent Scholarship* (DTS). Program ini merupakan upaya pemerintah untuk mengembangkan kemampuan masyarakat di bidang digital agar Indonesia menjadi salah satu negara dengan ekonomi digital terbesar di Asia Tenggara pada tahun 2030, seiring menyongsong era Revolusi Industri 4.0.

Gambar 4.8 Pelatihan dan Sertifikasi Kompetensi Bidang TIK Berbasis SKKNI Gelombang – 1 Tahun 2020 Secara *Online*

Sumber: bpptik.kominfo.go.id (2020)

Berdasarkan uraian catatan hasil wawancara tersebut, tampak bahwa peran pemerintah (Kemenkominfo RI) fokus pada membangun kompetensi SDM bidang TIK nasional (bersertifikat) yang umumnya atau cenderung dibutuhkan di berbagai sektor strategis nasional guna membangun, mengawaki, mengoperasikan, memelihara, dan mengembangkan sarana prasarana dan infrastruktur TIK di berbagai sektor strategis tersebut.

Gambar 4.9 Tiga Sasaran Strategis Pengembangan SDM dan Kesiapan Masyarakat

Sumber: Penyusunan *Roadmap* Pembangunan Sektor TIK Jangka Panjang s.d. 2045 Menuju 100 Tahun Indonesia Merdeka (2016, p.39)

Berkenaan dengan *roadmap* pembangunan kompetensi SDM, adalah sebagaimana telah diuraikan di atas yaitu membangun kompetensi SDM TIK nasional yang merujuk pada *roadmap* Pembangunan Sektor TIK Nasional 2016-2045 dengan manifesto untuk menyongsong 100 tahun Indonesia merdeka yaitu "*sektor TIK mandiri, berdaulat, berdaya saing, bermartabat dan beretika kepribadian dengan fungsi sebagai meta-infrastruktur yang efisien bagi penjaga kepentingan nasional pada sistem geopolitik dan ekonomi global, melalui tata kelola dinamis oleh masyarakat madani yang memiliki kesetaraan kapasitas kemampuan adaptif dinamis pada tingkat korporasi, pemerintah dan individu dalam meraih kesempatan dan sumber daya secara berkeadilan dalam mencapai kesejahteraan*". Strategi pengembangan SDM dan kesiapan masyarakat menuju 100 tahun Indonesia merdeka memiliki 3 (tiga) sasaran strategis seperti ditunjukkan pada sebagai manifestasi tiga faktor penting SDM yaitu penguasaan pasar TIK global, kapasitas produksi nasional, dan masyarakat berbudaya TIK yang tangguh. Dalam penyusunan *roadmap* empat aspek, yaitu pendidikan, pemerintah, industri, dan masyarakat. *Roadmap* menghasilkan rumusan pembangunan yang dibagi atas tiga kelompok kerja yaitu: a) infrastruktur

dan tata kelola TIK nasional; b) Internet, Aplikasi, Konten dan Digitalisasi; dan c) SDM dan *Social Readiness*.

Adapun wujud kompetensi SDM TIK nasional adalah merujuk pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang Kominfo (bersumber pada dokumen naskah Rencana Pengembangan SDM TIK di Indonesia (wawancara *online*, pada 8 September 2020). Melalui Sertifikasi SKKNI Bidang Kominfo, yang publikasi oleh Puslitbang SDPPI Balitbang SDM Kominfo tahun 2018), rincian kompetensi SDM TIK cukup banyak terdiri atas berbagai sektor dan bidang, antara lain: bidang keamanan Informasi, sektor TIK sub sektor operator komputer, *cloud computing*, *software development* (*programmer*), *mobile computing*, desain jaringan, *software design analysis*, dan lain sebagainya. Namun demikian, secara spesifik bila merujuk pada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada TIK, kompetensi SDM TIK mencakup 16 (enambelas) area fungsi TIK, sebagai berikut: a) *data management systems*; b) *programming and software develompment*; c) *hardware and digital peripherals*; d) *network and infrastructure*; e) *operation and systems tools*; f) *information systems and technology development*; g) *IT governance and management*; h) *IT project management*; i) *IT enterprise architecture*; j) *IT security compliance*; k) *IT service management systems*; l) *IT and computing facilities management*; m) *IT multimedia*; n) *IT mobility and internet of things (IoT)*; o) *integration application system*; dan p) *IT consultancy and advisory*.

4.3.4.4 BSSN.

BSSN menyatakan konfirmasi bahwa konsep SKSN yang digunakan dalam penelitian ini dapat merujuk pada konsep SKSN Indonesia 2020-2024 yang telah diterbitkan BSSN pada tahun 2019, namun belum resmi dipublikasi (belum memenuhi ketentuan sebagai dokumen peraturan

resmi). Dan lebih jauh konsep SKSN 2020-2024 yang dijadikan sebagai rujukan oleh peneliti dalam penelitian ini telah dikonfirmasi dan diberikan ijin BSSN sebagai referensi dalam penelitian ini, meskipun BSSN masih terus menyempurnakan konsep SKSN tersebut (wawancara *online*, pada 11 dan 13 September 2020).

Secara substansi, aspek peningkatan kompetensi SDM dalam konsep SKSN 2020-2024 rumusan BSSN masih tetap relevan, meski saat ini konsep SKSN 2020-2024 rumusan BSSN tersebut masih terus disempurnakan. Dalam konsep SKSN 2020-2024, aspek peningkatan kompetensi SDM keamanan siber (yang ditempatkan sebagai elemen *ways* strategi), memiliki peran dan fungsi hanya untuk membangun kompetensi SDM keamanan siber yang dibutuhkan oleh sektor-sektor strategis untuk memenuhi tuntutan keamanan siber, dan tidak mencakup kompetensi SDM pertahanan siber yang spesifik pada infrastruktur TIK di seluruh alutsista bidang pertahanan (wawancara *online*, pada 11 dan 13 September 2020).

Hasil penelitian mencatat bahwa upaya BSSN melalui konsep SKSN 2020-2024, di mana konsep SKSN fokus pada membangun kompetensi SDM keamanan siber yang diperlukan di berbagai sektor strategis nasional adalah untuk memenuhi tuntutan terwujudnya keamanan siber nasional pada infrastruktur TIK. Khusus untuk bidang pertahanan, maka untuk kompetensi SDM pertahanan siber hanya sebatas mampu memenuhi *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM keamanan siber yang dibutuhkan guna memenuhi tuntutan keamanan siber pada infrastruktur TIK pada sektor pertahanan, namun tidak atau belum spesifik untuk infrastruktur TIK pada alutsista-alutsista bidang pertahanan. Terbatasnya peran dan fungsi pembangunan kapasitas SDM dalam konsep SKSN 2020-2024 tersebut adalah karena kelembagaan BSSN yang masih baru, dan konsep SKSN juga masih belum final. Selain itu dalam berbagai momentum forum-forum pertemuan antara BSSN dengan bidang

pertahanan (Kemhan dan TNI), masih terbatas pada topik atau materi-materi umum membangun kerjasama bidang keamanan siber, misalnya: materi diskusi tentang peran keamanan siber pada strategi komunikasi humas dalam rangka hanneg. Sebagaimana tampak pada Gambar 4.10 tersebut, tampak substansi topik forum diskusi hanya terbatas membahas tentang keamanan siber pada konten informasi, dan belum menyentuh pada aspek sistem informasi, bahkan masih jauh dari detil pembahasan tentang topik maupun materi yang erat dengan fungsi hanneg pada *level* taktis, *level* operasional, maupun *level* strategis terhadap berbagai bentuk ancaman siber sebagai bentuk aktualisasi dinamika kapasitas dan kapabilitas pertahanan siber.

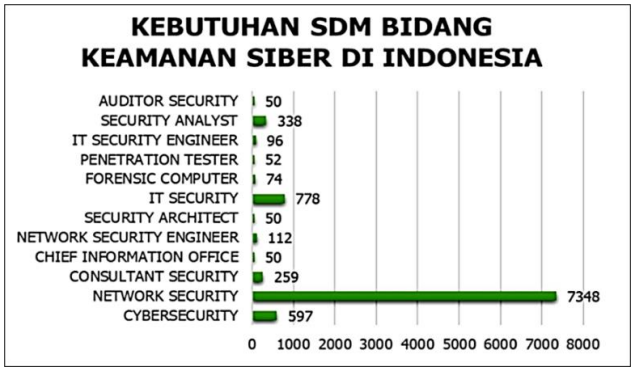
Gambar 4.10 Forum Komunikasi Bakohumas Bahas Keamanan *Cyber* Untuk Pertahanan Negara

Sumber: idu.ac.id (2019)

Berkenaan dengan *roadmap* program pembangunan SDM, bahwa BSSN telah menyusun semacam dokumen *roadmap* pebinaan SDM keamanan siber nasional, yaitu: Roadmap Pembinaan SDM Keamanan Siber dan Sandi 2020-2024 (Menuju SDM Keamanan Siber dan Sandi Yang Terpercaya, Profesional, dan Berdaya Saing). Dokumen ini dimaksudkan untuk mendukung upaya peningkatan kompetensi SDM keamanan siber pada konsep SKSN perbaikan (wawancara *online*, pada 11 dan 13 September 2020). Artinya bahwa *roadmap* tersebut juga dianggap baru

mampu mengakomodir kompetensi awal (*basic*) SDM keamanan siber yang dipersyaratkan/dibutuhkan/diperlukan untuk mewujudkan kompetensi SDM pertahanan siber.

Pembinaan SDM keamanan siber dalam *roadmap* tersebut bertujuan untuk mencapai SDM unggul di bidang keamanan siber, di mana langkah-langkah pembinanan meliputi aspek-aspek, antara lain: standardisasi SDM, peran dan fungsi pembinaan SDM oleh organisasi profesi, pengembangan kurikulum pusdiklat, *research and development*, pengembangan kompetensi, pemenuhan sertifikasi, monitoring dan evaluasi, *cybersecurity education* pada pendidikan dasar dan menengah, peran dan fungsi pusdiklat sebagai *corporate university*, serta peran dan fungsi STSN sebagai *centre of excelent*.



Gambar 4.11 Esensi Kompetensi SDM Keamanan Siber di Indonesia

Sumber: *Roadmap* Pembinaan SDM Keamanan Siber dan Sandi 2020-2024 (2019, p.45)

Terdapat faktor penting lain terkait esensi kompetensi SDM keamanan siber yang memiliki *knowledge* dan *skill* serta kapasitas dan kapabilitas yang menjadikannya spesifik dan terbatas pada bidang keamanan siber. Meski cukup banyak sumber literatur yang membahas tentang hal tersebut, namun peneliti hanya mengambil data kompetensi SDM keamanan siber nasional yang bersumber dari dokumen, sebagai berikut:

Pertama, *roadmap* pembinaan SDM keamanan siber dan sandi 2020-2024 di mana *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM keamanan siber yang dibutuhkan di Indonesia, meliputi antara lain: *auditor security*, *security analyst*, *IT security engineer*, *penetration tester*, *forensic computer*, *IT security*, *security architect*, *network security engineer*, *chief information office*, *consultant security*, *network security*, dan *cybersecurity.*

Kedua, Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber, yang mencantumkan *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM keamanan siber mencakup 30 (tiga puluh) okupasi pada level kualifikasi 5 s.d. 9 jenjang (level) kualifikasi KKNI, sebagai berikut: a) kualifikasi 5, teridentifikasi 4 (empat) okupasi pada fase *before attack* dan *during attack*, yaitu: *cryptographic technician*, *cryptographic administrator*, *junior cyber security*, dan *cyber security operator*; b) kualifikasi 6, teridentifikasi 10 (sepuluh) okupasi pada fase *before*, *during*, dan *after attack*, yang meliputi: *ICT security product evaluator*, *cryptographic analyst*, *cryptographic module analyst*, *vulnerability assessment analyst*, *network security administrator*, *cyber security administrator*, *cyber security awareness officer*, *cyber security analyst/cyber security incident analyst*, dan *digital evidence first responder*; c) kualifikasi 7, teridentifikasi 12 (dua belas) okupasi pada seluruh fase, meliputi: *cryptographic speialist*, *cryptographic engineer*, *ICT security product lead evaluator*, *cybersecurity manager*, *network security manager*, *cybersecurity awareness lead officer*, *incident response team manager*, *information security auditor*, *threat hunter*, *penetration tester*, *cybersecurity governance officer*, dan *digital forensic analyst*; d) kualifikasi 8, teridentifikasi 5 (lima) okupasi pada fase *before attack* dan *after attack*, meliputi: *cyber risk specialist*, *security architect*, *cryptographic specialist*, *cyber incident investigation manager*, dan *cyber forensic specialist*; dan e)

kualifikasi 9, teridentifikasi 1 (satu) okupasi pada seluruh fase, yaitu: *chief of information security officer*. *Knowledge* dan *skill* serta kapasitas dan kapabilitas bidang keamanan siber tersebut, kemudian ditingkatkan kompetensinya melalui konsep SKSN rumusan BSSN sehingga mampu menyelenggarakan kegiatan dan praktik-praktik keamanan siber secara nasional. Hal tersebut yang menurut pandangan peneliti merupakan wujud implementasi keamanan siber yang terintegrasi melibatkan seluruh komponen berikut sumber daya pemangku kepentingan siber nasional.

Gambar 4.12 Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber

Sumber: Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber (2019, p.vii)

4.2.2 Faktor-Faktor Yang Mendukung Dan Menghambat SKSN Indonesia Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata.

Pada sub fokus ini, hasil penelitian yang diperoleh berupa perspektif dan pandangan umum (sebagai gambaran dan/atau deskripsi) bersumber dari subyek-subyek penelitian terkait faktor-faktor yang mendukung dan

menghambat tata kelola (manajemen) strategi peningkatan kompetensi SDM keamanan siber pada konsep SKSN 2020-2024 terhadap upaya membangun SDM pertahanan siber untuk kepentingan sishankamrata.

4.2.2.1 Pushansiber Kemhan RI.

Menurut perspektif Pushansiber Kemhan, terdapat beberapa faktor pendukung, antara lain: dengan dilibatkannya Pushansiber Kemhan dalam berbagai kegiatan yang tidak (belum) terprogram yang diselenggarakan BSSN, antara lain: seminar, FGD, maupun *cybersecurity drill test* untuk sektor pemerintah (wawancara di Pushansiber Kemhan, pada 3 September 2020).

Gambar 4.13 Pushansiber KEMHAN Hadiri *Cybersecurity Drill Test* BSSN Untuk Sektor Pemerintah

Sumber: kemhan.go.id/bainstrahan (2019)

Kegiatan tersebut dipandang relevan (mendukung) terhadap upaya membangun kompetensi SDM pertahanan siber. Selain itu, meskipun belum tersedianya *roadmap* pembangunan kompetensi SDM pertahanan siber, namun hal tersebut tidak menjadi kendala tuntutan tugas dan fungsi, sehingga telah diantisipasi oleh pejabat pimpinan Pushansiber Kemhan yang baru melalui program *quick win* untuk kurun waktu 3 (tiga) bulan yang di dalamnya antara lain mencakup aspek upaya membangun kompetensi

SDM pertahanan siber, antara lain dengan melakukan *asessment* terhadap SDM pertahanan siber (berdasarkan peran dan fungsi). Pelaksanaannya dibantu dari pihak mitra (non BSSN).

Gambar 4.14 Pushansiber KEMHAN Hadiri *FGD Kajian Strategi Organisasi BSSN Dalam Mengkonsolidasi Unsur Keamanan Siber*

Sumber: kemhan.go.id/bainstrahan (2019)

Sedangkan untuk faktor-faktor penghambat (wawancara di Pushansiber Kemhan, pada 3 September 2020), antara lain: a) belum ada wujud/bentuk kerjasama terprogram antara Pushansiber Kemhan dengan BSSN yang relevan terhadap upaya membangun kompetensi SDM pertahanan siber, baik untuk jangka pendek, menengah, dan panjang; b) belum optimalnya komunikasi dan koordinasi antara Pushansiber Kemhan dengan BSSN; c) Kedua institusi (baik BSSN maupun Pushansiber Kemhan) masih sama-sama baru terbentuk; d) belum adanya realisasi alokasi anggaran untuk program kerja kedua instansi tersebut hingga 2019/2020; e) belum ada pedoman tata kelola (manajemen) SDM pertahanan siber. Terkait poin a) di atas, upaya kerjasama tersebut belum menyentuh aspek membangun kompetensi SDM pertahanan siber, dan itupun masih bersifat kunjungan koordinasi BSSN terkait identifikasi sektor infrastruktur informasi kritikal nasional (IIKN).

Gambar 4.15 Pushansiber KEMHAN Menerima Kunjungan BSSN Terkait Koordinasi Identifikasi Sektor IIKN

Sumber: kemhan.go.id/bainstrahan (2019)

4.2.2.2 Satsiber TNI.

Satsiber TNI berpandangan bahwa terdapat beberapa faktor yang selaras dengan tata kelola pembangunan kompetensi SDM keamanan siber (menurut konsep SKSN 2020-2024 rumusan BSSN) sekaligus mendukung terwujudya kompetensi SDM pertahanan siber (wawancara di Satsiber TNI, pada 11 September 2020), antara lain: a) Nota Kesepahaman (MoU) antara Satsiber TNI dengan BSSN telah resmi disepakati pada tahun 2018. MoU tersebut menjadi pedoman dalam mengatur rencana kerja sama dalam hal penguatan keamanan siber dan persandian di lingkungan TNI, di mana salah satu dari 6 (enam) ruang lingkupnya adalah terkait dengan peningkatan dan pengembangan SDM; b) Satsiber TNI telah dilibatkan dalam berbagai kegiatan tidak terprogram yang diselenggarakan BSSN (antara lain seminar dan FGD serta kegiatan *cybersecurity drill test*). Kegiatan tersebut dipandang relevan (mendukung) terhadap upaya membangun SDM pertahanan siber.

Gambar 4.16 Tim Siber TNI Melaksanakan Latihan ISTX

Sumber: penabali.com/berita (2019)

Dalam hal pemenuhan kebutuhan SDM pertahanan siber, Satsiber TNI telah menyiapkan proposal rencana program peningkatan kompetensi SDM pertahanan siber dan menyerahkan sepenuhnya kepada satuan kerja terkait, dalam hal ini adalah staf Panglima TNI bidang perencanaan dan anggaran, bidang personel, serta bidang pendidikan dan latihan. Meskipun proposal tersebut telah diajukan ke pimpinan, namun sampai saat ini belum ada tindak lanjut (wawancara di Satsiber TNI, pada 11 September 2020).

Satsiber TNI juga menilai bahwa SKSN penting bagi Indonesia, tidak hanya untuk kepentingan membangun keamanan siber secara nasional, namun juga terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Namun demikian, disamping faktor-faktor pendukung sebagaimana uraian di atas, maka untuk saat ini, masih terdapat faktor-faktor yang menghambat (wawancara di Satsiber TNI, pada 11 September 2020), antara lain: a) ketika pemerintah selaku regulator menyusun suatu kebijakan atau aturan yang relevan dengan hal-hal membangun kompetensi SDM, maka yang sering terjadi adalah belum adanya persamaan persepsi terhadap konteks SDM TIK (perspektif

Kominfo), SDM Keamanan Siber (perspektif BSSN), dan SDM Pertahanan Siber (perspektif bidang Pertahanan dan TNI); b) konsep regulasi perlu diturunkan atau dijabarkan dalam aturan-aturan pelaksanaan yang aplikatif dan komprehensif sesuai kebutuhan di lapangan; c) sejak nota kesepahaman (MoU) antara Satsiber TNI dengan BSSN, sampai saat ini masih belum ada tindak lanjut (*follow up*); d) belum ada pedoman tata kelola SDM pertahanan siber. Pandangan Satsiber TNI khususnya pada poin b) tersebut, adalah relevan dengan uraian gambaran umum obyek penelitian di lapangan tentang fakta situasi tata kelola (manajemen) dalam hal pembangunan kompetensi SDM TIK, SDM keamanan siber, dan SDM pertahanan siber yang satu sama lain relatif masih belum komprehensif, belum integratif, dan belum berkesinambungan.

4.2.2.3 Balitbang SDM Kemenkominfo RI.

Sebagai bagian dari pemerintah, khususnya regulator dalam bidang komunikasi dan informatika, Kementerian Kominfo RI belum mengetahui sepenuhnya tentang konsep SKSN 2020-2024 hasil rumusan BSSN maupun konsep SKSN yang dalam penyempurnaan. Terlebih dengan masih baru dibentuknya kelembagaan BSSN, maka Kominfo belum mampu memberikan pandangan tentang faktor-faktor yang mendukung maupun yang penghambat tata kelola strategi pembangunan kompetensi SDM keamanan siber dalam konsep SKSN 2020-2024 rumusan BSSN tersebut mampu mendukung kepentingan bidang pertahanan untuk mewujudkan kompetensi SDM pertahanan siber (wawancara *online*, pada 8 September 2020). Dari uraian tersebut peneliti berpendapat bahwa di dalam proses perumusan SKSN, tampaknya tidak sepenuhnya instansi terkait seperti Kominfo mengetahui hal tersebut, meski sepanjang pengetahuan peneliti beberapa instansi terkait diundang untuk terlibat di dalam proses perumusannya. Dalam hal ini terdapat masalah, mengapa hal tersebut

terjadi, adalah karena orang yang mewakili bukan dari bidang Balitbang SDM Kominfo.

4.2.2.4 BSSN

BSSN menyampaikan bahwa konsep SKSN 2020-2024 hasil rumusan BSSN telah disempurnakan dan diperbaiki BSSN sebagai konsep SKSN perbaikan (wawancara *online*, pada 11 dan 13 September 2020). Pada konsep perbaikan tersebut, telah dilakukan berbagai penyempurnaan dan perbakan terhadap 5 (lima) pilar yang ada pada konsep SKSN 2020-2024 rumusan BSSN. Bila dikaitkan dengan aspek peningkatan kompetensi SDM keamanan siber, maka perbaikan yang dilakukan telah diakomodir, di mana hal-hal yang bekenaan dengan upaya membangun kompetensi SDM keamanan siber nasional, telah dimasukan seluruhnya ke dalam pilar ke 3 (tiga) yaitu: pembangunan kapasitas dan budaya keamanan siber. Strategi dalam pembangunan kompetensi SDM keamanan siber nasional tersebut ditujukan untuk seluruh SDM nasional, baik di lingkungan pemerintah maupun masyarakat umum, (termasuk TNI/Polri) dalam bentuk berbagai macam kegiatan dan praktik latihan bertajuk membangun keamanan siber nasional yang antara lain: *cybersecurity drill test* maupun kegiatan serupa itu.

Aspek pembangunan kompetensi SDM keamanan siber nasional dalam konsep SKSN perbaikan, disusun dan dirumuskan secara *real* atau benar-benar sejalan (*in line*) dengan program-program pembangunan index keamanan siber nasional yang di *publish* oleh organisasi *International Telecomunication Union* (ITU) melalui *Global Cybersecurity Index* (GCI), dengan tujuan agar implementasi dari program-program strategis dalam konsep SKSN perbaikan tersebut benar-benar berperanan penting kepada peningkatan *index* keamanan siber nasional.

Tersusunnya dokumen *Roadmap* Pembinaan SDM Siber dan Sandi 2020-2024 juga dipandang mendukung konsep SKSN 2020-2024. Sebagaimana telah diutarakan bahwa selain untuk mendukung upaya peningkatan kompetensi SDM keamanan siber pada konsep SKSN perbaikan, berarti setidaknya *roadmap* inipun dinilai akan mampu memenuhi sebagian besar kriteria standar kompetensi kebutuhan SDM pertahanan siber yang dipersyaratkan/dibutuhkan/diperlukan.

Berkenaan dengan faktor-faktor yang menghambat (wawancara *online*, pada 11 dan 13 September 2020), BSSN berpandangan bahwa oleh karena situasi BSSN yang baru terbentuk di tahun 2017 berdasarkan Perpres RI Nomor 53 tahun 2017 tentang BSSN, dan kemudian diperkuat kembali pada tahun 2018 berdasarkan Perpres RI Nomor 133 tahun 2017 tentang BSSN. Dengan masih barunya kelembagan BSSN tersebut, tentu akan mempengaruhi kesiapan aspek-aspek fungsi dasar manajemen yang dibebankan atau menjadi tanggung jawab BSSN dalam membangun keamanan siber nasional, khususnya dalam hal tata kelola membangun kompetensi SDM keamanan siber nasional yang nota bene *output* dan *outcome*-nya juga sangat diperlukan bidang-bidang lain pemerintahan, termasuk dalam hal ini bidang pertahanan negara yang ingin mewujudkan kompetensi SDM pertahanan siber untuk sishankamrata. Faktor penghambat lainnya adalah bahwa meski konsep SKSN 2020-2024 hasil rumusan BSSN telah tersusun, serta telah dilakukan beberapa perbaikan dan penyempurnaan sebagai konsep SKSN perbaikan (penyempurnaan konsep SKSN 2020-2024), namun hingga saat ini, status konsep-konsep tersebut masih sebagai konsep semata, dan yang paling krusial adalah belum menjadi suatu bentuk ketentuan atau peraturan nasional. Akibatnya konsep SKSN rumusan BSSN tersebut masih belum menjadi atensi bagi seluruh pemangku kepentingan siber (termasuk dalam hal ini bidang pertahanan) di Indonesia. Sebenarnya hal-hal tersebut menunjukan adanya urgensi untuk segera terwujudnya SKSN, karena akan selalu menjadi

penghambat dalam implementasi akibat belum tersedianya standar-standar dan regulasi-regulasi di bidang keamanan siber yang berakibat pada timbulnya *overlaping* dan/atau tumpang tindih kepentingan antar instansi.

4.2.3 Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan Sishankamrata.

Pada sub fokus ini, hasil penelitian yang diperoleh berupa perspektif dan pandangan umum (gambaran dan/atau deskripsi) serta pendapat yang bersumber dari subyek-subyek penelitian, berkenaan dengan praktik-praktik kegiatan operasional pendidikan maupun latihan yang relevan dengan keamanan siber, dan yang selaras dengan tata kelola (manajemen) peningkatan kompetensi SDM keamanan siber (dalam konsep SKSN 2020-2024 rumusan BSSN), dan yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

4.2.3.1 Pushansiber Kemhan RI.

Pushansiber KEMHAN telah dilibatkan dalam kegiatan praktik keamanan siber (wawancara di Pushansiber Kemhan, pada 3 September 2020), yaitu: *cyber security drill test* yang diselenggarakan oleh BSSN pada tahun 2019. Dalam kegiatan tersebut, peserta *drill test* yang terlibat berasal dari berbagai instansi pemerintah (kementerian, lembaga, dan pemerintah daerah). Materi dalam praktek-praktek latihan adalah bertujuan untuk melatih bagaimana respon yang diambil oleh setiap instansi ketika terjadi insiden keamanan siber, termasuk melatih bagaimana prosedur, *interoperability* dan koordinasi serta teknis isian format pelaporan. Kepada Pusat Operasi Keamanan Siber Nasional (Pusopskamsibernas BSSN sebagai *leading sector*)

Gambar 4.17 Perolehan *Score Cybersecurity Drill Test*

Sumber: Laporan Kegiatan *Cybersecurity Drill Test* II *Government Sector* Tahun 2019 oleh Pushansiber Kemhan

Sebagai tambahan, menurut perspektif Pushansiber Kemhan, *Output* dan *Outcome* pasca kegiatan *cybersecurity drill test* tersebut masih belum tampak. Hal tersebut cukup beralasan karena sepanjang Pushansiber Kemhan menjalankan peran tugas dan fungsi rutin dalam pelaksanaan monitoring keamanan siber di lingkungan Kemhan, manakala terpantau ada anomali *cyber security*, maka mekanisme pelaporan sebagaimaa telah dilatihkan pada kegiatan *cybersecurity drill test* tersebut masih belum diaktualisasikan oleh Pushansiber Kemhan (wawancara di Pushansiber Kemhan, pada 3 September 2020).

4.2.3.2 Satsiber TNI.

Menurut perspektif Satsiber TNI, bahwa terdapat berbagai macam praktik kegiatan operasional dan latihan yang aplikatif dalam bidang keamanan siber (yang relevan dengan konsep SKSN) yang dinilai mendukung upaya bidang pertahanan dalam mewujudkan kompetensi SDM pertahanan siber. Beberapa praktik aplikatif tersebut antara lain: kegiatan *cybersecurity drill test* yang diselenggarakan BSSN pada tahun 2018. Kegiatan tersebut pernah diikuti oleh tim Satsiber TNI hanya sekali saja. Selain itu tim SDM Satsiber TNI juga dilibatkan dalam latihan bersama

Cobra Gold Exercise pada tahun 2018 dan 2019 (wawancara di Satsiber TNI, pada 11 September 2020).

Gambar 4.18 Kegiatan Latma *Cobra Gold Exercise* 2019 di Thailand

Sumber: beritasatu.com (2019)

Dalam kegiatan latihan bersama *Cobra Gold* pada tahun 2018 dan 2019, materi *cyber security* menjadi salah satu materi latihan diantara materi-materi latihan lainnya. Dalam skenario latihan, materi *cybersecurity* yang dilatihkan bertujuan untuk melatih para pelaku latihan (SDM) untuk mampu menghadapi adanya ancaman siber terhadap jaringan (*network*) yang dimiliki oleh kekuatan pasukan multinasional. Dari hal tersebut, peneliti berpendapat bahwa materi latihan *cybersecurity* merupakan materi yang tidak berdiri sendiri. Materi *cybersecurity* yang dilatihkan tersebut terbukti ber-*interoperability* dengan materi-materi latihan lainnya. Demikian halnya dengan kenyataan sebenarnya, implementasi praktik opersional keamanan siber dalam kehidupan sehari-hari tentu tidak berdiri sendiri, terdapat sinergitas dalam penyelenggaraan operasional keamanan siber dengan operasional-operasional non keamanan siber lainnya dalam satu situasi dan kondisi tertentu. Peneliti berpandangan juga bahwa interoperabilitas yang bersifat kompleks tersebut memang menjadi suatu bentuk praktik-praktik yang hanya bisa diraih melalui kegiatan pelatihan secara berkesinambungan sehingga mampu mendukung peningkatan kompetensi SDM pertahanan siber.

4.2.3.3 Balitbang SDM Kemenkominfo RI.

Dalam perspektif Kominfo (wawancara *online*, pada 8 Sptember 2020), praktik-praktik semacam kegiatan operasional maupun pelatihan yang relevan dengan aspek keamanan siber yang kemudian mendukung upaya terwujudnya kompetensi SDM pertahanan siber, antara lain adalah melalui kegiatan kompetisi *cyber jawara*, kegiatan pelatihan intensif *Digital Talent Scholarship* (DTS) Kominfo dan program beasiswa *Government Chief Information Officer* (G-CIO).

Gambar 4.19 Kegiatan *Cyber* Jawara Tahun 2015

Sumber: facebook.com/ Cyber Security IPB (2015)

Kegiatan kompetisi *Cyber* Jawara, adalah kompetisi tahunan di bidang keamanan siber yang sejak awal pertama diinisiasi oleh Id-SIRTII Kominfo sejak tahun 2012 dengan peserta terbuka untuk umum. Materi yang diperlombakan dalam kompetisi tersebut antara lain: *computer network defense (*yaitu mengatur pengamanan pada *server* sendiri dan pada saat yang sama berusaha menembus pengamanan pada server lawan), *penetration testing* (yaitu berusaha menembus keamanan *server* target yang telah ditentukan untuk mendapatkan data yang dilindungi), dan *capture the flag* (yaitu *problem solving* beragam *challenge* terkait keamanan siber, untuk mendapatkan poin sebanyak-banyaknya).

Gambar 4.20 Program DTS Kominfo Tahun 2020

Sumber: digitalent.kominfo.go.id (2020)

Program kegiatan *Digital Talent Scholarship* (DTS) Kominfo (wawancara *online*, pada 8 Sptember 2020), yaitu program beasiswa pelatihan intensif yang bertujuan untuk meningkatkan keterampilan dan daya saing SDM bidang TIK sebagai bagian dari program pembangunan prioritas nasional. Program pelatihan dikelompokan sebagai berikut: a) *Fresh Graduate Academy* (FGA), program pelatihan berbasis industri bagi lulusan S1 bidang TIK dan MIPA, terbuka bagi penyandang disabilitas; b) *Vocational School Graduate Academy* (VSGA), program pelatihan berbasis kompetensi nasional bagi lulusan SMK dan Pendidikan Vokasi bidang TI, Telekomunikasi, Desain, dan Multimedia; c) *Coding Teacher Academy* (CTA), program pelatihan pengembangan SDM Guru tingkat SD/SMP/MA/SMK/SMA; d) *Online Academy* (OA), program pelatihan *online* bagi masyarakat umum termasuk ASN, mahasiswa, dan pelaku industri; e) *Thematic Academy* (TA), program pelatihan multi disiplin bagi pengembangan SDM; f) *Regional Development Academy* (RDA), program pelatihan pengembangan SDM untuk meningkatkan kompetensi ASN di Kawasan Prioritas Pariwisata dan Kabupaten Prioritas Pembangunan; g) *Digital Entrepreneurship Academy* (DEA), program pelatihan pengembangan SDM yang talenta digital di bidang Usaha Mikro, Kecil, dan Menengah (UMKM).

Gambar 4.21 Sosialisasi Bimtek G-CIO Kominfo Tahun 2017

Sumber: proserti.kominfo.go.id/ Kominfo (2017)

Government CIO merupakan kegiatan bersifat bimbingan teknis (bimtek), di mana sasaran bimtek atau Pelatihan G-CIO ini adalah untuk penyiapan pejabat pemerintah yang bertanggungjawab dalam memimpin pengelolaan infrastruktur teknologi informasi di berbagai lembaga pemerintah dalam pengembangan *e-Government*, dan membantu penyediaan calon-calon Pejabat Pengelola Informasi dan Dokumentasi (PPID) di seluruh Indonesia, sedangkan untuk program jangka panjangnya, dilaksanakan melalui pemberian beasiswa pendidikan S2 Program Studi CIO di lima perguruan tinggi yaitu: ITB, ITS, UGM, UI dan UNP.

4.2.3.4 BSSN

BSSN berpandangan bahwa praktik-praktik yang aplikatif dan mendukung peningkatan kompetensi SDM keamanan siber sebagaimana konsep SKSN, salah satunya adalah kegiatan kegiatan *cybersecurity drill test* yang telah diselenggarakan BSSN sejak 2018 (wawancara *online*, pada 11 dan 13 Sptember 2020). Aspek peningkatan kompetensi SDM pada praktik kegiatan *cybersecurity drill test* tersebut adalah relevan dan tercantum di dalam dokumen konsep SKSN perbaikan, pada pilar ke 3 (tiga) yaitu: pembangunan kapasitas dan budaya keamanan siber, bagian ke

lima: yaitu membangun budaya keamanan siber, melalui literasi dan kampanye keamanan siber, sehingga terbentuk kesadaran keamanan siber terhadap *quarter helix* (pemerintah, swasta, akademisi, maupun masyarakat umum).

Gambar 4.22 BSSN *Cybersecurity Drill Test* (Sektor Pemerintah)

Sumber: bssn.go.id (2019)

Dalam kegiatan *cybersecurity drill test*, dilaksanakan latihan dalam bentuk praktik-praktik penanggulangan dan pemulihan insiden keamanan siber sebagai salah satu kegiatan utama dalam pengelolaan siber yang membutuhkan partisipasi aktif dari berbagai pihak. Praktik kolaborasi dan sinergitas menjadi hal mutlak dan wajib dilakukan dalam pengelolaan insiden siber, hal tersebut bertujuan membangun kerjasama dan interoperabiliti penanggulangan insiden siber. Kegiatan tersebut bertujuan untuk memberikan pemahaman, pengalaman, serta meningkatkan koordinasi dan komunikasi antara BSSN dengan seluruh *stakeholder* terkait, khususnya pada sektor pemerintah. Kegiatan ini diharapkan mampu meningkatkan kompetensi SDM dalam rangka penanggulangan dan pemulihan insiden keamanan siber secara nasional.

Dalam dokumen *Roadmap* Pembinaan SDM Keamanan Siber dan Sandi 2020-2024 (Menuju SDM Keamanan Siber dan Sandi Yang Terpercaya, Profesional, dan Berdaya Saing), terdapat juga program kegiatan praktik-praktik latihan keamanan siber yang aplikatif dalam kerangka pengembangan kompetensi, antara lain: *talent scouting* dan

pembinaan bidang keamanan siber untuk generasi muda dan mahasiswa dalam bentuk penyelenggaraan kompetisi (*capture the flag*, *cyber war game*, *cyber jawara*), *cybersecurity job fair*, serta kompetisi keamanan siber untuk ASN, TNI, dan Polri.

4.3 Pembahasan.

Pada bagian sebelumnya telah disampaikan pandangan-pandangan tentang teori manajemen menurut beberapa ahli seperti: John D. Millet, Hasibuan, dan George R. Terry, yang kemudian oleh peneliti dirangkum sebagai berikut: bahwa yang dimaksud dengan manajemen (atau dapat disebut juga sebagai tata kelola), adalah ilmu yang mengatur proses untuk mencapai tujuan yang telah ditetapkan sebelumnya guna mencapai tujuan sesuai rencana. Pada pembahasan ini, fungsi dasar manajemen yang meliputi POAC, juga akan dimanfaatkan sebagai alat bantu analisis terhadap proses tata kelola peningkatan kompetensi SDM keamanan siber (merujuk pada konsep SKSN rumusan BSSN) dalam mendukung upaya bidang pertahanan mewujudkan kompetensi SDM pertahanan siber. Selain itu hasil dari analisa tersebut juga diharapkan juga mampu menjawab urgensi SKSN dalam mendukung sishankamrata.

Untuk operasionalisasi teori manajemen George R. Terry, maka peneliti telah membagi data hasil penelitian ke dalam dua kelompok Faktor (F) kualitatif, yaitu: Faktor – 1 (F_1) untuk tata kelola kompetensi SDM TIK nasional (data dari subyek penelitian Balitbang SDM Kominfo) dan tata kelola kompetensi SDM keamanan siber (data dari subyek penelitian BSSN) yang akan dianalisis aspek fungsi dasar manajemen (POAC) nya terhadap Faktor – 2 (F_2) kompetensi SDM pertahanan siber (data dari subyek penelitian Pushansiber Kemhan dan Satsiber TNI) sebagai target capaian yang juga akan dianalisis fungsi dasar manajemen (POAC) nya.

Dalam pembahasan ini, proses tata kelola dalam membangun kompetensi SDM TIK nasional, ditempatkan peneliti sebagai F_1 bersama tata kelola peningkatan kompetensi SDM keamanan siber Hal tersebut dengan pertimbangan bahwa kompetensi SDM TIK nasional merupakan kompetensi awal (*basic*) untuk peningkatan kompetesi SDM keamanan siber, di mana kemudian keduanya (baik kompetensi SDM TIK nasional maupun kompetensi SDM keamanan siber) menjadi prasyarat utama dan penting dalam proses lanjut membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

4.3.1 Analisis Prinsip POAC Berkenaan Dengan Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata.

Pada bagian ini, prinsip POAC digunakan untuk menganalisis terhadap eksistensi *roadmap* atau program kegiatan pembangunan kompetensi SDM oleh masing-masing subyek penelitian, apakah sudah merujuk atau berafiliasi dengan strategi peningkatan kompetensi SDM keamanan siber (pada konsep SKSN 2020-2024 rumusan BSSN), dan yang relevan terhadap peningkatan kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Berdasarkan hasil penelitian, maka peneliti mengambil dan menyusun beberapa poin yang dianggap penting dan relevan untuk dituangkan ke dalam suatu tabel matrik untuk dianalisis prinsip-prinsip POAC-nya.

Untuk aspek *planning* (perencanaan) dalam matrik ini menempatkan *roadmap* terkait program kegiatan pembangunan kompetensi SDM pada masing-masing subyek penelitian sebagai salah satu faktor dalam proses untuk mencapai tujuan setiap organisasi dari subyek penelitian tersebut. Analisis aspek *planning* oleh peneliti adalah berdasarkan kepada 3 (tiga) aspek, yaitu: eksistensi, substansi, dan signifikansi, sebagai berikut: a)

untuk eksistensi adalah ada atau tidaknya *roadmap* di setiap subyek penelitian; b) untuk substansi adalah berafiliasi atau tidaknya *roadmap* satu dengan yang lain, namun yang lebih khusus adalah berafiliasi atau tidaknya *roadmap* setiap subyek penelitian dengan aspek peningkatan kompetensi SDM keamanan siber pada konsep SKSN rumusan BSSN (dalam menilai substansi, peneliti menempatkan materi pendidikan dan latihan sebagai yang utama); dan c) untuk signifikansi adalah apakah setiap *roadmap* dari masing-masing obyek penelitian menunjang upaya peningkatan kompetensi SDM pertahanan siber.

Untuk aspek *organizing* (pengorganisasian) dalam matrik ini analisis dilakukan terhadap bagaimana subyek penelitian dalam mengorganisir implementasi *roadmap* terkait program kegiatan pembangunan kompetensi SDM masing-masing guna tercapainya tujuan organisasinya. Analisis aspek *organizing* oleh peneliti adalah berdasarkan kepada aspek peran serta, yaitu wujud peran serta atau pelibatan setiap subyek penelitian di dalamnya. Tentu dalam hal melaksanakan analisis terhadap aspek *organizing* ini tidak mengabaikan aspek sebelumnya, yaitu aspek *planning*.

Untuk aspek *actuating* (pelaksanaan) dalam matrik ini analisis dilakukan untuk bagaimana setiap subyek penelitian mengaktualisasikan *roadmap* terkait program kegiatan pembangunan kompetensi SDM masing-masing dalam mencapai tujuan organisasinya. Analisis aspek *actuating* oleh peneliti adalah berdasarkan kepada aspek wujud atau bentuk pelaksanaannya, yaitu bagaimana wujud/bentuk kegiatan pendidikan dan latihan dalam rangka peningkatan kompetensi SDM masing-masing subyek penelitian diaktualisasikan. Dan tentu dalam hal melaksanakan analisis terhadap aspek *actuating* ini juga tidak mengabaikan aspek sebelumnya, yaitu aspek *planning* maupun *organizing*.

Untuk aspek *controlling* (pengawasan) pada matrik implementasi POAC ini, analisis dilakukan untuk bagaimana setiap subyek penelitian menjalankan atau melaksanakan fungsi kontrol dan pengawasan terhadap implementasi *roadmap* terkait program kegiatan pembangunan kompetensi SDM masing-masing guna tercapainya tujuan organisasi. Analisis aspek *controlling* oleh peneliti adalah terkait adanya standar kompetensi SDM capaian. Dalam hal melaksanakan analisis aspek *controlling* ini, peneliti tidak mengabaikan aspek sebelumnya, yaitu aspek *planning*, *organizing* dan *actuating*.

Tabel 4.1 Matrik Implementasi POAC Pada F_1 Yang Relevan Dengan Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Aspek *Roadmap* atau Program Peningkatan Kompetensi SDM			
Balitbang SDM Kominfo			
Sudah ada dan merujuk pada *Roadmap* Pembangunan Sektor TIK Nasional 2016-2045. *Roadmap* tidak (belum) berafiliasi pada konsep SKSN Fokus pada pembangunan SDM TIK nasional yang dimungkinkan untuk ditingkatkan kompetensinya menjadi SDM keamanan siber maupun SDM pertahanan siber	Pelaksana Balitbang SDM Kominfo bekerjasama dan/atau dibantu pihak terkait lainnya melibatkan SDM peserta pendidikan dan latihan berasal dari lingkungan instansi pemerintah, kalangan swasta, dan masyarakat umum	Melalui berbagai program pengembangan kompetensi SDM TIK yang materinya bersifat pendidikan dan latihan, antara lain: Program *Digital Talent Scholarship* (DTS) dan Program Beasiswa *Government Chief Information* (G-CIO)	Sebagai kontrol mengikuti standar kompetensi SDM TIK Berbasis Sertifikasi SKKNI Bidang Kominfo
BSSN			
Roadmap Pembinaan SDM Keamanan Siber dan Sandi 2020 – 2024 (Menuju SDM Keamanan Siber & Sandi Yang Terpercaya, Profesional, dan Berdaya Saing.	Pelaksana adalah Direktorat Pengendalian SDM, Deputi Bidang Pemantauan dan Pengendalian, bekerjasama dan/atau dibantu pihak terkait lainnya melibatkan SDM	Telah, sedang, dan akan dilaksanakan, antara lain: Penyiapan Standardisasi SDM, pembentukan organisasi profesi, pembentukan LSP, *integrated* Sisfo, pengembangan kurikulum diklat, *R& D*,	Sebagai kontrol pelaksanaan pembinaan kompetensi SDM keamanan siber merujuk pada *roadmap* pembinaan SDM keamanan siber dan sandi 2020-2024 maupun dokumen Peta Okupasi

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Sudah berafiliasi dengan konsep SKSN 2020-2024 maupun konsep SKSN perbaikan. Pembinaan kompetensi SDM keamanan siber dalam *roadmap* fokus/ bertujuan pd tercapainya SDM unggul di bidang keamanan siber	peserta dari lingkungan instansi pemerintah	pengembangan kompetensi, pemenuhan sertifikasi, monitoring & evaluasi, *cybersecurity education* pada pendidikan dasar & menengah, pusdiklat sebagai *corporate university*, dan STSN sebagai *centre of excelent*.	Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber

Sumber: diolah peneliti

Berikut adalah matrik analisis implementasi POAC terkait *roadmap* atau program peningkatan kompetensi SDM pada Faktor-2 (F_2) kualitatif meliputi kompetensi SDM pertahanan siber terhadap kompetensi SDM TIK nasional dan kompetensi SDM keamanan siber.

Tabel 4.2 Matrik Implementasi POAC Pada F_2 Yang Relevan Dengan Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Aspek *Roadmap* atau Program Peningkatan Kompetensi SDM			
Pushansiber Kemhan RI			
Belum ada *Roadmap* atau program kerja khusus terkait Pembangunan Kapasitas SDM Pertahanan siber nasional	Terlibat aktif sebagai peserta pada kegiatan pendidikan dan latihan keamanan siber yang diselenggarakan BSSN	*Cybersecurity Drill Test* tahun 2019 oleh BSSN	Sebagai kontrol masih mengikuti standar kompetensi SDM pertahanan siber yang merujuk pada Permenhan No.82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI Hasil partisipasi belum mencapai target kompetensi SDM pertahanan siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Satsiber TNI			
Belum ada *Roadmap* atau program kerja khusus terkait Pembangunan Kapasitas SDM Pertahanan siber nasional	a) Mabes TNI melalui Sops TNI sebagai pelaksana kegiatan pendidikan dan latihan yang menunjang peningkatan SDM pertahanan siber (masih terbatas dan insidentil) b) Terlibat aktif sebagai peserta pada kegiatan pendidikan dan latihan keamanan siber yang diselenggarakan BSSN	a) Latihan bersama *Cobra Gold* tahun 2018 dan 2019, Latihan ISTX b) *Cybersecurity Drill Test* 2018 oleh BSSN	Sebagai kontrol masih mengikuti standar kompetensi SDM pertahanan siber yang merujuk pada Permenhan No.82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI Hasil partisipasi belum mencapai target kompetensi SDM pertahanan siber

Sumber: diolah peneliti

Berdasarkan matrik analisis prinsip POAC pada tabel 4.1 dan 4.2 di atas, diperoleh hal-hal sebagai berikut:

a. Aspek *Planning* (perencanaan). Perencanaan pembangunan kompetensi SDM belum optimal, dengan masih adanya subyek yang belum memiliki *roadmap* (program) pembangunan kompetensi SDM. *Roadmap* pembinaan SDM keamanan siber BSSN yang berafiliasi dengan konsep SKSN, hal tersebut menunjukan belum terwujudnya kolaborasi antar subyek penelitian dalam penyusunan perencanaan pembangunan kompetensi SDM. *Roadmap* pembangunan kompetensi SDM dan kolaborasi dalam perencanaannya adalah penting, terutama untuk bidang pertahanan yang sangat bergantung pada ketersediaan *basic* kompetensi SDM TIK nasional dan yang telah ditingkatkan sebagai SDM keamanan siber. Seluruh subyek penelitian sependapat bahwa untuk mendukung terwujudnya kompetensi SDM pertahanan siber, sehingga eksistensi SKSN menjadi urgen dan penting dalam menjembatani kolaborasi dan

interoperabiliti aspek perencaan terhadap upaya membangun kompetensi SDM pertahanan siber.

b. Aspek *Organizing* (pengorganisasian). Setiap subyek penelitian mengorganisir upaya pembangunan kompetensi SDMnya masing-masing, meski dalam beberapa hal terjadi semacam *cross action* di mana subyek lain secara langsung maupun tidak langsung membantu aspek pengorganisasian yang dilakukan subyek penelitian lainnya. Pelibatan tersebut lazimnya dalam bentuk konsultasi dan supervisi maupun untuk dilibatkan sebagai pendukung maupun peserta kegiatan yang diorganisir subyek lain sebagai penyelenggara. Hal tersebut di atas menunjukan bahwa kolaborasi dan interoperabiliti dalam mengorganisir pelaksanaan kegiatan peningkatan kompetensi SDM menjadi penting, sehingga eksistensi SKSN menjadi urgen dan penting dalam menjembatani terhadap upaya membangun kompetensi SDM pertahanan siber.

c. Aspek *Actuating* (pelaksanaan). Setiap subyek penelitian telah berupaya melaksanakan kegiatan pembangunan dan peningkatan kompetensi SDM masing-masing. Mesipun demikian, sebagaimana diuraikan aspek pengorganisasian, maka dalam beberapa hal terjadi *cross action* di mana subyek lain secara langsung maupun tidak langsung membantu aspek pelaksanaan yang diselenggarakan subyek penelitian lainnya, baik dalam bentukpemberian konsultasi dan supervisi pendidikan dan pelatihan maupun untuk terlibat sebagai peserta pendidikan dan pelatihan. Hal tersebut di atas menunjukan bahwa kolaborasi dan interoperabiliti dalam pelaksanaan kegiatan peningkatan kompetensi SDM menjadi penting, sehingga eksistensi SKSN menjadi penting dalam menjembatani aspek *actuating* terhadap upaya membangun kompetensi SDM pertahanan siber.

d. Aspek *Controlling* (pengawasan). Setiap subyek penelitian melaksanakan aspek pengawasan terhadap pelaksanaan kegiatan pendidikan dan pelatihan berkenaan dengan upaya peningkatan kompetensi SDMnya masing-masing. Pengawasan yang dilakukan setiap subyek adalah merujuk kepada standar capaian kompetensi SDM masing-masing, sehingga yang terjadi kususnya untuk bidang pertahanan, *output* dan *outcome* dari pelaksanaan kegiatan pendidikan dan pelatihan untuk SDM pertahanan siber (semua bentuk kegiatan pendidikan dan latihan termasuk yang diselenggarakan BSSN), adalah masih jauh dari standar pencapaian kompetensi. Hal tersebut karena terdapat standar capaian yang sangat fundamental dalam kompetensi SDM pertahanan siber yang belum mampu dipenuhi pada kompetensi SDM TIK nasional maupun kompetensi SDM keamanan siber. Standar spesifik pada kompetensi SDM keamanan siber adalah *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM TIK maupun SDM keamanan siber yang ditransformasikan menjadi SDM dengan kompetensi pertahanan siber yang sangat dibutuhkan bidang pertahanan (TNI), khsususnya ketika pertahanan siber diaktualisasikan untuk tugas-tugas hanneg dalam suatu *theatre* sishankamrata (perang semesta) dan atau dalam bentuk gelar operasi militer, di mana alut sista strategis TNI yang berbasis TIK harus dipertahankan (misal: *Network Centric Warfare*) dan/atau alut sista TNI yang berbasis TIK dioperasionalkan (sebagai *cyber weapon*) untuk tujuan melakukan serangan-serangan siber terhadap ancaman siber lawan. Hal tersebut tentu menunjukan bahwa kompetensi SDM pertahanan siber memiliki spesifikasi kompetensi yang kental dengan berbagai aspek dan dinamika dalam bidang hanneg (taktis, operasional, dan strategis). Hal tersebut di atas menunjukan bahwa kolaborasi dan interoperabiliti dalam pengaturan standar pencapaian kompetensi SDM dalam

pelaksanaan kegiatan pendidikan dan pelatihan yang saling berkolaborasi juga menjadi penting. Dan oleh karena itu eksistensi SKSN menjadi penting dalam menjembatani aspek *controlling* terhadap upaya membangun kompetensi SDM pertahanan siber.

Berdasarkan hasil penelitian maupun pembahasan melalui matrik analisis prinsip POAC terhadap bagaimana setiap subyek penelitian menyelenggarakan tata kelola kompetensi SDM-nya masing-masing menunjukan bahwa eksistensi SKSN memiliki peran dan fungsi penting bagi bidang pertahanan terhadap upaya membangun terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Peran dan fungsi penting SKSN tersebut adalah dalam hal memenuhi sebagian besar tuntutan kriteria kompetensi SDM pertahanan siber yang spesifik yang tidak mungkin mengandalkan kompetensi SDM TIK nasional.

4.3.2 Analisis Prinsip POAC Pada Faktor-Faktor Yang Mendukung Dan Menghambat SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan Sishankamrata.

Pada bagian ini, prinsip POAC digunakan untuk menganalisis faktor-faktor yang mendukung dan menghambat SKSN dalam mendukung upaya terwujudnya kompetensi SDM pertahanan siber. Peneliti mengambil dan menyusun beberapa poin penting dan relevan dari hasil penelitian ke dalam tabel matrik untuk dianalisis prinsip-prinsip POAC-nya.

Untuk aspek *planning* (perencanaan) dalam matrik ini menempatkan hal-hal seperti misalnya: konsep-konsep, dokumen, inisiasi, kegiatan-kegiatan kerjasama (kesepakatan), maupun situasi dan kondisi tertentu oleh setiap subyek penelitian dipandang sebagai faktor pendukung maupun penghambat SKSN dalam mendukung upaya membangun kompetensi SDM pertahanan siber. Analisis aspek *planning* oleh peneliti bersifat

subyektif dan obyektif sebagaimana pandangan setiap subyek penelitian terhadap obyek penelitian, namun dengan tetap mempertimbangkan bahwa hal-hal mengenai konsep-konsep, dokumen, inisiasi, kegiatan-kegiatan kerjasama (kesepakatan) sebagaimana tersebut di atas akan diasumsikan peneliti sebagai telah dilakukannya suatu fungsi perencanaan.

Untuk aspek *organizing* (pengorganisasian) dalam matrik ini analisis dilakukan terhadap bagaimana subyek penelitian dalam mengorganisir konsep-konsep, dokumen, inisiasi, kegiatan-kegiatan kerjasama (kesepakatan) maupun situasi dan kondisi yang relevan dengan pembangunan kompetensi SDM namun berdampak terhadap eksistensi SKSN. Analisis aspek *organizing* oleh peneliti adalah berdasarkan kepada aspek peran serta subyek-subyek penelitian di dalamnya. Tentu dalam hal melaksanakan analisis terhadap aspek *organizing* ini tidak mengabaikan aspek sebelumnya, yaitu aspek *planning*.

Untuk aspek *actuating* (pelaksanaan) dalam matrik ini analisis dilakukan untuk bagaimana subyek penelitian dalam mengaktualisasikan konsep-konsep, dokumen, inisiasi, kegiatan-kegiatan kerjasama (kesepakatan) maupun situasi dan kondisi yang relevan dengan pembangunan kompetensi SDM namun berdampak terhadap eksistensi SKSN. Analisis aspek *actuating* oleh peneliti adalah berdasarkan kepada aspek peran serta subyek-subyek penelitian di dalamnya. Tentu dalam hal melaksanakan analisis terhadap aspek *actuating* ini tidak mengabaikan aspek sebelumnya, yaitu aspek *planning* dan *organizing*.

Untuk aspek *controlling* (pengawasan) dalam matrik ini analisis dilakukan untuk bagaimana subyek penelitian dalam melaksanakan pengawasan terkait konsep-konsep, dokumen, inisiasi, kegiatan-kegiatan kerjasama (kesepakatan) maupun situasi dan kondisi yang relevan dengan pembangunan kompetensi SDM namun berdampak terhadap eksistensi

SKSN. Analisis aspek *controlling* oleh peneliti adalah terkait adanya rujukan dan standar pencapaian. Dalam hal melaksanakan analisis aspek *controlling* ini juga tidak mengabaikan aspek sebelumnya, yaitu aspek *planning*, *organizing* dan *actuating*.

Tabel 4.3 Matrik Implementasi POAC Pada F_1 dan F_2 Terkait Faktor-Faktor Pendukung dan Penghambat SKSN Terhadap Upaya Membangun SDM Pertahanan Siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Faktor-Faktor Pendukung SKSN			
Pushansiber Kemhan RI			
Punya program *Quick Win* Pushansiber yang esensinya mencakup aspek membangun kompetensi SDM pertahanan siber	Pushansiber Kemhan selaku pelaksana dan peserta	Kegiatan *assesment* peran dan fungsi SDM pertahanan siber di lingkungan Pushansiber Kemhan	Sebagai kontrol hasil masih berpedoman standar kompetensi SDM pertahanan siber yang merujuk pada Permenhan No.82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI Hasil belum mencapai target kompetensi SDM pertahanan siber
Satsiber TNI			
Faktor MoU (Nota Kesepahaman) antara Satsiber TNI dengan BSSN untuk mengatur rencana kerja sama tentang Penguatan Keamanan Siber dan Persandian di Lingkungan TNI, di mana salah satu dari 6 (enam) ruang lingkupnya adalah terkait dengan peningkatan dan pengembangan SDM. Faktor pelibatan Satsiber TNI telah dilibatkan dalam berbagai kegiatan tidak terprogram BSSN	a) Untuk MoU, baik Satsiber TNI dan BSSN bersama-sama selaku pelaksana b) Untuk seminar dan *cybersecurity drill test*, BSSN sebagai pelaksana	a) MoU belum teraktualisasikan b) Berbagai seminar dan *cybersecurity drill test* telah dilaksanakan	a) Kontrol belum dapat dilaksanakan karena SKSN masih dalam konsepperbaikan oleh BSSN b) Untuk Satsiber, sebagai kontrol hasil berpedoman pada standar kompetensi SDM pertahanan siber yang merujuk pada Permenhan No.82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI dan hasilnya belum memenuhi capaian standar kompetensi SDM pertahanan siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
(antara lain seminar dan *cybersecurity drill test*).			
Balitbang SDM Kominfo			
Adanya dokumen Penyusunan *Roadmap* Pembangunan Sektor TIK yang Mengikat Secara Jangka Panjang s.d 2045 Menuju 100 Tahun Indonesia Merdeka dan dokumen Rencana Pengembangan SDM TIK di Indonesia Melalui Sertifikasi SKKNI Bidang Kominfo Selian itu juga tersusun dokumen Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber	Pelaksana Balitbang SDM Kominfo bekerjasama dengan BSSN	Dalam proses pelaksanaan sesuai *roadmap* maupun peta okupasi nasional yang sepakati	Fungsi kontrol mengikuti ketentuan yang tercantum pada *roadmap* pembangunan TIK nasional maupun peta okupasi nasional bidang kominfo
BSSN			
Konsep SKSN 2020-2024 rumusan BSSN telah disempurnakan dan diperbaiki BSSN sebagai konsep SKSN perbaikan meliputi aspek peningkatan kompetensi SDM keamanan siber, untuk SDM nasional, baik pemerintah dan masyarakat umum, (termasuk TNI/Polri) dalam bentuk berbagai praktik dan kegiatan pendidikan dan latihan keamanan siber nasional antara lain *cybersecurity drill test* maupun kegiatan lainnya.	Setiap bidang dalam BSSN terkait selau pelaksana	a) Perbaikan SKSN masih dalam proses b) Berbagai kegiatan seminar dan *workshop* yang mendukung terwujudnya SKSN terus dalam proses c) *Cybersecurity Drill Test* 2018 dan 2019 terselenggara sebagai proses yang mendukung konsep SKSN	SKSN disusun dan dirumuskan secara *real* dan *in line* dengan: a) program pembangunan *index* keamanan siber nasional di *publish* GCI oleh ITU b) R*oadmap* pembinaan SDM keamanan siber dan sandi 2020-2024 maupun c) Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Faktor-Faktor Penghambat SKSN			
Pushansiber Kemhan RI			
Sebagaimana BSSN, maka organisasi Pushansiber Kemhan masih baru terbentuk Belum ada kerjasama terprogram antara Pushansiber KEMHAN dengan BSSN Belum ada pedoman kompetensi SDM pertahanan siber. Belum adanya realisasi alokasi anggaran untuk program kerja kedua instansi hingga 2020	Pengorganisasian bersifat sektoral sebagaimana peran dan fungsi masing-masing (Pushansiber maupun BSSN) atau belun berinteroperabiliti	Pelaksanaan kegiatan masih sektoral sesuai peran dan fungsi Pushansiber Kemhan	Sebagai kontrol hasil masih berpedoman standar kompetensi SDM pertahanan siber yang merujuk pada Permenhan No.82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI SKSN belum menjadi standar Pushansiber dalam membangun SDM pertahana siber Hasil belum mencapai target kompetensi SDM pertahanan siber
Satsiber TNI			
Adanya perbedaan perspektif tentang SDM TIK (Kominfo), SDM Keamanan Siber (BSSN), dan SDM Pertahanan Siber (Kemhan/TNI); Regulasi nasional belum dijabarkan dalam aturan pelaksanaan yang aplikatif dan komprehensif sesuai kebutuhan di lapangan MoU Satsiber TNI dengan BSSN belum di *follow up* d) Belum ada pedoman tata kelola SDM pertahanan siber	Pengorganisasian masih bersifat sektoral sebagaimana peran dan fungsi masing-masing (Satsiber TNI maupun BSSN)	Pelaksanaan kegiatan masih sektoral sesuai peran dan fungsi Satsiber TNI	Sebagai kontrol masih berpedoman standar kompetensi SDM pertahanan siber yang merujuk pada Permenhan No.82 tahun 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI SKSN belum menjadi standar Satsiber TNI dalam membangun SDM pertahana siber Hasil belum mencapai target kompetensi SDM pertahanan siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Balitbang SDM Kominfo			
Kominfo belum mengetahui konsep SKSN 2020-2024 hasil rumusan BSSN (maupun konsep perbaikannya). Kelembagaan BSSN masih baru	Pengorganisasian masih bersifat sektoral sesuai peran dan fungsi Balitbang SDM Kominfo	Pelaksanaan kegiatan masih sektoral sesuai peran dan fungsi Balitbang SDM Kominfo	Fungsi kontrol mengikuti ketentuan yang tercantum pada *roadmap* pembangunan TIK nasional maupun peta okupasi nasional bidang kominfo
BSSN			
BSSN masih baru, sehingga mempengaruhi kesiapan membangun keamanan siber nasional yang *output* dan *outcome*-nya juga diperlukan oleh bidang pertahanan dalam membangun kompetensi SDM pertahanan siber. Konsep SKSN 2020-2024 rumusan BSSN, masih dalam perbaikan (penyempurnaan), dan belum menjadi ketentuan atau aturan nasional, akibatnya SKSN belum menjadi atensi seluruh pemangku kepentingan siber di Indonesia.	Setiap bidang terkait dalam BSSN diorganisir sebagai pelaksana untuk menuntaskan peran dan fungsi BSSN untuk terwujudnya keamanan siber nasional	Pelaksanaan kegiatan masih sektoral sesuai peran dan fungsi masing-masing bidang di lingkup BSSN untuk menuntaskan SKSN	Sebagai kontrol pelaksanaan tugas peran dan fungsi BSSN dalam menuntaskan perumusan SKSN khususnya untuk mendukung pembinaan kompetensi SDM pertahanan siber merujuk pada *roadmap* pembinaan SDM keamanan siber dan sandi 2020-2024 maupun dokumen Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber

Sumber: diolah peneliti

Berdasarkan matrik analisis prinsip POAC pada tabel 4.3 di atas, diperoleh hal-hal terkait faktor-faktor pendukung SKSN, sebagai berikut:

a. Aspek *Planning* (perencanaan). Adanya dokumen-dokumen yang relevan dengan pembangunan bidang TIK dan keamanan siber nasional, terwujudnya kerjasama dan/atau kesepakatan bersama, kegiatan pendidikan dan latihan yang bertajuk keamanan siber yang diselenggarakan BSSN serta relevan dalam mendukung upaya membangun kompetensi SDM pertahanan siber, adalah merupakan

indikator positif sebagai faktor-faktor yang mendukung diperlukannya SKSN. Hal tersebut juga menunjukan adanya upaya perencanaan kegiatan yang ditempuh oleh subyek-subyek penelitian meskipun konsep SKSN masih dalam proses penyelesaian.

b. Aspek *Organizing* (pengorganisasian). Setiap subyek penelitian mengorganisir instansinya baik secara sektoral sesuai peran tugas dan fungsi masing-masing, maupun berkolaborasi dengan BSSN sebagaimana kesepakatan kerjasama maupun pelaksanaan kegiatan seminar maupun pendidikan dan latihan bertajuk keamanan siber. Hal-hal tersebut di atas menunjukan bahwa fungsi pengorganisasian pada pelaksanaan kegiatan peningkatan kompetensi SDM menjadi faktor pendukung eksistensi SKSN untuk upaya membangun kompetensi SDM pertahanan siber.

c. Aspek *Actuating* (pelaksanaan). Setiap subyek penelitian berupaya melaksanakan kegiatan sesuai peran tugas dan fungsinya, baik secara sektoral maupun berklaborasi dengan BSSN dalam upaya pembangunan dan peningkatan kompetensi SDM-nya. Hal-hal tersebut di atas menunjukan bahwa fungsi pengorganisasian pada pelaksanaan kegiatan peningkatan kompetensi SDM tetap bejalan sekaligus secara tidak langsung menjadi faktor pendukung eksistensi SKSN terhadap upaya membangun kompetensi SDM pertahanan siber.

d. Aspek *Controlling* (pengawasan). Setiap subyek penelitian melaksanakan pengawasan merujuk kepada pedoman yang berlaku maupun standar capaian kompetensi SDM masing-masing. Hal tersebut menunjukan bahwa kolaborasi dan interoperabiliti dalam pengaturan standar pencapaian kompetensi SDM, melalui kegiatan pendidikan dan pelatihan menjadi penting. Kolaborasi dan

interoperabiliti dalam pengaturan standar capaian kompetensi SDM menjadi faktor pendukung penting terhadap eksistensi SKSN dalam upaya membangun kompetensi SDM pertahanan siber.

Berdasarkan matrik tersebut, beberapa faktor yang dipandang esensial sekaligus dominan mendukung konsep SKSN adalah: telah tersedianya dokumen *roadmap* dan standar pembangunan kompetensi SDM TIK dan SDM keamanan siber, serta telah terwujudnya kerjasama instansi dengan BSSN terkait pendidikan dan pelatihan keamanan siber. Selanjutnya, masih berdasarkan matrik analisis prinsip POAC pada tabel 4.3, diperoleh hal-hal terkait faktor-faktor yang menghambat SKSN, sebagai berikut:

a. Aspek *Planning* (perencanaan). Pada aspek ini, faktor masih barunya kelembagaan BSSN dan belum tuntasnya proses perbaikan konsep SKSN menjadi aspek dominan sebagai faktor penghambat eksistensi SKSN terhadap kepentingan bidang pertahanan dalam upaya mewujudkan kompetensi SDM pertahanan siber. Dikaitkan dengan fungsi perencanaan, maka tentulah faktor-faktor tersebut menjadi hal-hal diluar perencanaan BSSN. Hal tersebut juga menunjukan adanya hambatan dalam fungsi perencanaan yang dilaksanakan BSSN dalam menuntaskan SKSN sebagai hal urgen.

b. Aspek *Organizing* (pengorganisasian). Meskipun terdapat faktor penghambat terhadap SKSN, dan hal tersebut merupakan domain BSSN, maka setiap subyek penelitian hanya mengorganisir instansinya secara sektoral sesuai peran tugas dan fungsi masing-masing. Hal-hal tersebut di atas menunjukan bahwa fungsi pengorganisasian tetap berjalan, di mana BSSN berperan lebih aktif dalam mengorganisir peran dan fungsi menuntaskan SKSN.

c. Aspek *Actuating* (pelaksanaan). Setiap subyek penelitian hanya melaksanakan peran tugas dan fungsi secara sektoral, termasuk dalam hal ini BSSN yang dalam proses menuntaskan SKSN . Hal-hal tersebut di atas menunjukan bahwa fungsi *actuating* tetap berjalan, di mana BSSN berperan lebih aktif melaksanakan peran dan fungsinya dalam menuntaskan SKSN.

d. Setiap subyek penelitian berupaya melaksanakan kegiatan sesuai peran tugas dan fungsinya, baik secara sektoral maupun berklaborasi dengan BSSN dalam upaya pembangunan dan peningkatan kompetensi SDM-nya. Hal-hal tersebut menunjukan bahwa fungsi pengorganisasian pada pelaksanaan kegiatan peningkatan kompetensi SDM menjadi faktor pendukung eksistensi SKSN atas upaya membangun kompetensi SDM pertahanan siber.

e. Aspek *Controlling* (pengawasan). Subyek penelitian melaksanakan aspek pengawasan merujuk kepada pedoman yang berlaku maupun standar capaian kompetensi SDM masing-masing. SKSN belum menjadi atensi sekaligus standar dan pedoman rujukan bagi para subyek penelitian dikarenakan masih dalam proses penyelesaian oleh BSSN. Hal tersebut kembali menunjukan bahwa eksistensi SKSN penting dalam hal mengolaborasikan dan menginteroperabilitikan aspek pengaturan standar pencapaian kompetensi SDM, khususnya melalui kegiatan pendidikan dan pelatihan guna membangun kompetensi SDM pertahanan siber.

Berdasarkan matrik pembahasan tersebut, maka faktor penghambat SKSN yang dipandang paling fundamental mempengaruhi upaya bidang pertahanan dalam mewujudkan kompetensi SDM pertahanan siber adalah akibat belum tuntasnya konsep SKSN rumusan BSSN.

4.3.3 Analisis Prinsip POAC Pada Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan Sishankamrata.

Pada bagian ini, prinsip POAC digunakan untuk menganalisis wujud praktik-praktik kegiatan pendidikan dan pelatihan keamanan siber yang merujuk kepada konsep SKSN guna mendukung terwujudnya kompetensi SDM pertahanan siber. Berdasarkan uraian hasil penelitian, peneliti mengambil dan menyusun poin-poin penting dan relevan ke dalam tabel matrik untuk dianalisis prinsip-prinsip POAC-nya.

Untuk aspek *planning* (perencanaan), matrik ini menempatkan berbagai bentuk praktik dan kegiatan pendidikan dan pelatihan keamanan siber yang aplikatif menurut konsep SKSN sehingga mendukung terwujudnya kompetensi SDM pertahanan siber. Analisis aspek *planning* oleh peneliti adalah berdasarkan kepada upaya yang terencana, baik sektoral maupun kolaboratif dengan pihak-pihak lain yang terkait.

Untuk aspek *organizing* (pengorganisasian) dalam matrik ini analisis dilakukan terhadap bagaimana subyek-subyek penelitian untuk mengorganisir SDMnya dalam suatu penyelenggaraan kegiatan praktik-praktik pendidikan dan latihan keamanan siber. Analisis aspek *organizing* oleh peneliti adalah berdasarkan kepada aspek peran serta, yaitu wujud peran serta atau pelibatan setiap subyek penelitian di dalamnya. Tentu dalam hal melaksanakan analisis terhadap aspek *organizing* ini tidak mengabaikan aspek sebelumnya (*planning*).

Untuk aspek *actuating* (pelaksanaan) dalam matrik ini dilakukan analisis untuk bagaimana setiap subyek penelitian mengaktualisasikan praktik-praktik kegiatan pendidikan dan latihan keamanan siber yang

relevan terhadap peningkatan kompetensi SDM yang diperlukan/sesuai. Analisis aspek *actuating* adalah kepada wujud atau bentuk praktik-praktik kegiatan pendidikan dan latihan keamanan siber yang dilaksanakan. Dalam hal analisis aspek *actuating*, tidak mengabaikan aspek sebelumnya.

Untuk aspek *controlling* (pengawasan) dilakukan analisis dalam hal bagaimana setiap subyek penelitian menjalankan fungsi kontrol atau pengawasan terhadap implementasi praktik-praktik kegiatan pendidikan dan latihan keamanan siber yang dilaksanakan oleh SDM organisasinya. Analisis aspek *controlling* adalah terkait adanya standar kompetensi SDM capaian, dikaitkan dengan pencapaian target kompetensi SDM pertahanan siber yang spesifik, serta hal lain yang relevan. Dalam hal melaksanakan analisis aspek *controlling* ini juga tidak mengabaikan aspek sebelumnya.

Tabel 4.4 Matrik Implementasi POAC Pada F_1 dan F_2 Terkait Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Pushansiber Kemhan RI			
Kegiatan *Cyber Security Drill Test* yang diselenggarakan BSSN.	Pushansiber mengorganisir diri sebagai peserta kegiatan	Sebagai peserta *Cybersecurity Drill Test* tahun 2019 oleh BSSN	Merujuk pada Permenhan No.82 Th 2014 *Output* & *Outcome* giat belum dapat dilaksanakan *Cybersecurity drill test*: melatih: respon insiden keamanan siber, prosedur, interoperability, koordinasi, & teknis pelaporan Hasil partisipasi belum mencapai target spesifik kompetensi SDM pertahanan siber

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
Satsiber TNI			
a) Latihan Bersama *Cobra Gold Exercise*, antara TNI dengan Thailand di mana salah satu materinya adalah Operasi Siber Gabungan b) Kegiatan *Cybersecurity Drill Test* yang diselenggarakan BSSN	a) Sops Mabes TNI sebagai pelaksana, Satsiber TNI sebagai pelaku peserta latihan b) Satsiber TNI mengorganisir diri sebagai peserta dalam *cybersecurity drill test* BSSN	a) Latihan bersama *Cobra Gold* tahun 2018 dan 2019 b) *Cybersecurity Drill Test* 2018 oleh BSSN	Mengikuti standar kompetensi SDM pertahanan siber yang sesuai Permenhan No.82 th 2014 tentang Pedoman Pertahanan Siber Kemhan/TNI *Output* & *Outcome* dari kegiatan cybersecurity drill test belum dilaksanakan oleh peserta Materi praktik *cybersecurity drill test*: melatih respon terhadap insiden keamanan siber, melatih prosedur, interoperability dan koordinasi, serta teknis isian format pelaporan kepada Pusopskamsibernas BSSN Hasil partisipasi belum mencapai target kompetensi SDM pertahanan siber, khususnya *knowledge* dan *skill* serta kapasitas dan kapabilitas spesifik SDM pertahanan siber
Balitbang SDM Kominfo			
Praktik-praktik yang relevan dengan kegiatan pendidikan dan latihan keamanan siber, antara lain: Kompetisi *Cyber* Jawara, Pelatihan Intensif *Digital Talent Scholarship* (DTS) Kominfo, dan Program Beasiswa *Government Chief Information Officer* (G-CIO).	Balitbang SDM Kominfo sebagai pelaksana kegiatan kecuali untuk Kompetisi *Cyber* Jawara oleh ID-SIRTII Komifo (menginisiasi sejak 2012)	Kegiatan masih selalui dilaksanakan: Kompetensi Cyber Jawara 2012 sd 2020, *Digital Talent Scholarship* (DTS), dan Program Beasiswa *Government Chief Information Officer* (G-CIO).	Fungsi kontrol mengikuti ketentuan yang tercantum pada roadmap pembangunan TIK nasional maupun peta okupasi nasional bidang kominfo Fokus pada target terwujudnya kompetensi SDM TIK nasional, sebaliknya belum memenuhi kompetensi SDM pertahanan siber yang spesifik

Analisis Fungsi Dasar Manajemen			
Planning (P)	*Organizing* (O)	*Actuating* (A)	*Controlling* (C)
BSSN			
Kegiatan *Cyber Security Drill Test* adalah praktik pendidikan dan latihan keamanan siber Pada *Roadmap* Pembinaan SDM Keamanan Siber dan Sandi 2020-2024 terdapat program kegiatan praktik-praktik latihan keamanan siber yang aplikatif dalam kerangka pengembangan kompetensi, antara lain: *talent scouting* dan pembinaan bidang keamanan siber untuk generasi muda dan mahasiswa dalam bentuk penyelenggaraan kompetisi (*capture the flag*, *cyber war game*, *cyber jawara*), *cybersecurity job fair*, serta kompetisi keamanan siber untuk ASN, TNI, dan Polri.	BSSN mengorganisir diri selaku pelaksana kegiatan tersebut didukung oleh ID-SIRTII yang sejak 2018 di bawah BSSN	Yang telah, sedang, dan akan diaktuasikan: *Cybersecurity Drill test* dan *Cyber Jawara* Latihan bersama *Cobra Gold* tahun 2018 dan 2019 Yang masih dalam rencana program: *talent scouting*, *cybersecurity job fair*, dan kompetisi keamanan siber untuk ASN TNI dan Polri	Sebagai kontrol merujuk pada *roadmap* pembinaan SDM keamanan siber dan sandi 2020-2024 maupun dokumen Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber Belum memenuhi target kompetensi SDM pertahanan siber yang spesifik *Cybersecurity Drill Test* menjadi embrio dari upaya mewujudkan rencana kontijensi nasional bidang keamanan siber

Sumber: diolah peneliti

Berdasarkan matrik analisis prinsip POAC pada tabel 4.4 di atas, diperoleh hal-hal, sebagai berikut:

a. Aspek *Planning* (perencanaan). Terdapat berbagai praktik kegiatan pendidikan dan pelatihan keamanan siber yang aplikatif sekaligus mendukung terwujudnya kompetensi SDM pertahanan siber. Praktik-praktik kegiatan pendidikan dan latihan keamanan siber tersebut diikuti oleh semua subyek penelitian, dan relatif didominasi oleh program-program milik BSSN. Adapun yang diselenggarakan oleh selain BSSN, misalnya Kominfo, relatif

beragam, namun esensi materinya lebih fokus kepada *basic* pembangunan kompetensi SDM TIK nasional. Kemudian dengan subyek Pushansiber Kemhan maupun Satsiber TNI, relatif belum ada program serupa, karena secara kelembagaan kedua subyek penelitian tersebut masih baru, disamping belum adanya standar baku kompetensi SDM pertahanan siber yang berdampak pada belum adanya perencanaan maupun rancangan bagaimana membangun dan meningkatkan kompetensi SDM pertahanan siber. Sehingga hal tersebut menjadkan kedua subyek penelitian ini sangat bergantung kepada adanya *planning* kegiatan pendidikan dan pelatihan keamanan siber, setidaknya kompetensi tersebut mampu memenuhi sebagian besar persyaratan kompetensi SDM pertahanan siber. Mencermati praktik kegiatan pendidikan dan pelatihan BSSN, khususnya *cybersecurity dril test*, yang materi praktiknya adalah: melatih respon terhadap insiden keamanan siber, melatih prosedur, interoperability dan koordinasi, serta teknis mengisi dan menyampaikan pelaporan (sesuai format) kepada Pusopskamsibernas BSSN sebagai *point contact* kemanan siber nasional, maka dalam perspektif fungsi perencanaan, konsep praktik-praktik *cybersecurity drill test* yang aplikatif sekaligus sangat menunjang peningkatan kompetensi SDM pertahanan siber tersebut dapat diasumsikan sebagai embrio dari dari *national contigency plan for cybersecurity*. Mengapa demikian ? karena di dalam dinamika praktiknya bersifat semesta melibatkan SDM (warga negara), wilayah, berikut sarana prasarana dan sumber daya nasional lainnya dalam mengahadpi ancaman siber yang mengganggu kepentingan dan kedaulatan nasional.

b. Aspek *Organizing* (pengorganisasian). Setiap subyek penelitian mengorganisir instansinya baik secara sektoral sesuai peran tugas dan fungsi masing-masing, maupun berkolaborasi

dengan BSSN dan Kominfo, bertindak sebagai pelaksana maupun sebagai peserta dalam berbagai praktik kegiatan pendidikan dan latihan keamanan siber. Hal-hal tersebut di atas menunjukan bahwa fungsi pengorganisasian pada kegiatan tersebut relevan dengan konsep SKSN demi mendukung upaya membangun kompetensi SDM pertahanan siber.

c. Aspek *Actuating* (pelaksanaan). Setiap subyek penelitian melaksanakan sekaligus terlibat dalam berbagai praktik kegiatan pendidikan dan pelatihan keamanan siber sesuai kepentingan masing-masing. Hal-hal tersebut di atas menunjukan bahwa fungsi *actuating* tetap berjalan sekaligus relevan dengan konsep SKSN terhadap upaya membangun kompetensi SDM pertahanan siber.

d. Aspek *Controlling* (pengawasan). Setiap subyek penelitian melaksanakan pengawasan merujuk kepada pedoman yang berlaku maupun standar capaian kompetensi SDM masing-masing. Namun bila dihadapkan kepada standar capaian kompetensi SDM pertahanan siber, maka praktik-praktik kegiatan pendidikan dan pelatihan keamanan siber tersebut diyakini hanya mampu memenuhi sebagian besar standar capaian kompetensi SDM pertahanan siber.

Dari hasil penelitian dan pembahasan matrik analisis prinsip POAC tersebut, praktik-praktik kegiatan pendidikan dan latihan keamanan siber yang dianggap relevan dengan konsep SKSN, sekaligus aplikatif dalam mendukung terwujudnya kompetensi SDM pertahanan siber, antara lain praktik-praktik: *cybersecurity drill test*; *cyber* jawara; serta kompetisi keamanan siber untuk ASN, TNI, dan Polri. Bahwa praktik-praktik tersebut dipandang aplikatif karena bersifat lintas sektoral sekaligus mencerminkan prinsip-prinsip kesemestaan (melibatkan berbagai pemangku kepentingan siber nasional). Meskipun demikian, praktik-praktik tersebut diyakini belum

mampu memenuhi target capaian standar kompetensi SDM pertahanan siber yang sangat fundamental untuk bidang pertahanan, yaitu ketika pertahanan siber diaktualisasi dalam suatu *theatre* sishankamrata dan atau dalam bentuk gelar operasi militer, di mana alut sista TNI yang berbasis TIK harus dipertahankan (misal: *Network Centric Warfare*) dan/atau alutsista TNI yang berbasis TIK dioperasionalkan (sebagai *cyber weapon*) untuk tujuan melakukan serangan-serangan siber terhadap ancaman siber lawan.

4.3.4 Eksistensi Urgensi SKSN Dalam Upaya Peningkatan Kompetensi SDM Pertahanan Siber, Terhadap Teori Strategi dan Hanneg, Maupun Konseptual Ancaman dan Keamanan.

Dari keseluruh uraian pembahasan analisis fungsi dasar manajemen (POAC) terhadap tata kelola peningkatan kompetensi SDM di masing-masing subyek penelitian, maka eksistensi urgensi SKSN dihadapkan kepada terhadap teori strategi, teori pertahanan, dan konseptual keamanan maupun ancaman adalah sebagai berikut:

4.3.4.1 Eksistensi Urgensi SKSN Dalam Mewujudkan SDM Pertahanan Siber, Terhadap Konsep Teori Hanneg.

Pada UU Nomor 3 tahun 2002 tentang TNI dinyatakan bahwa hanneg merupakan salah satu fungsi pemerintahan yang sekaligus merupakan suatu usaha untuk mewujudkan satu kesatuan hanneg guna mencapai tujuan nasional dalam hal ini: melindungi segenap bangsa dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut serta melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial). Dan di dalam penelitian ini, uraian tersebut telah diasumsikan peneliti sebagai suatu konsep teori hanneg yang dianut Indonesia.

Usaha hanneg dalam rangka menghadapi ancaman siber, tentu diselenggarakan dan dipersiapkan pemerintah secara dini melalui suatu sishankamrata yang melibatkan segenap warga negara (SDM), SDA, SDB, serta sarana dan prasarana nasional yang ada di seluruh wilayah NKRI sebagai satu kesatuan pertahanan siber guna menghadapi berbagai bentuk ancaman siber. Kemampuan pertahanan siber sangat bergantung pada SDM pertahanan siber yang memiliki *basic knowledge* dan *skill* serta kapasitas dan kapabilitas dalam bidang TIK maupun keamanan siber. Upaya bidang pertahanan untuk transformasi membangun SDM pertahanan siber tidak berangkat dari titik nol, melainkan dengan meningkakan kompetensi SDM TIK maupun SDM keamanan siber yang telah dipersiapkan sebelumnya, baik oleh Kominfo maupun BSSN (melalui konsep SKSN). Tanpa adanya kompetensi SDM TIK maupun kompetensi SDM keamanan siber, maka upaya bidang pertahanan dalam mewujudkan kompetensi SDM pertahanan siber akan selalu menghadapi tantangan. Dengan demikian eksistensi SKSN sangat penting (urgen) bagi bidang hanneg, khususnya dalam upaya mewujudkan kompetensi SDM pertahanan siber untuk kepentingan sishankamrata.

4.3.4.2 Eksistensi Urgensi SKSN Dalam Mewujudkan SDM Pertahanan Siber, Terhadap Teori Strategi.

Pemerintah Indonesia dalam membangun keamanan siber nasional menempuh upaya dengan mendudukan SKSN sebagai suatu strategi nasional yang urgen (penting) sehingga harapan tercapainya tujuan keamanan siber nasional mampu terwujud secara efektif dan efisien dengan memanfaatkan segala sumber daya yang dimiliki. Sebagaimana tercantum pada Tabel 3.4 tentang Uraian Fungsi dan Indikator Faktor – 1 (F_1), di mana aspek peningkatan kompetensi SDM keamanan siber merupakan bagian dari elemen *ways* dalam konsep SKSN 2020-2024. Hal tersebut menunjukan bahwa eksistensi SKSN telah memenuhi sebagian

kecil dari elemen strategi. Dikaitkan dengan upaya terwujudnya kompetensi SDM pertahanan siber, maka upaya tersebut juga harus ditempuh sebagaimana langkah-langkah strategis peningkatan SDM keamanan siber pada konsep SKSN, terlebih karena kompetensi SDM pertahanan siber sangat menuntut standar dan kriteria kompetensi yang spesifik yang belum mampu dipenuhi oleh kompeensi SDM TIK maupun SDM keamanan siber. Hasil penelitian dan pembahasan telah menunjukan bahwa konsep SKSN telah mampu memenuhi sebagian besar standar dan kriteria kompetensi SDM pertahanan siber, sehingga untuk kriteria spesifik kompetensi SDM pertahanan siber menjadi tanggung jawab bidang pertahanan.

4.3.4.3 Eksistensi Urgensi SKSN Dalam Mewujudkan SDM Pertahanan Siber, Terhadap Konseptual Keamanan dan Ancaman.

Kemanan siber dalam konsep SKSN maupun pertahanan siber dalam kerangka sishankamrata, pada dasarnya keduanya memiliki tujuan yang sama, yaitu: untuk melindungi, menjaga, dan mempertahankan kepentingan nasional Indonesia dari berbagai bentuk ancaman siber. Meskipun kedua aspek memiliki kesamaan dalam hal esensi (substansi) ancaman siber yang dihadapi, namun dalam hal konseptual keamanan, terdapat perbedaan konteks tergantung kepada latarbelakang (motif) dan eskalasi dari ancaman siber tersebut. Pada eskalasi tertentu di mana ancaman siber dinilai berniat/bermotif mengganggu keamanan nasional, maka kompetensi SDM keamanan siber menjadi *leading sector* dalam kerangka keamanan nasional guna melindungi dan menjaga kepentingan nasional Indonesia. Sebaliknya ketika eskalasi ancaman siber dinilai memiliki niat (bermotif) mengganggu kedaulatan negara, maka kompetensi SDM pertahanan siber melalui sishankamrata menjadi *leading sector* dalam kerangka kerja tugas-tugas pertahanan negara guna mempertahankan kedaulatan NKRI demi kepentingan nasional Indonesia.

4.3.5 Matrik Deskripsi Area Fungsi Kompetensi SDM Pertahanan Siber Dengan Tolok Ukur Pada Kompetensi SDM TIK dan SDM Keamanan Siber.

Kompetensi SDM pertahanan siber yang tercantum dalam dokumen Pedoman Pertahanan Siber (Permenhan RI No.82/2014), belum mengacu kepada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada TIK maupun Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber, malah sebaliknya tidak lebih hanya dipahami sebagai konsep kompetensi SDM yang sekedar “memiliki kemampuan”. Peneliti berpandangan bahwa kompetensi SDM pertahanan siber seyogyanya dibangun secara lebih spesifik dan fokus pada *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM yang sedemikian rupa mampu mengaktualisasikan fungsi-fungsi pertahanan negara (dalam hal ini fungsi penangkalan, dan fungsi penindakan, serta fungsi perbantuan) dalam bidang pertahanan siber untuk menghadapi berbagai bentuk ancaman siber. Berikut ini matrik area fungsi kompetensi pertahanan siber yang dimungkinkan sebagai referensi untuk bidang pertahanan dalam merumuskan kembali konsep kompetensi SDM pertahanan siber yang lebih mampu dalam penyelenggaraan fungsi-fungsi pertahanan negara.

Tabel 4.5 Matrik Deskripsi Area Fungsi Kompetensi SDM Pertahanan Siber Bertolok Ukur Pada Kompetensi SDM TIK Dan SDM Keamanan Siber

	Kompetensi SDM					
	SDM TIK		SDM Keamanan Siber		SDM Pertahanan Siber	
Level KKNI	①	Meliputi 16 (Enambelas) Area Fungsi Teknologi Informasi & Komunikasi			①	Area Fugsi Pertahanan Siber
	②				②	
	③				③	
	④				④	
	⑤		⑤	Area Fungsi Keamanan Siber	⑤	
	⑥		⑥		⑥	
	⑦		⑦		⑦	
	⑧		⑧		⑧	
	⑨		⑨		⑨	

		Kompetensi SDM		
		SDM TIK	**SDM Keamanan Siber**	**SDM Pertahanan Siber**
***Knowledge* & *Skill* Serta Kapasitas & Kapabilitas Yang Mampu Menyelenggarakan Fungsi Khusus**	**Operasional Keamanan**		• Kemampuan SDM untuk menyelenggarakan fungsi keamanan informasi yang memenuhi fase-fase penanganan insiden keamanan siber yang terdiri dari 3 (tiga) fase, yaitu: a) fase sebelum insiden serangan siber (*before cyber attack*); b) fase ketika terjadinya insiden serangan siber (*during cyber attack*); dan c) fase setelah terjadinya insiden serangan siber (*after cyber attack*) • Kemampuan SDM untuk melaksanakan fungsi keamanan siber yang diselenggarakan dalam bentuk/wujud kegiatan terorganisir (strategi, taktis, operasional, dan bersifat kontjensi) secara terintegrasi melibatkan seluruh pemangku kepentingan siber nasional.	Kemampuan SDM untuk mampu melaksanakan fungsi-fungsi keamanan informasi maupun fungsi keamanan siber sebagaimana berlaku pada kompetensi SDM keamanan siber
	Operasional Pertahanan			Kemampuan SDM untuk mampu melaksanakan fungsi-fungsi pertahanan negara yang terdiri dari 3 (tiga) fungsi, yaitu: fungsi penangkalan, fungsi penindakan, dan fungsi penanggulangan, serta sebagai tambahan adalah fungsi perbantuan.
Keterangan		• *Leading Sector* adalah Kemenkominfo RI • Merujuk pada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada TIK	• *Leading Sector* adalah BSSN, merujuk pada SKSN • Kemampuan SDM sesuai fungsi ke-10 Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonsia Pada TIK (Fungsi ke 10 area fungsi TIK), yang kemudian dijabarkan kembali melalui Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber	• *Leading Sector* adalah Kemhan/TNI • Kompetensi SDM merujuk pada Permenhan No.82/2014 (Pedoman Pertahanan Siber) sebagai pedoman yang perlu penyesuaian terhadap Peta Okupasi TIK maupun Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber • Peningkatan dan penguatan kompetensi SDM fungsi keamaan siber menjadi pertahanan siber perlu selaras dengan SKSN • dalam hal pemberdayaan, harus ditrasnformasikan menjadi SDM pertahanan siber melalui mekanisme PSDN untuk Hanneg.

Sumber: diolah peneliti

BAB 5
KESIMPULAN DAN REKOMENDASI

5.1 Kesimpulan.

Pembahasan dan hasil penelitian dengan teknik penelitian lapangan dalam bentuk wawancara, observasi, dan dokumentasi terhadap subyek-subyek penelitian di: Pushansiber Kemhan RI, Satsiber TNI, Balitbang SDM Kemenkominfo RI, dan BSSN, terkait “Urgensi SKSN Dalam Mendukung Sistem Pertahanan dan Keamanan Rakyat Semesta : Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya SDM Pertahanan Siber”, dapat diambil beberapa kesimpulan untuk fokus rumusan masalah “Bagaimana eksistensi SKSN menjadi urgen terhadap upaya membangun kompetensi SDM pertahanan siber untuk kepentingan sishankamrata”, yang diuraikan dalam sub fokus-sub fokus kesimpulan, sebagai berikut:

5.1.1 Peran dan Fungsi SKSN Terhadap Upaya Membangun Kompetensi SDM Pertahanan Siber.

SKSN memiliki peran dan fungsi yang penting (urgensi) bagi bidang pertahanan terhadap upaya membangun terwujudnya kompetensi SDM pertahanan siber untuk kepentingan sishankamrata. Peran dan fungsi penting SKSN tersebut adalah dalam hal memenuhi sebagian besar kriteria standar kompetensi SDM pertahanan siber yang spesifik yang tidak terpenuhi oleh kompetensi SDM TIK nasional.

5.1.2 Faktor-Faktor Yang Mendukung dan Menghambat SKSN Indonesia Dalam Membangun SDM Pertahanan Siber.

Terdapat dua faktor dominan yang yang mendukung konsep SKSN, yaitu: *pertama*, tersedianya dokumen *roadmap* standar kompetensi

pembangunan kompetensi SDM TIK nasional dan SDM keamanan siber; dan *kedua*, telah terwujudnya kerjasama instansi dengan BSSN dalam bidang pendidikan dan pelatihan keamanan siber. Sedangkan untuk faktor penghambat, yang paling fundamental adalah belum tuntasnya konsep SKSN rumusan BSSN.

5.1.3 Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber.

Terdapat berbagai praktik kegiatan pendidikan dan pelatihan keamanan siber yang sesuai (relevan) dengan konsep SKSN sekaligus aplikatif dalam mendukung terwujudnya kompetensi SDM pertahanan siber, antara lain: *cybersecurity drill test*; *cyber* jawara; serta kompetisi keamanan siber untuk ASN, TNI, dan Polri. Praktik-praktik kegiatan pendidikan dan latihan keamanan siber tersebut dipandang aplikatif karena dilaksanakan secara lintas sektoral melibatkan berbagai pemangku kepentingan siber nasional, dan hal tersebut sangat relevan dengan sifat kesemestaan.

5.2 Rekomendasi.

Berdasarkan hasil penelitian, pembahasan, dan kesimpulan dari analisis fungsi dasar manajemen (POAC) terhadap upaya terwujudnya kompetensi SDM pertahanan siber, menunjukan bahwa eksistensi SKSN adalah penting (urgensi), khususnya untuk bidang pertahanan dalam mendukung sishankamrata. Berkenaan dengan hal tersebut, disampaikan rekomendasi kepada berbagai pihak, sebagai berikut:

5.2.1 Dalam perspektif bidang pertahanan, SKSN menjadi suatu hal yang urgen karena peran dan fungsinya dalam menjembatani peningkatan kompetensi SDM TIK menjadi SDM keamanan siber demi memenuhi

sebagian besar kriteria kompetensi pertahanan siber. Oleh karena itu Bidang pertahanan perlu mendorong BSSN untuk segera mewujudkan SKSN sebagai pedoman strategis yang tidak sekedar untuk kepentingan membangun keamanan siber nasional, namun juga demi kepentingan sishankamrata.

5.2.2 Praktik-praktik kegiatan pendidikan dan latihan bidang keamanan siber yang diselenggarakan BSSN, Bidang Kominfo, maupun bidang Pertahanan, di dalamnya terdapat esensi praktik-praktik dan dinamika operasional keamanan siber yang aplikatif di lapangan dalam menjawab berbagai tantangan dan ancaman, serangan, dan insiden siber. Apabila praktik-praktik kegiatan pendidikan dan latihan keamanan siber diselenggarakan secara terencana, reguler, terintegrasi, bertingkat dan berlanjut, serta *massive* (interoperabiliti dan berskala nasional), maka sejatinya akan menjadi embrio dari *contigency plan and action on national cybersecurity* (rencana kontijensi dan aksi untuk kemanan siber nasional). *Output* kontijensi merupakan bentuk kegiatan operasional keamanan siber berskala nasional, terorganisir, berinteroperabiliti, dan terencana, yang melibatkan segenap sumberdaya bidang TIK nasional, keamanan siber, dan pertahanan siber untuk menghadapi berbagai bentuk ancaman dan insiden siber yang mengganggu kepentingan nasional.

5.2.3 Bidang pertahanan (dalam hal ini Kemhan dan TNI), perlu menyusun dan menetapkan standar kompetensi SDM pertahanan siber yang dituangkan kedalam suatu *roadmap* pembangunan SDM pertahanan negara sebagai dokumen pendukung dan/atau turunan dari UU Nomor 23 tahun 2019 tentang PSDN untuk Hanneg. Aspek kompetensi SDM pertahanan siber dalam dokumen *roadmap* tersebut juga perlu berafiliasi dan berkolaborasi dengan *roadmap* pembangunan kompetens SDM TIK nasional maupun kompetensi SDM keamanan siber, sehingga tercapai SDM Indonesia yang tidak sekedar siap menghadapi tantangan ancaman

siber di era digital, namun juga unggul, kreatif, dan inovatif dalam menyongsong era Revolusi Industri 4.0.

5.2.4 Dalam tesis ini, terdapat dua aspek penting yang esensi dan dinamikanya saling berafiliasi, yaitu, keamanan siber dan pertahanan siber, karena keduanya merujuk pada fundamental *cybersecurity pilaars* yang sama, yaitu: *people*, *process*, dan *technology*. Penelitian dan pembahasan yang dilakukan dalam tesis ini hanya pada pilar *people* yang analisisnya terbatas pada aspek kompetensi SDMnya menggunakan teori dasar fungsi manajemen (POAC). Sangat dipersilakan bagi siapapun untuk melakukan penyempurnaan-penyempurnaan lebih lanjut terhadap penelitian ini, sekaligus memperluas cakupan analisis POAC terhadap pilar *process* maupun pilar *technology*. Beberapa hal terkait pilar *process* telah disinggung dalam tesis ini, khususnya tentang *cybersecurity drill test* yang diselenggarakan BSSN sebagai wujud praktik-praktik kegiatan diklat keamanan siber yang aplikatif guna membangun kompetensi SDM pertahanan siber. Praktik-praktik semacam *cybersecurity drill test* tersebut akan menjadi embrio dari wujud *contigency plan and action on national cybersecurity* (rencana kontijensi dan aksi keamanan siber nasional). Kontijensi merupakan aktualisasi dari pilar proses, di dalamnya meliputi kegiatan perencanaan dan aksi (operasional) yang melibatkan seluruh sumber daya TIK nasional untuk tujuan tercapainya keamanan siber nasional yang selaras dengan terwujudnya pertahanan siber untuk kepentingan hanneg.

DAFTAR PUSTAKA

Buku

Afrizal. (2017). Metode Penelitian Kualitatif: Sebuah Upaya Mendukung Penggunaan Penelitian Kualitatif dalam Berbagai Disiplin Ilimu. Depok: Rajawali Pers.

Arikunto, Suharsimi. (2014). Prosedur Penelitian: Suatu Pendekatan Praktik. Jakarta: Rineka Cipta.

Akbar, Husaini Usman, Purnomo Setiadi. (2009). Metodologi Penelitian Sosial. Jakarta: Bumi Aksara.

Bogdan. R.C. and Biklen, S.K. (1982). *Qualitative Research for Education: An. Introduction to Theory and Methods*, Boston: Allyn and Bacon, Inc.

Bungin, Burhan. (2011 dan 2012). Penelitian Kualitatif. Jakarta: Kencana Predana Media Group.

Cooper, H. (1984). The *Integrative Research Review: A Systematic Approach*. Beverly Hills, CA: Sage.

Creswell, John W. (2013). *Research Design*: Pendekatan Kualitatif, Kuantitatif, dan Mixed.Yogyakarta: Pustaka Pelajar.

Creswell, John W. (2015). Penelitian Kualitatif & Desain Riset.Yogyakarta: Pustaka Pelajar.

Hasibuan, Malayu. (2000 dan 2009). Manajemen Sumber Daya Manusia (Edisi Revisi). Jakarta: PT Bumi Aksara.

Iskandar. (2008). Metodologi Penelitian Pendidikan dan Sosial (Kuantitatif dan Kualitatif). Jakarta: GP Press.

Marshall, C., and Rossman,G.B. (2006). *Designing Qualitative Research* (4th ed.). Thousand Oaks, CA:Sage.

Marsono, dan Tri Legionosuko. (2020). Teori Strategi Dari Berbagai Ahli. Bogor: UNHAN Press.

Miles, Matthew B., dan A. Michael Huberman. (2014). Analisis Data Kualitatif: Buku Sumber Tentang Metode-Metode Baru. Jakarta: Universitas Indonesia (UI-Press).

Moleong, Lexy J. (2009). Metode Penelitian Kualitatif. Bandung: Remaja Rosdakarya.

Moleong, Lexy. J. (2014). Metodologi Penelitian Kualitatif (Edisi Revisi). Bandung: Remaja Rosdakarya.

Moustakas, C. (1994). *Phenomenological Research Methods*. Thousand Oaks.CA: Sage.

Nazir, Moh. (2017). Metode Penelitian. Bogor: Ghalia Indonesia.

Nieswiadomy, R.M. (1993). *Foundation of Nursing Research*. (2nd ed). Norwalk. CT: Appleton & Lange.

Patton, Michael Quinn. (1987). *Qualitative Evaluation Methods*. Beverly Hills: Sage Publication.

Robbins SP, dan Judge. (2007). Perilaku Organisasi, Jakarta: Salemba Empat.

Sekaran, Uma. (2011). *Research Methods for Business* (Metode Penelitian Untuk Bisnis). Jakarta: Salemba Empat.

Spencer, N.Lyle and Spencer, M. Signe. (1993). *Competence at Work: Models for Superior Performance*. New York: John Wiley & Son Inc.

Sugiyono. (2017 dan 2020). Metode Penelitian Kualitatif. Untuk Penelitian Yang Bersifat: Eksploratif, Enterpretif, Interaktif, dan Konstruktif. Bandung: Alfabeta.

Sugiyono. (2019). Metode Penelitian Kuantitatif, Kualitatif dan R&D. Bandung: Alfabeta.

Sukarna. (2011). Dasar-Dasar Manajemen. Bandung: CV. Mandar Maju.

Suparno, A. Suhaenah. (2001). Membangun Kompetensi Dasar. Jakarta: Direktorat Jendral Pendidikan Tinggi Departemen Pendidikan Nasional.

Terry, George Robert. (2006). Prinsip-Prinsip Manajemen. Jakarta: Bumi Aksara.

Tim Penyusun Kamus Pusat Bahasa. (2008). Kamus Bahasa Indonesia. Jakarta: Departemen Pendidikan Nasional.

Torang, Syamsir. (2013). Organisasi dan Manajemen (Perilaku, Struktur, Budaya & Perubahan Organisasi. Bandung: Alfabeta.

Wiersma, William. (1986). "*Research Methods in Education: An Introduction*" (4th *Edition*); Boston, London, Sydney, Toronto: Allyn and Bacon Inc.

Undang-Undang/Peraturan

Undang-Undang Dasar Negara Republik Indonesia tahun 1945

Undang-Undang RI Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang RI Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.

Undang-Undang RI Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

Undang-Undang RI Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang ITE.

Undang-Undang Republik Indonesia Nomor 23 tahun 2019 tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara.

Peraturan Pemerintah RI Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

Peraturan Menteri Pertahanan RI Nomor Per/22/M/XII/2007 tentang Strategi Pertahanan Negara Republik Indonesia.

Peraturan Menteri Pertahanan RI Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Peraturan Menteri Pertahanan RI Nomor 38 Tahun 2015 tentang Doktrin Pertahanan Negara 2015.

Peraturan Menteri Pertahanan RI Nomor 32 Tahun 2016 tentang Pedoman Pembinaan Kesadaran Bela Negara.

Peraturan Menteri Pertahanan RI Nomor 19 Tahun 2019 tentang Pertahanan Nir-militer.

Peraturan Menteri Komunikasi dan Informatika RI Nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI).

Keputusan Menteri Pertahanan RI Nomor Kep/104/M/I/2020 tanggal 20 Januari 2020 tentang Kebijakan Pertahanan Negara tahun 2020.

Keputusan Panglima TNI Nomor Kep/1355/XII/2018 Tanggal 18 Desember 2018 tentang Doktrin Siber Tentara Nasional Indonesia.

Dokumen

Badan Litbang SDM Kominfo. (2016). “Penyusunan Roadmap Pembangunan Sektor TIK yang Mengikat Secara Jangka Panjang s.d 2045 Menuju 100 Tahun Indonesia merdeka”. Jakarta: Badan Litbang SDM Kominfo.

Badan Siber dan Sandi Negara (BSSN). (2019). Draft/Konsep "Strategi Keamanan Siber Nasional (SKSN) 2020 – 2024". Jakarta: Badan Siber dan Sandi Negara.

Badan Siber dan Sandi Negara (BSSN). (2019). "Roadmap Pembinaan SDM Keamanan Siber dan Sandi 2020 – 2024 (Menuju SDM Keamanan Siber & Sandi Yang Terpercaya, Profesional, dan Berdaya Saing". Jakarta: Direktorat Pengendalian SDM, Deputi IV, Badan Siber dan Sandi Negara.

Badan Siber dan Sandi Negara (BSSN). (2019). "Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber". Jakarta: Badan Siber dan Sandi Negara.

Departemen Petahanan RI. 2007. Strategi Pertahanan Negara. Jakarta: Departemen Pertahanan Republik Indonesia.

Kementerian Pertahanan RI. 2014. Pedoman Pertahanan Siber. Jakarta: Kementerian Pertahanan Republik Indonesia.

Kementerian Pertahanan RI. 2015. Buku Putih Pertahanan Indonesia 2015. Jakarta: Kementerian Pertahanan Republik Indonesia.

Kementerian Pertahanan RI. 2015. Doktrin Pertahanan Negara 2015: Postur Pertahanan Negara. Jakarta: Kementerian Pertahanan Republik Indonesia.

Tentara Nasional Indonesia (TNI) dan Badan Siber Sandi Negara (BSSN). 2018. Nota Kesepahaman antara TNI dan BSSN (Nomor Kerma/44/XI/2018 dan Nomor PERJ.337/KBSSN/KH.02.01/11/2018). Jakarta: Mabes TI dan BSSN.

Puslitbang SDPPI Balitbang SDM Kominfo. (2018). "Rencana Pengembangan SDM TIK di Indonesia Melalui Sertifikasi SKKNI Bidang Kominfo". Jakarta: Puslitbang SDPPI Balitbang SDM Kominfo.

Jurnal

Nurkholis. (2013). "Pendidikan Dalam Upaya Memajukan Teknologi", Jurnal Kependidikan, Nopember 2013, Volume 1 Nomor 1, hh 24-44.

Referensi dari Sumber Elektronik

Ardiyanti, Handrini. (2014). "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia". Jurnal Politica DPR RI, Vol 5, Nomor 1 (1 Juni 2014), pp. 95-110. *Retrieved from*: https://www.academia.edu/36335260/CYBER_SECURITY_DAN_TANTANGAN_PENGEMBANGANNYA_DI_INDON, diakses pada 20 Juni 2020.

Anonim. (2017). “Rancangan Undang-Undang RI tentang Keamanan Nasional”, (Draft/Konsep pada Rapat tanggal 16 Oktober 2012). Retrieved from: https://fdokumen.com/download/?url=1a84f912c2bbfa7f6f1e329129dd758b89e52e98dfac50bd2cdb7e7b6f88b4b21f43e10ba32e34558d31ab2f6d0b1e307ab48aa02698b1fff4ff12931b2bd454Z+Lo2AN4pGynfvGFYm7/v9sTGxQ8Cssd98xyExU1QjwnlTkwg7TcsChR+XBhOaNFC0bJEPnq22QANK9rLcbUGw==, diakses pada 5 Agustus 2020.

Anonim. (2019). “Rancangan Undang-Undang RI tentang Keamanan dan Ketahanan Siber”, (Draft/Konsep pada Badan Legislasi DPR bulan Mei 2019). Retrieved from: http://institute.id/wp-content/uploads/2019/09/RUU-Keamanan-dan-Ketahanan-Siber.pdf, diakses pada 5 Agustus 2020.

Artiadi, Bagus. (2013). Media Informasi Ditjen Pothan Kemhan “Perlunya Pembangunan Pertahanan Siber (*Cyber Defense*) Yang Tangguh Bagi Indonesia”. Retrieved from https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence.pdf, diakses pada 5 Juli 2020.

Beritasatu. (2019). “Asops Panglima TNI Tinjau Tempat Latihan *Cobra Gold* 2019 di Thailand”. *Retrieved from*: https://www.beritasatu.com/asnie-ovier/nasional/539738/asops-panglima-tni-tinjau-tempat-latihan-cobra-gold-2019-di-thailand, diakses pada 25 September 2020.

BSSN. (2018). “Sejarah Pembentukan BSSN”. Retrieved from: https://bssn.go.id/sejarah-pembentukan-bssn/, diakses pada 25 November 2019.

BSSN. (2018). Photo “Penandatanganan MoU (Nota Kesepahaman Bersama) antara BSSN dan TNI”. *Retrieved from*: https://www.facebook.com/badansiberdansandinegara/photos/penandatanganan-mou-oleh-kepala-bssn-dr-djoko-setiadi-msi-dan-panglima-tni-marse/2057664020963438/, diakses pada 20 September 2019.

BSSN. (2019). Artikel “Pentingnya Kolaborasi Dan Kerjasama Dalam Keamanan Siber Untuk Menjamin Pertahanan Negara”. *Retrieved from*: https://bssn.go.id/pentingnya-kolaborasi-dan-kerjasama-dalam-keamanan-siber-untuk-menjamin-pertahanan-negara/, diakses pada 20 September 2019.

BSSN. (2019). “Kenali Penanganan Insiden Siber; BSSN Selenggarakan *Drill Test* II Sektor Pemerintah”. *Retrieved from*: https://bssn.go.id/kenali-penanganan-insiden-siber-bssn-selenggarakan-drill-test-ii-sektor-pemerintah/, diakses pada 20 September 2019.

Cyber Security IPB. (2015). Photo "Kegiatan Cyber Jawara 2015". *Retrieved from*: https://www.facebook.com/cysecipb/posts/cyber-jawara-adalah-kompetisi-tahunan-di-bidang-cyber-security-yang-diadakan-ole/682031931932070/, diakses pada 24 September 2020.

Direktorat Jenderal Aplikasi dan Informatika Kementerian Kominfo. (2016). "Kebijakan Keamanan dan Pertahanan Siber". *Retrieved from*: https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/, diakses pada 15 Juni 2020.

Eset, Microsoft Windows. (2010). "*Stuxnet Under the Microsoft*". Retrieved from: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf, diakses pada 21 Agustus 2020.

Islami, Maulia Jayantina. (2017). "Tantangan Dalam Implementasi Strategi Keamanan Siber Naisonal Indonesia Ditinjau Dari Penilaian *Global Cybersecurity Index*". Jurnal Masyarakat Telematika dan Informasi, Vol 8, Nomor 2 (Oktober – Desember 2017), pp. 137-144. Doi: http://dx.doi.org/10.17933/mti.v8i2.108, diakses pada 20 Juni 2020.

International Telecomunication Union (ITU). (2008). Recommendation ITU-T X.1205 "*Overview of Cybersecurity*". *Retrieved from*: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items, diakses pada 15 Juni 2020.

International Telecomunication Union (ITU). (2011). "*ITU National Cybersecurity Guide*". *Retrieved from*: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf, diakses pada 15 Juni 2020.

Keamanan (n.d). Dalam Kamus Besar Bahasa Indonesia (KBBI) *Online*. Retrieved from: https://kbbi.web.id/aman, diakses pada 10 Juni 2020.

Kementerian Pertahanan, Bainstrahan. (2019). "Pushansiber Menerima Kunjungan BSSN Terkait Koordinasi Identifikasi Sektor IIKN". *Retrieved from*: https://www.kemhan.go.id/bainstrahan/2019/02/20/pushansiber-menerima-kunjungan-bssn-terkait-koordinasi-identifikasi-sektor-iikn.html, diakses pada 25 September 2020.

Kementerian Pertahanan, Bainstrahan. (2019). "Kapushansiber Menerima Kunjungan Kerja Kepala BSSN". *Retrieved from*: https://www.kemhan.go.id/bainstrahan/2019/06/28/kapushansiber-menerima-kunjungan-kerja-kepala-bssn.html, diakses pada 25 September 2020.

Kementerian Pertahanan, Bainstrahan. (2019). "Puhansiber Hadiri *Cybersecurity Drill test*". *Retrieved from*: https://www.kemhan.go.id/bainstrahan/2019/03/28/pushansiber-

hadiri-kegiatan-cyber-security-drill-test.html, diakses pada 25 September 2020.

Kementerian Pertahanan, Bainstrahan. (2019). "FGD Kajian Strategi Organisasi BSSN Dalam Rangka Mengonsolidasi Unsur Keamanan Siber". *Retrieved from*: https://www.kemhan.go.id/bainstrahan/2019/03/18/fgd-kajian-strategi-organisasi-bssn-dalam-rangka-mengonsolidasi-unsur-keamanan-siber.html, diakses pada 25 September 2020.

Kementerian Pertahanan, Bainstrahan. (2019). "Ingin Bangun Pertahanan Siber Kemhan, Wamenhan: Yang Terpenting Adalah SDM". *Retrieved from*: https://www.kemhan.go.id/bainstrahan/2019/11/14/ingin-bangun-pertahanan-siber-kemhan-wamenhan-yang-terpenting-adalah-sdm.html, diakses pada 25 September 2020.

Kumparan (2019). "Kominfo Siapkan 25.000 Beasiswa *Digital Talent Scholarship* 2019". *Retrieved from*: https://kumparan.com/kumparantech/kominfo-siapkan-25-000-beasiswa-digital-talent-scholarship-2019-1qv9hh6yMgt, diakses pada 25 September 2020.

Kominfo. (2017). "Sosialisasi Beasiswa S2 Dalam Negeri Bidang Komunikasi Di Kota Pontianak". *Retrieved from*: https://proserti.kominfo.go.id/press-release/detail/17/sosialisasi-beasiswa-s2-dalam-negeri-bidang-komunikasi--di-kota-pontianak, diakses pada 26 September 2020.

Kominfo. (2020). "Program DTS Komifo Tahun 2020". *Retrieved from*: https://digitalent.kominfo.go.id/, diakses pada 27 September 2020.

Kominfo, BPPTIK. (2020). "Kepala Balitbang SDM Membuka Pelatihan dan Sertifikasi Kompetensi Bidang TIK Berbasis SKKNI Gelombang ke-1 Tahun 2020 Secara *Online*". *Retrieved from*: https://bpptik.kominfo.go.id/2020/06/10/7904/kepala-balitbang-sdm-membuka-pelatihan-dan-sertifikasi-kompetensi-bidang-tik-berbasis-skkni-gelombang-ke-1-tahun-2020-secara-online/, diakses pada 27 September 2020.

Opdebeeck, Jean Sebastien. (2018). "*People, Processes dan Technology are the pillars of CyberSecurity*". *Retrieved from*: https://www.vulpoint.com/people-processes-technology-cybersecurity/#page-content, diakses pada 20 Juni 2020.

Pascasarjana. (2016). Universitas Pendidikan Ganesha "Desain Penelitian Kualitatif". *Retrieved from*: http://pasca.undiksha.ac.id/wp-content/uploads/2019/06/2-DesainPenelitianKualitatif.pdf, diakses pada 15 Juli 2020.

Penabali. (2019). Berita "TNI Telah Kembangkan *Cyber*, Latihan ISTX Diaplikasikan Dalam Bertugas". *Retrieved from*: https://penabali.com/berita/tni-telah-kembangkan-cyber-latihan-istx-diaplikasikan-dalam-bertugas/, diakses pada 21 September 2020.

Puspen TNI. (2018). "Pangab Thailand Buka Latma *Cobra Gold* 2018". *Retrieved from*: https://tni.mil.id/view-126349-pangab-thailand-buka-latma-cobra-gold-2018.html, diakses pada 29 September 2020.

Smartivist. (2019). "Menyoal Standardisasi Kompetensi SDM Keamanan Siber". Retrieved from: http://www.smartcityindo.com/2019/12/menyoal-standardisasi-kompetensi-sdm.html, diakses pada 10 Juni 2020.

Subagyo, Agus. (2015). "Sinergi Dalam Menghadapi Ancaman *Cyber Warfare*". Jurnal Pertahanan dan Bela Negara, Vol 5, Nomor 1 (April 2015), pp. 89-108. Doi: http://dx.doi.org/10.33172/jpbh.v5i1.350, diakses pada 20 Juni 2020.

Tim Kerja Pertahanan Siber Kementerian Pertahanan RI. (2013). "Peta Jalan Strategi Nasional Pertahanan Siber". Retrieved from: https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf, diakses pada 5 Juli 2020.

Tim Peneliti Puslitbang SDPPI. (2018). "Rencana Pengembangan SDM TIK di Indonesia Melalui Sertifikasi SKKNI Bidang Kominfo". *Retrieved From*: https://balitbangsdm.kominfo.go.id/?mod=publikasi&a=dl&page_id=461&cid=29&download_id=195, diakses pada 5 Agustus 2020.

Universitas Pertahanan. (2019). "Forum Komunikasi Bakomumas Bahas Keamanan *Cyber* Untuk Pertahanan Negara". *Retrieved from*: https://www.idu.ac.id/berita/forum-komunikasi-bakohumas-bahas-keamanan-cyber-untuk-pertahanan-negara.html, diakses pada 30 September 2020.

Urgensi (n.d). Dalam Kamus Besar Bahasa Indonesia (KBBI) *Online*. Retrieved from: https://kbbi.web.id/urgensi, diakses pada 5 Agustus 2020.

Urgent (Def.1) (n.d). In *Oxford Learner's Dictionaries* o*nline*. Retrieved from: https://www.oxfordlearnersdictionaries.com/definition/english/urgent?q=urgent, diakses pada 5 Agustus 2020.

Wibowo, Satriyo. Fajar Rulhudana. (2018). "Keamanan Siber dalam Peta SDM Teknologi Indonesia". Retrieved from: https://inet.detik.com/cyberlife/d-4001592/keamanan-siber-dalam-peta-sdm-teknologi-indonesia, diakses pada 10 Juni 2020.

Zaelani, Hamzah. I Wayan Midhio dan Yono Reksoprodjo. (2018). "Pembangunan Kapasitas *Cyber Security* di Negara ASEAN: Analisis Komparatif Terhadap Brunei dan Indonesia". Jurnal Prodi Perang Asimetris, Vol 4, Nomor 1 (April 2018), pp. 77-92. *Retrieved from*: http://jurnalprodi.idu.ac.id/index.php/PA/article/view/197/179, diakses pada 8 Agustus 2020.

LAMPIRAN – LAMPIRAN

Lampiran – 1 (Surat Perintah Penelitian)

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN

SURAT PERINTAH
NOMOR : SPRIN/ 810 /V/2020

Menimbang : bahwa dalam rangka kegiatan tugas akhir Tesis Mahasiswa Pascasarjana Program Studi Strategi Perang Semesta Fakultas Strategi Pertahanan Universitas Pertahanan TA. 2019/2020 perlu di keluarkan Surat Perintah.

Dasar :
1. Peraturan Presiden Nomor 5 Tahun 2011 tentang Universitas Pertahanan sebagai Perguruan Tinggi yang Diselenggarakan Oleh Pemerintah;
2. Kalender Pendidikan Program Studi Strategi Perang Semesta Fakultas Strategi Pertahanan Universitas Pertahanan TA. 2019/2020.

DIPERINTAHKAN:

Kepada : Nama) Pangkat/Gol/NRP/NIP) Jabatan) sebagaimana tercantum dalam lampiran surat perintah ini

Untuk :
1. Seterimanya surat perintah ini, agar melaksanakan tugas sebagai Dosen Pembimbing Tesis pada Progam Studi Strategi Perang Semesta (SPS) Fakultas Strategi Pertahanan Universitas Pertahanan TA. 2019/2020.
2. Surat perintah ini berlaku mulai dari awal sampai berakhirnya periode Akademik TA. 2019/2020.
3. Melapor kepada Rektor Universitas Pertahanan atas pelaksanaan surat perintah ini.
4. Melaksanakan perintah ini dengan saksama dan penuh rasa tanggungjawab.

Selesai.

Dikeluarkan di Bogor
pada tanggal 18 Mei 2020

Rektor
Universitas Pertahanan,

Dr. Amarulla Octavian, S.T., M.Sc., DESD
Laksamana Muda TNI

Tembusan:
1. Warek Unhan
2. Dekan FSP Unhan
3. Karo Unhan.

Lampiran I Surat Perintah Rektor Unhan
Nomor : SPRIN/ 810 /V/ 2020
Tanggal : 18 Mei 2020

JUDUL TESIS DAN DOSEN PEMBIMBING
PRODI STRATEGI PERANG SEMESTA FAKULTAS STRATEGI PERTAHANAN
***COHORT*-11 TA 2019-2020**

NO	NAMA	JUDUL TESIS	DOSEN PEMBIMBING
1	AFRIZAL NURMAN NIM 120190101001	Implementasi Bela Negara di Lingkungan Organisasi Kemasyarakatan Sebagai Komponen Pendukung Pertahanan Negara (Studi Pada Organisasi Kemasyarakatan Gerakan Pemuda Ansor).	1. Mayjen TNI Dr. Hipdizah, S.Adm., M.Si. 2. Kolonel Caj Dr. Surryanto D.W, M.H., M.M.
2	AHMAD JUNAIDI SALEH NIM 120190101002	Fenomena Paradigmatif NKRI Bersyariah di Indonesia Dalam Perspektif Pertahanan Negara.	1. Brigjen TNI Dr. Yusuf, M.M. 2. Kolonel Czi Helda Risman, M.Han.
3	ATAM NIM 120190101003	Implikasi Program Deradikalisasi Narapidana Terorisme terhadap Aspek Pertahanan Negara (Studi Kasus di Lembaga Permasyarakatan Cipinang-Jakarta).	1. Mayjen TNI Dr. Deni Dadang AR, M.Si.(Han) 2. Brigjen TNI Dr. Joni Widjayanto, S.Sos., M.M.
4	HARIMURTI WICAKSONO NIM 120190101004	Peran Bawaslu Dalam Penanganan Pelanggaran Politik Uang untuk memperkuat Pertahanan Nirmiliter (Studi Kasus Pilkada Kabupaten/Kota Se Malang Raya).	1. Letjen (Purn) Dr. I Wayan Midhio, M.Phil. 2. Brigjen TNI Dr. Joni Widjayanto, S.Sos., M.M.
5	HERY MISBIANTORO NIM 120190101005	Tantangan Implementasi Bela Negara Masyarakat Hulu Sungai Citarum dalam Menghadapi Globalisasi Global.	1. Mayjen (Purn) Dr. M. Nakir, S.IP., M.AP. 2. Kolonel Czi Wayan Nuriada, SH., M.Si (Han)
6	IRWAN FIRDAUS NIM.120190101006	Pemilihan Pangkalan Strategis TNI AL di Wilayah ALKI 1 Untuk Mendukung Operasi Pertahanan Laut Dalam Menghadapi Ancaman Konflik di Laut China Selatan.	1. Mayjen (Mar/Purn) Dr. Ir. Syaiful Anwar, M.Bus., M.A. 2. Kolonel Lek Rayanda Barnas, M.Si (Han)
7	KARTOLI NIM.120190101007	Implementasi Pembinaan Kesadaran Berbangsa dan Bernegara Terhadap Narapidana Terorisme di Lembaga Pemasyarakatan Cipinang-Jakarta.	1. Mayjen (Purn) Dr. Muhammad Nakir, S.IP., M.H. 2. Kolonel Adm Afrizal Hendra, S.I.P., M. Si., M.Si (Han)
8	KUNTO WIBOWO AGUNG PRODJONOTO NIM. 120190101008	Strategi Pendaratan Pantai Sebagai Cara Bertindak dalam Operasi Penanggulangan Bencana TNI.	1. Mayjen (Purn) Dr. Drs. TSL Toruan, M.M., Dipl.S.S. 2. Kolonel Pas Dr. Drs. Marsono, M.Si.
9	NOVI HERIANTO NIM.120190101009	Tantangan Dilematis Implementasi Dewan Pertahanan Nasional.	1. Mayjen TNI Dr. Deni Dadang AR, M.Si.(Han 2. Kolonel Adm Afrizal Hendra, S.I.P., M. Si., M.Si (Han)
10	RAHMAT SADLI NIM.120190101010	Implementasi Bela Negara Resimen Mahasiswa Satuan 702 Universitas Negeri Makassar Sebagai Komponen Cadangan Dalam Sistem Pertahanan Negara.	1. Prof. Dr. H. Djaali 2. Dr. Drs. Sutrimo., M.M., M.Si
11	RIZQA NOOR ABDI NIM.120190101011	Implikasi Implementasi Regulasi Penataan Daerah terhadap Kebijakan Penataan Wilayah Pertahanan di Daerah.	1. Mayjen (Purn) Dr. Drs.TSL Toruan, M.M., Dipl.S.S. 2. Mayjen TNI Dr. Hipdizah, S.Adm., M.Si.
12	RUBY ALAMSYAH NIM.120190101012	Strategi Keamanan Siber Nasional dalam Mendukung Sistem Pertahanan Negara.	1. Letjen (Purn) Dr. I Wayan Midhio, M.Phil. 2. Dr. Agus Hasan S Reksoprodjo, ST., DIC.
13	WERIJON NIM.120190101013	Arah Baru Radikalisme Sebagai Ancaman terhadap Disintegrasi Bangsa.	1. Mayjen (Mar/Purn) Dr. Ir. Syaiful Anwar, M.Bus., M.A 2. Kolonel Czi Helda Risman, M.Han
14	YANA HARDIYANA NIM.120190101014	Fortifikasi Bakamla Sebagai *Coast Guard* Indonesia dalam Penegakan Hukum di Laut.	1. Laksda TNI Dr. Suhirwan, S.T., M.MT 2. Kolonel Pas Dr. Drs. Bastari R, M.Pd., M.Sc., M.Si (Han)

Rektor
Universitas Pertahanan,

Dr. Amerulla Octavian, S.T., M.Sc., DESD
Laksamana Muda TNI

Lampiran – 2 (Surat Permohonan Penelitian)

L-2.1 Surat Permohonan Izin Penelitian Kepada Kapushansiber Kemhan RI.

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN
Terakreditasi BAN-PT "A"

Nomor B/ 1820 /VIII/2020
Klasifikasi Biasa
Lampiran -
Hal Permohonan Izin Penelitian.

Bogor, 24 Agustus 2020

Kepada

Yth. Kepala Pusat Pertahanan Siber, Kemhan RI

di

Tempat

1 Dasar:

a. Peraturan Presiden RI Nomor 5 Tahun 2011 tanggal 7 Februari 2011 tentang Universitas Pertahanan Sebagai Perguruan Tinggi yang Diselenggarakan Oleh Pemerintah;

b. Surat Perintah Rektor Universitas Pertahanan Nomor 810/V/2020 tanggal 18 Mei 2020 tentang pembimbingan Tesis pada Program Studi Strategi Perang Semesta Fakultas Strategi Pertahanan Universitas Pertahanan;

c. Kalender Akademik Program Studi Strategi Perang Semesta Unhan TA. 2019/2020.

2. Sehubungan dasar di atas, mohon dapatnya Bapak/Ibu pejabat berkenan mengizinkan mahasiswa program studi Strategi Perang Semesta *Cohort* -11 Universitas Pertahanan TA. 2019/2020 atas nama Ruby Alamsyah NIM 120190101012 untuk melakukan penelitian melalui wawancara, observasi dan studi dokumen / laporan yang diperlukan dalam penyusunan tesis dengan judul " Urgensi Strategi Keamanan Siber Nasional Dalam mendukung Sistem Pertahanan Negara "

3. Mohon konfirmasi waktu dalam pelaksanaan pengumpulan data tersebut. *Contact Person* e-mail rbyalamsyah@gmail.com dan HP +62 817-381-992.

4. Demikian mohon menjadikan periksa.

a.n. Rektor
Universitas Pertahanan
Warek III Bid. Kerja Sama dan Kelembagaan,

Dr. Hipdizah, S.Adm., M.Si., CIQnR.
Mayor Jenderal TNI

Tembusan:
1 Sekjen Kemhan RI
2. Rektor Unhan
3. Kabainstrahan Kemhan RI

L-2.2 Surat Permohonan Izin Penelitian Kepada Komandan Satsiber TNI.

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN
Terakreditasi BAN-PT "A"

Nomor : B/ 1830 /VIII/2020
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan Izin Penelitian.

Bogor, 24 Agustus 2020

Kepada

Yth. Komandan Satuan Siber TNI,
Mabes TNI

di

Tempat

1. Dasar:
   a. Peraturan Presiden RI Nomor 5 Tahun 2011 tanggal 7 Februari 2011 tentang Universitas Pertahanan Sebagai Perguruan Tinggi yang Diselenggarakan Oleh Pemerintah;
   b. Surat Perintah Rektor Universitas Pertahanan Nomor 810/V/2020 tanggal 18 Mei 2020 tentang pembimbingan Tesis pada Program Studi Strategi Perang Semesta Fakultas Strategi Pertahanan Universitas Pertahanan;
   c. Kalender Akademik Program Studi Strategi Perang Semesta Unhan TA. 2019/2020.
2. Sehubungan dasar di atas, mohon dapatnya Bapak/Ibu pejabat berkenan mengizinkan mahasiswa program studi Strategi Perang Semesta *Cohort* -11 Universitas Pertahanan TA. 2019/2020 atas nama Ruby Alamsyah NIM 120190101012 untuk melakukan penelitian melalui wawancara, observasi dan studi dokumen / laporan yang diperlukan dalam penyusunan tesis dengan judul " Urgensi Strategi Keamanan Siber Nasional Dalam mendukung Sistem Pertahanan Negara ".
3. Mohon konfirmasi waktu dalam pelaksanaan pengumpulan data tersebut. *Contact Person* e-mail : rbyalamsyah@gmail.com dan HP +62 817-381-992.
4. Demikian mohon menjadikan periksa.

a.n. Rektor
Universitas Pertahanan
Warek III Bid. Kerja Sama dan Kelembagaan,

Dr. Hipdizah, S.Adm., M.Si., CIQnR.
Mayor Jenderal TNI

Tembusan:
1. Rektor Unhan
2. Kasatwas Unhan
3. Dekan FSP Unhan
4. Ka LPPM Unhan
5. Karorenku Unhan
6. Karo Aka dan Kemahasiswaan Unhan.

L-2.3 Surat Permohonan Izin Penelitian Kepada Kepala Balitban SDM Kementerian Kominfo.

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN
Terakreditasi BAN-PT "A"

Nomor : B/ 1830 /VIII/2020
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan Izin Penelitian.

Bogor, 24 Agustus 2020

Kepada

Yth. Kepala Badan Penelitian dan Pengembangan SDM
Kementerian Kominfo RI

di

Tempat

1. Dasar:
   a. Peraturan Presiden RI Nomor 5 Tahun 2011 tanggal 7 Februari 2011 tentang Universitas Pertahanan Sebagai Perguruan Tinggi yang Diselenggarakan Oleh Pemerintah;
   b. Surat Perintah Rektor Universitas Pertahanan Nomor 810/V/2020 tanggal 18 Mei 2020 tentang pembimbingan Tesis pada Program Studi Strategi Perang Semesta Fakultas Strategi Pertahanan Universitas Pertahanan;
   c. Kalender Akademik Program Studi Strategi Perang Semesta Unhan TA. 2019/2020.
2. Sehubungan dasar di atas, mohon dapatnya Bapak/Ibu pejabat berkenan mengizinkan mahasiswa program studi Strategi Perang Semesta *Cohort* -11 Universitas Pertahanan TA. 2019/2020 atas nama Ruby Alamsyah NIM 120190101012 untuk melakukan penelitian melalui wawancara, observasi dan studi dokumen / laporan yang diperlukan dalam penyusunan tesis dengan judul " Urgensi Strategi Keamanan Siber Nasional Dalam mendukung Sistem Pertahanan Negara ".
3. Mohon konfirmasi waktu dalam pelaksanaan pengumpulan data tersebut. *Contact Person* e-mail : rbyalamsyah@gmail.com dan HP +62 817-381-992.
4. Demikian mohon menjadikan periksa.

a.n. Rektor
Universitas Pertahanan
Warek III Bid. Kerja Sama dan Kelembagaan,

Dr. Hipdizah, S.Adm., M.Si., CIQnR.
Mayor Jenderal TNI

Tembusan:
1. Rektor Unhan
2. Kasatwas Unhan
3. Dekan FSP Unhan
4. Ka LPPM Unhan
5. Karorenku Unhan
6. Karo Aka dan Kemahasiswaan Unhan.

L-2.4 Surat Permohonan Izin Penelitian Kepada Kepala Badan Siber dan Sandi Negara.

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN
Terakreditasi BAN-PT "A"

Nomor : B/ 1830 /VIII/2020
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan Izin Penelitian.

Bogor, 24 Agustus 2020

Kepada

Yth. Kepala Badan dan Siber Sandi Negara

di

Tempat

1. Dasar:
   a. Peraturan Presiden RI Nomor 5 Tahun 2011 tanggal 7 Februari 2011 tentang Universitas Pertahanan Sebagai Perguruan Tinggi yang Diselenggarakan Oleh Pemerintah;
   b. Surat Perintah Rektor Universitas Pertahanan Nomor 810/V/2020 tanggal 18 Mei 2020 tentang pembimbingan Tesis pada Program Studi Strategi Perang Semesta Fakultas Strategi Pertahanan Universitas Pertahanan;
   c. Kalender Akademik Program Studi Strategi Perang Semesta Unhan TA. 2019/2020.
2. Sehubungan dasar di atas, mohon dapatnya Bapak/Ibu pejabat berkenan mengizinkan mahasiswa program studi Strategi Perang Semesta *Cohort* -11 Universitas Pertahanan TA. 2019/2020 atas nama Ruby Alamsyah NIM 120190101012 untuk melakukan penelitian melalui wawancara, observasi dan studi dokumen / laporan yang diperlukan dalam penyusunan tesis dengan judul " Urgensi Strategi Keamanan Siber Nasional Dalam mendukung Sistem Pertahanan Negara ".
3. Mohon konfirmasi waktu dalam pelaksanaan pengumpulan data tersebut. *Contact Person* e-mail : rbyalamsyah@gmail.com dan HP +62 817-381-992.
4. Demikian mohon menjadikan periksa.

a.n. Rektor
Universitas Pertahanan
Warek III Bid. Kerja Sama dan Kelembagaan,

Dr. Hipdizah, S.Adm., M.Si., CIQnR.
Mayor Jenderal TNI

Tembusan:
1. Rektor Unhan
2. Kasatwas Unhan
3. Dekan FSP Unhan
4. Ka LPPM Unhan
5. Karorenku Unhan
6. Karo Aka dan Kemahasiswaan Unhan.

Lampiran – 3 (Surat Keterangan Penelitian)

L-3.1 Surat Keterangan Penelitian di Pushansiber Kemhan RI.

BADAN INSTALASI STRATEGIS PERTAHANAN KEMHAN RI
PUSAT PERTAHANAN SIBER

SURAT KETERANGAN

Berdasarkan Surat Rektor Unhan Nomor: B/1820/VIII/2020 tanggal 24 Agustus 2020 tentang Permohonan Izin Penelitian Mahasiswa Program Pasca Sarjana Fakultas Strategi Pertahanan Universitas Pertahanan.

Dengan ini menerangkan bahwa mahasiswa Program Studi Strategi Perang Semesta (SPS) Cohort-11, Fakultas Strategi Pertahanan (FSP), Universitas Pertahanan TA.2019/2020, atas nama Ruby Alamsyah NIM 120190101012, telah melaksanakan penelitian untuk tesis berjudul "Urgensi Strategi Keamanan Siber Nasional Dalam Mendukung Sistem Pertahanan Negara: Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya SDM Pertahanan Siber", dengan teknik pengumpulan data melalui wawancara, observasi dan studi dokumen/laporan yang diperlukan.

Kegiatan tersebut dilaksanakan pada hari Kamis tanggal 3 September 2020, secara tatap muka di kantor Pushansiber Kemhan, Pondok Labu - Jakarta Selatan, serta berjalan baik dan lancar.

Demikian surat keterangan ini dibuat untuk digunakan sebagaimana mestinya.

Jakarta, 3 September 2020

a.n. Kepala Pusat Pertahanan Siber
Kabid Penjaminan Keamanan,

R. Trisatya Wicaksono, M.I.T.
Kolonel Sus NRP. 520738

L-3.2 Surat Keterangan Penelitian di Satsiber TNI.

MARKAS BESAR TENTARA NASIONAL INDONESIA
SATUAN SIBER

Jakarta, 21 Oktober 2020

Nomor : B/ 360-17/05/02/Satsiber
Klasifikasi : Biasa
Lampiran : -
Perihal : Kegiatan observasi di Satsiber TNI

Kepada
Yth. Rektor UNHAN
di
Tempat

1. Dasar :

a. Peraturan Panglima TNI nomor 71 Tahun 2019 tentang organisasi dan tugas Satuan Siber TNI; dan

b. Surat Rektor Universitas Pertahanan Nomor B/1820/VIII/2020 tanggal 24 Agustus 2020 tentang permohonan izin penelitian.

2. Sehubungan dasar di atas, menyampaikan bahwa atas nama bapak Ruby Alamsyah NIM 120190101012 mahasiswa program studi Strategi Perang Semesta *Cogort*-11 Universitas Pertahanan TA 2019/2020 telah melaksanakan wawancara dan observasi di Satsiber TNI.

3. Demikian mohon dimaklumi.

a.n. Komandan Satuan Siber TNI
Asisten Operasi,

Eko Wing Wahjudi, S.T
Kolonel Laut (E) NRP 9628/P

Tembusan:

- Dansatsiber TNI

L-3.3 Surat Izin dan Keterangan Penelitian dari/di Balitbang SDM Kominfo.

KEMENTERIAN KOMUNIKASI DAN INFORMATIKA RI
BADAN PENELITIAN DAN PENGEMBANGAN SUMBER DAYA MANUSIA
SEKRETARIAT BADAN PENELITIAN DAN PENGEMBANGAN SUMBER DAYA MANUSIA
"Menuju Masyarakat Informasi Indonesia"
Jl. Medan Merdeka Barat No. 9 Jakarta 10110 Telp./Fax. 021-3856068

Nomor : B- 922 /BLSDM.1/LT.01.02/09/2020 Jakarta, 7 September 2020
Perihal : Izin Penelitian

Kepada Yth.
Wakil III Bidang Kerja Sama dan Kelembagaan
Universitas Pertahanan
di –
Tempat

Menanggapi surat Saudara Nomor B/1870/VIII/2020 tertanggal 24 Agustus 2020 tentang Permohonan Ijin Penelitian, dapat kami sampaikan bahwa kami menyambut dengan baik permohonan ijin dimaksud untuk penyusunan tesis Sdr. Ruby Alamsyah dengan judul penelitian "Urgensi Strategi Keamanan Siber Nasional Dalam Mendukung Sistem Pertahanan Negara". Pelaksanaan penelitian melalui metode wawancara, observasi ataupun studi dokumen dapat dilaksanakan dengan menghubungi Pusat Penelitian dan Pengembangan Sumber Daya, Perangkat dan Penyelenggaraan Pos dan Informatika dengan Contact Person Sdr. Riza Azmi, Koordinator Bidang Penyelenggaraan Penelitian melalui surel riza001@kominfo.go.id.

Demikian hal ini disampaikan. Atas perhatian Saudara, kami ucapkan terima kasih

Ditandatangani secara elektronik oleh:
SEKRETARIS BADAN PENELITIAN DAN PENGEMBANGAN SUMBER DAYA MANUSIA
Haryati

Tembusan Yth.
1. Kepala Badan Litbang SDM (sebagai Laporan)
2. Kepala Pusat Penelitian dan Pengembangan Sumber Daya, Perangkat dan Penyelenggaraan Pos dan Informatika

KEMENTERIAN KOMUNIKASI DAN INFORMATIKA RI
BADAN PENELITIAN DAN PENGEMBANGAN SUMBER DAYA MANUSIA
PUSLITBANG SUMBER DAYA, PERANGKAT, DAN PENYELENGGARAAN POS DAN INFORMATIKA
Menuju Masyarakat Informasi Indonesia
Jl. Medan Merdeka Barat No. 9, Jakarta, 10110, Telp./Fax. 021-34833640
Email: puslitbang.sdppi@mail.kominfo.go.id, Website: https://balitbang.kominfo.go.id/

SURAT KETERANGAN

Nomor : 50 /BLSDM.2.1/LT.01.01/10/2020

Dengan ini menerangkan bahwa:

Nama	:	Kol. Ruby Alamsyah
Program Studi	:	Strategi Perang Semesta (SPS) Cohort-11
Fakultas	:	Strategi Pertahanan
Universitas	:	Universitas Pertahanan TA.2019/2020
Judul Thesis	:	"Urgensi Strategi Keamanan Siber Nasional dalam Mendukung Sistem Pertahanan Negara: Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya SDM Pertahanan Siber"
Ref. kegiatan	:	Surat Rektor Unhan Nomor: B/1820/VIII/2020 tanggal 24 Agustus 2020 tentang Permohonan Izin Penelitian Mahasiswa Program Pasca Sarjana Fakultas Strategi Pertahanan Universitas Pertahanan

telah melaksanakan wawancara untuk kegiatan penelitian dengan judul termaksud di atas yang dilaksanakan pada hari Selasa tanggal 8 September 2020 secara daring.

Demikian surat keterangan dibuat ini untuk digunakan sebagaimana mestinya dan mahasiswa tersebut harus melaporkan hasil kegiatan pengumpulan datanya kepada Kepala Puslitbang SDPPPI, Kementerian Komunikasi dan Informatika setelah data diolah.

Jakarta, 9 Oktober 2020

a.n Kepala Puslitbang SDPPPI
Kepala Bidang Penyelenggaraan Penelitian

Riza Azmi

L-3.4 Surat Keterangan Penelitian di BSSN.

BADAN SIBER DAN SANDI NEGARA
Jalan Raya Muchtar Nomor 70, Kel. Bojong Sari Lama, Kec. Bojong Sari, Depok 16518
Telepon (021) 77973360, Faksimile (021) 78844104, 77973579
Website : https://bssn.go.id, *E-mail* : humas@bssn.go.id

SURAT KETERANGAN

NOMOR: KET.603/BSSN/D4/KP.07.01/10/2020

Yang bertanda tangan di bawah ini,

nama : Dame Ria Munthe, S.E.
NIP : 19621004 198310 2 001
jabatan : Direktur Pengendalian Sumber Daya Manusia

dengan ini menerangkan bahwa

nama : Ruby Alamsyah
NIM : 120190101012
progdi : Strategi Perang Semesta (SPS) Cohort-11
fakultas : Fakultas Strategi Pertahanan (FSP)

berdasarkan Surat Rektor Universitas Pertahanan Nomor: B/1820/VIII/2020 tanggal 24 Agustus 2020 tentang Permohonan Izin Penelitian Mahasiswa Program Pasca Sarjana Fakultas Strategi Pertahanan Universitas Pertahanan telah melaksanakan penelitian untuk tesis berjudul "**Urgensi Strategi Keamanan Siber Nasional Dalam Mendukung Sistem Pertahanan Negara: Analisis Fungsi Dasar Manajemen Terhadap Upaya Terwujudnya SDM Pertahanan Siber**", dengan teknik pengumpulan data melalui wawancara, observasi, dan studi dokumen/laporan yang diperlukan.

Kegiatan tersebut dilaksanakan pada hari Jumat tanggal 11 September 2020 dan hari Senin tanggal 14 September 2020, secara daring (webinar via *zoom meeting*), berjalan baik dan lancar.

Demikian surat keterangan ini dibuat untuk digunakan sebagaimana mestinya.

Depok, 13 Oktober 2020

Ditandatangani secara elektronik oleh:
DIREKTUR PENGENDALIAN SDM

Dame Ria Munthe, S.E.
Pembina Utama Madya (IV/d)

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang telah diterbitkan oleh Balai Sertfikat Elektronik (BSrE), Badan Siber dan Sandi Negara

Lampiran – 4 (Panduan Pertanyaan Wawancara)

Panduan wawancara disusun dalam bentuk pertanyaan kepada para responden/informan setiap subyek penelitian, guna menggali data dan informasi yang relevan terhadap fokus penelitian "*Bagaimana eksistensi SKSN penting terhadap upaya membangun kompetensi SDM pertahanan siber untuk sishankamrata*".

L-4.1 Pertanyaan Penelitian Untuk Pushansiber Kemhan RI.

Bidang / Sektor	:	Bidang Pertahanan
Subyek Penelitian	:	Pushansiber Kemhan RI
Responden / Informan	:	Kepala Pusat Pertahanan Siber Kemhan, yang dalam hal ini didelegasikan kepada pejabat Kepala Bidang Jaminan Keamanan, Pushansiber Kemhan, yaitu: Kolonel Sus Tri Satya

Sub Fokus	Uraian Pertanyaan	Catatan
Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan SISHANNEG ?	Pertanyaan 1 Menurut perspektif Pushansiber Kemhan, bagaimana kiranya signifikansi SKSN terhadap implementasi pembangunan kompetensi SDM yang dilaksanakan BSSN maupun Instansi Pushansiber Kemhan, yang berimplikasi kepada eksistensi SKSN khususnya terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG Pertanyaan 2 Apakah Pushansiber Kemhan sudah punya semacam *roadmap* atau rencana program kerja pembangunan SDM yang memiliki kapasitas dan kapabilitas yang relevan dengan bidang TIK atau	Informan mendeskripsikan pandangannya tentang bagaimana implementasi peran dan fungsi SKSN terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG/SISHANKAMRATA. Dalam hal tersebut adalah signifikansi eksistensi peran dan fungsi SKSN Indonesia terhadap misalnya *roadmap* atau program pembangunan SDM nasional yang kemudian ditata kelola menurut konsep SKSN guna mendukung upaya terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA).

Sub Fokus	Uraian Pertanyaan	Catatan
	keamanan siber atau pertahanan siber ?	
Faktor-Faktor Yang Mendukung dan Menghambat SKSN Indonesia Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	Pertanyaan 1 Dari sudut pandang Pushansiber Kemhan, apa saja faktor-faktor yang mendukung sehingga tata kelola SKSN (konsep SKSN rumusan BSSN) penting terhadap upaya membangun SDM pertahanan siber Pertanyaan 2 Dari sudut pandang Pushansiber Kemhan, apa saja faktor-faktor yang menghambat tata kelola SKSN berdampak pada upaya membangun SDM pertahanan siber	Informan diminta menyampaikan pandangan-pandangan instansi terkait faktor-faktor apa saja yang mendukung dan menghambat tata kelola (manajemen) kompetensi SDM keamanan siber terkait konsep SKSN Indonesia terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)
Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	Dari sudut pandang Pushansiber, apa saja bentuk praktik-praktik kegiatan keamanan siber yang aplikatif yang relevan dengan konsep SKSN (khususnya aspek peningkatan kompetensi SDM keamanan siber) yang mendukung upaya terwujudnya kompetensi SDM pertahanan siber	Informan menyampaikan pandangan-pandangan berkenaan dengan wujud praktik-praktik keamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN Indonesia) yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)

L-4.2 Pertanyaan Penelitian Untuk Satsiber TNI.

Bidang / Sektor	:	Bidang Pertahanan Khususnya TNI
Subyek Penelitian	:	Satsiber TNI
Responden / Informan	:	Komandan Satsiber TNI, yang dalam hal ini didelegaskan kepada pejabat Asisten Operasi Satsiber TNI, yaitu: Kolonel Laut (E) Eko Wing W., S.T., beserta Staf

Sub Fokus	Uraian Pertanyaan	Catatan
Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan SISHANNEG ?	Pertanyaan 1 Menurut perspektif Satsiber TNI, bagaimana kiranya signifikansi SKSN terhadap implementasi pembangunan kompetensi SDM yang dilaksanakan BSSN maupun Instansi Mabes TNI (Satsiber TNI), yang berimplikasi kepada eksistensi SKSN khususnya terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG Pertanyaan 2 Apakah Satsiber TNI sudah punya semacam *roadmap* atau rencana program kerja pembangunan SDM yang memiliki kapasitas dan kapabilitas yang relevan dengan bidang TIK atau keamanan siber atau pertahanan siber ?	Informan mendeskripsikan pandangannya tentang bagaimana implementasi peran dan fungsi SKSN terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG/SISHANKAMRATA. Dalam hal tersebut adalah signifikansi eksistensi peran dan fungsi SKSN Indonesia terhadap misalnya *roadmap* atau program pembangunan SDM nasional yang kemudian ditata kelola menurut konsep SKSN guna mendukung upaya terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA).
Faktor-Faktor Yang Mendukung dan Menghambat SKSN Indonesia Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	Pertanyaan 1 Dari sudut pandang Satsiber TNI, apa saja faktor-faktor yang mendukung sehingga tata kelola SKSN (konsep SKSN rumusan BSSN) penting terhadap upaya membangun SDM pertahanan siber	Informan diminta menyampaikan pandangan-pandangan instansi terkait faktor-faktor apa saja yang mendukung dan menghambat tata kelola (manajemen) kompetensi SDM keamanan siber terkait konsep SKSN Indonesia terhadap upaya membangun SDM pertahanan siber untuk kepentingan

Sub Fokus	Uraian Pertanyaan	Catatan
	Pertanyaan 2 Dari sudut pandang Satsiber TNI, apa saja faktor-faktor yang menghambat tata kelola SKSN berdampak pada upaya membangun SDM pertahanan siber	SISHANNEG (SISHANKAMRATA)
Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	Dari sudut pandang Satsiber TNI, apa saja bentuk praktik-praktik kegiatan keamanan siber yang aplikatif yang relevan dengan konsep SKSN (khususnya aspek peningkatan kompetensi SDM keamanan siber) yang mendukung upaya terwujudnya kompetensi SDM pertahanan siber	Informan menyampaikan pandangan-pandangan berkenaan dengan wujud praktik-praktik keamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN Indonesia) yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)

L-4.3 Pertanyaan Penelitian Untuk Balitbang SDM Kominfo.

Bidang / Sektor	:	Bidang Komunikasi dan Informatika (KOMINFO)
Subyek Penelitian	:	Balitbang SDM Kemenkominfo RI
Responden / Informan	:	Kepala Pusat Badan Penelitian dan Pengembangan SDM Kemkominfo, yang dalam hal ini didelegasikan kepada pejabat Kepala Pusat Penelitian dan Pengembangan Sumber Daya Perangkat, dan Penyelenggaraan Pos dan Informatika (Puslitbang SDPPPI) Kominfo, yaitu Bapak Bonnie M. Thamrin Wahid Manan beserta staf.

Sub Fokus	Uraian Pertanyaan	Catatan
Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan SISHANNEG ?	Pertanyaan 1 Menurut perspektif Balitbang SDM Kemenkominfo RI, bagaimana kiranya signifikansi SKSN terhadap implementasi pembangunan kompetensi SDM yang dilaksanakan BSSN maupun Instansi Kemenkominfo, yang berimplikasi kepada eksistensi SKSN khususnya terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG Pertanyaan 2 Apakah Pemerintah melalui Kominfo (dhi Balitbang SDM Kominfo), sudah memiliki semacam *roadmap* atau rencana program kerja pembangunan SDM yang memiliki kapasitas dan kapabilitas yang relevan dengan bidang TIK atau keamanan siber atau pertahanan siber ?	Informan mendeskripsikan pandangannya tentang bagaimana implementasi peran dan fungsi SKSN terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG/SISHANKAMRATA. Dalam hal tersebut adalah signifikansi eksistensi peran dan fungsi SKSN Indonesia terhadap misalnya *roadmap* atau program pembangunan SDM nasional yang kemudian ditata kelola menurut konsep SKSN guna mendukung upaya terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA).
Faktor-Faktor Yang Mendukung dan Menghambat SKSN Indonesia Terhadap Upaya Membangun	Pertanyaan 1 Dari sudut pandang Balitbang SDM Kemenkominfo RI, apa saja faktor-faktor yang mendukung sehingga tata	Informan diminta menyampaikan pandangan-pandangan terkait faktor-faktor apa saja yang mendukung dan menghambat tata kelola (manajemen)

Sub Fokus	Uraian Pertanyaan	Catatan
SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	kelola SKSN (konsep SKSN rumusan BSSN) penting terhadap upaya membangun SDM pertahanan siber <u>Pertanyaan 2</u> Dari sudut pandang Balitbang SDM Kemenkominfo RI, apa saja faktor-faktor yang menghambat tata kelola SKSN berdampak pada upaya membangun SDM pertahanan siber	kompetensi SDM keamanan siber terkait konsep SKSN Indonesia terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)
Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	Dari sudut pandang Balitbang SDM Kemenkominfo RI, apa saja bentuk praktik-praktik kegiatan keamanan siber yang aplikatif yang relevan dengan konsep SKSN (khususnya aspek peningkatan kompetensi SDM keamanan siber) yang mendukung upaya terwujudnya kompetensi SDM pertahanan siber	Informan menyampaikan pandangan-pandangan berkenaan dengan wujud praktik-praktik keamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN Indonesia) yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)

L-4.4 Pertanyaan Penelitian Untuk Kepala BSSN.

Bidang / Sektor	:	Bidang Keamanan Siber Nasional
Subyek Penelitian	:	Badan Siber dan Sandi Negara (BSSN)
Responden / Informan	:	Kepala BSSN, yang dalam hal ini didelegasikan kepada pejabat Deputi IV Bidang Pemantauan dan Pengendalian, BSSN, yaitu Mayjen TNI (Mar) Dr. Suharyanto, S.E., M.M. yang secara teknis oleh staf di lingkungan Direktorat Pengendalian SDM beserta staf, yaitu Bapak Anas Hilal dan Bapak Rian Irawan.

Sub Fokus	Uraian Pertanyaan	Catatan
Peran dan Fungsi SKSN Terhadap Upaya Membangun SDM Pertahanan Siber Untuk Kepentingan SISHANNEG ?	<u>Pertanyaan 1</u> Menurut perspektif BSSN, bagaimana kiranya signifikansi SKSN terhadap implementasi pembangunan kompetensi SDM yang dilaksanakan BSSN maupun Instansi pemangku kepentingan siber lainnya, yang berimplikasi kepada eksistensi SKSN khususnya terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG <u>Pertanyaan 2</u> Apakah BSSN sudah punya semacam *roadmap* atau rencana program kerja pembangunan SDM yang memiliki kapasitas dan kapabilitas yang relevan dengan bidang TIK atau keamanan siber atau pertahanan siber ?	Informan mendeskripsikan pandangannya tentang bagaimana implementasi peran dan fungsi SKSN terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG/SISHANKAMRATA. Dalam hal tersebut adalah signifikansi eksistensi peran dan fungsi SKSN Indonesia terhadap misalnya *roadmap* atau program pembangunan SDM nasional yang kemudian ditata kelola menurut konsep SKSN guna mendukung upaya terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA).
Faktor-Faktor Yang Mendukung dan Menghambat SKSN Indonesia Terhadap Upaya Membangun SDM Pertahanan Siber Untuk	<u>Pertanyaan 1</u> Dari sudut pandang BSSN, apa saja faktor-faktor yang mendukung sehingga tata kelola SKSN (konsep SKSN rumusan BSSN) penting	Informan diminta menyampaikan pandangan-pandangan instansi terkait faktor-faktor apa saja yang mendukung dan menghambat tata kelola (manajemen) kompetensi SDM keamanan siber terkait konsep SKSN

Sub Fokus	Uraian Pertanyaan	Catatan
Kepentingan SISHANNEG (SISHANKAMRATA).	terhadap upaya membangun SDM pertahanan siber <u>Pertanyaan 2</u> Dari sudut pandang BSSN, apa saja faktor-faktor yang menghambat tata kelola SKSN berdampak pada upaya membangun SDM pertahanan siber	Indonesia terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)
Praktik-Praktik Keamanan Siber Yang Aplikatif Sesuai Konsep SKSN Yang Mendukung Terwujudnya Kompetensi SDM Pertahanan Siber Untuk Kepentingan SISHANNEG (SISHANKAMRATA).	Dari sudut pandang BSSN, apa saja bentuk praktik-praktik kegiatan keamanan siber yang aplikatif yang relevan dengan konsep SKSN (khususnya aspek peningkatan kompetensi SDM keamanan siber) yang mendukung upaya terwujudnya kompetensi SDM pertahanan siber	Informan menyampaikan pandangan-pandangan berkenaan dengan wujud praktik-praktik keamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN Indonesia) yang mendukung terwujudnya kompetensi SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)

Lampiran – 5 (Dokumen Pendukung Data Penelitian)

L-5.1 Dokumen Pushansiber Kemhan RI.

a. Laporan Kegiatan *Cybersecurity Drill Test* 2018

BADAN INSTALASI STRATEGIS NASIONAL KEMHAN RI
PUSAT PERTAHANAN SIBER

NOTA DINAS
NOMOR : B/ND/ /III/2019/PUSHANSIBER

Kepada : Yth. Kabainstranas Kemhan
Dari : Kapushansiber Bainstrahan Kemhan
Perihal : Laporan Kegiatan *Cyber Security Drill Test*

1. Dasar:
   a. Peraturan Menteri Pertahanan Nomor 2 Tahun 2017 tentang Organisasi dan Tata Kerja Kementerian Pertahanan (Berita Negara Republik Indonesia Tahun 2017 Nomor 444).
   b. Undangan dari BSSN dengan Nomor : 343/BSSN/D3/KH.01.02/02/2019 tanggal 12 Februari 2019 tentang Undangan Kegiatan *Cyber Security Drill Test*, di Jakarta.
2. Sehubungan dasar di atas, dengan hormat dilaporkan hasil kegiatan sebagai berikut:
   a. Penyelenggaraan kegiatan ini dalam rangka pelaksanaan tugas Badan Siber dan Sandi Negara (BSSN) di bidang keamanan siber terutama untuk sektor pemerintah yang mengambil tema : "Membangun Kesadaran Respon Insiden Melalui *Cyber Security Drill Test*" yang dilaksanakan pada tanggal 25-27 Maret 2019 di Hotel Mercure, Jakarta, Indonesia.
   b. Peserta terdiri dari 44 instansi pusat dan setiap instansi mengirim perwakilan 2 orang, perwakilan dari Pushansiber Bainstrahan diwakili oleh :
      1) Kolonel Sus R. Trisatya Wicaksono, M.I.T
      2) CPNS Viko Aldiano Anggoro Pamungkas, S.Kom
3. Materi Acara:
   a. Hari Pertama: Pembukaan dan Materi *Cyber Security Drill Test.*
      1) Marsda TNI Asep Chaerudin Deputi Bidang Penanggulangan dan Pemulihan BSSN dengan materi "Membangun Kesadaran Respon Insiden Melalui *Cyber Security Drill Test.*"

         Marsda TNI Asep Chaerudin Deputi Bidang Penanggulangan dan Pemulihan BSSN dalam pembukaannya menjelaskan bahwa tujuan kegiatan ini adalah untuk membangun kesiapan para *stakeholder* dalam menangani insiden keamanan siber guna mendorong terwujudnya tata kelola penanggulangan dan pemulihan insiden siber

nasional dan juga sebagai sarana peningkatan wawasan bagi *stakeholder* sektor pemerintah dalam rangka penanganan insiden keamanan siber. Berdasarkan evaluasi isu siber tahun 2018 diketahui bahwa kendala dalam respon insiden siber adalah belum adanya PoC atau *Point of Contact* dari *stakeholder* dan masih terbatasnya kesadaran dan kemampuan dari *Point of Contact* tersebut dalam merespon insiden siber.

2) Restu Widodo dari Direktorat Penanggulangan dan Pemulihan Pemerintah BSSN dengan materi: "*Government CSIRT.*" Beliau dalam paparannya memberikan definisi singkat tentang visi BSSN dan juga data serangan siber pada tahun 2018 yang mana insiden tertinggi terjadi pada bulan juni bersamaan dengan pesta Pilkada yang terjadi di Indonesia.

   CSIRT (*Computer Security Incident Response Team*) dianggap sebagai tim atau entitas dalam suatu lembaga yang menyediakan layanan dan dukungan kepada organisasi untuk mencegah, mengelola dan menanggapi insiden keamanan informasi.

   Government CSIRT (GOV-CSIRT) ditetapkan oleh kepala BSSN dan tanggung jawab sebagai ketua GOV-CSIRT adalah Direktur Penanggulangan Dan Pemulihan Pemerintah pada Deputi Bidang Penanggulangan Dan Pemulihan BSSN. Beliau juga mengemukakan pentingnya pembentukan CSIRT dari setiap stakeholder yang ada.

   Terdapat 5 tahapan dalam pembentukan CSIRT kepada setiap *stakeholder* tetapi saat ini baru mulai pada tahap 1 yaitu edukasi organisasi.

3) Bisyron Wahyudi dari ID-SIRTII/CC dengan materi: "*Incident Handling Drill Exercise".* Bapak Bisyron Wahyudi dalam paparannya menjelaskan bahwa sepanjang tahun 2018 menurut data dari sensor monitoring ID-SIRTII telah terjadi sebanyak 232.447.974 serangan siber dengan detil sebagai berikut :

   a) Domain terbanyak diserang : go.id
   b) 2.885 laporan pengaduan publik
   c) 122.435.215 total aktivitas malware
   d) Negara Indonesia target serangan terbanyak
   e) Negara Indonesia sumber serangan terbanyak
   f) 1.875 total informasi celah keamanan
   g) Port terbanyak diserang : 53 (DNS)
   h) 16.939 total insiden website.

   Sistem monitoring ID-SIRTII sendiri yang telah bergabung dengan BSSN dan menjadi contact point CSIRT nasional memasang sensor–

sensor pada setiap NAP (*Network Access Provider*) titik paling atas atau terluar. NAP sendiri merupakan perusahaan-perusahaan yang memiliki ijin untuk menyediakan layanan internet langsung ke luar negeri menggunakan media kabel bawah laut, sehingga setiap paket yang keluar maupun masuk dari dan ke Indonesia dapat terpantau oleh sensor.

Bapak Bisyron Wahyudi juga memaparkan *cyber attack life cycle* yang diantaranya adalah *Reconnaissance* (pengintaian), *Weaponize* (tools yang digunakan), *Deliver* (pengiriman serangan), *Exploit* (Eksploitasi kerentanan yang ditemukan), *control* (pengambilan alih), *execute* (menjalankan program jahat), dan *maintain* (pembuatan *backdoors*)

b. Hari Kedua: simulasi *Cyber Security Drill Test.*

Kegiatan ini diawali dengan pembagian kelompok dimana Pushansiber berada di kelompok 1 dari total 3 kelompok, setiap kelompok diberikan asset berupa : *web server*, akun email, akun IDS Snorby, dan beberapa *tools* untuk analisa log. Hal yang ditekankan dari simulasi ini adalah bagaimana koordinasi dan respon dari para *stakeholder* dalam menghadapi adanya ancaman siber.

Simulasi dimulai dengan adanya email aduan dari masyarakat melalui perantara CSIRT BSSN yang ditujukan kepada instansi yang kita awaki yang menyatakan bahwa masyarakat kesulitan untuk mengakses suatu halaman web. Sebagai *stakeholder* dituntut untuk melakukan koordinasi sesuai dengan panduan dari CSIRT BSSN dan melakukan analisa awal yang selanjutnya akan dimonitor oleh CSIRT BSSN dan ketika insiden siber tersebut sudah berhasil di atasi maka dari *stakeholder* diminta untuk membuat laporan berupa bukti, analisa dan langkah yang telah dijalankan untuk sebagai arsip agar penanganan insiden tersebut menjadi efektif kedepannya.

c. Hari Ketiga: evaluasi *Cyber Security Drill Test*.

Kegiatan ini sebagai akhir dari rangkaian kegiatan dimana panitia melakukan evaluasi dari setiap kelompok, hasil dari panitia menyebutkan bahwa dari setiap kelompok sudah melakukan koordinasi dan analisa dengan baik sesuai dengan panduan dari BSSN.

BSSN menekankan bahwa hal terpenting dari suatu insiden adalah koordinasi antar instansi dan melaporkan setiap insiden siber yang terjadi kemudian untuk koordinasi yang lebih efektif, BSSN menyarankan untuk setiap instansi memberikan PoC (*Point of Contact*) yang berfungsi sebagai kontak terpercaya (*trusted*) dari suatu instansi untuk *sharing information* terkait isu siber.

BSSN juga melakukan *soft launching website* https://govcsirt.bssn.go.id yaitu *website* milik BSSN yang memuat informasi, pelayanan aduan, kegiatan (*event*) seputar BSSN sebagai CSIRT pemerintah.

4. Kesimpulan dan Saran

a. Kesimpulan

1) Badan Siber dan Sandi Negara sebagai pelaksana tugas di bidang keamanan siber nasional menekankan pentingnya pembentukan CSIRT yang baru dimulai pada tahap 1 yaitu edukasi dari setiap stakeholder. Tugas dari CSIRT sendiri adalah untuk mencegah, mengelola dan menanggapi insiden keamanan informasi. Kemudian memberikan *PoC* (*Point Of Contact*) tunggal untuk pelaporan

2) Melalui *Cyber Security Drill Test*, setiap *stakeholder* diedukasi tentang bagaimana koordinasi apabila terjadi insiden siber melalui simulasi insiden yang dapat dipelajari.

b. Saran.

Kegiatan *Cyber Security Drill Test* ini agar dilaksanakan secara rutin oleh BSSN guna melatih sekaligus mensosialisasikan tahapan penanganan insiden untuk setiap *stakeholder*, dan diharapkan Pusat Pertahanan Siber Kementerian Pertahanan untuk selalu dilibatkan kembali dalam kegiatan tersebut.

5. Penutup.

Demikian laporan kegiatan *Cyber Security Drill Test* ini dibuat untuk dapat digunakan sebagai bahan evaluasi dan saran masukan bagi Pimpinan dalam menentukan kebijakan selanjutnya.

Jakarta, Maret 2019

Kepala Pusat Pertahanan Siber,

Raja H. Manalu, S.Sos, M.I.P.
Marsekal Pertama TNI

Paraf :

1. Kabid Takol :
2. Kabid Jamkam :
3. Andya Bid SisOps :
4. Kasubbag TU :

Tembusan:

- Ses Bainstranas Kemhan.

b. Laporan FGD Proteksi, Penanggulangan, dan Pemulihan Insiden Siber Bersama *Stakeholder* Pemerintah Pusat dan Daerah (Jakarta 9 s.d. 10 Agustus 2018).

KEMENTERIAN PERTAHANAN RI
PUSAT PERTAHANAN SIBER

LAPORAN KEGIATAN FOCUS GROUP DISCUSSION
PROTEKSI, PENANGGULANGAN DAN PEMULIHAN INSIDEN SIBER
BERSAMA *STAKEHOLDER* PEMERINTAH PUSAT DAN DAERAH
Jakarta, 9 – 10 Agustus 2018

1. Dasar:

   - Surat Kepala Badan Siber dan Sandi Negara nomor 2080/BSSN/KH.01.02/07/2018 tanggal 23 Juli 2018 perihal Undangan Focus Group Discussion (FGD) tentang Proteksi, Penanggulangan dan Pemulihan Insiden Siber Bersama *Stakeholder* Pemerintah Pusat dan Daerah.

2. Sehubungan dengan hal tersebut, dengan hormat dilaporkan hasil kegiatan tersebut sebagai berikut:

   a. Penyelenggaraan. Kegiatan FGD diselenggarakan oleh Badan Siber dan Sandi Negara (BSSN) dan dilakukan pada tanggal 9 Agustus s.d. 10 Agustus 2018 di Hotel Royal Kuningan.

   b. Peserta. Peserta kegiatan FGD berasal dari 85 instansi Pemerintah Pusat dan 34 Pemerintah Daerah dengan jumlah peserta 259 orang.

3. Materi Acara:

   a. Hari pertama:

      1) Diskusi Panel Sesi I.

         a) Marsda TNI Asep Chaerudin (Deputi III BSSN) dengan materi "Strategi Keamanan Siber Nasional"
         b) Agung Nugraha, S.IP, M.Si (Han) (Plt Deputi II BSSN) dengan materi "Transformasi Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara".

      2) Diskusi Panel Sesi II.

         a) Dr. Bisyron Wahyudi (Senior Analis BSSN dan Wakil Ketua Id-SIRTII BSSN) dengan materi "*Cyber Incident Management and Response*".

b) Dr. Hening Widiatmoko, M.A (Kepala Dinas Komunikasi dan Informasi Pemprov Jawa Barat) dengan materi "Jabar Prov CSIRT"
c) Herry Siswanto, S.E, M.B.A (Kepala Pusat Sistem Informasi dan Teknologi Keuangan, Setjen Kementerian Keuangan) dengan materi "Pengelolaan Keamanan Informasi Kementerian Keuangan".
d) Anton Setiyawan, S.Si, M.M (Direktur Proteksi Ekonomi Digital, Deputi III BSSN).

b. Hari kedua:

1) Paparan Teknis:
a) Ahmad Muammar dengan materi "*How to Secure Web Application*".
b) Digit Oktavianto dengan materi "*How to Response Against Web Security Incident*".
c) Anggrahito dengan materi "Penerapan *Vulnerability Assessment* dan *Penetration Test* bagi pelaksanaan Audit Keamanan Informasi Sektor Pemerintah".

2) Pembentukan Forum Keamanan Siber Sektor Pemerintah.

4. Hasil kegiatan FGD:

a. Dukungan dan komitmen setiap pimpinan tertinggi instansi Pemerintah Pusat dan Kepala Daerah merupakan kunci keberhasilan pelaksanaan kebijakan, program, dan kegiatan keamanan siber atau keamanan informasi sektor pemerintah.
b. Guna mengatasi permasalahan SDM keamanan siber atau keamanan informasi di Instansi Pemerintah, khususnya Pemerintah Daerah diperlukan langkah-langkah sebagai berikut:

1) BSSN akan berupaya memberikan dukungan fasilitasi SDM kepada Pemerintah Daerah dalam waktu tertentu dengan memperhatikan ketersediaan SDM dan anggaran BSSN.
2) Instansi Pemerintah khususnya Pemerintah Daerah harus menyusun formasi kebutuhan SDM dan memanfaatkan momentum penerimaan CPNS untuk pengisian formasi pelaksana urusan persandian atau keamanan informasi.

3) Perlu adanya insiasi untuk mewujudukan fungsional khusus yang berkaitan dengan keamanan siber/sandiman agar petugas keamanan siber ini mendapatkan penghargaan yang layak.

c. Perlunya MOU antara BSSN dengan Kementerian dan Lembaga terkait keamanan siber atau keamanan jaringan informasi sektor Pemerintah.
d. Instansi pemerintah pusat dan Pemerintah Daerah harus membentuk *Computer Security Incident Response Team (CSIRT)* atau tim penanggulangan insiden keamanan informasi.
e. BSSN akan mengeluarkan kebijakan dan standar di bidang penanggulangan insiden keamanan informasi atau keamanan siber, terutama pada integrasi sistem antar Kementerian/Lembaga/Dinas.
f. BSSN akan melaksanakan *Cyber Drill* bagi sektor pemerintah untuk penanggulangan insiden keamanan informasi dan siber dimulai tahun 2018.
g. Instansi pemerintah harus menunjuk pejabat yang diberikan kewenangan untuk menjadi *Point Of Contact* (POC) insiden keamanan informasi atau keamanan siber dan melaporkannya kepada kepala BSSN paling lambat tanggal 31 agustus 2018.
h. Instansi pemerintah pusat dan daerah menerapkan keamanan siber atau keamanan informasi pada penyelenggaraan *e-government* yang meliputi data dan informasi, infrastruktur, dan aplikasi.
i. Telah diinisiasi pembentukan forum keamanan siber sektor pemerintah dengan nama "*government cyber security forum*" atau GCSF. Forum tersebut merupakan wadah untuk peningkatan efektivitas koordinasi, komunikasi, berbagi informasi dan konsolidasi para pemangku kepentingan keamanan siber sektor pemerintah. Forum ini akan dikonsolidasikan oleh Direktorat Proteksi Pemerintah Deputi Bidang Proteksi.
j. Dalam melaksanakan tugas keamanan informasi instansi Pemerintah Pusat dan Daerah wajib berkonsultasi kepada BSSN.

5. Penutup. Demikian laporan pelaksanaan Focus Group Discussion disusun untuk dapat digunakan sebagai bahan evaluasi dan saran masukan bagi Pimpinan dalam menentukan kebijakan selanjutnya.

Jakarta, 10 Agustus 2018

Kepala Pusat Pertahanan Siber

Raja H. Manalu, S.Sos, M.I.P.
Marsekal Pertama TNI

c. Laporan Kegiatan FGD Kajian Strategis Organisasi BSSN Dalam Rangka Mengonsolidasi Unsur Keamanan Siber (Jakarta 18 Maret 2019).

KEMENTERIAN PERTAHANAN RI
PUSAT PERTAHANAN SIBER

LAPORAN KEGIATAN *FOCUS GROUP DISCUSSION*
KAJIAN STRATEGI ORGANISASI BSSN DALAM RANGKA MENGONSOLIDASI UNSUR KEAMANANSIBER
Jakarta, 18 Maret 2019

1. Dasar:

   - Surat Kepala Badan Siber dan Sandi Negara nomor 585/BSSN/SU/KH.01.02/03/2019 tanggal 1 Maret 2019 perihal Undangan Focus Group Discussion (FGD) Kajian Strategi Organisasi BSSN dalam Rangka Mengonsolidasi Unsur Keamanan Siber.

2. Sehubungan dengan hal tersebut, dengan hormat dilaporkan hasil kegiatan tersebut sebagai berikut:

   a. Penyelenggaraan. Kegiatan FGD diselenggarakan oleh Badan Siber dan Sandi Negara (BSSN) dan dilakukan pada tanggal 18 Maret 2019 di Ruang Rapat Opska, Gedung A BSSN Lantai II, Jalan Harsono R.M No.70 Ragunan Jakarta Selatan.

   b. Peserta. Peserta kegiatan FGD berasal dari 7 instansi Pemerintah yaitu:

      1) Kemenko Polhukam, dihadiri oleh Marsma TNI DR. Sigit Priyono.
      2) Kemhan (Pushansiber), dihadiri oleh Kolonel Sus Trisatya Wicaksono, M.IT.
      3) Kemkominfo, dihadiri oleh Ibu Meutia Rahmatika.
      4) Kemenlu, dihadiri oleh Bapak Reza Reflusmen J.
      5) Polri, dihadiri oleh Kombes Kurniadi.
      6) BIN, dihadiri oleh Kolonel Sus M.E Sudrajat.
      7) BSSN, dihadiri oleh para Kabid terkait.

   c. Moderator. Acara dipandu oleh Prof. Ricardus Eko Indrajit.

3. Acara:

a. Acara dibuka dengan sambutan oleh Sekretaris Utama (Sestama) BSSN bapak Syahrul Mubarak, S.IP, M.M. Dalam sambutannya Sestama menjelaskan secara singkat sejarah berdirinya BSSN, beliau berharap agar para peserta FGD sebagai *stakeholder* dapat memberikan masukan tentang peran, tugas dan fungsi BSSN, *resources* yang dimiliki serta *positioning* BSSN menurut kepentingan *stakeholder*.

b. FGD dimulai dengan paparan singkat Prof Eko Indarjit yang menjelaskan tujuan dari FGD dan dilanjutkan dengan survei menggunakan aplikasi menti.com untuk menjaring pendapat *stakeholder* tentang peran BSSN dalam dunia siber Indonesia, sektor apa saja yang paling penting harus dijaga keamanan sibernya serta harapan *stakeholder* dengan adanya BSSN.

c. Penyampaian saran dan harapan dari peserta.

1) Deputi VII Kemenkopolhukam. Saat ini keamanan siber menjadi salah satu kekuatan nasional, BSSN diharapkan dapat mengkoordinasikan keterkaitan hubungan antar lembaga pemerintah, akademisi, industri dan komunitas. Selain itu BSSN harus membangun penguatan regulasi dan hukum.

2) Pushansiber. BSSN diharapkan segera membentuk CERT nasional dan CERT sektor, menyusun protap/mekanisme kerja antara BSSN dan stakeholder, peningkatan *capacity building* yang terkonsep sebagai *leading sector*, perlu *interchange* data sektor strategis yang diamankan oleh BSSN, perlunya perekrutan SDM cyber melalui PTN/PTS yang berkualitas maupun Diklat sejenis.

3) Deputi VI Divisi Siber BIN. BSSN mampu menciptakan sinergi antar unit siber yang ada di Indonesia baik pusat dan daerah. Sebagai contoh NU bisa membuat NU Cyber dengan mengumpulkan anak-anak yang berkemampuan siber.

4) Direktorat Tindak Pidana Siber. BSSN diharapkan dapat mengkoordinasikan dan berkolaborasi dengan Komite Akreditasi Nasional (KAN) untuk pengelolaan laboratorium digital forensik yang terakreditasi. Agar BSSN mengupayakan adanya peraturan yang memfasilitasi pemilik data elektronik supaya bisa memberikan data

kepada penegak hukum berkaitan dengan penyebaran berita hoax. BSSN diharapkan dapat mengeluarkan peraturan yang mengantisipasi kecepatan kemajuan teknologi, sebagai contoh Undang-undang Tindak Pidana Pencucian Uang (TPPU).

5) Kementerian Luar Negeri. Diharapkan BSSN mengatur alur informasi yang *seamless* berkaitan dengan diplomasi siber dalam konteks bilateral, regional dan multilateral. BSSN agar membentuk unit yang mengkoordinasikan kerjasama internasional supaya penanganan suatu isu terkait hubungan antar negara bisa lebih fokus. BSSN agar membantu Kementerian Luar negeri memberi informasi rekomendasi negara mana yang berpotensi melakukan kerjasama maupun yang berpotensi menyerang Indonesia.

6) Kemenkominfo. Agar BSSN membuat standar-standar keamanan teknis untuk *certificate of authorities* (CA).

4. Kesimpulan:

a. Persoalan keamanan siber merupakan *cross cutting issue* sehingga diperlukan kerjasama atau multi *stakeholder* (kolaborasi) antara pemerintah, akademisi, komunitas dan industri. Selain itu kerjasama nasional, regional dan internasional juga diperlukan untuk menangani permasalahan siber.

b. Perlunya standarisasi alutsista keamanan siber sehingga seluruh kementerian dan lembaga mempunyai peralatan keamanan siber yang relatif sama. BSSN bertanggungjawab terhadap interoperbilitas dari seluruh peralatan keamanan siber nasional.

c. BSSN dapat memberikan akreditasi lembaga pendidikan tinggi untuk mencetak ahli-ahli siber untuk mengisi kekosongan tenaga ahli siber sekaligus akreditasi untuk memberikan sertifikasi profesi ahli siber.

5. Penutup. Demikian laporan pelaksanaan *Focus Group Discussion* disusun untuk dapat digunakan sebagai bahan evaluasi dan saran masukan bagi Pimpinan dalam menentukan kebijakan selanjutnya.

Jakarta, 22 Maret 2019

Kepala Bidang Penjaminan Keamanan
Pusat Pertahanan Siber

Trisatya Wicaksono, M.IT
Kolonel Sus Nrp 520738

d. Laporan Kegiatan *Cybersecurity Drill Test* II *Government Sector* (Jakarta 5 s.d. 7 November 2019).

KEMENTERIAN PERTAHANAN RI
BADAN INSTALASI STRATEGIS PERTAHANAN

Nomor : B/ /XI/2019/BAINSTRAHAN
Klasifikasi : Biasa
Lampiran : 1 lembar
Hal : Laporan Kegiatan *Cyber Security Drill Test* II *Government Sector*

Jakarta, November 2019

Kepada
Yth. Sekjen Kemhan
di
Jakarta

1. Dasar:
   - Surat Deputi Bidang Penanggulangan dan Pemulihan BSSN Nomor : 3120/BSSN/D3/KH.02.01/10/2019 tanggal 7 Oktober 2019 tentang Undangan Kegiatan *Cyber Security Drill Test* II Sektor Pemerintah Tahun 2019, di Jakarta.

2. Sehubungan dasar tersebut di atas, dengan hormat dilaporkan hasil kegiatan sebagai berikut:
   a. Kegiatan *Cyber Security Drill Test* II diselenggarakan dalam rangka pelaksanaan tugas Badan Siber dan Sandi Negara (BSSN) di bidang keamanan siber untuk sektor pemerintah, dengan tema "Kesiapan Pembentukan CSIRT Organisasi di Sektor Pemerintah". Kegiatan dilaksanakan pada tanggal 5 s.d. 7 November 2019 di Hotel ASTON TB Simatupang, Jakarta, Indonesia.
   b. Peserta terdiri dari 50 orang peserta, 25 peserta dari instansi pusat dan 25 peserta dari Dinas Kominfo Daerah. Perwakilan dari Kemhan a.n. Penda III/a Bilal Abdussalam, S.Kom NIP. 199210032018021002 jabatan Pranata Komputer Pertama Pushansiber Bainstrahan Kemhan.

3. Materi Acara:
   a. Hari Pertama: *Training Online* OIC-Cert dan Validasi Indeks Maturitas Insiden Keamanan Siber.
      1) **Dr. Charles Lim**, dalam paparannya memberikan seminar mengenai Apa itu *Malware*, dan bagaimana menganalisa *Malware*.

         Pemateri juga menyampaikan mengenai perkembangan *malware* setiap tahun semakin meningkat, jika dilihat presentase dari tahun 2009 yaitu sebanyak 29 juta jenis malware dan di tahun 2018 sebanyak 796 juta jenis malware.

2) Validasi Indeks Maturitas Penanganan Insiden Keamanan Siber, kegiatan ini diasistensi oleh pegawai BSSN dan dilakukan penilaian mengenai Kematangan Penanganan insiden di Kementerian Pertahanan, ada beberapa faktor yang dinilai, dan hasil dari penilaian ini Kementerian Pertahanan mendapatkan **Indeks Kematangan** dengan nilai **1.71**

b. Hari Kedua: Pembukaan, Seminar Tentang *Cyber Security Incident Response* dan simulasi *Cyber Security Drill Test.*

1) **Ir. Inu Baskara, MMSI**, Direktur Penanggulangan dan Pemulihan Pemerintahan Badan Siber dan Sandi Negara dalam pembukaannya menjelaskan bahwa tujuan Kegiatan *Cyber Security Drill Test* ini dilaksanakan untuk memberikan pemahaman, pengalaman, serta peningkatan koordinasi dan komunikasi antara BSSN dengan *stakeholder* yang terkait khususnya dalam sektor pemerintah, kegiatan ini diharapkan dapat meningkatkan kapabilitas kita semua dalam rangka penanggulangan dan pemulihan terhadap insiden keamanan siber nasional.

Pembentukan CSIRT sektor pemerintah ini dilakukan untuk menyiapkan instansi pemerintah dalam melaksanakan penanggulangan dan pemulihan insiden keamanan siber secara mandiri, dibawah koordinasi BSSN. Dalam mencapai hal tersebut, pada tahun 2019 BSSN telah melaksanakan asistensi pembentukan CSIRT di 26 instansi pemerintah pusat dari 25 instansi pemerintah provinsi, selanjutnya mulai tahun 2020 hingga tahun 2024 akan dilakukan pembentukan CSIRT hingga nantinya diharapkan seluruh pemerintah pusat dan pemerintah provinsi yang menjadi target pembentukan CSIRT telah terwujud atau memiliki CSIRT.

Berdasarkan laporan tahunan yang dikeluarkan oleh BSSN, serangan siber di Indonesia mengalami peningkatan di tahun 2017 ke tahun 2018, yakni sekitar 205 juta serangan menjadi sekitar 232 juta serangan, serangan terhadap domain pemerintah, yakni .go.id menjadi domain terbanyak diserang, hal ini tentunya sangat merugikan karena berdampak pada menurunnya reputasi pemerintah pusat maupun daerah, serta mengganggu pelayanan publik kepada masyarakat. Mengantisipasi hal ini, BSSN melalui Direktorat Penanggulangan dan Pemulihan Pemerintah memiliki berbagai program agar *stakeholder* siap melaksanakan penanggulangan dan pemulihan Insiden Keamanan Siber Sektor Pemerintah diantaranya penyusunan peraturan dan kebijakan, asistensi penanggulangan dan pemulihan operasional tim respon insiden, asistensi pembentukan CSIRT dan pelaksanaan *Cyber Security Drill Test.*

2) Kegiatan ini diawali dengan pembagian kelompok dimana Pushansiber mewakili KEMHAN berada di kelompok 2 dari total 3 kelompok, masing-masing kelompok terdiri dari 9-12 Kementerian. Setiap kelompok diberikan persoalan berupa : *Incident Handling*. Hal yang ditekankan dari simulasi ini adalah bagaimana respon dari para *stakeholder* dalam menghadapi adanya ancaman siber, dan bagaimana tim CSIRT menanggapi dan menganalisa jika terjadi insiden di instansi masing-masing.

3) **Agustinus Toad, SE**, Subdirektorat Penanggulangan dan Pemulihan Pemerintahan Wilayah II menyampaikan Hasil Asistensi Pembentukan CSIRT Instansi Pemerintah diantaranya sudah dilakukan asistensi pembentukan CSIRT pada 25 Instansi Pusat dan 15 Pemerintah Daerah Wilayah I.

c. Hari Ketiga: Sharing Session oleh Kemenkeu.

1) **Edy Nuryanto, SE, MM** - Dalam paparannya menyampaikan materi mengenai "**Pengelolaan Keamanan Informasi**" di Kementerian Keuangan. Bahwa Konsep Pengelolaan Keamanan Informasi pengelolaan TIK yang handal dan aman tidak luput dari *PEOPLE, PROCESS, TECHNOLOGY,* dan yang paling penting adalah peran serta pimpinan tinggi Kemenkeu (*Budget*, RaPim TIK, DKO, IKU dan *Management Risk*). Masalah *Downtime*, Kemenkeu melaksanakan DRC *Drill* Sistem Informasi Kemenkeu Secara berkala guna untuk mengurangi *downtime* yang panjang menjadi lebih singkat. Terkait Prosedur Penanganan Insiden atau gangguan sesuai alur ITSM, Kemenkeu telah menggunakan *ticketing* dalam proses pengaduannya, sehingga termonitor, sesuai prosedur dan terselesaikan dengan baik.

Berkaitan dengan banyaknya sistem di Kementerian Keuangan yang sudah berbasiskan IT seperti E-FILING, E-BILLING, E-FAKTUR, dll, Hal Terpenting yaitu peraturan-peraturan kebijakan regulasi TIK Kemenkeu yang diterbitkan sejak tahun 2009-2019, sehingga mempermudah dalam menerapkan kebijakan internal dan sosialisasi mengenai pentingnya keamanan informasi pada beberapa bagian Kementerian Keuangan yang memiliki aset-aset kritis tersebut agar tidak mudah diretas dari internal maupun eksternal, sehingga aset-aset tersebut dapat berjalan dengan aman dan baik tanpa adanya gangguan dan dapat diakses dimanapun dan kapanpun.

4. Kesimpulan dan Saran

a. Kesimpulan

1) Badan Siber dan Sandi Negara sebagai pelaksana tugas di bidang kemanan siber nasional menyampaikan pentingnya pembentukan CSIRT dan saat ini baru dimulai pada tahap pertama yaitu edukasi dari setiap *stakeholder*. Tugas dari CSIRT sendiri adalah untuk mencegah, mengelola dan menanggapi insiden keamanan informasi. Kemudian memberikan *PoC* (*Point Of Contact*) tunggal untuk pelaporan.

2) Melalui *Cyber Security Drill Test*, setiap *stakeholder* diedukasi tentang bagaimana koordinasi apabila terjadi insiden siber melalui simulasi insiden yang dapat dipelajari, Pushansiber sebagai perwakilan Kementerian Pertahanan dalam kegiatan ini mendapatkan poin terbesar dari seluruh peserta yang ikut andil dalam kegiatan ini yaitu ***495***, sehingga Pushansiber berhasil menjadi peserta terbaik 1 pada kelompok dua di kegiatan ini.

b. Saran

Pada Tahun 2020 ada dua Paket Pelatihan dari BBSN yaitu paket pelatihan khusus untuk peningkatan kompetensi dan paket untuk sertifikasi internasional untuk dua orang perwakilan dari 25 CSIRT yang teregistrasi di BSSN, 15 CSIRT tahap satu dan 10 CSIRT di tahap dua. Pelatihan dilaksanakan di Jakarta dalam 10 hari kerja, diharapkan Pusat Pertahanan Siber Kementerian Pertahanan dapat ikut berpartisipasi dengan mempersiapkan dua orang anggotanya untuk mengikuti pelatihan.

5. Penutup

Demikian laporan kegiatan *Cyber Security Drill Test* II *Gov Sector* ini dibuat untuk dapat digunakan sebagai bahan evaluasi dan saran masukan bagi Pimpinan dalam menentukan kebijakan selanjutnya.

Kepala Badan Instalasi Strategis Pertahanan,

Bambang Kusharto, S.Sos., M.M.

Tembusan :

1. Menteri Pertahanan
2. Wakil Menteri Pertahanan
3. Irjen Kemhan
4. Dirjen Strahan
5. Karopeg Setjen Kemhan
6. Kapus Bainstrahan Kemhan.

L-5.2 Dokumen Satsiber TNI.

a. Nota Kesepahaman antara TNI dan BSSN

NOTA KESEPAHAMAN

antara

TENTARA NASIONAL INDONESIA

dan

BADAN SIBER DAN SANDI NEGARA

Nomor Kerma/44/XI/2018
Nomor PERJ.337/KBSSN/KH.02.01/11/2018

tentang

PENGUATAN KEAMANAN SIBER DAN PERSANDIAN DI LINGKUNGAN TENTARA NASIONAL INDONESIA

Pada hari ini Kamis tanggal delapan bulan November tahun dua ribu delapan belas (8-11-2018), bertempat di Jakarta, kami yang bertanda tangan di bawah ini:

I. **MARSEKAL TNI HADI TJAHJANTO, S.I.P.,** Panglima Tentara Nasional Indonesia, dalam kedudukan dan jabatan tersebut bertindak untuk dan atas nama Tentara Nasional Indonesia, berkedudukan di Markas Besar TNI, Cilangkap, Jakarta 13870, selanjutnya disebut **PIHAK PERTAMA**;

II. **DJOKO SETIADI,** Kepala Badan Siber dan Sandi Negara, dalam kedudukan dan jabatan tersebut bertindak untuk dan atas nama Badan Siber dan Sandi Negara, berkedudukan di Jalan Harsono RM Nomor 70, Jakarta Selatan 12550, selanjutnya disebut sebagai **PIHAK KEDUA;**

PIHAK PERTAMA dan **PIHAK KEDUA** yang selanjutnya secara bersama sama disebut **PARA PIHAK** dalam kedudukan dan jabatan tersebut di atas, terlebih dahulu menerangkan hal-hal sebagai berikut:

1. bahwa **PIHAK PERTAMA** yang mempunyai tugas menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia yang berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, serta melindungi segenap bangsa dan seluruh tumpah darah Indonesia dari ancaman dan gangguan terhadap keutuhan bangsa dan negara;

2. bahwa **PIHAK KEDUA** yang mempunyai tugas melaksanakan keamanan siber secara efektif dan efesien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber;

3. **PARA PIHAK** sepakat melaksanakan kerjasama memperkuat keamanan siber di lingkungan TNI.

Dengan memperhatikan peraturan perundang-undangan sebagai berikut:

1. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 3, Tambahan Lembaran Negara Republik Indonesia Nomor 4169);

2. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 127, Tambahan Lembaran Negara Republik Indonesia Nomor 4439);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Nomor 5952);

4. Peraturan Pemerintah Pengganti Undang-Undang Nomor 23 Tahun 1959 tentang Keadaan Bahaya;

5. Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi dan Tata Kerja Lembaga Pemerintah Non Kementerian sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 145 Tahun 2015 tentang Perubahan Kedelapan atas Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi dan Tata Kerja Lembaga Pemerintah Non Kementerian (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 122);

6. Peraturan Presiden Nomor 10 Tahun 2010 tentang Susunan Organisasi TNI sebagaimana telah diubah dengan Peraturan Presiden Nomor 62 Tahun 2016 tentang perubahan atas Peraturan Presiden Nomor 10 Tahun 2010 tentang Susunan Organisasi TNI; dan

7. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara 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 Republik Indonesia Tahun 2017 Nomor 277).

Berdasarkan pertimbangan tersebut **PARA PIHAK** sepakat untuk membuat dan menandatangani Nota Kesepahaman tentang Penguatan Keamanan Siber dan Persandian di Lingkungan TNI dengan ketentuan dan syarat-syarat sebagai berikut:

Pasal 1
Maksud dan Tujuan

Maksud dari Nota Kesepahaman ini adalah untuk mengatur rencana kerja sama tentang Penguatan Keamanan Siber dan Persandian di Lingkungan Tentara Nasional Indonesia dengan tujuan agar dapat dijadikan sebagai pedoman bagi **PARA PIHAK** dalam mengimplementasikan Nota Kesepahaman ini.

Pasal 2
Ruang Lingkup

Ruang lingkup Nota Kesepahaman ini meliputi:

a. pengamanan Teknologi Informasi dan Komunikasi;

b. perlindungan Informasi dan Transaksi Elektronik;

c. penyiapan Penanggulangan Insiden Siber;

d. penguatan sumber daya dalam bidang Keamanan Siber dan Persandian;

e. peningkatan dan Pengembangan Sumber Daya Manusia; dan

f. pemanfaatan lain yang disepakati **PARA PIHAK**.

Pasal 3
Pembiayaan

Segala pembiayaan yang timbul dalam pelaksanaan Nota Kesepahaman ini dibebankan kepada **PARA PIHAK** yang dilaksanakan menurut ketentuan peraturan perundang-undangan yang berlaku.

Pasal 4
Masa Berlaku

(1) Nota Kesepahaman ini berlaku selama 5 (lima) tahun sejak ditandatangani oleh **PARA PIHAK** dan dapat diperpanjang atas kesepakatan **PARA PIHAK**.

(2) Dalam hal Nota Kesepahaman ini berakhir dan tidak diperpanjang lagi atau diakhiri karena permintaan tertulis oleh salah satu pihak karena alasan lain, maka pengakhiran Nota Kesepahaman ini tidak mengakibatkan perjanjian-perjanjian yang telah dibuat berkaitan dengan pelaksanaan Nota Kesepahaman berakhir sampai dengan berakhirnya perjanjian tersebut.

Pasal 5
Tindak Lanjut

(1) Pelaksanaan Nota Kesepahaman ini akan diatur lebih lanjut dalam Perjanjian Kerja Sama yang mengatur mengenai hak dan kewajiban **PARA PIHAK** sesuai dengan peraturan perundang-undangan.

(2) **PARA PIHAK** dapat melakukan pertemuan secara berkala dan/atau sewaktu-waktu apabila diperlukan untuk membahas implementasi Nota Kesepahaman ini.

(3) **PARA PIHAK** sepakat untuk menindak lanjuti Nota Kesepahaman ini dengan Perjanjian Kerja Sama dalam kurun waktu paling lambat 6 (enam) bulan sejak ditandatangani Nota Kesepahaman ini.

Pasal 6
Ketentuan Lain

Hal-hal yang tidak atau belum diatur dalam Nota Kesepahaman ini akan diatur dalam amandemen/*addendum* berdasarkan persetujuan **PARA PIHAK** yang merupakan bagian tidak terpisahkan dari Nota Kesepahaman ini.

Pasal 7
Penutup

Demikian Nota Kesepahaman ini dibuat dan ditandatangani di Jakarta dalam rangkap 2 (dua) di atas kertas bermeterai cukup, mempunyai kekuatan hukum yang sama masing-masing untuk **PARA PIHAK**.

PIHAK PERTAMA PANGLIMA TENTARA NASIONAL INDONESIA,	PIHAK KEDUA KEPALA BADAN SIBER DAN SANDI NEGARA,
TTD	TTD
HADI TJAHJANTO, S.I.P. MARSEKAL TNI	DJOKO SETIADI

b. Organisasi dan Tugas Satsiber TNI (Halaman 1 sd 3)

TENTARA NASIONAL INDONESIA

PERATURAN PANGLIMA TENTARA NASIONAL INDONESIA
NOMOR 71 TAHUN 2019

TENTANG

ORGANISASI DAN TUGAS
SATUAN SIBER TENTARA NASIONAL INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

PANGLIMA TENTARA NASIONAL INDONESIA,

Menimbang : bahwa dalam rangka mengoptimalkan pelaksanaan tugas, peran dan fungsi, serta optimalisasi kinerja di lingkungan Satuan Siber Tentara Nasional Indonesia guna mendukung tugas pokok Tentara Nasional Indonesia, serta untuk melaksanakan ketentuan Pasal 196 ayat (2) Peraturan Presiden Nomor 66 Tahun 2019 tentang Susunan Organisasi Tentara Nasional Indonesia, perlu menetapkan Peraturan Panglima Tentara Nasional Indonesia tentang Organisasi dan Tugas Satuan Siber Tentara Nasional Indonesia;

Mengingat : 1. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 127, Tambahan Lembaran Negara Republik Indonesia Nomor 4439);

2. Peraturan Presiden Nomor 66 Tahun 2019 tentang Susunan Organisasi Tentara Nasional Indonesia;

3. Peraturan Panglima TNI Nomor 37 Tahun 2019 tentang Struktur Organisasi, Jabatan, dan Kepangkatan di Lingkungan Tentara Nasional Indonesia;

4. Peraturan Panglima TNI Nomor 41 Tahun 2019 tentang Pokok-Pokok Organisasi dan Prosedur Markas Besar Tentara Nasional Indonesia;

MEMUTUSKAN:

Menetapkan: PERATURAN PANGLIMA TENTARA NASIONAL INDONESIA TENTANG ORGANISASI DAN TUGAS SATUAN SIBER TENTARA NASIONAL INDONESIA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Panglima ini yang dimaksud dengan:

1. Tentara Nasional Indonesia yang selanjutnya disingkat TNI adalah komponen utama yang siap digunakan untuk melaksanakan tugas pertahanan negara.

2. Validasi adalah proses penyempurnaan organisasi yang pada dasarnya merupakan upaya untuk lebih memaksimalkan keberhasilan pencapaian tujuan organisasi.

3. Satuan Siber TNI yang selanjutnya disebut Satsiber TNI adalah badan pelaksana pusat yang berkedudukan langsung di bawah Panglima.

4. Siber adalah ruang maya yang terbentuk dari konvergensi teknologi jaringan, perangkat keras dan perangkat lunak di mana manusia dapat melakukan aktivitas sehari-hari.

5. Panglima TNI yang selanjutnya disebut Panglima adalah perwira tinggi militer yang memimpin TNI.

6. Jabatan Fungsional TNI adalah kedudukan yang menunjukkan tugas, tanggung jawab, wewenang, dan hak seorang Prajurit Tentara Nasional Indonesia dalam suatu satuan organisasi Tentara Nasional Indonesia yang dalam pelaksanaan tugasnya mensyaratkan penguasaan pengetahuan, keahlian, dan/atau keterampilan bidang tertentu.

7. Pegawai Negeri Sipil yang selanjutnya disingkat PNS adalah warga negara Indonesia yang memenuhi syarat tertentu, diangkat sebagai Pegawai ASN secara tetap oleh pejabat pembina kepegawaian untuk menduduki jabatan pemerintahan.

Pasal 2

Validasi organisasi Satsiber TNI merupakan implementasi penataan organisasi di lingkungan Markas Besar TNI.

BAB II
KEDUDUKAN, TUGAS DAN FUNGSI

Pasal 3

Satsiber TNI merupakan Badan Pelaksana Pusat di Tingkat Markas Besar TNI yang berkedudukan langsung di bawah Panglima.

Pasal 4

Satsiber TNI bertugas menyelenggarakan kegiatan dan Operasi Siber di lingkungan TNI dalam rangka mendukung tugas pokok TNI.

Pasal 5

Dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 4, Satsiber TNI mempunyai fungsi sebagai berikut:

a. Fungsi utama:

1. perencanaan kegiatan dan Operasi Siber TNI dalam rangka penangkalan, penindakan, pemulihan dan dukungan operasi;

2. perencanaan administrasi dan logistik untuk kegiatan dan Operasi Siber TNI dalam rangka penangkalan, penindakan, pemulihan dan dukungan operasi;

3. penangkalan siber, yaitu menyelenggarakan segala usaha, pekerjaan, kegiatan dan tindakan yang terencana dan sistematis dalam melaksanakan penangkalan siber meliputi *monitoring*, deteksi, observasi serta mitigasi dan *cyber awareness* untuk melindungi infrastruktur kritis TNI dari berbagai macam dimensi ancaman siber;

4. penindakan siber, yaitu menyelenggarakan segala usaha, pekerjaan, kegiatan dan tindakan yang terencana serta sistematis dalam melaksanakan aksi strategis dan terukur meliputi eksploitasi dan Pusprop guna memperoleh keunggulan siber dalam operasi;

5. pemulihan siber, yaitu menyelenggarakan segala usaha, pekerjaan, kegiatan dan tindakan yang terencana dan sistematis dalam melaksanakan pemulihan insiden siber sebagai dampak dari berbagai bentuk serangan siber meliputi forensik, pemeliharaan dan instalasi serta *Military Computer Emergency Response Team* (*Mil-CERT*); dan

6. bantuan siber, yaitu menyelenggarakan segala usaha, pekerjaan, kegiatan dan tindakan yang terencana dan sistematis dalam melaksanakan perbantuan siber yang meliputi pembangunan sistem dan dukungan operasi, baik dari aspek teknis maupun nonteknis yang menyangkut operasi dan kegiatan siber.

b. Fungsi Umum:

1. perencanaan yaitu menyelenggarakan kegiatan fungsi perencanaan program dan anggaran rutin dalam rangka mendukung operasional tugas Satsiber TNI;

2. pengamanan dan kegiatan yaitu menyelenggarakan kegiatan fungsi pengamanan dan kegiatan dalam rangka mendukung tugas Satsiber TNI;

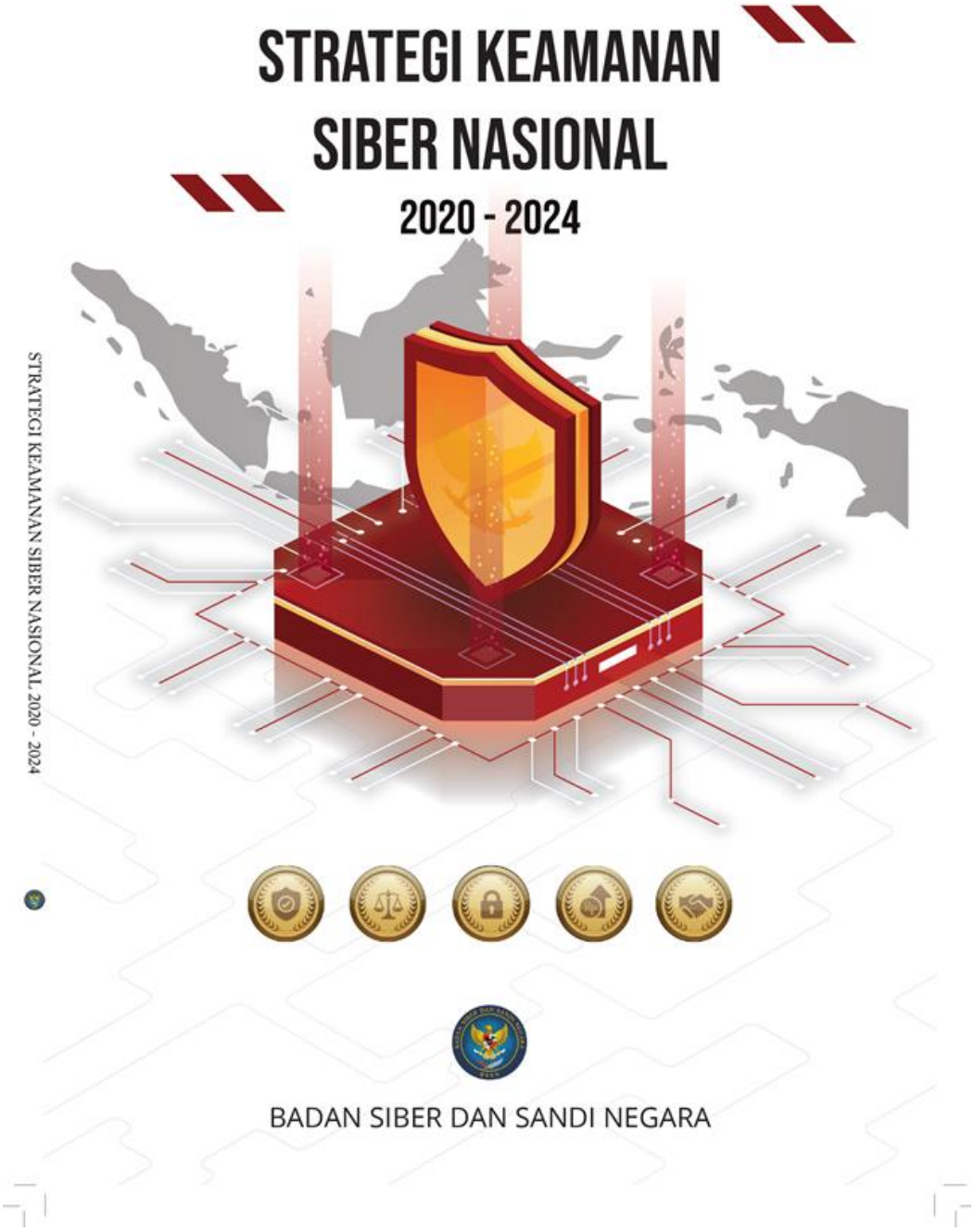
3. personel yaitu menyelenggarakan kegiatan fungsi personel dalam rangka mendukung tugas Satsiber TNI;

4. logistik yaitu menyelenggarakan kegiatan fungsi logistik dalam rangka mendukung tugas Satsiber TNI; dan

5. informasi dan pengolahan data yaitu menyelenggarakan kegiatan fungsi penyajian informasi dan pengolahan data dalam rangka mendukung tugas Satsiber TNI.

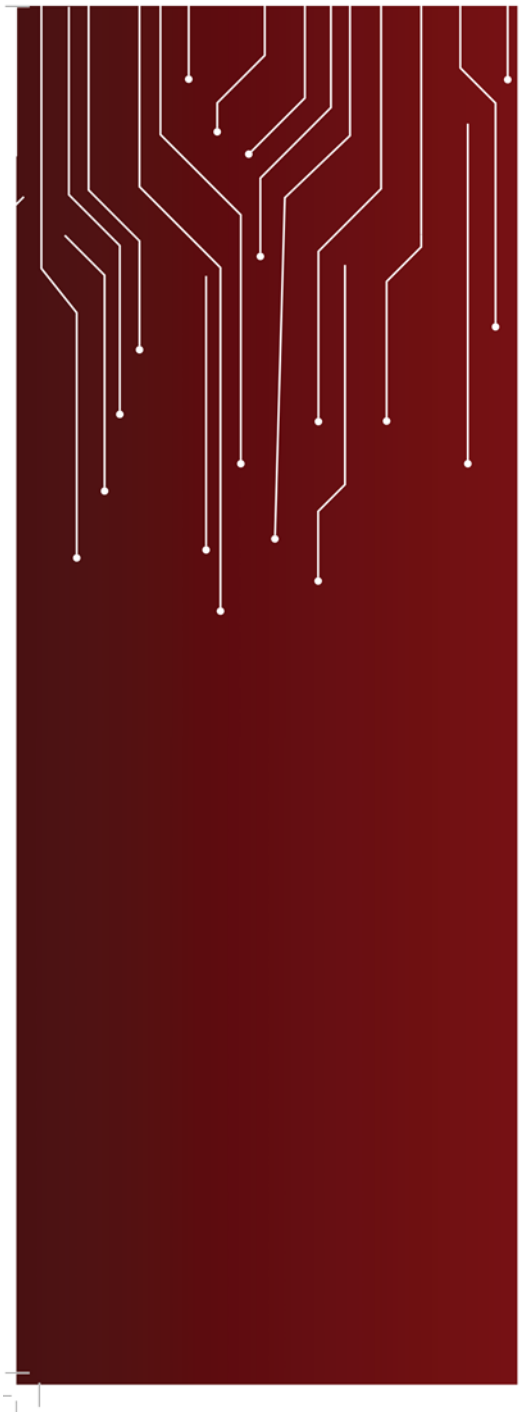
L-5.3 Dokumen BSSN.

Konsep SKSN 2020-2024 rumusan BSSN dan diterbitkan secara internal pada 2019 (catatan: *copy* halaman pada bagian sampul depan, daftar isi, kata pengantar, pendahuluan, lima pilar SKSN dan instrumen monitoring).



Penerbit
Badan Siber dan Sandi Negara cq Direktorat Proteksi Pemerintah
Jl. Harsono RM No. 70
aIndonesia

Penerbitan
Diterbitkan di Jakarta, Indonesia
Tersedia berdasarkan permintaan



Fungsi SKSN 2020 – 2024

Strategi Keamanan Siber Nasional ini merupakan dokumen yang memiliki dua fungsi. Pertama, fungsi strategis dari dokumen ini adalah untuk menjabarkan kerangka kerja pembangunan dan pengembangan di bidang keamanan siber yang secara jelas menunjukkan tujuan nasional yang hendak diwujudkan, aneka pilar yang diprioritaskan, tahapan, waktu, serta indikator pelaksanaan, dan uraian mengenai peranan dari segenap pemangku kepentingan yang terkait. Kedua, fungsi yuridis dari dokumen ini adalah sebagai suatu acuan hukum yang bersifat nasional, bagi segenap jajaran pemerintahan baik di tingkat pusat maupun di daerah.

Badan Siber dan Sandi Negara iii

Daftar Isi

1 2

Pembukaan

- *Kata Pengantar* vi
- *Pendahuluan* viii

Bagian 1
Umum

1. *Bab Satu* 1
2. *Definisi dan Pemangku Kepentingan* 2
   - *Definisi Keamanan Siber* 2
   - *Definisi SPBE* 2
   - *Definisi Infrastruktur Informasi Kritikal Nasional* 2
   - *Definisi Public-Private Partnership* 3
   - *Definisi Sektor Strategis* 3
   - *Pemangku Kepentingan* 3
3. *Bab Dua* 5
   - *Tujuan dan Pertumbuhan*
4. *Bab Tiga* 7
   - *Tujuan Keamnan Nasional*

3

Bagian 2
Pilar Keamanan Siber

1. *Pilar Kesatu* 10
2. *Ketahanan Siber Indonesia* 10
   (Cyber Resilience)
   - *Permasalahan dan Tantangan* 10
   - *Arah Kebijakan* 11
   - *Sasaran* 11
3. *Pilar Kedua* 12
4. *Kepastian Hukum Ruang Siber* 12
   (Cyberspace Law Harmonization and Enforcement)
   - *Permasalahan dan Tantangan* 12
   - *Arah Kebijakan* 14
   - *Sasaran* 14
5. *Pilar Ketiga* 15
6. *Kemampuan Teknologi Siber* 15
   (Cyber Technology Capacity)
   - *Permasalahan dan Tantangan* 15
   - *Arah Kebijakan* 16
   - *Sasaran* 16
7. *Pilar Keempat* 17
8. *Dukungan Pertumbuhan Ekonomi Digital* 17
   (Digital Economy Growth Support)
   - *Permasalahan dan Tantangan* 17
   - *Arah Kebijakan* 18
   - *Sasaran* 18
9. *Pilar Kelima* 19
10. *Kerjasama Internasional dan Nasional* 19
    (International and National Cyber Engagement)
    - *Permasalahan dan Tantangan* 19
    - *Arah Kebijakan* 20
    - *Sasaran* 20

4

Bagian 3
Rencana Aksi

1. *Pilar Satu* 22
   - *Ketahanan Siber Indonesia*
2. *Pilar Dua* 23
   - *Kepastian Hukum Ruang Siber*
3. *Pilar Tiga* 24
   - *Kemampuan Teknologi Siber*
4. *Pilar Empat* 25
   - *Dukungan Pertumbuhan Ekonomi Digital*
5. *Pilar Lima* 26
   - *Kerjasama Internasional dan Nasional*

5

Penutupan

- *Panduan Monitoring dan Evaluasi* 30
- *Lampiran* 32-38

Kata Pengantar

Sebagaimana disampaikan oleh Presiden RI, Bapak Ir. Joko Widodo, dalam Pidato Pelantikan Presiden dan Wakil Presiden Terpilih Periode 2019 – 2024 yang lalu, cita-cita Indonesia di masa satu abad berdirinya republik ini, kelak di tahun 2045, adalah Indonesia yang menjadi Negara maju dengan pendapatan per kapita IDR 320 juta per tahun atau IDR 27 juta per kapita per bulan. Indonesia juga ditargetkan untuk memiliki Produk Domestik Bruto yang mencapai US$ 7 triliun dan masuk dalam kelompok 5 (lima) besar ekonomi dunia dengan tingkat kemiskinan yang mencapai nol persen.

Untuk mencapai cita-cita tersebut perlu melakukan lompatan yang besar *(great leap forward*), dalam bentuk langkah nyata dan terukur dalam satu fase jangka pendek dan menengah. Oleh karena itulah, sebagaimana dikatakan bapak presiden, dalam 5 (lima) tahun ke depan, pembangunan sumber daya manusia akan menjadi prioritas utama Indonesia. Pertanyaannya SDM yang bagaimana? SDM yang dibangun, salah satunya adalah SDM yang menguasai ilmu pengetahuan dan teknologi, terutama yang berkaitan dengan lalu lintas ruang siber (*cyber space*).

Seiring dengan semakin vitalnya pemanfaatan ruang siber, maka bahaya keamanan yang dapat mengancam keberlangsungan perekonomian nasional dan keselamatan warga negara juga diprediksi akan semakin kompleks dan intens. Patut dicermati bahwa risiko insiden siber terhadap Indonesia sangat besar. Oleh karena itu, Badan Siber dan Sandi Negara (BSSN) sebagai badan pemerintahan yang diberikan tugas khusus oleh Presiden untuk menjaga keamanan siber, perlu memiliki kebijakan dan strategi yang sesuai untuk digunakan sebagai acuan dalam rangka melaksanakan tugasnya.

Urgensi untuk mengamankan ruang siber Indonesia lewat sebuah perencanaan yang matang mulai dari pemetaan masalah yang dihadapi hingga berbagai fokus dan target yang menjadi orientasi membuat pentingnya sebuah dokumen terintegrasi mengenai strategi keamanan siber nasional. Karena itulah BSSN perlu untuk menyusun sebuah dokumen nasional/ Indonesia terkait strategi keamanan siber (*national cybersecurity strategy*). Sebelumnya BSSN telah melakukan kajian strategi keamanan siber guna menyusun sebuah kerangka kerja (*frame work*) di bidang keamanan siber. Seiring dengan rencana strategis pembangunan nasional berikutnya, perlu ditinjau strategi yang sudah ada apakah masih sesuai dengan strategi dan arah pembangunan nasional berikutnya.

Strategi keamanan siber nasional/Indonesia adalah sebuah dokumen strategis yang bukanlah hasil kerja tunggal dari BSSN tetapi sebuah hasil gotong royong/kolaborasi dari semua pemangku kepentingan terkait yang tentunya memiliki kepentingan terhadap keamanan ruang siber. Berdasarkan hasil kajian BSSN, terdapat 5 pilar capaian keamanan siber yang menjadi fokus *National Cybersecurity Strategy* 2020 – 2024.

Ketahanan Siber Indonesia

Pilar pertama ini memiliki arah kebijakan dalam hal meningkatkan pengetahuan, kemampuan dan kolaborasi dalam mengantisipasi terjadinya serangan siber disertai penentuan langkah-langkah yang diperlukan untuk membatasi, memproteksi dan mencegah serangan serta penanganan insiden/penanggulangan serangan siber yang berfokus pada 3 area utama yaitu sistem pemerintahan berbasis elektronik (SPBE), infrastruktur kritis nasional dan aktivitas ekonomi digital.

Kepastian Hukum Ruang Siber

Pilar kedua ini fokus dalam peningkatan legitimasi dan penegakan hukum untuk memberikan perlindungan keadilan yang lebih baik kepada masyarakat khususnya terkait risiko insiden dan konflik siber serta memperjelas tugas, fungsi dan kewenangan antar lembaga pemerintah yang dapat mendorong efektivitas koordinasi dan kolaborasi seluruh pemangku kepentingan.

Penguasaan Teknologi Keamanan Siber

Di pilar berikutnya, arah kebijakan yang menjadi fokus adalah meningkatkan pengetahuan, kemampuan serta kolaborasi penta-helix dalam merumuskan dan mengeksekusi kebijakan siber antara pemerintah, masyarakat atau komunitas, akademisi, pebisnis atau pengusaha dan terakhir media. Pilar ini juga mendorong terciptanya personil siber yang mampu menguasai, memodifikasi dan/atau memutakhirkan seluruh ragam teknologi yang terkait untuk mengantisipasi ancaman dan dampak serangan siber.

Dukungan Pertumbuhan Ekonomi Digital

Fokus pilar ini adalah menetapkan langkah-langkah dalam meningkatkan kontribusi sektor keamanan siber terhadap perekonomian digital sehingga pemanfaatan ruang siber semakin produktif, investasi bertumbuh, neraca perdagangan surplus serta lapangan kerja dan tingkat kesejahteraan pekerja terutama di sektor ekonomi digital semakin tinggi.

Kerjasama nasional dan internasional

Pilar ini memiliki fokus arah kebijakan dalam peningkatan peran Indonesia dalam berbagai forum dan agenda diplomasi dan kolaborasi siber di tingkat internasional dalam

melindungi kedaulatan ruang siber nasional, menjaga perdamaian dunia, memajukan perekonomian nasional, meningkatkan kesejahteraan bangsa dan menegaskan kualitas positif yang menjadi karakter kultural bangsa. Selain itu, perlu pula digarisbawahi konsep teknologi netral di ruang siber di mana Indonesia tidak mengacu kepada pihak tertentu, institusi manapun, negara manapun, sesuai kebijakan politik luar negeri Indonesia yaitu bebas dan aktif.

Puji syukur dipanjatkan ke hadirat Tuhan Yang Maha Esa, karena atas Ridha-Nya Dokumen "Strategi Keamanan Siber Nasional 2020-2024" ini dapat diselesaikan. Dokumen ini dirumuskan bersama oleh berbagai pemangku kepentingan di bidang keamanan siber, diantaranya terdiri dari sektor pemerintah, sektor infrastruktur kritis, akademisi, serta komunitas, yang telah berkontribusi dan berkolaborasi untuk dapat mencapai hasil rancangan yang reliabel, implementatif, dan optimal dalam rangka mencapai Pilar Keamanan Siber yang ditetapkan.

Kami ucapkan terimakasih kepada segenap pihak yang telah berkontribusi dalam penyusunan Strategi Keamanan Siber Nasional 2020 – 2024 ini. Saran dan masukan dari para pembaca untuk penyempurnaan dokumen ini sangat kami harapkan. Atas perhatiannya kami ucapkan terima kasih.

Pendahuluan

Keamanan sistem siber Indonesia perlu terpelihara dengan baik, agar keamanan nasional Indonesia juga semakin baik dan pertumbuhan perekonomian Indonesia juga dapat meningkat secara sehat. Untuk mewujudkan hal itu, perlu adanya strategi yang bersifat nasional untuk melindungi, merespon, dan mempertahankan segala hal yang merupakan kepentingan siber Indonesia. Strategi nasional tersebut haruslah ada agar segenap upaya dan sumber daya dapat terjalin secara sinergis dan berkelanjutan.

Pengalaman yang telah dilalui oleh Indonesia memberikan pelajaran bahwa ancaman terhadap keselamatan, kedaulatan, dan keamanan bangsa dan negara Indonesia adalah nyata. Ancaman tersebut dapat tampak secara terang-terangan dan dapat pula yang tersembunyi. Namun demikian, kondisi ketertiban umum dan perekonomian Indonesia pada saat ini menunjukkan bahwa Indonesia sesungguhnya memiliki fondasi yang kuat untuk memelihara keamanannya. Fondasi itulah yang perlu dikuatkan, disinergikan, dan dioptimalkan agar tingkat ketahanan Indonesia dalam menghadapi ancaman yang bersifat multi-dimensi, baik yang berasal dari dalam negeri maupun yang berasal dari luar negeri, dapat semakin baik.

Dalam konteks pemeliharaan keamanan siber, penguatan fondasi dapat berarti empat hal. Pertama, bahwa segala kerentanan yang dapat meningkatkan ancaman atau bahaya di bidang siber harus dapat dideteksi dan diidentifikasi. Kedua, segala aset yang penting untuk hajat hidup orang banyak, harus dapat dilindungi atau dibentengi dari kemungkinan adanya sabotase, serangan, atau aneka upaya lain untuk menghancurkan atau merusaknya. Ketiga, segala sabotase, serangan, atau aneka upaya lain yang sedang berlangsung harus dapat ditanggulangi secepatnya dan kerusakan, kehilangan, atau kehancuran yang telah terjadi harus dapat dipulihkan secepatnya. Keempat, segala komponen dalam penyelenggaraan keamanan siber yaitu manusia, perangkat teknis, dan perangkat non teknis, harus dapat dipantau dan dikendalikan agar tidak menambah banyak atau menambah besar kerentanan.

Berlandaskan pada pemahaman tersebut, maka perlu adanya suatu strategi nasional yang memberikan kejelasan bahwa Indonesia tidak melihat ancaman di bidang siber secara sempit dari aspek teknikal saja dan hanya terbatas pada lingkup serangan yang ditujukan pada infrastruktur informasi yang kritikal. Tetapi Indonesia telah melihat ancaman di bidang siber dengan perspektif yang luas.

Indonesia memerlukan wawasan yang luas tersebut, karena peradaban dunia kini telah bergeser ke revolusi industri keempat yaitu *artificial intelligence revolution* yang bercirikan semakin masifnya pemanfaatan teknologi tinggi yang berbasis pada teknologi digital. Obyek keamanan siber Indonesia tidak hanya sistem siber milik pemerintah, baik di tingkat pusat maupun di daerah. Tetapi meliputi pula segenap infrastruktur informasi kritikal dan sistem siber yang vital untuk terselenggaranya transaksi elektronik dan/atau perekonomian digital, yang sebagian besar mungkin dimiliki oleh swasta.

Oleh karena luasnya pemangku kepentingan (*stakeholders*) dalam pemeliharaan keamanan siber ini, maka segala upaya pelaksanaan keamanan siber perlu berbasiskan pada kolaborasi yang efektif di antara seluruh pemangku kepentingan siber nasional. Juga perlu adanya upaya diplomasi siber untuk memajukan segenap kepentingan Indonesia dalam bidang keamanan siber di tingkat internasional.

Strategi Keamanan Siber Nasional ini merupakan dokumen yang memiliki dua fungsi. Pertama, fungsi strategis dari dokumen ini adalah untuk menjabarkan kerangka kerja pembangunan dan pengembangan di bidang keamanan siber yang secara jelas menunjukkan tujuan nasional yang hendak diwujudkan, aneka pilar yang diprioritaskan, tahapan, waktu, serta indikator pelaksanaan, dan uraian mengenai peranan dari segenap pemangku kepentingan yang terkait. Kedua, fungsi yuridis dari dokumen ini adalah sebagai suatu acuan hukum yang bersifat nasional, bagi segenap jajaran pemerintahan baik di tingkat pusat maupun di daerah.

Dalam dokumen Rencana Pembangunan Jangka Panjang Nasional telah dirumuskan visi pembangunan Indonesia, yaitu bertransformasi dari kondisi saat ini sebagai negara dengan pendapatan menengah menjadi negara yang berpendapatan tinggi. Oleh karena itu penguatan fondasi di segenap sektor dipandang sangat penting untuk mewujudkan visi tersebut.

RPJMN 2020 – 2024 telah merumuskan bahwa negara wajib terus hadir dalam melindungi segenap bangsa, memberikan rasa aman serta pelayanan publik yang berkualitas pada seluruh warga negara dan menegakkan kedaulatan negara. Pemerintah akan terus berupaya meningkatkan tata kelola pemerintahan yang baik dan transparan yang dapat diakses oleh semua masyarakat melalui… (diantaranya) tata kelola keamanan siber. Penguatan keamanan dan ketahanan siber ditandai dengan meningkatnya skor Indonesia dalam *Global Cybersecurity Index*.

Pembangunan keamanan siber Indonesia memiliki dua dimensi. Dimensi pertama, keamanan siber untuk meningkatkan pertumbuhan ekonomi nasional. Dimensi kedua, keamanan siber sebagai bagian dari upaya mewujudkan keamanan nasional.

Dalam konteks dukungan untuk pertumbuhan ekonomi, adalah patut diinsyafi bahwa pembangunan akan sulit berjalan dengan baik apabila tidak ada rasa aman untuk bekerja atau berusaha. Kini dengan semakin bergantungnya manusia, pemerintah, dan pebisnis pada infrastruktur, sistem, dan perangkat siber, digitalisasi ekosistem bisnis di berbagai

sektor membuat Indonesia harus siap dalam menghadapi aneka tantangan dan ancaman terhadap sektor perekonomiannya yang telah berbasis digital.

Ada 3 (tiga) jenis aset yang dapat menjadi target ancaman siber, yaitu:

1. ***Physical assets*** (misalnya sarana prasarana/ infrastruktur, *fixed devices*, *mobile devices*, dsb.),
2. ***Virtual assets*** (contohnya data, *intellectual property rights information, computer application*, dsb.), dan
3. P***ositional assets*** atau aset yang terkait dengan kedudukan sosial (misalnya reputasi, pengaruh, dsb.).

Dengan mempertimbangkan data terkait jumlah perusahaan penyedia infrastruktur siber, aplikasi Internet yang dimiliki perusahaan domestik yang digunakan secara masif, besarnya jumlah kartu kredit dan kartu debit yang telah diterbitkan, jumlah perusahaan domestik yang telah berekspansi ke luar negeri dan mengelola sistem elektronik di luar negeri, serta jumlah percobaan atau aktual serangan siber yang terjadi atau ditujukan ke aset di Indonesia, maka saat ini profil risiko siber Indonesia berada pada tingkat signifikan ke tingkat sangat besar.

Dalam konteks keamanan nasional, segala upaya, pekerjaan, kegiatan, dan/atau tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat melemahkan, merugikan, dan/atau menghancurkan kepentingan nasional Indonesia di bidang siber, merupakan ancaman bagi keamanan siber Indonesia. Dimensi ancaman keamanan siber dapat meliputi 3 hal, yaitu: a) ancaman terhadap ekosistem siber pemerintah, b) ancaman terhadap ekosistem siber yang bersifat infrastruktur kritikal, dan c) ancaman terhadap ekosistem siber yang penting untuk perekonomian nasional.

Tujuan ancaman siber dapat bermacam-macam tergantung pada motivasi dari pelaku ancaman. Mengingat bahwa ancaman dapat hadir sewaktu-waktu tanpa terduga, maka segenap pemangku kepentingan siber nasional haruslah senantiasa siaga dalam merespon ancaman dan memitigasi risiko, termasuk mempertahankan diri.

Dengan profil risiko siber yang demikian maka idealnya ekosistem penyelenggaraan keamanan siber Indonesia haruslah paling sedikit berada di tingkat kematangan menengah (*intermediate maturity*), yang dicirikan oleh adanya suatu penyelenggaraan keamanan siber yang rinci dan berbasis prosedur formal, yang melakukan pengawasan secara obyektif dan konsisten, serta segenap pemangku kepentingan siber nasional telah memiliki mekanisme analisis dan pelaksanaan manajemen risiko yang inheren di dalam kebijakan strategis dan operasional dari institusinya.

Pasar pada ekonomi digital Indonesia tidak akan bertumbuh dengan baik apabila Indonesia tidak mampu mengelola risiko keamanan siber dengan baik. Mengingat bahwa tidak mungkin profil risiko keamanan siber Indonesia akan mengecil, maka adalah suatu *conditio sine qua non* bahwa tingkat kematangan ekosistem keamanan siber Indonesia harus dinaikkan.

Apabila Indonesia dapat mewujudkan iklim keamanan siber yang kondusif, maka pasar ekonomi digital tersebut akan bertumbuh semakin besar. Kondisi tersebut akan membuat bisnis barang dan/atau jasa yang terkait dengan pemanfaatan siber, atau secara khusus terkait produk keamanan siber juga semakin marak. Dari kondisi itu diharapkan akan semakin banyak lapangan pekerjaan atau wirausaha yang bertumbuh dan memperkuat perekonomian Indonesia.

Pada kenyataannya saat ini tingkat kematangan ekosistem keamanan siber Indonesia secara nasional masih berada pada tingkat kematangan dasar (*baseline maturity*), yang dicirikan oleh minimnya aturan hukum yang memberikan panduan dasar bagi para pihak yang mengelola sistem elektronik atau infrastruktur siber. Akibatnya suatu acuan minimum dalam penyelenggaraan keamanan siber yang berkualitas belum tersedia, kualitas pelayanan rendah, respon, penanggulangan, dan pemulihan terhadap insiden siber berlangsung lambat, serta pengawasan belum berlangsung secara efektif.

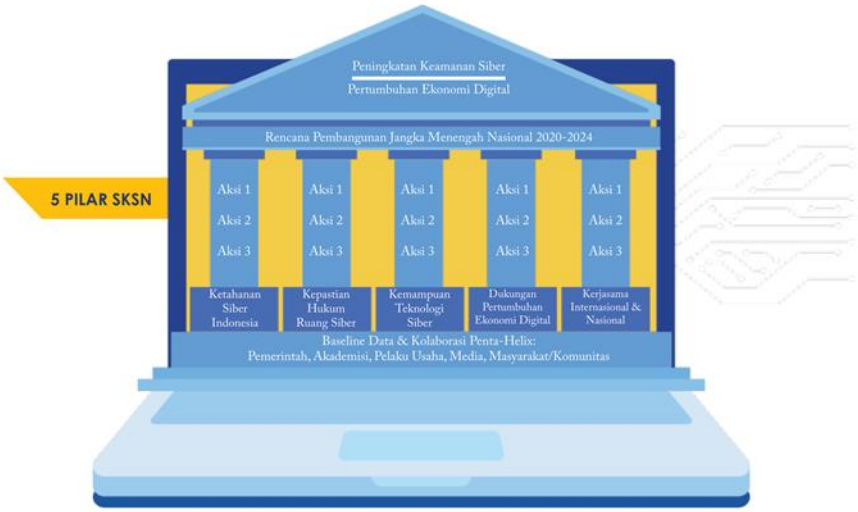
Untuk menaikkan tingkat kematangan keamanan siber Indonesia, kata kuncinya adalah kolaborasi antar pemangku kepentingan siber nasional. Pemerintah tidak bisa bekerja sendiri, karena:

1. Banyak aset siber yang vital dan penting bagi hajat hidup orang banyak dimiliki oleh swasta,
2. Banyak ahli yang memiliki skill dan networking yang luas di bidang siber berada di institusi perguruan tinggi, di kalangan aktivis siber, maupun di kalangan korporasi,
3. Urusan siber merupakan urusan trans-nasional karena arsitektur siber itu sendiri pada hakekatnya bersifat global, sehingga perlu ada kerjasama atau upaya diplomasi di tingkat internasional.

Berdasarkan pada berbagai pertimbangan tersebut, maka fungsi dari Kebijakan Strategi Keamanan Siber Nasional ini adalah sebagai suatu acuan yuridis yang bersifat nasional, bagi segenap jajaran pemerintahan baik di tingkat pusat maupun di daerah. Dimulai sejak saat berlakunya Kebijakan ini, maka segenap upaya perencanaan, penganggaran, pengadaan, pengelolaan aset negara, pembentukan regulasi, pelaksanaan kewenangan pemerintahan, pengawasan, dan penindakan administratif yang terkat dengan sektor keamanan siber, di seluruh badan pemerintahan di tingkat pusat dan daerah, harus selaras dengan Kebijakan Strategi Keamanan Siber Nasional ini.

Dalam menyusun dokumen ini kami menerapkan kerangka berpikir bahwa untuk mengukur tingkat urgensi pembentukan Strategi Keamanan Siber Nasional, maka perlu dilakukan analisis untuk mengetahui apakah tingkat kematangan ekosistem keamanan siber Indonesia (*cyber security maturity level*) pada saat ini telah setara dengan profil risiko keamanan siber yang dihadapi (*cyber security risk profile*). Premis yang digunakan adalah sebagai berikut:

STRATEGI KEAMANAN SIBER NASIONAL



> *If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels.*

Premis tersebut kami maknai sebagai berikut. Bahwa apabila pemerintah Indonesia memandang tingkat kematangan ekosistem keamanan sibernya belum setara dengan profil risiko keamanan siber yang dihadapi, maka pemerintah Indonesia seyogyanya mempertimbangkan untuk mengurangi risiko tersebut atau mengembangkan strategi untuk menaikkan tingkat kematangan ekosistem keamanan sibernya.

Berdasarkan data sekunder atau literatur yang diperoleh, situasi profil risiko keamanan siber Indonesia pada saat ini menurut kami adalah pada tingkatan Signifikan ke Sangat Besar. Idealnya ketika profil risiko keamanan siber Indonesia berada di tingkatan Signifikan ke Sangat Besar, maka tingkat kematangan ekosistem keamanan siber Indonesia minimum berada di tingkatan Menengah (*Intermediate*) ke Telah Maju (*Advanced*). Namun pada saat ini, tingkat kematangan ekosistem keamanan siber Indonesia adalah berada pada skala Paling Dasar (*Baseline*).

Ciri khas yang menunjukkan bahwa saat ini tingkat kematangan ekosistem keamanan siber Indonesia berada di skala Paling Dasar (*Baseline*) adalah sedikitnya aturan hukum dalam tata tertib pengelolaan keamanan siber di Indonesia.

Di masa yang akan datang adalah mustahil untuk mengurangi profil risiko keamanan siber. Pemanfaatan siber dan eksistensi aset siber yang melayani kebutuhan bangsa dan negara Indonesia akan semakin banyak, semakin kompleks, semakin luas sebarannya, dan semakin bernilai komersial dan strategis. Oleh karena itu, kami berpandangan di masa mendatang profil risiko keamanan siber Indonesia akan bertambah semakin besar. Oleh karena itu, tidak ada pilihan lain, Indonesia harus mengakselerasi tingkat kematangan ekosistem keamanan

sibernya. Oleh karenanya pembentukan Strategi Keamanan Siber Nasional tidak hanya urgen, tetapi juga suatu *conditio sine qua non*, suatu yang semestinya harus ada.

Selain pertimbangan tersebut, adanya suatu Strategi Keamanan Siber Nasional merupakan keharusan untuk melaksanakan ketentuan Pasal 94 ayat (1) huruf a Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal tersebut menyatakan bahwa Strategi Keamanan Siber Nasional merupakan bagian dari Strategi Keamanan Nasional, yang di dalamnya meliputi pembangunan budaya keamanan siber, yang mana penetapan Strategi Keamanan Siber Nasional tersebut ditujukan untuk melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum.

Selanjutnya dalam rangka menghasilkan suatu dokumen Strategi Keamanan Siber Nasional yang selaras dengan Rencana Pembangunan Jangka Panjang Nasional dan juga selaras dengan model yang lazim di tingkat internasional khususnya di *International Telecommunication Union*, maka dokumen ini disusun berdasarkan beberapa premis.

Pertama, bahwa target pembangunan nasional Indonesia pada tahun 2045 sedikitnya ada tiga, yaitu: (1) terwujudnya pendapatan per kapita sebesar IDR 320 Juta per tahun, (2) Produk Domestik Bruto mencapai US$ 7 Triliun, dan (3) tingkat kemiskinan nasional mendekati nol.

Kedua, bahwa suatu Strategi Keamanan Siber Nasional harus memuat unsur: (1) Ends (target akhir yang hendak dituju), (2) Ways (aneka jalan untuk mewujudkan target tersebut), dan (3) Means (cara-cara yang ditempuh pada setiap jalan yang telah ditentukan yang terdiri dari 5 (lima) kategori yaitu: (a) aspek hukum, (b) aspek teknikal dan procedural, (c) aspek organisasional, (d) aspek pembangunan kapasitas, dan (e) aspek kerjasama internasional).

Ketiga, bahwa ketiga target pembangunan nasional sebagaimana dimaksud pada butir pertama merupakan kepentingan umum yang dimaksud pada Pasal 94 ayat (1) huruf a PP 71/2019 dan juga merupakan Ends dari Strategi Keamanan Siber Nasional. Sedangkan, Pilar-Pilar pada dokumen Strategi Keamanan Siber Nasional ini merupakan Ways yang menurut hasil kajian dipandang paling efektif dan efisien untuk melindungi kepentingan umum tersebut dari segala gangguan sebagai penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum.

Pilar Satu
Ketahanan Siber Indonesia

Kategori	Aksi	Keluaran	Pelaksana Utama (Funding, Skills, and Management)	Mitra Kolaborasi (Co-Funding, Skills, and/or Networking)	Sasaran (Beneficiaries)
Penyiapan Konsep Teknokratik dan/atau Aturan	Penyusunan, pendiseminasian, dan pemberlakuan arsitektur atau rancang bangun, serta standar dan kriteria keamanan	1. Arsitektur atau Rancang Bangun Keamanan 2. Standar dan Kriteria Keamanan 3. Kegiatan Diseminasi	BSSN	Kemenko Polhukam, Kementerian Kominfo, Kementerian BUMN, dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis
Peningkatan Kompetensi SDM	Edukasi, peningkatan kompetensi, dan pembinaan secara aktif untuk mendorong kepatuhan terhadap standar dan kriteria keamanan	1. Penyusunan Kurikulum dan Standar Modul Nasional 2. Kegiatan Pelatihan dan/atau Pendidikan 3. Kegiatan Pengujian Kompetensi 4. Penyelenggaraan Konsultasi 5. Kegiatan Asesmen	BSSN	Instansi Pengatur dan Pengawas Sektor dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis
Pembangunan dan/atau Penyelenggaraan Sarana Prasarana	Pembangunan pusat operasi keamanan nasional dan pusat operasi keamanan di tiap pengelola sistem elektronik pada sektor strategis secara terpadu	1. National Security Operation Center 2. Security Operation Center	1. BSSN 2. Seluruh pemilik atau penyelenggara sistem elektronik pada sektor strategis	Kemenkeu, Bappenas, Kementerian BUMN, dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis
Penguatan Koordinasi dan Kolaborasi	Mengintensifkan koordinasi dan kerjasama operasional antar tim respon kedaruratan (CERT/CSIRT) di tiap pengelola sistem elektronik pada sektor strategis, serta mengintensifkan pelibatan komunitas dan partisipasi sukarela dari pengelola sistem elektronik pada sektor strategis untuk menemukan celah kerentanan keamanan dan menutup celah kerentanan yang telah ditemukan	1. National CERT/CSIRT 2. CERT/CSIRT 3. National Threat Analysis Center 4. Program Voluntary Vulnerability Disclosure (Bug Hunting)	BSSN	Kemenko Polhukam, CERT, CSIRT (domestik dan luar negeri, pemerintah dan swasta), Komunitas Bug Hunter, Pelaku Usaha Jasa Pengujian Keamanan, dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis
Manajemen	Meningkatkan efektifitas dalam administrasi, pelayanan, dan pengambilan keputusan	1. Statistik dan Direktori Ketahanan Siber Indonesia 2. Kegiatan monitoring dan evaluasi 3. Kegiatan Audit	BSSN	BPS, KEMENPAN-RB, dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis

Pilar Dua
Kepastian Hukum Ruang Siber

Kategori	Aksi	Keluaran	Pelaksana Utama (Funding, Skills, and Management)	Mitra Kolaborasi (Co-Funding, Skills, and/or Networking)	Sasaran (Beneficiaries)
Penyiapan Konsep Teknokratik dan/atau Aturan	Pemantapan tata hukum ruang siber	1. UU Keamanan dan Ketahanan Siber 2. UU Persandian 3. UU Pelindungan Data Pribadi	Kementerian Kumham, Kementerian Sekretariat Negara, BSSN, Kementerian Kominfo	Penta-Helix	Aparatur pemerintahan
Peningkatan Kompetensi SDM	Edukasi, peningkatan kompetensi, dan pembinaan secara aktif untuk mendorong kepatuhan aparat pemerintahan terhadap tata hukum ruang siber	1. Penyusunan Kurikulum dan Standar Modul Nasional 2. Kegiatan Pelatihan dan/atau Pendidikan 3. Kegiatan Pengujian Kompetensi 4. Penyelenggaraan Konsultasi 5. Kegiatan Asesmen	BSSN, POLRI, Kejaksaan, dan Kementerian Kominfo	Instansi Pengatur dan Pengawas Sektor dan unsur Penta-Helix lain	Aparatur pemerintahan
Pembangunan dan/atau Penyelenggaraan Sarana Prasarana	Penguatan sarana berbasis teknologi informasi dan komunikasi yang terpadu untuk menangani kejahatan siber	1. Sistem Informasi Terpadu Penegakan Hukum Tindak Pidana Siber 2. Pembangunan laboratorium forensik	BSSN, POLRI, Kejaksaan, dan Kementerian Kominfo	POLRI, Kejaksaan, Kominfo, Kemenkeu, Bappenas, Kementerian BUMN, dan unsur Penta-Helix lain	Aparatur pemerintahan
Penguatan Koordinasi dan Kolaborasi	Memperluas pelibatan komunitas dan akademisi untuk membantu memberikan dukungan dan peningkatan kualitas penerapan pendekatan saintifik dalam pembuktian suatu perkara	1. Kesepakatan bersama untuk menggunakan standar dan kriteria dalam penentuan saksi ahli di bidang Hukum Siber dan/atau Forensik Digital	BSSN, POLRI, Kejaksaan, dan Kementerian Kominfo	Kemenko Polhukam, Hakim, Advokat, Akademisi, dan unsur Penta-Helix lain	Aparatur penegak hukum
Manajemen	Meningkatkan efektifitas dalam administrasi, pelayanan, dan pengambilan keputusan	1. Statistik dan Direktori Kepastian Hukum Ruang Siber 2. Kegiatan monitoring dan evaluasi 3. Kegiatan Audit	BSSN	BPS, KEMENPAN-RB, dan unsur Penta-Helix lain	Aparatur Pemerintahan (termasuk Aparatur Penegak Hukum)

Pilar Tiga
Kemampuan Teknologi Siber

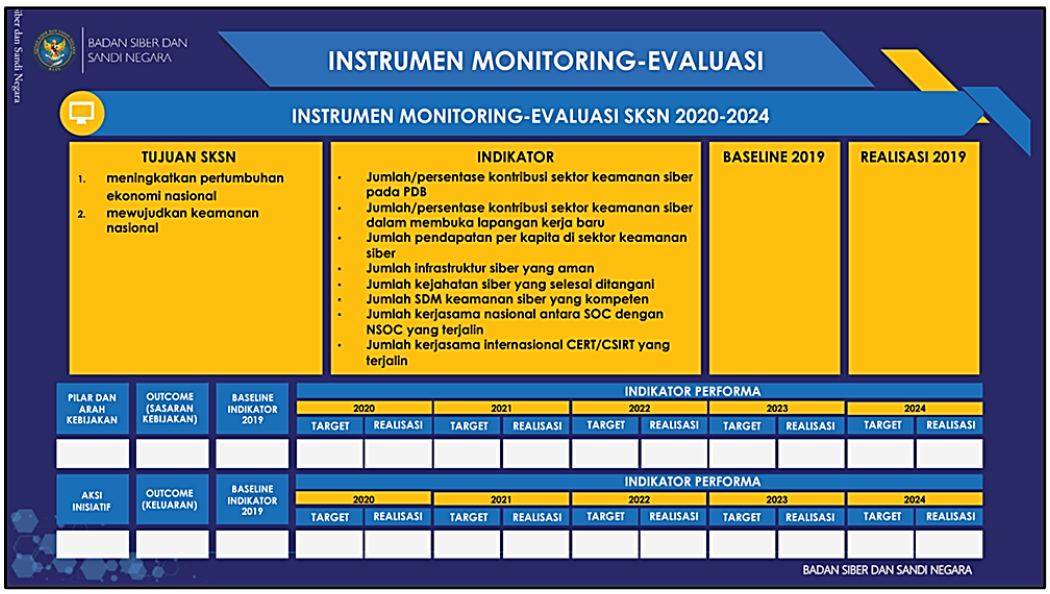
Kategori	Aksi	Keluaran	Pelaksana Utama (Funding, Skills, and Management)	Mitra Kolaborasi (Co-Funding, Skills, and/or Networking)	Sasaran (Beneficiaries)
Pembangunan dan/atau Penyelenggaraan Sarana Prasarana	Pembangunan laboratorium pada beberapa universitas yang ditetapkan sebagai center of excellence dalam penelitian dan pengembangan inovasi di bidang teknologi siber	1. Laboratorium pengujian dan manufaktur produk siber 2. Cyber-Range (Fasilitas simulasi latihan menghadapi serangan siber)	BSSN	Kementerian Keuangan, Bappenas, Kementerian BUMN, Ditjen KI, BPPT, Perguruan Tinggi, Registry Protokol Internet, Registry Nama Domain, Komunitas Bug Hunter, dan unsur Penta-Helix lain	Peneliti
Penguatan Koordinasi dan Kolaborasi	Pemberian dukungan finansial kepada para inventor untuk pelaksanaan penelitian dan pengujian pasar dari produk hasil penelitian di bidang teknologi siber	1. Hibah penelitian untuk aparatur pemerintahan, akademisi di perguruan tinggi, peneliti di lembaga litbang nirlaba, dan pelaku usaha start up 2. Hibah inkubasi bisnis untuk pelaku usaha start up	BSSN	Kementerian Keuangan, Kementerian Pendidikan dan Kebudayaan, Kementerian BUMN, dan unsur Penta-Helix lain	Peneliti
Manajemen	Meningkatkan efektifitas dalam administrasi, pelayanan, dan pengambilan keputusan	1. Statistik dan Direktori Kemampuan Teknologi Siber 2. Kegiatan monitoring dan evaluasi 3. Kegiatan Audit	BSSN	BPS, KEMENPAN-RB, dan unsur Penta-Helix lain	Peneliti

Pilar Empat
Dukungan Pertumbuhan Ekonomi Digital

Kategori	Aksi	Keluaran	Pelaksana Utama (Funding, Skills, and Management)	Mitra Kolaborasi (Co-Funding, Skills, and/or Networking)	Sasaran (Beneficiaries)
Penyiapan Konsep Teknokratik dan/atau Aturan	Memberikan kemudahan dan insentif untuk membuka usaha baru di bidang keamanan siber	1. Standar dan Kriteria dual-use goods di lingkup keamanan siber 2. Usaha di bidang keamanan siber yang tidak termasuk Daftar Negatif Investasi 3. Pengalokasian tata ruang dan lahan untuk lokasi industri 4. Kemudahan dan kecepatan dalam pemrosesan perizinan usaha industri keamanan siber 5. Insentif perpajakan untuk industri keamanan siber	BKPM, Kementerian Agraria, Kementerian Perindustrian, Kementerian Keuangan, BSSN	Penta-Helix	Pelaku usaha di bidang keamanan siber
Penguatan Koordinasi dan Kolaborasi	Meningkatkan kuantitas produk keamanan siber yang tingkat kandungan komponen dalam negerinya signifikan	1. Pemberian bantuan penyediaan sertifikat digital 2. Pemberian bantuan konsultasi 3. Hibah untuk penyelenggaraan pameran produk teknologi keamanan siber di dalam negeri atau penetrasi pasar di luar negeri	BSSN, Kementerian Perdagangan	Kemenkeu, Bappenas, Kementerian BUMN, dan unsur Penta-Helix lain	Pelaku usaha di bidang keamanan siber
Manajemen	Meningkatkan efektifitas dalam administrasi, pelayanan, dan pengambilan keputusan	1. Statistik dan Direktori Dukungan Pertumbuhan Ekonomi Digital 2. Kegiatan monitoring dan evaluasi 3. Kegiatan Audit	BSSN	BPS, KEMENPAN-RB, dan unsur Penta-Helix lain	Pelaku usaha di bidang keamanan siber

Pilar Lima
Kerjasama International dan Nasional

Kategori	Aksi	Keluaran	Pelaksana Utama (Funding, Skills, and Management)	Mitra Kolaborasi (Co-Funding, Skills, and/or Networking)	Sasaran (Beneficiaries)
Peningkatan Kompetensi SDM	Pelibatan jurnalis, praktisi, serta akademisi untuk penyusunan dan pendiseminasian konten edukasi yang mengkampanyekan pentingnya memelihara keamanan siber	1. Penyusunan Kurikulum dan bahan ajar perkuliahan tentang keamanan siber 2. Kegiatan Pelatihan dan/atau Pendidikan	BSSN	Asosiasi Jurnalis, Asosiasi Media, Asosiasi Dosen, dan unsur Penta-Helix lain	Masyarakat luas
Penguatan Koordinasi dan Kolaborasi	Peningkatan pencapaian pada HoneyNET Project	1. Threat Map yang mutakhir 2. Malicious Domain List yang mutakhir	BSSN	The HoneyNET Project, Komunitas Bug Hunter, CERT/CSIRT, Registry Protokol Internet, Registry Nama Domain, dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis
Penguatan Koordinasi dan Kolaborasi	Penyelenggaraan latihan bersama secara berkelanjutan	1. Government Cyber Exercise 2. Government-Internet Registry Cyber Exercise 3. Government-Energy Infrastructure Cyber Exercise 4. Government-Financial Infrastructure Cyber Exercise 5. Government-Transportation and Logistics Infrastructure Cyber Exercise 6. Government-Health Infrastructure Cyber Exercise 7. Cyber Defense Exercise	BSSN	Registry, Komunitas Bug Hunter, CERT/CSIRT, dan unsur Penta-Helix lain	Pengelola sistem elektronik pada sektor strategis
Penguatan Koordinasi dan Kolaborasi	Penyelenggaraan kegiatan untuk berbagi informasi secara berkelanjutan	1. Kegiatan pendiseminasian konten edukasi seputar keamanan siber 2. Forum pertemuan berkala tingkat nasional	BSSN	Kemenko Polhukam, Jurnalis, dan unsur Penta-Helix lain	Masyarakat luas
Penguatan Koordinasi dan Kolaborasi	Optimalisasi peranan dari focal point di bidang keamanan siber untuk memajukan kepentingan nasional Indonesia di lingkup internasional	1. Pertemuan regional rutin tahunan di Indonesia sebagai upaya untuk membangun Confidence Building 2. MoU dengan CERT/CSIRT di luar negeri 3. MoU Hubungan Timbal Balik untuk kemudahan akuisisi bukti elektronik yang bersifat lintas batas negara 4. MoU untuk menarik investasi ke dalam negeri Indonesia dan mempermudah penetrasi produk keamanan siber Indonesia dipasarkan di luar negeri 5. MoU untuk pembiayaan pendidikan bagi ASN, TNI/POLRI, dan pemangku kepentingan lain 6. MoU untuk menguatkan komitmen menjaga ekosistem siber dalam rangka memelihara perdamaian dunia, memberantas kejahatan siber, melindungi privasi, dan mengupayakan Internet sebagai sumber daya bersama	BSSN, Kemlu	Penta-Helix	Masyarakat luas
Manajemen	Meningkatkan efektifitas dalam administrasi, pelayanan, dan pengambilan keputusan	1. Statistik dan Direktori Kerjasama Internasional dan Nasional di Lingkup Keamanan Siber 2. Kegiatan monitoring dan evaluasi 3. Kegiatan Audit	BSSN	BPS, KEMENPAN-RB, dan unsur Penta-Helix lain	Masyarakat luas



Lampiran – 6 (Display Hasil Kondensasi Data Penelitian)

Pertanyaan	Pushansiber KEMHAN	Satsiber TNI	Balitbang SDM Kominfo	BSSN
Implementasi peran dan fungsi SKSN terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG (SISHANKAMRATA)				
Menurut perspektif instansi masing-masing, bagaimana kiranya signifikansi SKSN terhadap implementasi pembangunan kompetensi SDM yang dilaksanakan BSSN maupun instansi pemangku kepentingan siber, yang berimplikasi kepada eksistensi SKSN khususnya terhadap upaya membangun SDM pertahanan siber untuk kepentingan SISHANNEG	Pushansiber TNI belum mengetahui adanya SKSN maupun konsep SKSN rumusan BSSN. Namun demikian berpendapat bahwa apabila SKSN tersebut terwujud, maka eksistensinya akan menjadi vital dan penting tidak hanya sekedar untuk membangun kapasitas dan kapabilitas SDM keamanan siber nasional saja, namun juga akan sangat mendukung terwujudnya SDM pertahanan siber. → (Aspek POAC)	Satsiber TNI belum mengetahui adanya SKSN maupun konsep SKSN rumusan BSSN. Namun demikian, bahwa kiranya MoU (Nota Kesepahaman) antara Satsiber TNI dengan BSSN yang mengatur rencana kerja sama tentang Penguatan Keamanan Siber dan Persandian di Lingkungan TNI, di mana salah satu dari 6 (enam) ruang lingkupnya adalah terkait dengan peningkatan dan pengembangan SDM. Dan melalui MoU ini, sebagaimana tercantum dalam konsep SKSN, maka BSSN akan mengimplementasikan peran penting dalam mendukung upaya membangun SDM keamanan siber yang pada dasanya juga merupakan SDM pertahanan siber untuk kepentingan SISHANNEG. Satsiber TNI sependapat bahwa SKSN penting bagi Indonesia di era digital. Dan bila dihadapkan kepada upaya membangun SDM keamanan siber nasional, maka eksistensi SKSN juga menjadi penting khususnya terhadap upaya bidang pertahanan membangun	Balitbang SDM Kominfo pada dasarnya memahami tentang SKSN, namun sejak BSSN terbentuk belum mengetahui tentang konsep SKSN 2020-2024 rumusan BSSN. Berkenaan dengan SKSN, maka Balitbang SDM Kominfo adalah sebagaimana merujuk pada PP No.71/2019 tentang PSTE, pasal 94 ayat (1) huruf a, di mama penetapan strategi keamanan siber nasional yang merupakan bagian dari strategi keamanan nasional, termasuk pembangunan budaya keamanan siber adalah merupakan peran pemerintah. Adapun dengan konsep SKSN rumusan BSSN, itu diluar sepengetahuan Kominfo meskipun BSSN dalam hal tersebut juga merupakan bagian dari institusi pemerintahan. Dalam konteks SDM keamanan siber maupun SDM pertahanan siber, maka terminologi yang digunakan oleh Kementerian Kominfo (dalam hal ini Balitbang SDM Kominfo) adalah SDM bidangTeknologi Informasi dan Komunikasi (TIK).	BSSN konfirm bahwa konsep SKSN yang digunakan dalam penelitian ini adalah konsep SKSN Indonesia 2020-2024 hasil rumusan BSSN yang telah diterbitkan oleh BSSN tahun 2019 namun belum resmi dipublish. Konsep SKSN 2020-2024 yang dijadikan sebagai rujukan oleh peneliti dalam penelitian ini telah dikonfirmasi dan diberikan ijin BSSN sebagai referensi dalam penelitian ini, meskipun BSSN masih terus menyempurnakan konsep SKSN tersebut. Secara substansi, aspek peningkatan kompetensi SDM dalam konsep SKSN 2020-2024 rumusan BSSN masih tetap relevan, meski saat ini konsep SKSN 2020-2024 rumusan BSSN tersebut masih terus disempurnakan. Dalam konsep SKSN 2020-2024, aspek peningkatan kompetensi SDM keamanan siber (yang merupakan elemen *ways* strategi) memiliki peran dan fungsi hanya untuk membagun kompetensi SDM keamanan siber yang dibutuhkan oleh sektor-sektor strategis

		kapasitas dan kapabilitas SDM pertahanan siber untuk mendukung kepentingan SISHANNEHG.	Balitbang SDM Kominfo dalam melaksanakan tugas dan fungsi membangun SDM TIK nasional merujuk pada *Roadmap* Pembangunan TIK Nasional yang berfokus pada pembangunan infrastruktur TIK dengan menitikberatkan pada pembangunan SDM TIK, peningkatan layanan TIK dan pengembangan TIK yang memiliki nilai tambah bagi pertumbuhan ekonomi dan meneguhkan kedaulatan bangsa. Dari hal tersebut maka tampak dalam perspektif Kominfo pembangunan SDM bidang TIK masih menitikberatkan kepada sektor ekonomi di mana pembangunan SDM bidang TIK nasional cenderung diproyeksikan untuk siap bersaing di dunia industri.	sesuai tuntutan keamanan siber, dan tidak termasuk kompetensi SDM pertahanan siber yang spesifik khususnya untuk infrastruktur TIK pada alut-alut sista. Dalam konsep SKSN perbaikan, terdapat sedikit perubahan, diantaranya fungsi SKSN dirumuskan antara lain sebagai: a) kerangka kerja pembangunan dan pengembangan di bidang keamanan siber yang menunjukan tujuan nasional yang hendak diwujudkan, pilar dan inisiatif yang diprioritaskan, tahapan, waktu, serta indikator pelaksanaan, dan uraian mengenai peranan dari segenap pemangku kepentingan yang terkait; b) pedoman bagi menteri dan pimpinan lembaga di bidang keamanan siber dalam menetapkan kebijakan nasional dan sektoral yang terkait dengan SKSN yang dituangkan dalam dokumen rancana strategis di bidang tugas masing-masing sebagai bagian dari Rencana Pembangunan Jangka Menengah Nasional (RPJMN). Dan berkenaan dengan pengembangan kompetensi SDM keamanan siber telah termasuk di dalam konsep perbaikan SKSN. Konsep SKSN perbaikan akan didorong menjadi Peraturan Presiden (Perpres)

				RI. Akan ada semacam Dewan Pengarah SKSN yang diketuai langsung oleh Presiden RI, dengan dibantu oleh Menkopolhukam RI sebagai Ketua Harian, dan Kepala BSSN sebagai Wakil ketua Harian, serta berbagai instansi terkait sebagai anggota. Konsep SKSN perbaikan tersebut, pada saatnya nanti diimplementasikan, tidak semata menjadi tanggung jawab BSSN, namun semua pihak. Pada konsep SKSN perbaikan tersebut terdapat lima pilar perbaikan/ penyempurnaan dari lima pilar pada konsep SKSN 2020-2024. Untuk aspek pembangunan kompetensi SDM keamanan siber pada konsep SKSN perbaikan, telah diakomodir di dalam pilar ke 3 (tiga) yaitu: pembangunan kapasitas dan budaya keamanan siber. Strategi dalam pembangunan kompetensi SDM keamanan siber tersebut adalah ditujukan, baik untuk seluruh SDM nasional, baik pemerintah dan masyarakat umum, (termasuk TNI/Polri) dalam bentuk berbagai macam kegiatan dan praktik latihan bertajuk membangun keamanan siber nasional antara lain *cybersecurity drill test* maupun kegiatan lainnya.

				Untuk mendukung upaya peningkatan kompetensi SDM keamanan siber pada konsep SKSN perbaikan tersebut, BSSN telah menyusun semacam dokumen *roadmap* pebinaan SDM keamanan siber nasional yaitu: Roadmap Pembinaan SDM Siber dan Sandi 2020-2024.
Apakah instansi sudah punya semacam *roadmap* atau rencana program kerja pembangunan SDM yang memiliki kapasitas dan kapabilitas yang relevan dengan bidang TIK atau keamanan siber atau pertahanan siber ?	Sampai saat ini Pushansiber belum mempunyai *roadmap* atau rencana program kerja pembangunan SDM tersebut. Pemenuhan SDM tersebut hanya terbatas memenuhi kebutuhan di lingkungan Kemhan (Pudatin dan Pushansiber), yang bersumber baik dari internal (Kemhan dan TNI), maupun dari eksternal (bersifat kontrak kerja) yang setiap tahun jumlahnya terbatas atau belum mampu memenuhi kebutuhan sesuai kapasitas dan kapabilitas yang dipersyaratkan.	Dalam hal pemenuhan kebutuhan akan SDM pertahanan siber, Satsiber TNI telah menyiapkan proposal rencana program peningkatan kapasitas dan kapabilitas SDM pertahanan siber dan menyerahkan sepenuhnya kepada satuan kerja terkait, dalam hal ini staf Panglima TNI bidang perencanaan dan anggaran, bidang personalia, dan bidang pendidikan dan latihan. Sampai saat proposal tersebut masih belum ditindak lanjuti. Di sisi lain, TNI juga masih belum memiliki *roadmap* terkait rencana kerja pembangunan SDM. Guna mengatasi hal tersebut, Satsiber TNI tetap berupaya membangun kapasitas dan kapabilitas SDM pertahanan siber, dengan mengikutkan SDM Satsiber TNI pada berbagai program dan kegiatan yang dilaksanakan oleh pihak lain, baik dalam bentuk seminar maupun pelatihan-pelatihan, baik di dalam negeri mapupun luar negeri (misalnya	Berkenaan dengan roadmap pembangunan kompetensi SDM, adalah sebagaimana telah diuraikan di atas yaitu membangun kompetensi SDM TIK nasional yang merujuk pada roadmap Pembangunan Sektor TIK Nasional 2016-2045. Roadmap tersebut disusun dengan memperhatikan skenario sektor TIK Indonesia. Roadmap ini menghasilkan rumusan pembangunan yang dibagi atas tiga kelompok kerja yaitu: a) infrastruktur dan tata kelola TIK nasional; b) Internet, Aplikasi, Konten dan Digitalisasi; dan c) SDM dan Social Readiness.	BSSN telah menyusun semacam dokumen *roadmap* pebinaan SDM keamanan siber nasional, yaitu: Roadmap Pembinaan SDM Siber dan Sandi 2020-2024. Dokumen ini dimaksudkan untuk mendukung upaya peningkatan kompetensi SDM keamanan siber pada konsep SKSN perbaikan. Artinya bahwa *roadmap* ini juga mengakomodir kebutuhan SDM keamanan siber sebagai kompetensi awal yang dibutuhkan/diperlukan untuk kompetensi SDM pertahanan siber. Pembinaan SDM keamanan siber dalam *roadmap* tersebut bertujuan demi tercapainya SDM unggul di bidang keamanan siber, di mana langkah-langkah pembinanan mencakup aspek-aspek: standardisasi SDM, pembentukan organisasi profesi, pembentukan lembaga sertifikasi profesi (LSP), integrated sistem informasi, pengembangan kurikulum pusdiklat, *research & development*,

		di Thailand pada Latihan Cobra Gold tahun 2018 dan tahun 2019)		pengembangan kompetensi, pemenuhan sertifikasi, monitoring dan evaluasi, *cybersecurity education* pada pendidikan dasar dan menengah, pusdiklat sebagai *corporate university*, dan STSN sebagai *centre of excelent*.
Faktor-faktor yang mendukung dan menghambat tata kelola SKSN Indonesia terhadap upaya membangun SDM pertahanan siber dalam SISHANNEG				
Dari sudut pandang masing-masing instansi, apa saja faktor-faktor yang mendukung sehingga tata kelola SKSN (konsep SKSN rumusan BSSN) penting terhadap upaya membangun SDM pertahanan siber	Pushansiber KEMHAN telah dilibatkan dalam berbagai kegiatan tidak terprogram yang diselenggarakan BSSN (antara lain seminar dan *drill test*). Kegiatan tersebut dipandang relevan (mendukung) terhadap upaya membangun SDM pertahanan siber Ketiadaan *roadmap* pembangunan kapasitas dan kapabilitas SDM telah diantisipasi pimpinan Pushansiber yang baru melalui program *quick win* kurun waktu 3 (tiga) bulan yang di dalamnya antara lain mencakup aspek upaya membangun kompetensi SDM pertahanan siber, antara lain dengan melakukan *asessment* terhadap SDM pertahanan siber (berdasarkan peran dan fungsi). Pelaksanaannya dibantu pihak mitra (non BSSN).	Telah ada MoU (Nota Kesepahaman) antara Satsiber TNI dengan BSSN dengan maksud untuk mengatur rencana kerja sama tentang Penguatan Keamanan Siber dan Persandian di Lingkungan TNI, di mana salah satu dari 6 (enam) ruang lingkupnya adalah terkait dengan peningkatan dan pengembangan SDM. Satsiber TNI telah dilibatkan dalam berbagai kegiatan tidak terprogram yang diselenggarakan BSSN (antara lain seminar dan *drill test*). Kegiatan tersebut dipandang relevan (mendukung) terhadap upaya membangun SDM pertahanan siber.	Kementerian Kominfo RI belum mengetahui sepenuhnya tentang konsep SKSN 2020-2024 hasil rumusan BSSN. Terlebih dengan masih baru dibentuknya kelembagaan BSSN, maka Kominfo belum mampu memberikan pandangan tentang faktor-faktor yang mendukung tata kelola strategi pembangunan kompetensi SDM keamanan siber dalam konsep SKSN 2020-2024 sehingga rumusan BSSN tersebut mampu mendukung kepentingan bidang pertahanan untuk mewujudkan kompetensi SDM pertahanan siber. Namun demikian terdapat faktor-faktor yang dipandang mendukung yaitu: a) dokumen Penyusunan Roadmap Pembangunan Sektor TIK yang Mengikat Secara Jangka Panjang s.d 2045 Menuju 100 Tahun Indonesia Merdeka; dan Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber; dan c) Rencana Pengembangan	Konsep SKSN 2020-2024 rumusan BSSN telah disempurnakan dan diperbaiki BSSN sebagai konsep SKSN perbaikan. Pada konsep perbaikan tersebut, dilakukan penyempurnaan dan perbakan terhadap 5 (lima) pilar pada konsep SKSN 2020-2024 rumusan BSSN. Berkenaan dengan aspek peningkatan kompetensi SDM keamanan siber, maka perbaikan yang dilakukan telah diakomodir di mana hal-hal yang bekenaan dengan membangun kompetensi SDM keamanan siber dimasukan seluruhnya di dalam pilar ke 3 (tiga) yaitu: pembangunan kapasitas dan budaya keamanan siber. Strategi dalam pembangunan kompetensi SDM keamanan siber tersebut adalah ditujukan, baik untuk seluruh SDM nasional, baik pemerintah dan masyarakat umum, (termasuk TNI/Polri) dalam bentuk berbagai macam kegiatan dan praktik latihan bertajuk membangun keamanan siber nasional antara lain

			SDM TIK di Indonesia Melalui Sertifikasi SKKNI Bidang Kominfo	*cybersecurity drill test* maupun kegiatan lainnya. Aspek pembangunan kompetensi SDM keamanan siber dalam konsep SKSN perbaikan, disusun dan dirumuskan secara *real* atau benar-benar sejalan (*in line*) dengan program-program pembangunan *index* keamanan siber nasional yang di *publish* melalui *Global Cybersecurity Index* (GCI) oleh organisasi *International Telecomunication Union* (ITU), dengan tujuan agar implementasi dari program-program strategis dalam konsep SKSN perbaikan tersebut benar-benar berperanan penting kepada peningkatan index keamanan siber nasional.
Dari sudut pandang masing-masing instansi, apa saja faktor-faktor yang menghambat tata kelola SKSN berdampak pada upaya membangun SDM pertahanan siber	Faktor-faktor penghambat antara lain: a) belum ada wujud/bentuk kerjasama terprogram antara Pushansiber KEMHAN dengan BSSN yang relevan terhadap upaya membangun SDM pertahanan siber, baik untuk jangka pendek, menengah, dan panjang; b) belum optimalnya komunikasi dan koordinasi antara Pushansiber Kemhan dengan BSSN; c) Kedua institusi (baik BSSN maupun Pushansiber Kemhan) masih sama-sama baru terbentuk; d) belum adanya realisasi alokasi anggara untuk program kerja kedua instansi	SKSN penting, namun demikian ketika pemerintah selaku regulator menyusun suatu kebijakan atau aturan yang relevan dengan SDM bidang keamanan siber, maka yang sering terjadi adalah: a) belum adanya persamaan persepsi terhadap konteks SDM TIK (perspektif Kominfo), SDM Keamanan Siber (perspektif BSSN), dan SDM Pertahanan Siber (Perspektif bidang Pertahanan dan TNI); b) konsep regulasi perlu diturunkan atau dijabarkan dalam aturan-aturan pelaksanaan yang aplikatif dan	Kementerian Kominfo RI belum mengetahui sepenuhnya tentang konsep SKSN 2020-2024 hasil rumusan BSSN. Terlebih dengan masih baru dibentuknya kelembagaan BSSN, maka Kominfo belum mampu memberikan pandangan tentang faktor-faktor yang menghambat strategi pembangunan kompetensi SDM keamanan siber dalam konsep SKSN 2020-2024 rumusan BSSN tersebut sehingga mampu mendukung kepentingan bidang pertahanan untuk mewujudkan kompetensi SDM pertahanan siber.	BSSN baru terbentuk di tahun 2017 berdasarkan Perpes Nomor 53 tahun 2017 tentang BSSN, dan kemudian dikuatkan kembali pada tahun 2018 Perpres Nomor 133 tahun 2017 tentang BSSN. Dengan masih barunya kelembagan tersebut, maka akan mempengaruhi kesiapan aspek-aspek fungsi dasar manajemen dibebankan atau menjadi tanggung jawab BSSN dalam kerangka membangun bidang keamanan siber secara nasional, khususnya dalam hal tata kelola membangun kompetensi SDM

	hingga 2020; e) belum ada pedoman tata kelola (manajemen) SDM pertahanan siber.	komprehensif sesuai kebutuhan di lapangan; c) sejak nota kesepahaman (MoU) antara Satsiber TNI dengan BSSN, sampai saat ini masih belum ada tindak lanjut (*follow up*); d) belum ada pedoman tata kelola SDM pertahanan siber		keamanan siber nasional yang nota bene *output* dan *outcome*-nya juga sangat diperlukan oleh bidang-bidang pemerintahan lain termasuk dalam hal ini bidang pertahanan negara untuk kepentingan terwujudnya kompetensi SDM pertahanan siber. Adapun dengan telah tersusunnya konsep SKSN 2020-2024 hasil rumusan BSSN, maupun yang mana konsep tersebut kemudian disempurnakan kembali sebagai konsep SKSN perbaikan (penyempurnaan konsep SKSN 2020-2024), di mana sampai saat konsep tersebut masih berstatus konsep, dan belum menjadi sebagai suatu bentuk ketentuan atau peraturan nasional. Akibatnya maka SKSN belum menjadi atensi seluruh pemangku kepentingan siber di Indonesia. Sebenarnya hambatan-hambatan tersebut menunjukan adanya urgensi untuk segera terwujudnya SKSN, karena akan selalu menjadi penghambat dalam implementasi akibat belum tersedianya standar-standar dan regulasi-regulasi di bidang keamanan siber yang berakibat pada timbulnya overlaping dan/atau tumpang tindih kepentingan antar instansi.

Wujud praktik-praktik keaamanan siber yang aplikatif (menurut kerangka kerja konsep SKSN Indonesia) guna terwujudnya kemampuan SDM pertahanan siber dalam SISHANNEG				
Dari sudut pandang masing-masing instansi, apa saja bentuk praktik-praktik kegiatan keamanan siber yang aplikatif yang relevan dengan konsep SKSN (khususnya aspek peningkatan kompetensi SDM keamanan siber) yang mendukung upaya terwujudnya kompetensi SDM pertahanan siber	Pushansiber KEMHAN pernah dilibatkan dalam kegiatan praktek yaitu: *Cyber Security Drill Test* yang diselenggaakan oleh BSSN pada tahun 2019. Dalam kegiatan yang pesertanya melibatkan instansi-instansi pemerintah (kementerian dan lembaga serta Pemda) tersebut terdapat praktek-praktek latihan bagaimana respon yang diambil oleh setiap instansi ketika terjadi insiden keamanan siber, termasuk melatih bagaimana prosedur, interoperability dan koordinasi serta teknis format isian dalam melaksanakan pelaporan. Kepada Pusat Operasi Keamanan Siber Nasional (Pusopskamsibernas BSSN sebagai *leading sector*) Menurut perspektif Pushansiber Kemhan, *Output* dan *Outcome* dari kegiatan tersebut belum terlaksana, karena ketika meskipun dalam pelaksanaan monitoring terdapat anomali *cyber security*, mekanisme pelaporan sebagaimaa telah dilatihkan dalam *cybersecurity drill test* tersebut masih belum dipraktekan oleh Pushansiber Kemhan.	Satsiber pernah dilibatkan dalam kegiatan praktek yaitu: *Cyber Security Drill Test* yang diselenggarakan oleh BSSN pada tahun 2018 SDM Satsiber TNI terlibat dalam latihan bersama antara Indonesia dan Thailand (*Cobra Gold Exercise*) dengan materi Operasi Siber Gabungan.	Dalam prespektif Kominfo, praktik-praktik semacam kegiatan operasional maupun pelatihan yang relevan dengan aspek keamanan siber yang mendukung upaya terwujudnya kompetensi SDM pertahanan siber, antara lain melalui kegiatan kompetisi cyber jawara, kegiatan pelatihan intensif Digital Talent Scholarship (DTS) Kominfo dan program beasiswa Government Chief Information Officer (G-CIO). Kegiatan kompetisi Cyber Jawara, adalah kompetisi tahunan di bidang keamanan siber yang sejak awal pertama diinisiasi oleh Id-SIRTII Kominfo sejak tahun 2012 dengan peserta terbuka untuk umum. Materi yang diperlombakan dalam kompetisi tersebut antara lain: computer network defense (yaitu mengatur pengamanan pada server sendiri dan pada saat yang sama berusaha menembus pengamanan pada server lawan), penetration testing (yaitu berusaha menembus keamanan server target yang telah ditentukan untuk mendapatkan data yang dilindungi), dan capture the flag (yaitu problem solving beragam challenge terkait keamanan	BSSN berpandangan bahwa praktik-praktik yang aplikatif tersebut salah satunya adalah kegiatan *cybersecurity drill test* untuk sektor pemerintah. Aspek terkait praktik semacam *cybersecurity drill test* tersebut, adalah relevan dan sebagaimana tercantum di dalam dokumen konsep SKSN perbaikan, pada pilar ke 3 (tiga) yaitu: pembangunan kapasitas dan budaya keamanan siber, bagian ke lima: yaitu membangun budaya keamanan siber, melalui literasi dan kampanye keamanan siber, sehingga terbentuk kesadaran keamanan siber terhadap *quarter helix* (pemerintah, swasta, akademisi, maupun masyarakat umum). Dalam dokumen Roadmap Pembinaan SDM Keamanan Siber dan Sandi 2020-2024 (Menuju SDM Keamanan Siber dan Sandi Yang Terpercaya, Profesional, dan Berdaya Saing), terdapat juga program kegiatan praktik-praktik latihan keamanan siber yang aplikatif dalam kerangka pengembangan kompetensi, antara lain: talent scouting dan pembinaan bidang keamanan siber untuk generasi muda dan mahasiswa dalam bentuk penyelenggaraan kompetisi (capture the flag, cyber war game, cyber jawara),

			siber, untuk mendapatkan poin sebanyak-banyaknya). Program kegiatan Digital Talent Scholarship (DTS) Kominfo yaitu program beasiswa pelatihan intensif yang bertujuan untuk meningkatkan keterampilan dan daya saing SDM bidang TIK sebagai bagian dari program pembangunan prioritas nasional. Program pelatihan dikelompokan sebagai berikut: a) Fresh Graduate Academy (FGA), yaitu program pelatihan berbasis industri bagi lulusan S1 bidang TIK dan MIPA, terbuka bagi penyandang disabilitas; b) Vocational School Graduate Academy (VSGA), yaitu program pelatihan berbasis kompetensi nasional bagi lulusan SMK dan Pendidikan Vokasi bidang TI, Telekomunikasi, Desain, dan Multimedia; c) Coding Teacher Academy (CTA), yaitu program pelatihan pengembangan SDM Guru setingkat SMA/SMK/MA/SMP/SD; d) Online Academy (OA), yaitu program pelatihan online bagi masyarakat umum termasuk ASN, mahasiswa, dan pelaku industri; e) Thematic Academy (TA), yaitu program pelatihan multi disiplin bagi pengembangan SDM; f) Regional Development Academy (RDA), yaitu program pelatihan pengembangan SDM yang ditujukan untuk meningkatkan	cybersecurity job fair, serta kompetisi keamanan siber untuk ASN, TNI, dan Polri.

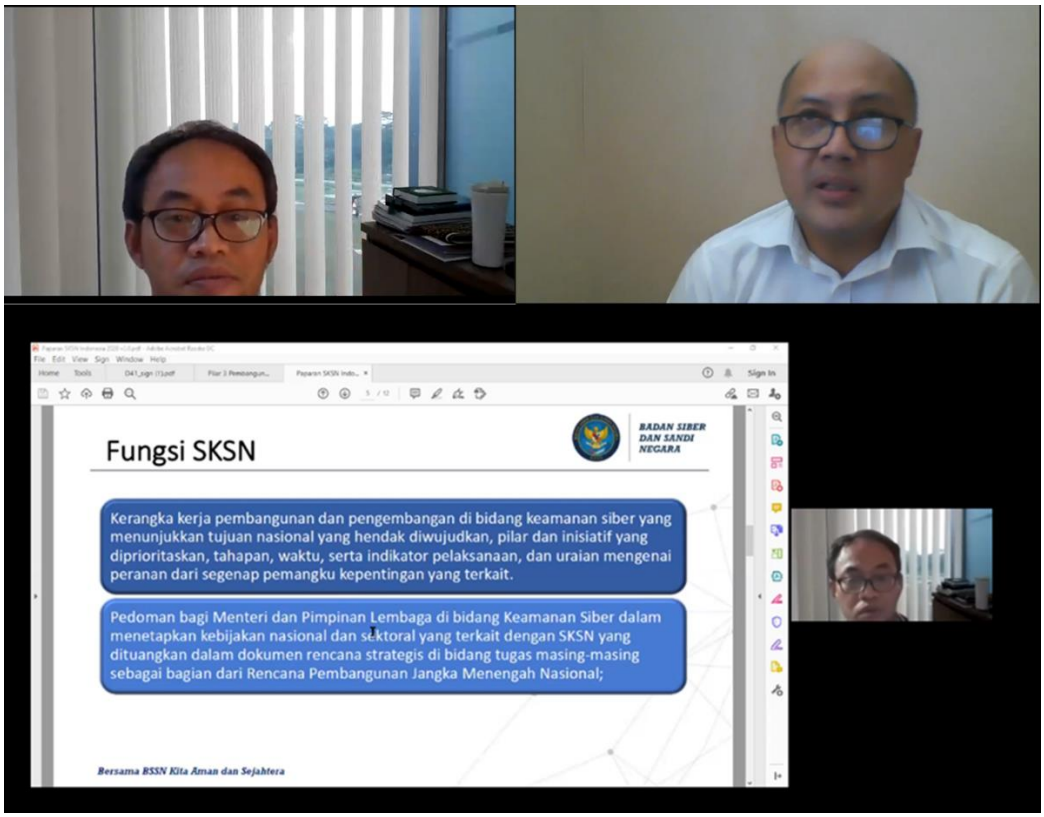
			kompetensi ASN di Kawasan Prioritas Pariwisata dan Kabupaten Prioritas Pembangunan; g) Digital Entrepreneurship Academy (DEA), yaitu program pelatihan pengembangan SDM yang talenta digital di bidang Usaha Mikro, Kecil, dan Menengah (UMKM). Government CIO merupakan kegiatan bersifat bimbingan teknis (bimtek), di mana sasaran bimtek atau Pelatihan G-CIO ini adalah untuk penyiapan pejabat pemerintah yang bertanggungjawab dalam memimpin pengelolaan infrastruktur TI di berbagai lembaga pemerintah dalam pengembangan e-Government, dan membantu penyediaan calon-calon Pejabat Pengelola Informasi dan Dokumentasi (PPID) di seluruh Indonesia, sedangkan untuk program jangka panjangnya, dilaksanakan melalui pemberian beasiswa pendidikan S2 Program Studi CIO di lima perguruan tinggi yaitu : ITB, ITS, UGM, UI dan UNP.	

Lampiran – 7 (Dokumentasi Wawancara)

L-7.1 Dokumentasi Wawancara secara tatap muka dengan staf Satsiber TNI.

L-7.2 Dokumentasi Wawancara secara *online* dengan Kapuslitbang SDPPI Balitbang SDM Kemenkominfo beserta staf (Via Webinar - *Zoom Meeting*).

L-7.3 Dokumentasi Wawancara secara *online* dengan Staf Kedeputian IV BSSN (via Webinar – *zoom meeting*).



RIWAYAT HIDUP PENELITI

Ruby Alamsyah, lahir di Medan pada tanggal 12 Maret 1969. Anak ke-1 dari pasangan Bapak Brigadir Jenderal TNI (Purn) Dr. H. Dedem Ruchlia, Drs., M.Sc., dan Ibu Hj. Susindari. Menyelesaikan pendidikan SD Sugiyono (Bersubsidi) Panca Arga – Magelang, lulus tahun 1982, SMP Negeri 3 Bandung, lulus tahun 1985, SMA Negeri 5 Bandung, lulus tahun 1988, melanjutkan program Magister (S-2) di Universitas Pertahanan.

Peneliti saat ini bekerja/menjabat sebagai Staf Ahli Pang C (Ops) Panglima Koarmada - I TNI AL, mengawali karir tersebut di tahun 2018.

Peneliti masih aktif sebagai Perwira TNI AL. Mengawali karir sebagai Perwira TNI AL pada tahun 1992. Jabatan-jabatan yang pernah diemban antara lain: penugasan di KRI Balikpapan, KRI Pati Unus, KRI Siliman, KRI Sultan Thaha Syaifuddin, dan KRI Barakuda mulai dari Perwira Navigasi Operasi, Perwira Navigasi, Perwira Bahari, dan Palaksa, hingga Jabatan Komandan. Staf Operasi Mabesal, Staf Operasi Gugus Tempur Laut Koarmabar, Staf Operasi Resimen Taruna AAL, Kepala Sub Bidang Sistem Informasi dan TIK Bakorkamla RI, Pranata TIK di Disinfolahtal, Sahli Ops Pushidrosal, dan Sahli Pang C (Ops) Koarmada I.

Berbagai pendidikan militer yang pernah diikuti, yaitu: AKABRI Laut Angkatan XXXVIII (1992), Diklapa I, Diklapa II Artileri, Dikreg Seskoal TP 2007 (Angkatan XVL). Beberapa di luar negeri, yaitu: *Royal Australian Navy* (RAN) *Maritime Security Period* (MSP) 2000 - Australia, *The 3rd International Course for Planner and Executor of Naval Operations International Institute of Humanitarian Law* (IIHL) San Remo – Italy 2003.

Berbagai pengalaman tugas antara lain: Dalam berbagai Satuan Tugas di lingkungan TNI/TNI AL di seluruh Indonesia termasuk tim Satgas Tanggap Darurat Bencana Tsunami Aceh (2005), Tim *Desk Cyberspace* Nasional Kemenkopolhukam RI (2014-2016), Pokja Penyiapan *Cyber* TNI AL (2016-2018), Tim Perumus Doktrin Siber TNI (2018), Tim Perancang dan Penyelenggara Latihan Operasi Pertahanan Siber TNI AL (2016-2018), Tim Kerja Kominfo – Perumusan Legalitas Perlindungan IIKN Nasional (2017-2018), Tim Kerja BSSN – Penyusunan Strategi Keamanan Siber Indonesia (2018), dan Tim Sinergi Media Sosial Aparatur Negara (SIMAN) Kemenko Polhukam RI (2018/2019).

Menikah dengan Rr. Mira M.S.R., S.Psi., M.M. pada tahun 1995 di Bandung dan dikaruniai seorang putri Sheyla Nadya Alamsyah, S.Psi.