LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PENINGKATAN PERTAHANAN SIBER
DALAM RANGKA MENDUKUNG KETAHANAN NASIONAL

Oleh :

Indan Gilang Buldansyah, S.Sos.

Marsekal Pertama TNI

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN SINGKAT ANGKATAN (PPSA) XXIV
LEMBAGA KETAHANAN NASIONAL RI
TAHUN 2023

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

KATA PENGANTAR

Assalamualaikum Wr Wb, salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur kehadirat Tuhan Yang Maha Esa serta atas segala rahmat dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Singkat Angkatan (PPSA) XXIV telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia, sebuah Kertas Karya Ilmiah Perseorangan (Taskap) dengan judul **"*Peningkatan* Pertahanan Siber Dalam Rangka Mendukung Ketahanan Nasional".**

Penentuan Tutor dan Judul Taskap ini didasarkan pada Surat Deputi Pendidikan Pimpinan Tingkat Nasional Lemhannas RI Nomor B/95/V/2023 tanggal 22 Mei 2023 tentang Hasil Rapat Penetapan Judul Taskap Peserta PPSA XXIV Lemhannas RI untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah Penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPSA XXIV di Lemhannas RI tahun 2023. Ucapan yang sama juga disampaikan kepada Pembimbing atau Tutor Taskap kami Bapak Mayjen TNI (Purn) Hari Mulyono, S.E., M.M. dan Tim Penguji Taskap serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari bahwa kualitas Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon adanya masukan guna penyempurnaan naskah ini. Besar harapan kami agar Taskap ini dapat bermanfaat sebagai sumbangan pemikiran penulis kepada Lemhannas RI, termasuk bagi siapa saja yang membutuhkannya.

Semoga Tuhan Yang Maha Esa senantiasa memberikan berkah dan bimbingan kepada kita semua dalam melaksanakan tugas dan pengabdian kepada Negara dan bangsa Indonesia yang kita cintai dan kita banggakan.

Sekian dan terima kasih. Wassalamualaikum Wr. Wb.

Jakarta, Oktober 2023

Penulis

Indan Gilang Buldansyah, S.Sos.
Marsekal Pertama TNI

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini :

   Nama : Indan Gilang Buldansyah, S.Sos.
   Pangkat : Marsekal Pertama TNI
   Jabatan : Staf Khusus KASAU
   Instansi : Markas Besar TNI AU
   Alamat : Mabesau, Cilangkap Jakarta Timur

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPSA) ke XXIV tahun 2023 menyatakan dengan sebenarnya bahwa :

   a. Kertas Karya Ilmiah Perseorangan (Taskap) yang saya tulis adalah asli.
   b. Apabila ternyata sebagian atau seluruhnya tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia dinyatakan tidak lulus pendidikan.

2. Demikian pernyataan keaslian ini dibuat untuk dapat digunakan seperlunya.

Jakarta, Oktober 2023

Penulis

Indan Gilang Buldansyah, S.Sos.
Marsekal Pertama TNI

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PENINGKATAN PERTAHANAN SIBER
DALAM RANGKA MENDUKUNG KETAHANAN NASIONAL

DAFTAR ISI

TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1. Latar Belakang

Perkembangan dunia khususnya sejak awal abad ke-21 telah mengalami perubahan signifikan yang secara khusus hal tersebut diakselerasi dengan penemuan-penemuan di bidang teknologi informasi. Perkembangan teknologi informasi telah membawa perubahan yang signifikan terhadap umat manusia, teknologi informasi menjadikan hubungan atau komunikasi antar manusia semakin mudah tanpa terpengaruh oleh ruang dan waktu. Perubahan tersebut telah membawa dunia masuk ke dalam globalisasi dimana terdapat perubahan dinamika lingkungan global yang ditandai dengan ciri kemajuan teknologi dan informasi, saling ketergantungan antar negara dan pengaburan daripada batas-batas negara (*borderless*).

Perkembangan teknologi telah memberikan dampak yang besar terhadap pertahanan Indonesia. Dalam era digital seperti saat ini, teknologi informasi dan komunikasi telah menjadi aspek penting dalam strategi pertahanan negara. Teknologi tersebut digunakan dalam pengembangan sistem pertahanan siber yang efektif dan mampu melindungi infrastruktur penting dari serangan siber. Selain itu, teknologi juga digunakan dalam pengembangan sistem pertahanan udara, laut, dan darat untuk mengatasi ancaman yang datang dari luar negeri. Dalam perkembangannya, teknologi juga memungkinkan pengembangan senjata dan sistem pertahanan yang lebih canggih dan efektif. Oleh karena itu, penggunaan teknologi yang tepat dapat membantu meningkatkan kemampuan pertahanan negara dalam menghadapi berbagai ancaman yang ada.

Perkembangan siber di Indonesia telah mengalami pertumbuhan yang signifikan dalam beberapa tahun terakhir. Dengan populasi pengguna internet yang terus meningkat, Indonesia menjadi salah satu negara dengan tingkat penetrasi internet yang tinggi di Asia Tenggara. Berdasarkan data *dari We Are Social* 2023, terdapat hampir 216 juta pengguna internet di Indonesia, atau

sekitar 78 persen dari populasi di Indonesia[1]. Dibandingkan dengan tahun lalu, jumlah pengguna tersebut meningkat sebanyak 10 juta orang atau 5,2 persen dari tahun 2022. Tingkat penetrasi internet pada periode tahun 2022-2023 juga mengalami peningkatan 1,17 persen. Kecepatan *mobile Internet* di Indonesia berdasarkan *Ookla* rata-rata 17,27 Mbps, meningkat sebesar 9,24 persen dibandingkan tahun 2022. Sedangkan *fix internet* sebesar 24,32 Mbps, meningkat 20,8 persen dibandingkan tahun 2022. Selanjutnya, sebanyak 353,8 juta koneksi seluler aktif di Indonesia, atau 128 persen dari total populasi di Indonesia yang berjumlah 276,4 juta orang. Dari data tersebut dapat terlihat juga bahwa terdapat 64 juta orang di Indonesia yang belum tersentuh oleh internet.

Peningkatan jumlah pengguna internet di era digital saat ini tidak bisa dilepaskan dari kuantitas peningkatan serangan siber. Pada dokumen laporan tahun 2022, Badan Siber dan Sandi Negara (BSSN) menyebutkan prediksi ancaman siber pada tahun 2023 antara lain *ransomware*, data breach, serangan APT, *phishing*, *crypto jacking*, *distributed denial of service attack, serangan remote desktop protocol, social engineering, web defacement*, *artificial intelligence (AI)* dan *internet of things (IoT) cybercrime*[2]. Laporan tersebut diperkuat dengan pernyataan Fortinet bahwa pada tahun 2023 ini serangan siber akan semakin canggih, hal ini dapat terjadi pada semua pihak bahkan yang tidak memiliki kemampuan teknis dapat melakukan serangan[3].

Peningkatan aktivitas siber di Indonesia mengacu pada pertumbuhan dan perkembangan aktivitas yang terkait dengan dunia maya, termasuk komunikasi, ekonomi, dan keamanan di ranah siber. Beberapa faktor yang telah berkontribusi terhadap peningkatan kegiatan siber di Indonesia antara lain meningkatkan akses internet, pertumbuhan *e-commerce*, dan penetrasi *smartphone*. *E-commerce* atau perdagangan elektronik telah mengalami pertumbuhan pesat di Indonesia. *Platform e-commerce* seperti Tokopedia, Shopee, dan Bukalapak telah mendapatkan popularitas yang besar. Namun,

[1] Kemp, Simon. 2023. Digital 2023: Indonesia. https://datareportal.com/reports/digital-2023-indonesia. Diunduh tanggal 12 Juni 2023.
[2] https://bssn.go.id/annualreport2022/ Diunduh tanggal 10 Juni 2023 pukul 10:14 WIB
[3] https://swa.co.id/swa/trends/technology/waspada-tren-serangan-siber-di-2023-lebih-mutakhir Diunduh tanggal 10 Juni 2023 pukul 10:23 WIB

peningkatan kegiatan siber juga memiliki beberapa tantangan, termasuk ancaman keamanan siber seperti serangan siber, penipuan *online*, pencurian data, dan penyebaran konten ilegal. Serangan siber merujuk pada upaya yang dilakukan oleh pihak yang tidak berwenang untuk mengakses, merusak, mengganggu, atau menghancurkan sistem komputer, jaringan, atau infrastruktur digital[4]. Serangan siber dapat berupa serangan *malware*, serangan DDoS (*Distributed Denial of Service*), serangan *phishing*, *ransomware*, dan lain sebagainya. Tujuan serangan siber bisa beragam, mulai dari pencurian data pribadi, merusak reputasi, hingga mencuri informasi rahasia atau merusak operasional suatu organisasi atau negara. Sedangkan penipuan *online* adalah praktik yang melibatkan penggunaan internet dan teknologi digital untuk memperoleh informasi pribadi atau keuangan dari orang lain secara curang. Contoh penipuan *online* termasuk penipuan melalui *email* (*phishing*), penipuan investasi palsu, penjualan barang palsu atau tidak ada, penipuan kartu kredit, dan penipuan cinta *online*. Selanjutnya, penipuan online sering kali bertujuan untuk mendapatkan keuntungan finansial atau informasi pribadi yang bisa disalahgunakan. Pencurian data terjadi ketika pihak yang tidak berwenang berhasil mengakses dan mendapatkan informasi yang sensitif atau rahasia dari sistem komputer, jaringan, atau perangkat digital. Data yang dicuri dapat berupa data pribadi (seperti nama, alamat, nomor kartu kredit), informasi bisnis, informasi keuangan, atau bahkan rahasia perdagangan atau rancangan teknologi. Pencurian data sering kali dilakukan oleh peretas (*hacker*) yang ingin memperoleh keuntungan finansial atau digunakan untuk melakukan tindakan kriminal lainnya. Sedangkan penyebaran konten ilegal merujuk pada tindakan menyebarkan atau membagikan materi atau konten yang melanggar hukum atau norma yang berlaku. Ini dapat mencakup konten yang melibatkan kekerasan, pornografi anak, diskriminasi rasial, pencemaran nama baik, atau materi yang melanggar hak cipta. Penyebaran konten ilegal dapat terjadi melalui internet, media sosial, *platform file sharing*, atau melalui pesan elektronik. Penyebaran konten

[4] Farizy, Salman. 2020. *Keamanan Sistem Informasi*. Jakarta: Unpam Press.

ilegal dapat dikenakan sanksi hukum dan memiliki konsekuensi serius terhadap individu atau organisasi yang terlibat.

Ancaman-ancaman siber tersebut dapat memengaruhi berbagai sektor seperti pemerintahan, militer, ekonomi, infrastruktur kritis, dan lain sebagainya. Infrastruktur kritis merujuk pada sekelompok sistem fisik, jaringan, dan aset yang sangat penting bagi kelangsungan hidup, keamanan, dan keberlanjutan suatu negara atau masyarakat (Lebo, 2020). Infrastruktur kritis mencakup sektor-sektor yang vital dan strategis dalam ekonomi, pertahanan, keamanan, kesehatan, transportasi, energi, telekomunikasi, air, dan lain-lain.

Karakteristik dari infrastruktur kritis adalah bahwa kegagalan, gangguan, atau kerusakan pada infrastruktur ini dapat memiliki dampak yang serius dan luas terhadap kehidupan masyarakat, kegiatan ekonomi, dan fungsi-fungsi penting lainnya. Kerusakan atau kegagalan dalam infrastruktur kritis dapat menyebabkan gangguan pada pelayanan publik, kehilangan nyawa, kerugian ekonomi, dan ketidakstabilan sosial. Keamanan infrastruktur kritis menjadi sangat penting, karena serangan atau gangguan pada infrastruktur ini dapat memiliki konsekuensi serius. Oleh karena itu, perlindungan dan pengamanan infrastruktur kritis melibatkan upaya pencegahan, deteksi, perlindungan, dan tanggap darurat untuk melawan ancaman siber, serangan teroris, bencana alam, atau kejadian lain yang dapat mengancam keberlanjutan infrastruktur tersebut.

Kementerian dan Lembaga di Indonesia tidak terlepas dari serangan siber. Berdasarkan data yang didapatkan dari laporan Badan Intelijen Negara (BIN) di mana BIN melalui Deputi-VI bidang Intelijen Siber telah menempatkan perangkat sensor untuk mendeteksi serangan siber di Kementerian dan Lembaga. Khususnya pada periode semester I tahun 2023, jumlah serangan siber yang terjadi sebanyak 121.196.623 serangan. Selama periode enam bulan pertama tahun 2023, serangan siber tertinggi terjadi pada bulan Maret sebanyak 24.726.465 serangan, kemudian pada bulan April mengalami penurunan. Pada bulan Mei 2023 serangan siber kembali mengalami peningkatan karena pelaksanaan KTT ASEAN di Labuan Bajo. Sedangkan pada bulan Juni 2023, tren serangan siber Kembali menurun dengan jumlah

14.440.709 serangan. Jenis serangan siber yang terjadi di kementerian dan lembaga di Indonesia antara lain eksploitasi kerentanan sistem keamanan siber dan serangan *malware.* Berkaitan dengan data-data sensitif yang berada di kementerian dan lembaga juga rentan mengalami kebocoran karena aktivitas serangan siber, seperti bocornya 337 juta data Penduduk dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri pada bulan Juli 2023 lalu yang diduga berasal dari *server* dukcapil.kemendagri.go.id.

Berdasarkan uraian di atas, masifnya serangan siber bersifat destruktif hampir di semua aspek kehidupan sehingga berdampak pada menurunnya ketangguhan ketahanan nasional. Oleh karena itu kemampuan pertahanan siber di Indonesia yang menjadi fokus pembahasan adalah dilihat dari aspek sumber daya manusia (SDM), teknologi, serta kebijakan dan regulasi. Dalam hal ini dibutuhkan strategi pertahanan siber yang mampu mencegah, mengatasi, dan merespon serangan siber dengan cepat dan tepat. Salah satu strategi yang dapat dilakukan adalah pertahanan siber mendalam. Pertahanan siber mendalam (*defense in depth*) adalah pendekatan strategis dalam keamanan siber yang melibatkan penggunaan berbagai lapisan pertahanan untuk melindungi sistem komputer dan jaringan dari ancaman dan serangan siber (Krisnata, 2022). Konsep ini didasarkan pada prinsip bahwa tidak ada satu tindakan atau teknologi yang dapat memberikan keamanan yang sempurna, sehingga diperlukan kombinasi langkah-langkah pertahanan yang berlapis-lapis. Diharapkan melalui peningkatan pertahanan siber nasional dapat memberikan kontribusi yang signifikan terhadap ketahanan nasional dalam era digital saat ini melalui langkah-langkah yang tepat dalam melindungi infrastruktur, informasi sensitif, ekonomi, dan masyarakat, negara dapat menghadapi tantangan ancaman siber dengan lebih baik, menjaga stabilitas nasional, dan melindungi kepentingan nasional secara keseluruhan. Pertahanan siber yang kuat dan mampu mencegah serta mengatasi segala bentuk ancaman dan serangan siber, pada akhirnya dapat mendukung ketangguhan ketahanan nasional. Oleh karena itu maka penulis mengajukan Kertas Karya Ilmiah Perseorangan (Taskap) yang berjudul **Peningkatan Pertahanan Siber Dalam Rangka Mendukung Ketahanan Nasional**.

2. Rumusan Masalah

Berdasarkan latar belakang serta fakta kondisi yang terjadi, maka rumusan masalah yang akan dibahas dalam Taskap ini adalah ***Bagaimana peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional?***

Untuk menjawab dan menemukan solusi atas permasalahan yang telah dijelaskan pada Rumusan Masalah, maka pertanyaan kajian yang akan dibahas dalam Taskap ini antara lain sebagai berikut:

a. Bagaimana kondisi kemampuan pertahanan siber pada Kementerian dan Lembaga dilihat dari aspek teknologi, sumber daya manusia (SDM) dan regulasi?
b. Apa saja dampak yang disebabkan oleh serangan siber di Kementerian dan Lembaga?
c. Bagaimana strategi dan upaya untuk meningkatkan pertahanan siber pada Kementerian dan Lembaga dalam rangka mendukung ketahanan nasional?

3. Maksud dan Tujuan

a. Maksud

Maksud dari penulisan Taskap ini untuk menggambarkan dan menganalisis permasalahan pertahanan siber saat ini serta memecahkan permasalahan yang terjadi untuk meningkatkan pertahanan siber khususnya pada Kementerian dan Lembaga dalam rangka mendukung ketahanan nasional.

b. Tujuan.

Adapun tujuan penulisan Taskap ini adalah sebagai sumbangan pemikiran dan rekomendasi kepada pemangku kebijakan untuk memecahkan permasalahan yang terkait dengan peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional.

4. Ruang Lingkup dan Sistematika

a. Ruang Lingkup.

Ruang lingkup taskap ini meliputi kondisi kemampuan pertahanan siber serta strategi dan upaya dalam meningkatkan pertahanan siber nasional dalam rangka mendukung ketahanan nasional. Penulisan Taskap ini dibatasi pada peningkatan pertahanan siber di Kementerian dan Lembaga Pemerintah.

b. Sistematika.

Sistematika penulisan Taskap ini disusun secara seksama guna menghasilkan kajian yang jelas dan terlihat sebagai suatu kesatuan yang koheren. Adapun tata urutannya adalah sebagai berikut:

Bab I Pendahuluan. Bab pertama akan dijelaskan tentang latar belakang pokok permasalahan yang dibahas yaitu perlunya peningkatan pertahanan siber nasional dalam rangka mewujudkan ketahanan nasional, perumusan masalah, maksud serta tujuan penulisan, ruang lingkup pembahasan dan tata tulis /sistematika dalam penulisan, metode serta pendekatan yang akan digunakan, dan beberapa pengertian yang digunakan dalam penulisan Taskap untuk menyamakan persepsi guna memahami pembahasan berdasarkan berbagai sumber yang jelas dan dapat dipertanggungjawabkan.

Bab II Landasan Pemikiran. Bab kedua Taskap ini menguraikan tentang Landasan Pemikiran yang digunakan untuk keperluan pembahasan pada bab-bab selanjutnya, meliputi peraturan perundang-undangan, data dan fakta kondisi saat ini yang berhubungan erat dengan pembahasan, kerangka teoretis berupa teori-teori yang digunakan sebagai pisau analisis, serta faktor-faktor perkembangan lingkungan strategis baik global, regional, maupun nasional yang berpengaruh terhadap peningkatan pertahanan siber sehingga dapat mendukung ketahanan nasional.

Bab III Pembahasan. Pada bab ini akan diuraikan analisis setiap pokok-pokok bahasan dengan menggunakan bahasan yang telah diuraikan pada bab Landasan Pemikiran. Pokok-pokok kajian yang dibahas antara lain kondisi kemampuan pertahanan siber dilihat dari aspek SDM, aspek teknologi, serta regulasi yang ada, dampak serangan siber di Kementerian dan Lembaga dianalisis dengan metode PESTLE, serta strategi dan upaya untuk meningkatkan pertahanan siber dalam rangka mendukung ketahanan nasional.

Bab IV Penutup. Pada bagian terakhir diuraikan simpulan yang diperoleh dari seluruh pembahasan dengan solusi untuk masing-masing pokok pembahasan. Kemudian juga dikemukakan rekomendasi yang berisikan saran masukan pada pembahasan Taskap ini.

5. Metode dan Pendekatan

a. Metode Analisis

Metode penulisan taskap ini menggunakan metode kualitatif-deskriptif analitis yang menekankan pada pengumpulan data sekunder berupa kajian pustaka, studi dokumen dari data, dengan metodologi pembahasan menggunakan Analisis PESTLE yaitu analisis pada aspek *Political* (Politik), *Economy* (Ekonomi), *Social* (Sosial), *Technological* (Teknologi), *Legal* (Hukum), *Environment* (Lingkungan)[5].

b. Pendekatan

Penulisan Taskap menggunakan pendekatan dengan perspektif kepentingan nasional melalui analisis multidisiplin ilmu yang selaras dengan kerangka teoretis yang akan dipergunakan dalam pembahasan. Pedekatan yang dimaksud adalah adanya korelasi antara pertahanan siber nasional yang outputnya adalah kemampuan pertahanan siber

[5] Tanya Sammut-Bonnici and David Galea. 2015. *PEST Analysis.* Wiley Encyclopedia of Management, edited by Professor Sir Cary L Cooper.

yang mendalam, dan kepentingan nasional yakni terwujudnya ketahanan nasional.

6. Pengertian

Berikut adalah daftar pengertian kata dan istilah yang digunakan dalam Kertas Karya Ilmiah Perseorangan ini:

a. **Peningkatan**. Menurut KBBI kata "peningkatan" berasal dari kata dasar "tingkat". Peningkatan dapat menyatakan suatu proses atau cara, maupun tindakan untuk meningkatkan (dalam hal usaha, aktivitas, dan lain sebagainya)[6].

b. **Siber**. Istilah siber dalam bahasa Indonesia berasal dari bahasa Inggris *Cyber* yang merupakan kata singkatan dari *cybernetics* yaitu ilmu komunikasi dan sistem kontrol otomatis pada mesin dan makhluk hidup (sibernetika). Sedangkan secara etimologi *cybernetics* berasal dari bahasa Yunani "*kybernēt"* yang berarti "terampil dalam mengatur atau memerintah". Siber adalah sesuatu yang berhubungan dengan sistem komputer dan informasi. Dalam perkembangannya, siber dapat diartikan yang berhubungan dengan internet. Istilah Siber dapat berhubungan dengan semua aspek komputasi, termasuk menyimpan data, melindungi data, mengakses data, memproses data, mentransmisikan data dan menghubungkan data[7].

c. **Pertahanan Siber**. Pertahanan siber (*cyber defense*) berdasarkan Permenhan RI Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara. Urgensi pertahanan siber ditujukan untuk mengantisipasi datangnya ancaman ancaman dan serangan siber yang terjadi dan menjelaskan posisi ketahanan saat ini, sehingga diperlukan kesiapan dan ketanggapan dalam menghadapi ancaman serta memiliki

[6] https://kbbi.web.id/tingkat Diunduh tgl 10 Juni 2023 pukul 13:46 WIB
[7] https://www.kanalinfo.web.id/pengertian-siber-cyber Diunduh tgl 27 September 2023 pukul 13:07 WIB

kemampuan untuk memulihkan akibat dampak serangan yang terjadi di ranah siber.

d. **Ketahanan Nasional**. Ketahanan Nasional (Tannas) didefinisikan sebagai kondisi dinamis bagi bangsa Indonesia yang mencakup seluruh aspek kehidupan bangsa dalam delapan gatra yang saling terintegrasi, berisi keuletan dan ketangguhan dalam mengembangkan suatu kekuatan nasional, untuk mengatasi dan menghadapi segala bentuk ancaman, gangguan, hambatan dan tantangan (AGHT) yang berasal dari dalam dan dari luar, dalam rangka menjamin integritas, kelangsungan hidup, identitas bangsa dan negara, serta perjuangan bangsa dalam mewujudkan tujuan nasionalnya[8].

e. **Pertahanan Siber Mendalam**. Pertahanan Siber Mendalam adalah sebuah strategi pertahanan yang melibatkan penggunaan berbagai lapisan pertahanan dalam sistem komputer dan jaringan untuk melindungi aset digital dari serangan dan ancaman siber[9].

f. **Teknologi.** Secara etimologis, kata Teknologi bersumber dari bahasa Yunani, yaitu *techne* yang memiliki arti seni, keterampilan, kerajinan, dan *logia* yang memiliki arti studi ilmu pengetahuan. Secara terminologi, teknologi diartikan sebagai pengetahuan untuk menjadikan sesuatu[10]. Teknologi sebagai metode, sarana dan proses dalam menerapkan dan memanfaatkan beberapa disiplin Ilmu Pengetahuan yang memiliki manfaat lebih lanjut baik pada kelangsungan hidup, pemenuhan kebutuhan, maupun untuk meningkatkan kualitas kehidupan manusia[11].

g. **Infrastruktur Kritis**. Infrastruktur kritis merujuk pada sistem dan aset fisik yang sangat penting untuk operasional suatu negara atau masyarakat. Infrastruktur ini mencakup sektor-sektor yang vital dalam ekonomi, keamanan, pertahanan, kesehatan, transportasi, energi,

---

[8] Tim Pokja Geostrategi Indonesia dan Ketahanan Nasional. 2023. *Bidang Studi Geostrategi Indonesia dan Ketahanan Nasional*. Jakarta: Lemhannas RI

[9] https://aws.amazon.com/id/what-is/cybersecurity/ Diunduh tgl 10 Juni 2022 pukul 13:51 WIB

[10] Muhammad Yaumi. 2018. *Media Dan Teknologi Pembelajaran*, Cetakan Pertama. Jakarta: Prenadamedia Group

[11] UU RI Nomor 11 Tahun 2019 tentang Sistem Nasional Ilmu Pengetahuan Dan Teknologi Pasal 1 Angka 3

telekomunikasi, air, dan lain-lain[12]. Kerusakan, gangguan, atau kegagalan dalam infrastruktur kritis dapat memiliki dampak serius pada kehidupan masyarakat, perekonomian, dan fungsi penting lainnya.

h. **Kerahasiaan (*Confidentiality*)**. Kerahasiaan mengacu pada perlindungan informasi dari akses yang tidak sah atau tidak diotorisasi[13]. Tujuan kerahasiaan adalah memastikan bahwa informasi hanya dapat diakses oleh orang-orang yang memiliki hak atau izin untuk melakukannya. Untuk mencapai kerahasiaan, langkah-langkah seperti enkripsi data, pengaturan akses yang ketat, dan penggunaan mekanisme otentikasi digunakan untuk melindungi informasi dari ancaman pengungkapan yang tidak sah.

i. **Integritas (*Integrity*)**. Integritas berkaitan dengan keutuhan dan keandalan informasi. Integritas menjamin bahwa informasi tetap utuh, tidak dimanipulasi, dan tidak mengalami perubahan yang tidak sah[14]. Perlindungan integritas melibatkan langkah-langkah seperti penggunaan tanda tangan digital, *hash functions*, dan kontrol akses yang ketat untuk memastikan bahwa informasi tidak diubah oleh pihak yang tidak berwenang.

j. **Ketersediaan (*Availability*)**. Ketersediaan berfokus pada memastikan bahwa informasi dan sistem yang mengelolanya dapat diakses dan digunakan oleh pihak yang berwenang ketika diperlukan[15]. Ketersediaan melibatkan langkah-langkah untuk mencegah atau mengatasi gangguan atau serangan yang dapat mengganggu aksesibilitas informasi, seperti kegagalan perangkat keras, serangan DDoS (*Distributed Denial of Service*), atau bencana alam. Upaya dilakukan untuk memastikan bahwa sistem dan data dapat diakses dan beroperasi dengan optimal.

[12] https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf Diunduh tgl 10 Juni 2022 pukul 13:57 WIB
[13] https://jdih.kemenkeu.go.id/fulltext/2010/479~KMK.01~2010KepLamp.pdf Diunduh tgl 10 Juni 2022 pukul 14:02 WIB
[14] Ibid
[15] Ibid

k. **Kementerian dan Lembaga**. Kementerian merupakan lembaga eksekutif dalam pemerintahan Indonesia yang membidangi urusan tertentu, memiliki tugas, fungsi, dan susunan organisasi yang diatur oleh Peraturan Presiden (Perpres). Pembentukan dan pengubahannya dilakukan oleh Presiden. Jumlah kementerian maksimum sesuai aturan dalam UU RI Nomor 39 Tahun 2008 adalah 34 kementerian[16].

Lembaga merupakan organisasi pemerintah yang memiliki tugas dan fungsi yang lebih spesifik serta tidak berada di bawah dan bertanggung jawab kepada Presiden. Lembaga dapat dibentuk dengan berbagai jenis peraturan perundang-undangan, baik Undang-Undang, Peraturan Pemerintah (PP), Perpres, maupun Keputusan Presiden (Kepres)[17].

Badan Usaha Milik Negara (BUMN) adalah badan usaha yang seluruh atau sebagian besar modalnya dimiliki oleh negara melalui penyertaan secara langsung untuk mensejahterakan masyarakat Indonesia. BUMN dioperasikan dan dikendalikan oleh pemerintah secara penuh. Dalam hal ini pemerintah memiliki kekuasaan dalam pengambilan keputusan strategis dan pengawasan terhadap BUMN. BUMN memiliki badan hukum dan bertujuan untuk mewujudkan kesejahteraan masyarakat umum, memberikan tambahan pendapatan bagi negara, serta menjadi salah satu pelaku pada kegiatan perekonomian nasional. Kebanyakan dari BUMN yang ada di Indonesia bergerak di bidang pelayanan publik[18]. Dalam tulisan ini, Badan Usaha Milik Negara (BUMN) adalah bagian dari Kementerian.

[16] https://www.gramedia.com/literasi/kementerian-negara-indonesia/ Diunduh tgl 10 Juni 2022 pukul 14:12 WIB
[17] https://www.setneg.go.id/baca/index/klasifikasi_dan_puu_lns Diunduh tgl 10 Juni 2022 pukul 14:15 WIB
[18] https://bisnis.tempo.co/read/1683911/pengertian-bumn-ciri-ciri-jenis-tugas-dan-tujuannya Diunduh tgl 10 Juni 2022 pukul 14:20 WIB

BAB II
LANDASAN PEMIKIRAN

7. Umum.

Pada bab pertama telah dilakukan pembahasan tentang peningkatan aktivitas siber di Indonesia yang mayoritas membawa dampak negatif, sehingga dibutuhkan strategi pertahanan siber yang mampu mencegah, mengatasi, dan merespon serangan siber dengan cepat dan tepat. Strategi pertahanan tersebut adalah pertahanan siber yang didasarkan pada prinsip bahwa tidak ada satu tindakan atau teknologi yang dapat memberikan keamanan yang sempurna, sehingga diperlukan kombinasi langkah-langkah pertahanan yang berlapis-lapis.

Selanjutnya pada bab landasan pemikiran ini akan disampaikan beberapa dokumen atau pustaka yang dapat digunakan sebagai landasan pembahasan dan analisis permasalahan terkait peningkatan pertahanan siber nasional dalam rangka mewujudkan ketahanan nasional berupa peraturan perundangan yang berlaku dan relevan dengan pembahasan. Kemudian kerangka teoretis yang meliputi beberapa teori dan konsepsi yang digunakan sebagai pisau analisis dalam menemukan pemecahan masalah. Selain itu, juga akan dijelaskan beberapa data dan fakta aktual terkait kondisi pertahanan siber serta pengaruh perkembangan lingkungan strategis baik global, regional maupun nasional, sehingga diharapkan dengan landasan berpikir ini akan diperoleh suatu pemecahan masalah yang terukur dan komprehensif.

8. Peraturan perundang-undangan.

Regulasi atau peraturan perundang-undangan sangat dibutuhkan sebagai payung hukum dalam segala bentuk aktivitas yang mendukung terwujudnya upaya meningkatkan pertahanan siber sehingga dapat mendukung ketahanan nasional. Beberapa peraturan perundang-undangan yang digunakan dalam analisis dan pembahasan sebagai berikut:

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

Pasal 1 menjelaskan bahwa Sistem Pertahanan Negara merupakan sistem yang terdiri dari keterlibatan semua komponen bangsa, kewilayahan, dan sumber daya nasional lainnya. Sistem ini disiapkan oleh pemerintah secara dini dan dijalankan dengan totalitas, integrasi, arahan, dan berkelanjutan untuk memastikan kedaulatan negara, integritas wilayah, dan keamanan seluruh bangsa dari segala bentuk ancaman. Pasal 20 ayat 5 menyatakan bahwa semua aset nasional, termasuk sumber daya manusia (SDM), sumber daya alam serta buatan, nilai/norma, teknologi, dan pendanaan, dapat diberdayakan guna meningkatkan kapabilitas pertahanan negara.

Pada bagian penjelasan Pasal demi Pasal, penjelasan Pasal 12 menyebutkan bahwa kepentingan nasional merupakan kondisi utuhnya NKRI sesuai Pancasila dan UUD NRI 1945, serta adanya jaminan terhadap kelancaran pelaksanaan dan keamanan terhadap jalannya keberlanjutan pembangunan nasional guna mencapai tujuan nasional. Kepentingan nasional tersebut dapat direalisasikan dengan mempertimbangkan tiga aturan pokok antara lain berkaitan dengan tata kehidupan nasional sesuai Pancasila dan UUD NRI 1945, tercapainya tujuan nasional dan tangguhnya ketahanan nasional berdasarkan wawasan nusantara, serta keterpaduan dalam pendayagunaan seluruh potensi dan kekuatan nasional. Pasal 12 berimplikasi bahwa fungsi pemerintahan negara diantaranya menjaga kepentingan nasional dan memberikan dukungan pada kebijakan pertahanan, yaitu dalam program Keamanan Siber Nasional melalui *Cyberdefense* dengan membangun dan membina kemampuan serta daya tangkal terhadap ancaman terhadap kedaulatan dan keutuhan wilayah NKRI.

b. **Undang-Undang RI nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam Undang-Undang RI nomor 19 Tahun 2016 tentang Perubahan Atas**

Undang-Undang RI nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Pada Bab II Pasal 3 dinyatakan bahwa Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilakukan dengan tetap menaati prinsip-prinsip kejelasan hukum, mengedepankan asas manfaat, berhati-hati dalam segala bentuk aktivitas, dilakukan dengan itikad baik, serta memberikan kebebasan kepada masing-masing individu untuk memilih teknologi atau tetap bersikap netral terhadap teknologi yang digunakan. UU ITE secara langsung berhubungan dengan pertahanan siber karena memberikan dasar hukum bagi pemerintah dan aparat penegak hukum untuk menangani segala bentuk kejahatan yang terjadi di dunia maya. Dalam konteks pertahanan siber, UU ITE digunakan untuk memerangi serangan siber, melindungi infrastruktur teknologi informasi serta kepentingan nasional.

c. **Undang-Undang RI Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP)**.

UU PDP memiliki peran penting dalam melindungi hak privasi dan data pribadi warga negara dalam penggunaan teknologi informasi. UU ini mengatur regulasi dan pengawasan terhadap pengumpulan, pengolahan, penyimpanan, dan penggunaan data pribadi oleh entitas publik maupun swasta. Pada Pasal 1 angka 2 UU PDP, yang dimaksud dengan Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.

UU PDP penting untuk menciptakan kepercayaan dalam perekonomian digital, memastikan privasi dan perlindungan data pribadi, meningkatkan kepercayaan konsumen, memberikan kerangka kerja untuk pengelolaan data pelanggan dan pengguna, mendorong responsibilitas perusahaan dalam mengelola data secara etis, serta memfasilitasi pertumbuhan dan inovasi dalam ekosistem

bisnis digital. Pada Pasal 58 Ayat (1) disebutkan bahwa Pemerintah berperan dalam penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang. Sedangkan ketentuan pidana sebagai sanksi pidana dan denda terhadap pelanggaran hukum terkait Data Pribadi, dijelaskan pada Pasal 67 dan 68.

d. **Peraturan Presiden RI Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN)**

Perpres ini merupakan peraturan yang mengatur pembentukan dan fungsi BSSN sebagai lembaga yang bertanggung jawab dalam mengoordinasikan kebijakan, program, dan kegiatan dalam bidang keamanan siber dan sandi negara di Indonesia. Dalam konteks perekonomian, BSSN memiliki beberapa fungsi terkait dengan keamanan siber salah satunya adalah melakukan Pencegahan dan Penanggulangan Serangan Siber. BSSN berperan dalam melakukan pencegahan dan penanggulangan serangan siber. BSSN bekerja sama dengan berbagai pihak terkait, termasuk sektor swasta, untuk mengidentifikasi, mengatasi, dan merespons serangan siber.

e. **Peraturan Presiden RI Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital**.

Dalam Perpres ini, semua penyelenggara Infrastruktur Informasi Vital (IIV) diharuskan untuk menjaga kelangsungan infrastruktur informasi vital, mencegah kerusakan, gangguan, dan/atau kehancuran yang diakibatkan oleh serangan siber, meningkatkan kesiapan menghadapi kejadian siber, dan mempercepat upaya pemulihan setelah terjadi serangan siber[19]. Perlindungan IIV yang diterapkan mencakup identifikasi sektor IIV, pelaksanaan perlindungan IIV, pembinaan dan pengawasan perlindungan IIV, serta koordinasi dalam menjalankan perlindungan IIV.

[19] Perpres RI Nomor 82 tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital

f. **Peraturan Presiden RI Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber**.

Pasal 3 Perpres ini menyatakan bahwa “Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber merupakan acuan bagi instansi penyelenggara negara dan pemangku kepentingan untuk mewujudkan kekuatan dan kapabilitas siber dalam rangka mencapai stabilitas keamanan siber”. Sedangkan tujuan yang ingin dicapai diantaranya dijelaskan pada Pasal 4 huruf c yaitu “meningkatkan kekuatan dan kapabilitas keamanan siber yang andal dan berdaya tangkal”.

Pada Pasal 7 huruf a terkait fokus area Strategi Keamanan Siber Nasional diantaranya melalui tata kelola yang meliputi penguatan ekosistem Keamanan Siber termasuk di dalamnya sumber daya manusia (SDM), proses, dan teknologi.

g. **Peraturan Menteri Pertahanan RI Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber**.

Permenhan ini bertujuan untuk memberikan pedoman yang jelas dan terarah dalam melindungi sistem pertahanan siber di Indonesia. Dengan adanya regulasi ini, maka diharapkan dapat meningkatkan kemampuan dan kesiapan pertahanan siber negara serta kemampuan dalam melindungi kepentingan nasional pada bidang pertahanan siber.

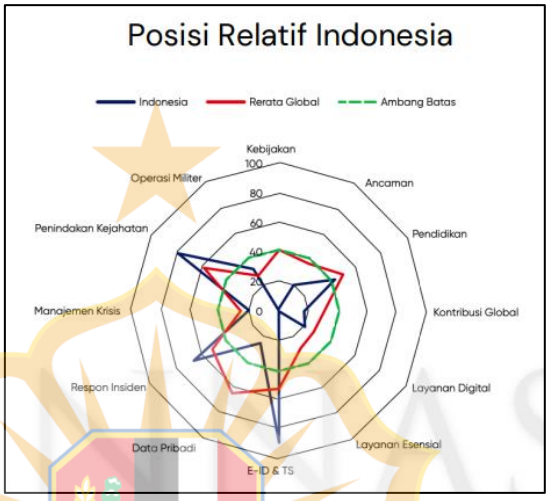
9. Data dan Fakta.

Data dan fakta berikut merupakan gambaran kondisi pertahanan dan keamanan siber di Indonesia yang dapat dijadikan sebagai bahan analisis peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional. Berikut beberapa data dan fakta yang dapat dihimpun:

a. Indeks Keamanan Siber Nasional

Pada tahun 2022 lalu, merujuk pada laporan *National Cyber Security Index* (NCSI) menyatakan bahwa keamanan siber Indonesia

menduduki peringkat 6 dari 10 negara di kawasan ASEAN, dan secara global menempati peringkat 83 dari 160 negara. Nilai keamanan siber sebagai hasil riset NCSI sebesar 38,96 dari skala 100 di mana nilai ini dalam kategori **kurang baik** dan berada di bawah nilai rata-rata secara global (lihat Gambar 1).



Gambar 1. Indeks Keamanan Siber Indonesia Tahun 2022
Sumber: *E-Governance Academy*, 2022

Indonesia memiliki skor di bawah rerata global pada delapan indikator kapasitas keamanan siber, antara lain Kebijakan keamanan siber, risiko ancaman, pendidikan, kontribusi secara global, layanan esensial, layanan digital, keamanan data pribadi, dan kemampuan dalam manajemen krisis (lihat Tabel 1).

Tabel I. Nilai Indikator Kapasitas Keamanan Siber Indonesia Tahun 2022
Sumber: *E-Governance Academy*, 2022

No	Kapasitas	Indonesia	Rerata Global
1	Kebijakan	0	40
2	Ancaman	20	38
3	Pendidikan	44	50
4	Kontribusi Global	17	30
5	Layanan Digital	20	27
6	Layanan Esensial	0	29
7	E-ID & TS	89	52
8	Data Pribadi	25	64
9	Respons Insiden	67	51
10	Manajemen Krisis	20	25
11	Penindakan Kejahatan	78	59
12	Operasi Militer	33	27

> Rerata Global < Rerata Global

b. Indeks Inovasi Global Indonesia

Terhadap indeks inovasi global, Indonesia menempati peringkat ke 87 dari 132 negara dengan nilai indeks 55,3. Hasil penilaian ini menunjukkan bahwa Indonesia belum mampu menunjang dan memproduksi aktivitas atau produk inovatif. Terdapat enam variabel dari Indonesia yang harus diperbaiki (lihat Tabel 2).

Tabel II. Nilai Variabel Indeks Inovasi Indonesia Tahun 2022
Sumber: WIPO *Global Innovation Index*, 2022

No	Variabel	Indonesia	Rata-Rata Global
1	Kepuasan Pasar	48,50	47,60
2	Kepuasan Bisnis	17,50	29,76
3	Pengetahuan dan Keluaran Teknologi	18,30	24,06
4	Keluaran Kreativitas	17,30	26,51
5	Institusi	51,20	64,94
6	Penelitian dan SDM	22,40	64,94
7	Infrastruktur	41,40	41,48

c. Indeks Kesiapan Digital

Berdasarkan indeks kesiapan digital, Indonesia masih belum sepenuhnya memiliki kesiapan dalam mengeksploitasi kesempatan yang ditawarkan oleh teknologi informasi dan komunikasi. Dalam hal ini Indonesia menduduki peringkat 66 dari 130 negara dengan nilai 50,37 yang berada di bawah rerata global yaitu 52,22. Terhadap variable indeks kesiapan digital, Indonesia memiliki skor di bawah rerata global pada tiga variabel kesiapan digital yaitu variabel SDM, khususnya terkait kesiapan sektor bisnis dalam memanfaatkan teknologi informasi dan komunikasi, tata kelola, dan dampak (lihat Tabel 3).

Tabel III. Nilai Variabel Indeks Kesiapan Digital Indonesia Tahun 2021
Sumber: Portulans Academy, 2022

No	Variabel	Indonesia	Rerata Global
1	Teknologi	50,07	45,23
2	Manusia	44,69	48,75
3	Tata Kelola	55,02	57,20
4	Dampak	51,70	54,98

d. Penetrasi Internet di Indonesia

Hasil Survei terhadap Penetrasi Internet Indonesia dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2023, menunjukkan bahwa pada periode tahun 2022-2023 total pengguna internet di Indonesia sebesar 215,63 juta jiwa, di mana jumlah ini sama dengan 78,19 persen dari populasi penduduk Indonesia. Peningkatan jumlah tersebut sebesar 2,67 persen dari periode tahun sebelumnya. Tingkat penetrasi internet pada periode tahun 2022-2023 juga mengalami peningkatan 1,17 persen[20]. Tren penetrasi internet di Indonesia cenderung mengalami peningkatan signifikan (lihat Gambar 2).

Gambar 2. Jumlah Pengguna Internet di Indonesia
Sumber: Infografis Indonesia Baik, 2023

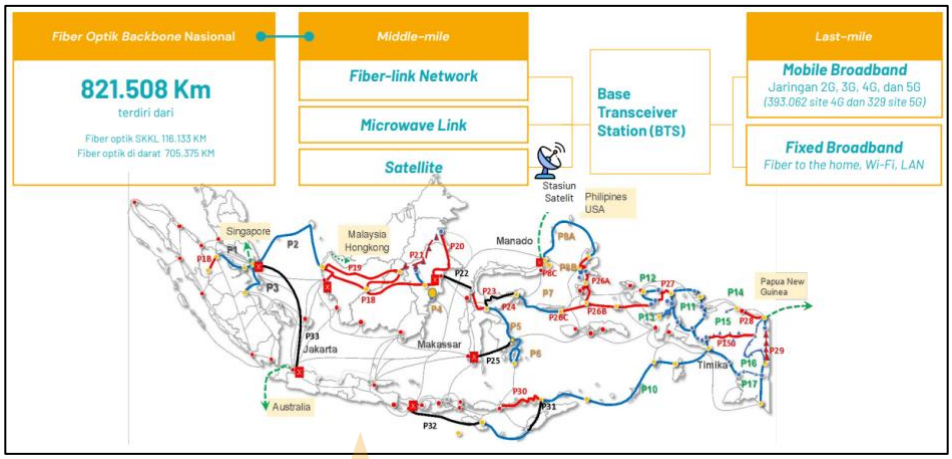
[20] https://indonesiabaik.id/infografis/pengguna-internet-di-indonesia-makin-tinggi Diunduh pada 11 Juni 2023. Pukul 09:46 WIB

e. Lanskap Aktivitas Digital Masyarakat Indonesia

Kementerian Komunikasi dan Informatika (Kemenkominfo) telah melakukan penyusunan Peta Jalan (*Roadmap*) Indonesia Digital tahun 2021-2024 untuk menuntun perjalanan transformasi digital yang komprehensif dan sinergis pada empat aspek, antara lain aspek Infrastruktur Digital, Pemerintahan Digital, Ekonomi Digital, dan Masyarakat Digital (lihat Gambar 3). Terkait infrastruktur, pada tahun 2022 Kemenkominfo mempercepat pemerataan pembangunan infrastruktur digital di Indonesia baik pada lapisan *backbone, middle-mile*, maupun lapisan *last-mile* (lihat Gambar 4). Peringkat Indonesia pada IMD World Digital Competitiveness Ranking 2022 untuk Infrastruktur Teknologi Informasi dan Komunikasi (TIK) menduduki posisi ke 45, lebih unggul dibandingkan dengan Malaysia di peringkat 49. Akan tetapi peringkat Indonesia tersebut masih belum bisa menyaingi Thailand di peringkat ke 15 dan Singapura di peringkat ke 9[21].

Gambar 3. Lanskap Aktivitas Digital Masyarakat Indonesia
Sumber: Paparan Dirjen APTIKA Kominfo, 2023

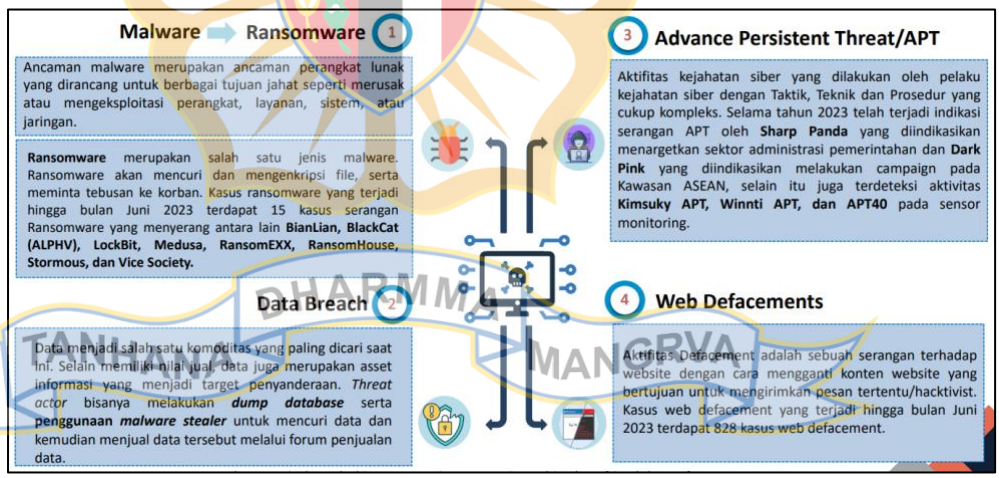
[21] Prof. Ir. Teddy Mantoro, MSc, PhD, SMIEEE. 2023. *Akselerasi Transformasi Digital, Infrastruktur Digital, dan Ekosistem Digital Dalam Mewujudkan Transformasi Digital Indonesia*. Disampaikan pada Diskusi Panel BS Strategi dengan tema Strategi Percepatan Transformasi Digital untuk Pembangunan Nasional yang Berkelanjutan, PPSA XXIV Lemhannas RI tanggal 6 Juli 2023



Gambar 4. Infrastruktur Digital Indonesia
Sumber: Paparan Dirjen APTIKA Kominfo, 2023

f. Tren Serangan Siber di Indonesia

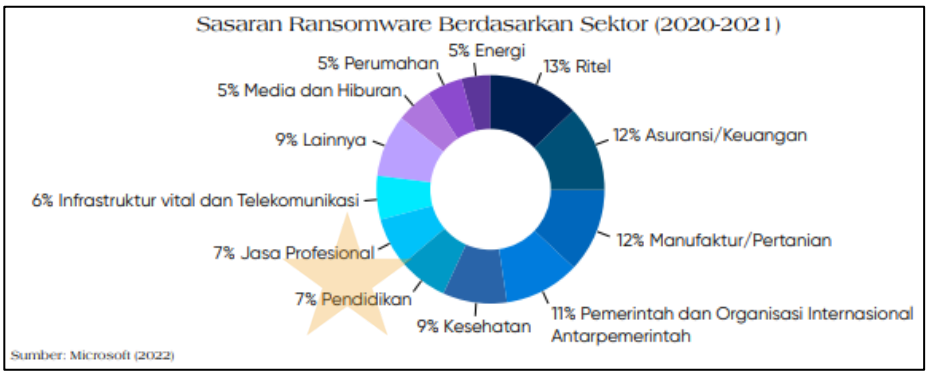
Bentuk serangan siber bermacam-macam, pada tahun 2023 ini tren serangan siber antara lain *Advanced Persistent Threat* (APT), *cybercrime-as-a-service* (CaaS) melalui *ransomware* dan *malware* yang mendominasi dari ketiganya, *Data Breach*, dan *Web Defacements* (lihat Gambar 5).



Gambar 5. Bentuk Serangan Siber Tahun 2023
Sumber: BSSN, 2023

Ransomware merupakan salah satu bentuk serangan siber yang sering terjadi di Indonesia, sebagai contoh gangguan layanan BSI (Bank Syariah Indonesia) karena *ransomware* yang

melumpuhkan layanan perbankan selama lima hari[22]. Sasaran *Ransomware* di Indonesia pada periode tahun 2020 sampai 2021 terjadi hampir di semua sektor (lihat Gambar 6).



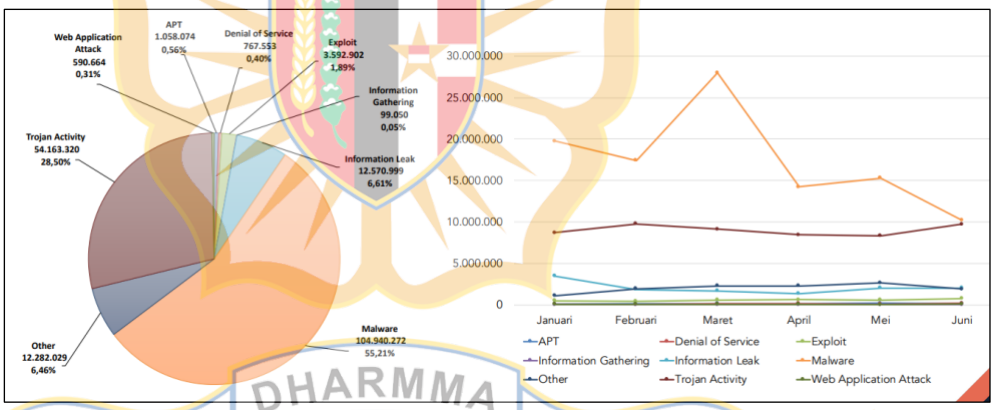
Gambar 6. Sasaran *Ransomware* Berdasarkan Sektor
Sumber: Indonesia X Geo V, 2023

Kebocoran data juga sering terjadi, lembaga keamanan digital asal Belanda, *Surfshark*, menempatkan Indonesia di posisi ke-3 negara dengan kebocoran data tertinggi di dunia[23]. Pada bulan Mei tahun 2020 telah terjadi kebocoran 91.000.000 data yaitu identitas *user* Tokopedia[24]. Kemudian pada bulan November 2020, 5.800.000 data identitas pengguna salah satu platform pemesanan hotel, Red Doorz, juga mengalami kebocoran data[25]. Menurut data yang dihimpun dari ASEAN *Cyberthreat* 2021, Indonesia menduduki urutan paling tinggi dalam serangan *malware* di antara negara ASEAN lainnya dengan total 1.3 juta kasus[26].

[22] https://www.bbc.com/indonesia/articles/cn01gdr7eero Diunduh tanggal 4 Juli 2023 pukul 15:26 WIB
[23] https://hypernet.co.id/id/2023/03/09/cybercrime-dan-6-fakta-menariknya/, Diunduh pada tanggal 5 Juni 2023 pukul 20.15 WIB.
[24] Laporan Hasil Monitoring Keamanan Siber Tahun 2020, BSSN.
[25] Ibid.
[26] https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan, Diunduh pada tanggal 5 Juni pukul 19.45 WIB.

g. Tren Anomali Trafik

Pada periode tanggal 1 Januari sampai 22 Juni 2023, telah ditemukan 190.064.862 anomali trafik yang berhasil dihimpun oleh BSSN, dengan tiga kategori terbesarnya antara lain Malware mencapai 55,21 persen, aktivitas Trojan 28,50 persen, dan *information leak* sebesar 6,61 persen (lihat Gambar 7). Dari total anomaly trafik tersebut, sebanyak 148.495.076 anomali diindikasikan berhasil menginfeksi (*Compromise*) dan 2.550.872 anomali dengan status serangan berhasil (*Attack Successful*). Anomali dengan status compromise dan attack successful berasal dari kategori Malware (61,60 persen), *Trojan Activity* (35,85 persen), *Other* (1,05 persen), APT (0,70 persen), *Exploit* (0,57 persen), *Information Leak* (0,22 persen), dan *Web Application Attack* (0,01 persen). Daftar 3 anomali tertinggi dari setiap klasifikasi yang diindikasikan *compromise* dan *attack successful* ditunjukkan pada Tabel 4 di bawah ini.



Gambar 7. Anomali Trafik Serangan Siber Semester I Tahun 2023
Sumber: BSSN, 2023

Tabel IV. Tiga Anomali Tertinggi dengan Indikasi Compromise *dan Attack Successful* Tahun 2023
Sumber: BSSN, 2023

KLASIFIKASI	THREAT NAME	TOTAL
Malware	PhishingSite Other Malware activity	27.395.839
	MiningPool Mining Virus activity	13.564.323
	fakeTelegram Malicious Download activity	8.099.241
Trojan Activity	Generic Trojan RAT activity	41.331.939
	CobaltStrike RAT activity	3.554.442
	Emotet Stealer Trojan activity	1.246.816
Other	MSSQL database account brute force guess	763.491
	Website Automatic Directory Listing Detection	490.614
	TELNET account violence guess	102.021

10. Kerangka Teoretis

Kerangka teoretis digunakan sebagai salah satu pisau analisis dalam menyelesaikan permasalahan dalam hal ini meningkatkan pertahanan siber dalam mendukung ketahanan nasional. Teori yang digunakan terdiri dari teori penerimaan teknologi informasi, konsep pertahanan siber, konsep pertahanan mendalam, konsep *pentahelix*, konsep ketahanan nasional, dan analisis PESTLE dengan penjelasan sebagai berikut:

a. **Teori Penerimaan Teknologi Informasi**.

Teori Penerimaan Teknologi Informasi (*Technology Acceptance Model*/TAM) merupakan sebuah teori yang menggambarkan beberapa faktor yang memengaruhi dalam adopsi (penerimaan) dan pemanfaatan teknologi informasi. Teori ini diperkenalkan oleh Fred Davis pada tahun 1989, dan kemudian dikembangkan oleh Venkatesh dan Davis pada tahun 2000 (Venkatesh & Davis, 2000). Menurut teori ini, penerimaan teknologi informasi tergantung pada dua faktor utama, yaitu persepsi pengguna terhadap kemanfaatan (*perceived usefulness*) dan kemudahan pemanfaatan (*perceived ease of use*) teknologi tersebut. Persepsi kemanfaatan berhubungan dengan sejauh mana teknologi tersebut dapat membantu pengguna dalam menyelesaikan tugas-tugasnya, sedangkan persepsi pada kemudahan pemanfaatan berkaitan dengan sejauh mana teknologi tersebut dengan mudahnya dimanfaatkan oleh pengguna. TAM juga mengidentifikasi faktor-faktor lain yang memengaruhi penerimaan teknologi informasi, seperti persepsi terhadap kualitas informasi, persepsi terhadap keandalan sistem, dan persepsi terhadap kemudahan untuk mempelajari teknologi tersebut.

b. **Konsep Pertahanan Siber**.

Konsep pertahanan siber adalah rangkaian strategi dan taktik yang digunakan untuk melindungi sistem, jaringan, perangkat, dan data dari serangan siber yang merugikan. Konsep ini didasarkan pada prinsip-prinsip dasar pertahanan, termasuk identifikasi, deteksi, perlindungan, respons, dan pemulihan (Kizza, 2017). Beberapa

prinsip dan strategi yang digunakan dalam teori pertahanan siber adalah lapisan pertahanan, pengawasan aktivitas, peran dan tanggung jawab, pencegahan dan deteksi serta penyediaan *backup*. Lapisan pertahanan adalah penerapan berbagai lapisan pertahanan untuk melindungi sistem dari serangan. Setiap lapisan memberikan perlindungan tambahan dan meningkatkan kompleksitas untuk menghindari serangan. Sedangkan pengawasan aktivitas merupakan kegiatan pengawasan terhadap aktivitas sistem secara terus-menerus untuk mengidentifikasi serangan yang sedang atau akan terjadi. Selanjutnya, perlu dilakukan pengaturan peran dan tanggung jawab yang jelas bagi para pemangku kepentingan dan personel keamanan siber dalam melindungi sistem. Kemudian, penerapan strategi pencegahan dan deteksi untuk mencegah serangan dan mengidentifikasi serangan yang terjadi. Dan terakhir adalah penyediaan cadangan untuk data, sistem, dan aplikasi agar bisa dipulihkan dengan cepat dalam kasus serangan.

c. **Konsep Pertahanan Mendalam (*defense in depth*)**.

Konsep pertahanan mendalam dalam dunia militer adalah strategi pertahanan yang melibatkan penggunaan serangkaian posisi pertahanan yang terdiri dari beberapa lapisan yang saling mendukung (Prescot, 2011). Setiap lapisan memiliki tugas dan tanggung jawab yang berbeda-beda dalam menghadapi serangan musuh. Konsep ini didasarkan pada prinsip bahwa pertahanan harus difokuskan pada membuat serangan musuh menjadi semakin sulit dan mahal, dengan mengurangi kemampuan musuh untuk mencapai sasaran strategis dan membuatnya mengalami kerugian besar dalam setiap tahapan serangan. Beberapa prinsip dan strategi yang digunakan dalam konsep pertahanan mendalam adalah penggunaan posisi yang terintegrasi, peningkatan kekuatan pertahanan di setiap lapisan, penggunaan wilayah sebagai pertahanan dan peningkatan kemampuan komunikasi.

d. **Konsep Pentahelix**

Konsep Pentahelix oleh Riyanto (2018) adalah model kerja sama yang melibatkan pemerintah, dunia usaha, akademisi, masyarakat, dan media untuk memperkuat sinergi dan kolaborasi dalam berbagai aspek, termasuk kebijakan pemerintah dan penguatan infrastruktur digital (Putri Rizkiyah et.all., 2019). Pemerintah berperan sebagai regulator dan pengambil kebijakan untuk mendukung perkembangan infrastruktur digital dan menciptakan lingkungan inovasi. Dunia usaha bertindak sebagai penggerak ekonomi dan inovasi, berkontribusi pada pertumbuhan industri digital dan lapangan kerja. Akademisi menyediakan pengetahuan, riset, dan inovasi untuk mengarahkan perkembangan infrastruktur digital yang berkelanjutan. Masyarakat berkontribusi dalam pengambilan suatu keputusan dan memperoleh manfaat langsung dari infrastruktur digital. Media berperan sebagai penghubung untuk menyampaikan informasi dan meningkatkan kesadaran tentang pentingnya infrastruktur digital. Kolaborasi yang baik diharapkan menciptakan lingkungan yang kondusif bagi perkembangan teknologi digital yang inklusif dan berkelanjutan. Dalam hal ini dapat memperkuat kolaborasi guna meningkatkan pertahanan siber.

e. **Konsep Ketahanan Nasional**

Konsepsi Ketahanan Nasional adalah suatu pandangan atau gagasan tentang bagaimana suatu negara atau bangsa dapat melindungi serta mempertahankan keamanan, kedaulatan, dan keutuhan wilayahnya dari berbagai ancaman baik dari dalam maupun dari luar[27]. Konsepsi ini melibatkan berbagai aspek yang saling terkait, termasuk aspek militer, politik, ekonomi, sosial, budaya, dan lingkungan. Dalam menghadapi tantangan era modern, aspek serangan siber menjadi semakin penting dalam menjaga pertahanan dan keamanan nasional.

[27] Tim Pokja Bahan Ajar BS Ketahanan Nasional. 2023. *Materi Pokok Bidang Studi Ketahanan Nasional.* Jakarta: Lemhannas RI

Pentingnya konsepsi ketahanan nasional karena serangan siber dapat mengancam kerahasiaan dan integritas data penting yang berkaitan dengan pertahanan nasional, keamanan, dan kebijakan strategis. Konsepsi ketahanan nasional memperhatikan bagaimana melindungi dan mengamankan data dan informasi penting dari serangan siber. Konsepsi ketahanan nasional harus mencakup rencana tanggap darurat dan pemulihan untuk menghadapi serangan siber. Ini termasuk kebijakan, prosedur, dan teknologi yang dirancang untuk mendeteksi, menghadapi, dan memulihkan diri dari dampak serangan siber. Dengan demikian, konsepsi ketahanan nasional telah berkembang dengan meliputi tantangan baru yang muncul dari pesatnya perkembangan teknologi, termasuk serangan siber. Penggunaan teknologi informasi dan komunikasi yang semakin luas juga menuntut negara-negara untuk memperkuat pertahanan negara dalam menjaga kedaulatan, keamanan, dan keutuhan wilayahnya.

f. **Analisis PESTLE**

Fathi S. M. Abdullah (2009) dalam Siti Paramadita et.al. (2020) mendeskripsikan Analisis PESTLE sebagai *"*alat yang berguna untuk mengerti 'gambaran besar' dari sebuah lingkungan tempat sebuah organisasi/perusahaan beroperasi. Analisis PESTLE juga dapat digunakan untuk mencari tahu kesempatan dan ancaman yang ada di lingkungan tersebut"[28].

11. Lingkungan Strategis.

a. Global.

Perkembangan lingkungan strategis di tingkat global mencakup berbagai isu keamanan yang menunjukkan tren meningkatnya konflik di berbagai wilayah di seluruh dunia. Hal ini juga memunculkan peningkatan serangan siber, polarisasi politik global, dan intervensi militer gabungan[29]. Konflik Rusia ke Ukraina beberapa waktu lalu

[28] Siti Paramadita et.al. 2020. *Analisis PESTLE Terhadap Penetrasi Gojek Di Indonesia*. Jurnal Pengabdian dan Kewirausahaan- Vol. 4 No. 1 2020
[29] Ditjen Strahan Kemhan, Perkembangan Lingkungan Stategis tahun 2021, h 1

selain serangan konvensional juga melibatkan perang siber. Selama perang antara Ukraina dan Rusia, Ukraina menerima serangan siber lebih banyak daripada Rusia. Serangan ini dapat mencakup serangan terhadap infrastruktur, pencurian data, dan spionase. Perang siber antara Rusia dan Ukraina melibatkan serangan terhadap situs web pemerintah, bank, dan infrastruktur kritis seperti pembangkit tenaga listrik. Serangan ini dapat memiliki dampak yang signifikan, seperti gangguan pasokan air bersih, energi, dan layanan kesehatan[30].

Dalam era digital dan saling terhubung, pertahanan siber telah menjadi faktor penting dalam pertahanan negara. Negara-negara di seluruh dunia telah menyadari pentingnya melindungi infrastruktur militer, sistem komunikasi, dan data sensitif dari peperangan siber[31]. Di era Geo V saat ini, persaingan teknologi antarnegara adidaya dapat terlihat dalam sektor teknologi 5G dan semikonduktor sebagai salah satu representasi dari konektivitas *global supply chain*. Terdapat tujuh kawasan yang terlibat dalam rantai pasok tersebut dengan tahapan yang berbeda yaitu AS, Tiongkok, Malaysia, Taiwan, Korea Selatan, dan Jepang. Antara satu dan lainnya terdapat ketergantungan, namun di sisi lain tidak menutup kemungkinan adanya kompetisi seperti antara AS dan Tiongkok. Tiongkok meningkatkan swasembada dan memisahkan diri dari teknologi AS, serta berusaha meningkatkan teknologi semikonduktor walaupun masih tertinggal jauh dari AS, Jepang, Taiwan, dan Korea Selatan.

Tiongkok telah mengembangkan kebijakan *Belt and Road Initiative* (BRI) melalui teknologi 5G yang dilakukan oleh Huawei diantaranya dengan membangun infrastruktur digital, keamanan internet, membangun komunitas bersama di dunia digital, serta menggabungkan kepentingan ekonomi dan keamanan. Kemudian melalui program *Digital Silk Road*, Tiongkok melakukan pendekatan aspek kesejahteraan untuk mengembangkan kemampuan negara-

[30] https://www.dw.com/id/perang-siber-infrastruktur/a-64063719
[31] Tzeng, Yusio. 2022. *China's Military Modernization in Autonomous, Cyber, and Space Weapons*. Meeting China's Emerging Capabilities Countering Advances in Cyber, Space, And Autonomous Systems. The National Bureau of Asian Research

negara berkembang untuk mencapai era digital, program Pendidikan digital, meningkatkan kesehatan masyarakat dengan memanfaatkan AI.

Perkembangan ilmu pengetahuan dan teknologi sendiri telah memiliki dampak yang signifikan pada perkembangan global. Perkembangan teknologi telah mendorong pertumbuhan ekonomi global, inovasi dalam bidang teknologi informasi, komunikasi, transportasi, dan manufaktur. Dalam bidang Teknologi Informasi dan Komunikasi (TIK), kemajuan dalam teknologi komunikasi, terutama internet, telah mengubah cara orang berinteraksi dan mengakses informasi. Selain membawa dampak positif, perkembangan TIK juga membawa dampak negatif salah satunya terkait keamanan siber. Serangan siber dapat dimanfaatkan untuk mencuri data sensitif, baik itu informasi pemerintah, militer, atau korporat. Data tersebut bisa mencakup informasi rahasia, informasi keuangan, rancangan produk, atau rahasia dagang. Pencurian data sensitif dapat merugikan keamanan nasional, privasi individu, atau kepentingan ekonomi.

Terdapat peluang dan kendala terkait pengaruh lingkungan strategis global terhadap peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional. Peluang yang dapat dimanfaatkan antara lain:

1) Modernisasi peralatan dan perangkat lunak pada bidang siber yang menjadi salah satu prioritas dalam upaya menyelamatkan kedaulatan nasional masing-masing negara termasuk Indonesia dari berbagai bentuk serangan siber.
2) Kerjasama bilateral dengan negara adidaya baik dengan AS maupun Tiongkok terkait pengembangan teknologi siber dan pencegahan serangan siber.
3) Perkembangan ilmu pengetahuan dan teknologi dalam bidang siber di dunia yang sangat pesat di berbagai sektor.

Selain peluang, juga terdapat kendala yang harus dihadapi dan perlu mendapatkan perhatian antara lain:

1) Perang siber antara Rusia dan Ukraina yang berpotensi menyebabkan penjahat siber di seluruh dunia untuk melakukan aktivitas kriminal siber, seperti *phishing* dan *scam*[32].
2) Potensi penyalahgunaan kemampuan AI (*artificial intelligence*) dalam serangan di dunia siber yang terdiri dari *malware*, *ransomware*, *social engineering*, dan propaganda.
3) Penguasaan teknologi siber setiap negara yang berbeda-beda.

b. Regional.

Kondisi regional terutama di kawasan ASEAN terkait dengan pertahanan dan keamanan dari serangan siber sangat penting. Serangan siber menjadi ancaman yang semakin meningkat di era digital ini, dan negara-negara di kawasan tersebut telah meningkatkan upaya pertahanan dan keamanan dalam menghadapinya, saling bertukar informasi mengenai ancaman siber, dan kerjasama dalam menanggapi serangan siber yang melintasi batas negara.

Merujuk pada data yang disampaikan oleh Frost and Sullivan, kuantitas ancaman siber wilayah di ASEAN merupakan yang tertinggi kedua secara global di bawah Amerika Utara. Pada pernyataan tersebut juga dijelaskan terkait total biaya yang harus dikeluarkan untuk menangani kejahatan siber di ASEAN pada tahun 2025 yang berpotensi menembus angka $171 miliar[33]. Ancaman kejahatan siber yang dihadapi oleh negara-negara di ASEAN antara lain serangan *phising*, infeksi *malware*, dan serangan *ransomware*. Melihat tingginya serangan siber di wilayah ASEAN, *Indonesia* mempelopori pembangunan ekosistem keamanan siber yang aman dan stabil di kawasan Asia Tenggara. Hal ini dilakukan dengan membentuk komunitas ASEAN-CERT yang secara resmi dibentuk pada bulan Januari 2011 dalam konferensi di Kuala Lumpur, Malaysia. Tujuan

[32] https://www.antaranews.com/berita/2737877/mewaspadai-dampak-serangan-siber-perang-rusia-ukraina
[33] Frost and Sullivan (2018) dalam Cybersecurity in ASEAN: An Urgent Call to Action, ATKearney

pembentukan komunitas ASEAN-CERT tersebut untuk meningkatkan keamanan siber di wilayah regional Asia Tenggara.

Negara-negara anggota ASEAN telah menyadari bahwa kerjasama regional sangat penting untuk menghadapi serangan siber. Pada tahun 2018, ASEAN meluncurkan Inisiatif Keamanan Siber ASEAN (ACSI) untuk mempromosikan kerjasama regional dalam pertahanan siber. ACSI bertujuan untuk meningkatkan kapasitas anggota ASEAN dalam menghadapi serangan siber melalui pertukaran informasi, pelatihan, dan kerjasama dalam penanggulangan serangan siber. Selain itu, beberapa negara di ASEAN juga telah mengadopsi kebijakan dan peraturan terkait keamanan siber, serta meningkatkan upaya mereka dalam meningkatkan kesadaran masyarakat tentang serangan siber dan pentingnya keamanan siber. Singapura adalah salah satu negara ASEAN yang paling maju dalam hal pertahanan siber. Mereka telah membangun pusat keunggulan siber dan memperkuat kerjasama dengan negara-negara mitra untuk menghadapi serangan siber.

Peluang yang dapat dimanfaatkan pada lingkungan strategis regional terhadap peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional diantaranya adanya komitmen dari negara-negara ASEAN untuk bekerjasama dalam menghadapi serangan siber dalam ACSI. Kemudian salah satu negara anggota ASEAN yaitu Singapura memiliki indeks ketahanan siber yang paling baik sehingga dapat dijadikan sebagai acuan negara lain di ASEAN untuk meningkatkan keamanan dan pertahanan sibernya, serta melaksanakan kerjasama bilateral.

Sedangkan kendala yang dihadapi antara lain tingginya potensi negara-negara ASEAN untuk dijadikan sebagai target serangan siber dan lokasi kawasan Asia Tenggara yang berada di wilayah persaingan teknologi antarnegara adidaya yaitu AS dan Tiongkok. Selain itu tingkat penguasaan teknologi siber masing-masing negara di Asia Tenggara sangat beragam.

c. Nasional.

Perkembangan isu global dan regional secara langsung akan memengaruhi dinamika pertahanan dan keamanan nasional. Selain itu, isu-isu nasional juga sangat memengaruhi kebutuhan peningkatan pertahanan siber guna mendukung ketahanan nasional.

1) **Geografi**. Secara geografis, letak strategis Indonesia di kawasan Asia Tenggara dan ketersediaan sumber kekayaan alam (SKA) yang melimpah menjadikannya sering menjadi target spionase siber oleh aktor negara dan non-negara. Luasnya wilayah Indonesia dengan kondisi topografi dan bentuk kepulauan menjadi tantangan dalam pembangunan infrastruktur digital yang semakin berat. Disisi lain kondisi geologis Indonesia memberikan keuntungan ketersediaan bahan mineral.
2) **Demografi**. Berdasarkan data dari BPS (2022), Indonesia memiliki pertumbuhan penduduk sebesar 1,17 persen[34]. Pertumbuhan penduduk yang tidak seimbang dengan ketersediaan sumber daya dapat memengaruhi kualitas hidup masyarakat. Dengan pertumbuhan teknologi informasi dan penggunaan internet yang luas, jumlah data pribadi yang dikumpulkan dan disimpan oleh pemerintah, lembaga swasta, dan individu juga semakin meningkat. Permasalahan demografi seperti urbanisasi, migrasi, dan pertumbuhan penduduk yang tinggi dapat meningkatkan risiko kebocoran atau penyalahgunaan data pribadi. Pertahanan siber menjadi penting untuk melindungi data pribadi yang sensitif dari serangan siber dan kejahatan siber. Indonesia juga memperoleh bonus demografi, dengan mayoritas generasi X dan Z yang familiar dengan dunia siber.
3) **Sumber Kekayaan Alam.** Potensi kekayaan alam Indonesia yang melimpah khususnya bahan mineral tembaga, emas, nikel

[34] BPS. 2022. Laju Pertumbuhan Penduduk, 2020-2022. https://www.bps.go.id/indicator/12/1976/1/laju-pertumbuhan-penduduk.html, Diunduh tanggal 20 Juni 2023 pukul 09.57 WIB.

berkualitas tinggi yang dapat dijadikan sebagai bahan baku dalam pembuatan perangkat elektronik dan semikonduktor. Hal ini dapat mendukung pembangunan infrastruktur digital yang canggih.

4) **Ideologi.** Melihat derasnya arus globalisasi saat ini, kemudahan akses informasi dan penetrasi internet di Indonesia yang mengalami peningkatan, bukan tidak mungkin serangan-serangan siber yang terjadi akan digunakan untuk menyebarkan propaganda, disinformasi, dan memengaruhi opini publik. Pihak yang melakukan serangan dapat mencoba mengubah pandangan ideologi suatu negara, memicu konflik sosial, atau merusak stabilitas politik dengan memanfaatkan media sosial dan platform *online*. Oleh karena itu, ketahanan nasional terhadap serangan siber dalam bidang ideologi diperlukan untuk melindungi keutuhan dan stabilitas ideologi negara.

5) **Politik**. Pemerintah telah menerapkan kebijakan untuk memperkuat keamanan dan pertahanan ruang siber di Indonesia. Berbagai kebijakan pemerintah telah disahkan sebagai payung hukum dalam segala aktivitas ruang siber. Namun kebijakan melalui regulasi tersebut juga seharusnya diperkuat dengan sanksi hukum yang jelas, tegas, dan dilaksanakan sesuai ketentuan yang telah tertulis dalam kebijakan pemerintah tersebut. Melihat perkembangan geopolitik global maka kebijakan pertahanan tersebut tidak hanya berlaku untuk menangkal ancaman fisik, tetapi juga ancaman siber yang bersifat non-fisik. Serangan siber yang sering terjadi dapat menyasar sistem politik suatu negara dengan mencuri informasi rahasia, merusak infrastruktur elektronik, atau bahkan mengganggu jalannya pemilihan umum. Ancaman ini dapat memengaruhi integritas sistem politik dan stabilitas pemerintahan. Oleh karena itu diperlukan pertahanan siber yang handal guna mendukung terciptanya stabilitas politik nasional.

Di sisi lain, menjelang pelaksanaan pemilu serentak tahun 2024 maka potensi serangan siber semakin meningkat. Potensi serangan siber pada sistem informasi KPU, maraknya kampanye hitam yang memanfaatkan ruang siber serta masifnya penyebaran hoaks dan ujaran kebencian melalui media sosial perlu diwaspadai.

6) **Ekonomi.** Perekonomian dapat memberikan dampak yang signifikan terhadap pertahanan dan keamanan siber di Indonesia. Di era digital saat ini hampir semua sektor meliputi sektor publik, industri, perbankan, perdagangan, infrastruktur, dan pertahanan nasional semuanya sangat bergantung pada sistem teknologi informasi, di mana ketergantungan ini menimbulkan kerentanan terhadap serangan siber. Keamanan siber masih menjadi tantangan utama dalam perekonomian digital Indonesia. Pada tahun 2022 lalu, sekitar 52 persen perusahaan di Indonesia pernah mengalami insiden serangan siber paling tidak sekali dalam satu tahun. Potensi serangan siber ini semakin membahayakan terutama yang berhubungan dengan perekonomian negara. Serangan siber dapat menyebabkan kerugian ekonomi yang signifikan dengan mengganggu operasional perusahaan, mencuri data bisnis, atau memblokir akses ke sistem keuangan. Keberlanjutan ekonomi suatu negara dapat terancam apabila infrastruktur kritis seperti perbankan, transportasi, atau energi menjadi target serangan siber.

Penggunaan *e-commerce* yang semakin meningkat dan tingginya pengguna *internet banking* berpotensi menjadi sasaran serangan siber. Serangan siber yang berpotensi terjadi adalah *phising*, serangan *phishing* menyasar pada UMKM di Indonesia dengan jumlah serangan yang meningkat sebesar 56 persen pada tahun 2020. Selain itu terdapat serangan *ransomware* yang dapat mengganggu operasional *e-commerce* dan mengakibatkan hilangnya data atau kerugian finansial. Serangan

Ransomware menargetkan organisasi-organisasi di Indonesia, termasuk organisasi-organisasi yang bergerak di industri energi, telekomunikasi, teknologi tinggi, dan finansial. Meningkatnya intensitas serangan siber juga dapat memengaruhi keamanan transaksi digital. *Booming*nya *e-commerce* sejak awal pandemi juga turut berkontribusi terhadap meningkatnya kasus penipuan *online*.

7) **Sosial Budaya.** Sasaran strategis keamanan siber Indonesia adalah mewujudkan keamanan pada layanan publik, ketahanan siber, penegakan hukum siber, budaya keamanan siber, dan pertahanan negara. Pembinaan dan pembiasaan ketahanan nasional dalam berbagai aspek akan menentukan kualitas pertahanan negara. Era digital yang memberikan kesempatan bagi semua pihak untuk mengakses dan menggunakan layanan di dalamnya juga memiliki dampak negatif yaitu penyalahgunaan ruang siber oleh pihak yang tidak bertanggung jawab untuk melakukan serangan-serangan dengan tujuan tertentu. Masyarakat Indonesia sangat cepat beradaptasi dengan era digital, namun tidak semuanya memiliki literasi digital yang tinggi. Tingkat literasi digital di Indonesia masih relatif rendah, hanya sebesar 62 persen apabila dibandingkan dengan literasi digital negara-negara ASEAN yang rata-rata mencapai 70 persen[35]. Serangan siber dapat menyebabkan ketegangan sosial dan budaya dengan memanipulasi informasi atau memicu konflik antar golongan. Penyebaran propaganda atau konten yang merusak dapat memengaruhi kesatuan sosial dan harmoni masyarakat di mana hal ini berpotensi melemahkan identitas dan ketahanan nasional.

8) **Pertahanan dan Keamanan**. Serangan siber dapat merusak sistem pertahanan dan keamanan suatu negara dengan mencuri informasi militer, mengganggu jaringan komunikasi, atau

[35] https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62 Diunduh tanggal 5 Juli 2023 pukul 19:24 WIB

memanipulasi sistem senjata. Keamanan siber memiliki peranan krusial dalam memastikan bahwa informasi sensitif, data pribadi, sistem, dan infrastruktur digital terlindungi dari segala bentuk ancaman dan serangan melalui ranah siber baik secara langsung maupun tidak langsung. Keberhasilan serangan siber terhadap infrastruktur kritis atau data militer dapat mengancam keamanan nasional dan kesiapan pertahanan. Pertahanan siber menjadi penting untuk menjaga keamanan dan stabilitas nasional dengan melindungi infrastruktur digital, mengatasi propaganda dan disinformasi *online*, serta menghadapi ancaman serangan siber. Perkembangan teknologi telah memengaruhi pertahanan siber di Indonesia, oleh karena itu perlu dilakukan adaptasi terhadap perkembangan teknologi dan memperkuat pertahanan siber agar dapat menghadapi ancaman siber yang semakin kompleks.

Terdapat beberapa peluang dan kendala yang berkaitan dengan perkembangan lingkungan strategis nasional terhadap peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional. Peluang yang dapat dimanfaatkan antara lain:

1) Ketersediaan penduduk usia produktif karena Bonus Demografi yang dapat diberdayakan untuk menjadi tenaga ahli bidang siber.
2) Tersedianya SKA yang melimpah, dapat dimanfaatkan untuk mendukung upaya peningkatan pertahanan siber.
3) Tren pertumbuhan teknologi konektivitas yang cepat memberikan peluang dalam berinovasi.

Sedangkan kendala yang dihadapi dan perlu mendapatkan perhatian bersama antara lain:

1) Intensitas serta spektrum ancaman siber yang semakin luas dan selalu berkembang.
2) Rendahnya kesadaran individu dalam menghadapi serangan dan ancaman siber.
3) Keterbatasan literasi digital masyarakat Indonesia.

4) Kondisi terbatasnya infrastruktur digital dan pemerataan akses teknologi digital.

BAB III

PEMBAHASAN

12. Umum.

Data dan fakta terkait siber di Indonesia menunjukkan kemampuan pertahanan siber di Indonesia khususnya di lingkungan Kementerian dan Lembaga pemerintah yang masih rentan. Kemampuan pertahanan siber dipengaruhi oleh tiga aspek dominan, yaitu aspek SDM, teknologi dan regulasi. Diperlukan strategi dan upaya untuk meningkatkan kemampuan pertahanan siber yang diformulasikan dengan mengamati data dan fakta, dan dilakukan analisis melalui beberapa teori dan konsepsi yang relevan antara lain yaitu teori penerimaan teknologi, konsep pertahanan siber, konsep pertahanan mendalam, konsep *pentahelix*, konsep ketahanan nasional, dan analisa dampak serangan siber dengan metode PESTLE.

Analisa yang akan dilakukan juga melihat pertimbangan pada kondisi perkembangan lingkungan strategis serta peluang yang dapat dimanfaatkan untuk memberikan dukungan dan kendala yang harus diatasi agar strategi dan upaya peningkatan pertahanan siber dalam rangka mendukung ketahanan nasional dapat berjalan dengan optimal. Pada bagian awal pembahasan akan disampaikan kondisi kemampuan pertahanan siber dilihat dari aspek sumber daya manusia (SDM), teknologi, dan regulasi, kemudian dampak serangan siber pada kementerian dan lembaga, serta strategi dan upaya yang dapat diimplementasikan untuk meningkatkan pertahanan siber dalam rangka mendukung ketahanan nasional.

13. Kemampuan Pertahanan Siber pada Kementerian dan Lembaga di Indonesia Dilihat dari Aspek Sumber Daya Manusia, Teknologi, dan Regulasi.

Kondisi secara umum saat ini, keamanan siber di Indonesia menghadapi tantangan yang beragam. Sebagaimana telah dibahas pada bab sebelumnya bahwa tren serangan siber di Indonesia semakin meningkat dan beragam, sehingga tanpa adanya pengendalian dan pengawasan, maka keamanan dimensi sosial, politik, dan ekonomi, termasuk pertahanan dan keamanan

akan berpotensi terancam melalui aktivitas di ranah digital. Terdapat tiga hal dalam manajemen keamanan siber yang harus dibangun dan dipertimbangkan antara lain *people, process,* dan *technology*. Data dan fakta terkait siber di Indonesia menunjukkan kemampuan pertahan siber di Indonesia masih rentan, capaian indeks keamanan siber nasional, indeks inovasi global, dan indeks kesiapan digital masih rendah dan berada di bawah rata-rata indeks global. Pada bagian lain, data menunjukkan tren serangan siber dan anomali trafik yang semakin meningkat ditengah semakin tingginya penetrasi internet dan meningkatnya aktivitas digital masyarakat Indonesia. Kondisi tersebut dipengaruhi oleh tiga aspek dominan, yaitu aspek SDM, teknologi dan regulasi. Kemampuan pertahanan siber pada aspek SDM, teknologi dan regulasi akan diuraikan pada bagian ini, untuk mendapatkan gambaran lebih jelas dan detail.

a. **Sumber Daya Manusia (SDM).**

SDM berkontribusi pada kemampuan pertahanan siber, berbagai insiden yang terjadi karena serangan siber disebabkan oleh faktor SDM. Tantangan SDM dalam keamanan siber di Indonesia mengacu pada kesenjangan pemahaman dan keterampilan terkait dengan praktik keamanan siber di kalangan pengguna internet dan pekerja di berbagai sektor. Meskipun penetrasi pengguna internet di Indonesia setiap tahun semakin meningkat, namun pemahaman terhadap risiko keamanan siber dan keterampilan yang memadai untuk melindungi diri dari serangan siber masih sangat rendah[36]. Tantangan pada aspek SDM dijelaskan sebagai berikut:

1) **Kurangnya pemahaman tentang risiko keamanan siber**. Mayoritas pengguna internet tidak menyadari potensi ancaman yang ada ketika berinteraksi dengan dunia maya. Misalnya, tindakan seperti menggunakan kata sandi yang lemah, berbagi informasi pribadi secara tidak bijaksana, atau mengklik tautan yang

[36] Christmartha, Gultom, Aritonang. (2020). *Strategi Pengembangan Sumber Daya Manusia Siber Nasional Guna Mendukung Pertahanan Negara*. Jurnal Pemikiran dan Penelitian Manajemen Pertahanan. Unhan

mencurigakan tanpa verifikasi yang dapat membuka celah bagi serangan siber.

2) **Kurangnya pemahaman tentang praktik keamanan *online***. Beberapa pengguna ruang siber mungkin tidak menyadari pentingnya mengaktifkan dua faktor autentifikasi, memperbarui perangkat lunak secara teratur, atau menggunakan layanan VPN (*Virtual Private Network*) saat mengakses jaringan publik. Tanpa pemahaman ini, mereka cenderung rentan terhadap serangan siber yang dapat mencuri informasi pribadi, mengakses akun penting, atau merusak perangkat mereka. Hal ini bersesuaian dengan kondisi rendahnya variabel SDM pada indeks kesiapan digital Indonesia, di mana nilai yang diperoleh Indonesia pada tahun 2022 lalu untuk variabel SDM yaitu 44,69 yang berada di bawah rata-rata global. Banyaknya kasus kebocoran data di internet karena peretasan juga disebabkan oleh kurangnya pemahaman tentang praktik keamanan di ruang siber.

3) **Minimnya keterampilan keamanan siber di kalangan karyawan Kementerian dan Lembaga**. Karyawan dalam berbagai sektor sering berinteraksi dengan data sensitif dan infrastruktur yang penting untuk perusahaan. Tanpa pemahaman dan keterampilan yang memadai, mereka mungkin tidak dapat mengidentifikasi atau melaporkan serangan siber, menyebabkan insiden keamanan tidak terdeteksi atau tidak ditangani dengan tepat.

4) **Minimnya ketersediaan SDM yang memiliki keahlian di bidang siber**. Indeks keamanan siber Indonesia pada tahun 2022 menunjukkan kondisi yang kurang baik terhadap keamanan siber di Indonesia di mana delapan dari dua belas indikatornya berada di bawah rata-rata global. Lanskap keamanan siber Indonesia sebenarnya tidak jauh berbeda dengan negara lain, hanya saja ketersediaan SDM yang terlatih dan memiliki keahlian dengan beberapa sertifikasi sangat minim. Peningkatan keamanan siber perlu memperhatikan pembangunan SDM, budaya, kedisiplinan, pemahaman tata kelola, dan kepatuhan yang sesuai dengan

praktik-praktik keamanan siber secara global. Indonesia memperoleh bonus Demografi dengan mayoritas penduduk usia produktif namun ketersediaan SDM yang memiliki keahlian di bidang siber sangat minim, sebagai perbandingan SDM keamanan siber di Tiongkok mencapai sekitar 25 ribu orang[37]. Berdasarkan analisis BSSN pada tahun 2022, kebutuhan SDM keamanan siber di seluruh instansi Kementerian dan Lembaga mencapai 8 ribu sampai 9 ribu orang, sedangkan kebutuhan SDM keamanan siber di sektor industri mencapai hampir 10 ribu orang. Sehingga, total kebutuhan SDM keamanan siber di Indonesia sekitar 19 ribu orang[38].

5) **Rendahnya literasi digital**. Berdasarkan data dari *Institute for Management Development* (IMD), pada tahun 2023 Indonesia berada di urutan ke-51 dari 63 negara terkait literasi digital[39]. Sebagai perbandingan literasi digital Korea Selatan mencapai 97 persen sedangkan Indonesia masih mencapai 62 persen. Capaian ini juga terbilang masih rendah dibandingkan negara-negara ASEAN yang telah mencapai nilai rata-rata literasi digital sebesar 70 persen[40].

Kurangnya pemahaman tentang risiko keamanan siber dan praktik keamanan *online*, minimnya keterampilan keamanan siber dan ketersediaan SDM yang memiliki keahlian dalam bidang siber di Kementerian dan Lembaga berkontribusi terhadap insiden kebocoran data kependudukan dan terganggunya operasional BSI, menyebabkan rendahnya indeks global pada bidang keamanan siber, dan meningkatnya intensitas serangan siber di Indonesia. Kondisi riil lainnya adalah literasi digital beberapa karyawan Kementerian dan Lembaga juga masih rendah.

---

[37] https://www.republika.id/posts/20379/urgensi-sdm-keamanan-siber
[38] https://www.medcom.id/nasional/politik/8Kyzja2N-bssn-dibutuhkan-18-ribu-personel-sdm-untuk-keamanan-siber
[39] https://news.detik.com/berita/d-6770000/mahfud-kutip-data-pemenuhan-literasi-digital-di-indonesia-sangat-rendah
[40] https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62

Kondisi SDM saat ini yang cenderung mengabaikan faktor keamanan dalam ruang siber dan beberapa permasalahan dalam memahami keamanan siber sesuai dengan analisis **Teori Penerimaan Teknologi Informasi** di mana penerimaan teknologi informasi tergantung pada dua faktor utama, yaitu persepsi pengguna terhadap kegunaan dan kemudahan penggunaan teknologi tersebut. Teknologi melalui internet dan segala bentuk keuntungan yang ditawarkan dapat dengan mudah diakses, hal ini terlihat dari semakin meningkatnya penetrasi pengguna internet di Indonesia dari tahun ke tahun. Akan tetapi, penggunaan ruang siber tersebut belum diikuti dengan persepsi pengguna terhadap keamanan informasi di ruang digital. Hal inilah yang kemudian juga menyebabkan nilai indeks keamanan siber Indonesia masih dalam kategori kurang baik khususnya pada indikator keamanan data pribadi yang berkaitan dengan SDM.

Kondisi faktual SDM tersebut berimplikasi pada serangan siber di lingkungan Kementerian dan Lembaga, sebagai contoh yang terjadi di Kementerian Dalam Negeri (Kemendagri) terkait data Penduduk dan Pencatatan Sipil (Dukcapil) yang mengalami kebocoran pada bulan Juli 2023 lalu. Sebanyak 337 juta data yang diduga dari *server* dukcapil.kemendagri.go.id diperjualbelikan di forum *online hacker Breach Forums*, di DARKWEB oleh *hacker* dengan nama samaran RRR[41]. Kemendagri dan BSSN melakukan investigasi untuk menemukan penyebab kebocoran data tersebut karena diduga terdapat unsur kelalaian atau keterlibatan individu yang mengakibatkan kegagalan perlindungan data. Kondisi faktual SDM tersebut berkontribusi terhadap indeks global di bidang siber khususnya pada indeks keamanan siber, kesiapan digital, dan beberapa insiden yang terjadi akibat serangan siber. Berdasarkan **Konsep Ketahanan Nasional**, serangan siber berimplikasi pada ketahanan nasional karena dampak yang ditimbulkan menyebabkan gangguan atau ancaman pada setiap gatra yang

[41] Dr. Rudi Rusdiah BE, M.A. 2023. *Geopolitik Digital: Implikasi & Tantangan Keamanan Big Data dalam era Transformasi Digital 2045*. Paparan disampaikan pada Seminar Ketahanan Nasional Transformasi Digital Indonesia 2045 Lemhannas RI tanggal 7 Agustus 2023

kemudian memengaruhi gatra lainnya. Seperti contoh kasus kebocoran data, insiden kebocoran data yang memiliki akses pada kekuasaan negara dapat mengancam keamanan nasional. Kebocoran data juga dapat menimbulkan dampak negatif yang akan berpengaruh secara langsung atau tidak langsung seperti penyebaran ideologi transnasional, pornografi, perdagangan narkoba, kelompok kriminal terorganisir dan sebagainya yang dapat menurunkan ketangguhan ketahanan nasional.

b. **Teknologi**

Perkembangan teknologi informasi dan komunikasi semakin pesat di era digital saat ini, hampir semua aspek kehidupan nasional sangat bergantung dengan teknologi. Memasuki era Geopolitik V (Geo V), konektivitas menjadi aspek yang berupaya dibangun untuk menyebarkan pengaruh di tingkat global, oleh karena itu era Geo V sangat erat hubungannya dengan perkembangan teknologi dan perluasan spektrum ancaman.

Di Indonesia, dengan semakin meningkatnya penetrasi pengguna internet setiap tahunnya, namun belum diikuti dengan tingkat adopsi teknologi serta kesadaran dalam mengamankan informasi pribadi dalam menggunakan teknologi tersebut.

Aspek teknologi berimplikasi terhadap kemampuan pertahanan siber di Indonesia. Data dan fakta terkait siber menunjukkan dominasi aspek teknologi dalam rendahnya indeks global pada indeks keamanan siber nasional, indeks inovasi global, indeks kesiapan digital serta meningkatnya tren serangan siber dan tren anomali trafik. Adopsi teknologi digital di Indonesia mengalami peningkatan pesat sejak tahun 2022. Masyarakat Indonesia cenderung lebih menerima dan mengadopsi sebuah teknologi apabila mereka menganggapnya mudah digunakan.

Kemampuan pertahanan siber aspek teknologi didukung oleh beberapa hal, meliputi infrastruktur digital, keamanan jaringan yang rentan terhadap serangan siber, kerentanan pada keamanan perangkat keras dan perangkat lunak, kurangnya kemampuan identifikasi dan deteksi dini, lambatnya tanggapan dan penanganan keamanan siber,

minimnya perlindungan data dan informasi, serta rendahnya inovasi teknologi. Aspek teknologi pada kemampuan pertahanan siber dapat dijelaskan sebagai berikut:

1) **Infrastruktur Digital yang belum Menjangkau seluruh Wilayah**

Infrastruktur digital di Indonesia belum menjangkau seluruh wilayahnya, masih ada rakyat Indonesia belum mendapatkan akses internet terutama yang tinggal di daerah 3T (tertinggal, terdepan, dan terluar). Berdasarkan survei yang dilakukan oleh Kemenkominfo dan Katadata *Insight Center* (KIC) melalui laporan Status Literasi Digital Indonesia tahun 2022, sebanyak 12 persen responden di daerah 3T belum mendapatkan sinyal telepon, di mana sebagian besar responden dalam survei tersebut berasal dari Kabupaten Timor Tengah Selatan[42]. Pada Kementerian dan Lembaga yang memiliki kantor di daerah, termasuk didalamnya desa-desa di daerah 3T juga kesulitan mendapatkan akses internet karena jaringan yang tidak stabil. Infrastruktur digital yang ada di Indonesia meliputi *Backbone* serat optik nasional sepanjang 821.508 Km, 559.020 *base transceiver station* (BTS), dan satelit berkapasitas lima Gbps yang terdiri dari 5 satelit telekomunikasi komersial nasional dan empat satelit komunikasi asing yang disewakan. Pemerintah melalui Kemenkominfo juga telah menggelar *High Throughput Multifunction* Satellite (SATRIA-1) berkapasitas 150 Gpbs yang menyediakan akses internet pada 150.000 fasilitas publik pada tahun 2021, mengembangkan jaringan 5G, membentuk Pusat Data Nasional (PDN), dan pengembangan pusat pemantauan telekomunikasi untuk memantau kualitas pengalaman (*quality of experience* - QoE) dan kualitas layanan (*quality of services* - QoS) di seluruh Indonesia. Selanjutnya, akan dilakukan pengembangan Infrastruktur TIK untuk mendukung transformasi digital sebagai proyek besar dalam RPJMN 2020-2024. Jumlah penggunan PDN saat ini berjumlah 331

[42] https://databoks.katadata.co.id/datapublish/2023/07/11/belum-semua-warga-ri-dapat-akses-internet-dan-sinyal-selular-di-dekat-rumahnya-terutama-wilayah-3t

Kementerian dan Lembaga dan Pemerintah Daerah seluruh Indonesia dan telah dipasang 7.771 *Virtual Machine* (Ditjen Aptika Kominfo, 2023).

2) **Keamanan Jaringan yang Rentan terhadap Serangan Siber**. Keamanan jaringan merupakan salah satu pilar utama dalam upaya melindungi infrastruktur teknologi informasi dari serangan siber. Keamanan jaringan di Kementerian dan Lembaga masih rentan terhadap serangan siber sehingga kondisi integritas, kerahasiaan, dan ketersediaan data yang berada dalam jaringan seringkali mengalami kebocoran, seperti bocornya 337 juta data Penduduk dan Pencatatan Sipil (Dukcapil) Kemendagri pada bulan Juli 2023 lalu yang diduga berasal dari *server* dukcapil.kemendagri.go.id. Serangan siber dalam hal ini mampu merusak atau mengganggu operasional jaringan apabila keamanan jaringan tidak optimal.

3) **Kerentanan pada Keamanan Perangkat Keras (*hardware*) dan Perangkat Lunak (*software*)**. Keamanan perangkat keras dan perangkat lunak perlu diperbaiki untuk melindungi sistem dari berbagai ancaman siber, termasuk *malware*, virus, dan eksploitasi kerentanan keamanan. Jenis kerentanan terbanyak khususnya pada Sektor Administrasi Pemerintahan berupa CVE-2006-20001 dengan jumlah serangan 4.687 kali yang memiliki nilai 7,5 dengan tingkat dampak ***HIGH***. Kerentanan ini terjadi pada Apache HTTP *Server* versi 2.4.54 dan sebelumnya. dengan potensi dampak terjadinya *out-of-bounds write*. Sedangkan kerentanan kategori ***CRITICAL*** terbanyak berupa kerentanan CVE-2022-28615, CVE-2022-31813 pada Apache HTTP *Server* dengan potensi dampak penyerang dapat mengakses sistem dan memengaruhi aspek *confidentiality* dan *availability* sistem (BSSN, 2023). Keamanan perangkat dan perangkat lunak berimplikasi pada integritas, kerahasiaan, dan ketersediaan data, serta operasional Kementerian dan Lembaga.

4) **Kurangnya Identifikasi dan Deteksi Dini**. Identifikasi dan deteksi dini merupakan komponen krusial dalam upaya meningkatkan

keamanan siber. Serangan siber yang di Kementerian dan Lembaga dapat terjadi kapan saja, terbukti dengan banyaknya notifikasi serangan siber. Menurut data dari BSSN, periode tahun 2021 sampai bulan Agustus 2023 terdapat notifikasi indikasi seragan siber sebanyak 5.102 kali, sedangkan salah satu bentuk serangan siber yaitu *Ransomware* meningkat 11 detik pada tahun 2021 dan diprediksi akan menyerang perusahaan setiap 2 detik pada tahun 2031[43]. Melihat fakta tersebut, identifikasi dan deteksi dini sangat penting sehingga memungkinkan untuk mengambil tindakan pencegahan atau tanggap cepat dalam mengatasi insiden keamanan.

5) **Lambatnya Tanggapan dan Penanganan Keamanan Siber**. Tanggapan dan penanganan keamanan yang cepat dan efisien terhadap serangan siber merupakan aspek kritis dalam keamanan siber. Keterlambatan dalam menanggapi dan menangani serangan siber dapat menyebabkan dampak destruktif pada keamanan data sensitif atau yang bersifat rahasia pada Kementerian dan Lembaga. Rencana respons dan prosedur tanggap bencana harus disiapkan dengan matang untuk menghadapi serangan siber dengan tepat waktu dan efektif. Hal ini sangat penting mengingat kapasitas Manajemen Krisis pada indeks keamanan siber nasional di Indonesia masih memperoleh skor 20, yang berada di bawah nilai rata-rata global.

6) **Minimnya Perlindungan Data dan Informasi**. Perlindungan data dan informasi merupakan salah satu aspek kritis dalam keamanan siber. Kondisi di Indonesia dapat dikatakan terjadi krisis perlindungan data dan informasi, penyimpanan data dan informasi cukup lemah di Indonesia. Sebagai buktinya, kasus kebocoran data terjadi di sejumlah instansi baik pemerintah maupun swasta seperti kebocoran 2 juta data nasabah BRI Life serta dokumen penting

[43] Dr. Sulistyo. 2023. *Strategi Mewujudkan Ketahanan Siber Nasional*. Paparan disampaikan pada Seminar Ketahanan Nasional Transformasi Digital Indonesia 2045 Lemhannas RI tanggal 24 Agustus 2023

lainnya pada tahun 2021[44]. Data sensitif bahkan rahasia yang disimpan dan ditransmisikan melalui jaringan belum sepenuhnya dilakukan pengamanan dan terenkripsi sehingga berpotensi menimbulkan pencurian data oleh pihak yang tidak bertanggung jawab.

7) **Rendahnya inovasi teknologi**. Hal ini terlihat dari nilai indeks inovasi Indonesia khususnya pada variabel Pengetahuan dan Keluaran Teknologi yang mendapatkan nilai dibawah rata-rata global pada tahun 2022 lalu menurut *WIPO Global Innovation Index*. Berbagai faktor yang menyebabkan rendahnya inovasi teknologi di Indonesia antara lain faktor pendukung yang lemah, pengembangan profesional yang kurang memadai, kolaborasi yang terbatas, minimnya akses informasi, dan faktor budaya seperti resistensi terhadap perubahan dan pengambilan risiko, dalam beberapa kasus, kurangnya penerimaan ide dan solusi baru dapat menghambat inovasi teknologi di Indonesia.

Kondisi belum meratanya infrastruktur digital, kerentanan pada keamanan jaringan, keamanan perangkat keras dan perangkat lunak, kurangnya identifikasi dan deteksi dini serangan siber, lambatnya tanggapan dan penanganan keamanan siber, minimnya perlindungan data dan informasi, serta rendahnya inovasi teknologi pada aspek teknologi di lingkungan Kementerian dan Lembaga berimplikasi terhadap kemampuan pertahanan siber, terjadinya insiden serangan siber serta terhadap rendahnya indeks global terkait keamanan siber antara lain indeks keamanan siber nasional, indeks inovasi global, dan indeks kesiapan digital. Di sisi lain juga berkontribusi pada peningkatan tren serangan siber dan tren anomali trafik.

c. **Regulasi dan Kebijakan**.

Regulasi dan kebijakan menjadi perhatian dalam upaya mengantisipasi serangan siber di Indonesia. Tantangan bidang regulasi

[44]https://www.dpr.go.id/berita/detail/id/34375/t/Perlindungan+Data+Pribadi+di+Indonesia+Dinilai+Masih+Lemah

dan kebijakan dalam keamanan siber di Indonesia meliputi beberapa aspek yang kompleks dan perlu diperhatikan dengan serius. Beberapa tantangan utama yang dihadapi antara lain[45]:

1) **Ketertinggalan Regulasi terhadap Perkembangan Teknologi**. Keamanan siber merupakan isu yang terus berkembang seiring dengan kemajuan teknologi. Tantangan pertama adalah ketertinggalan regulasi terhadap dinamika dan inovasi teknologi yang terjadi dengan cepat. Regulasi dan kebijakan yang ada mungkin belum sepenuhnya mencakup aspek-aspek baru seperti keamanan *Internet of Things* (IoT), keamanan *cloud computing*, atau teknologi terkini lainnya.
2) **Kurangnya Koordinasi antar Kementerian dan Lembaga**. Bidang keamanan siber melibatkan banyak lembaga pemerintah yang memiliki tanggung jawab yang terkait, seperti Kementerian Komunikasi dan Informatika, Kementerian Pertahanan, Kementerian Keuangan, BSSN, BIN dan lain-lain. Dalam hal ini masih belum terdapat mekanisme koordinasi yang efektif antara lembaga-lembaga tersebut untuk memastikan keselarasan dalam mengatasi ancaman siber dan penegakan regulasi yang konsisten.
3) **Regulasi dan Kebijakan Keamanan Siber yang Saling Tumpang Tindih**. Regulasi keamanan siber yang tumpang tindih mengacu pada situasi di mana terdapat beberapa regulasi yang memiliki kewenangan atau tanggung jawab yang serupa dalam mengatur keamanan siber, atau dapat dikatakan tidak adanya koordinasi dan harmonisasi antara berbagai regulasi yang terkait dengan keamanan siber. Hal ini dapat menyebabkan kebingungan, ketidakjelasan, dan bahkan konflik antara lembaga atau badan yang bertanggung jawab. Beberapa contoh tumpang tindihnya regulasi dan kebijakan dalam pertahanan dan keamanan siber antara lain pentingnya menghindari tumpang tindih antara Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan

[45] Ibid.

Siber (RUU KKS) yang sedang disusun dengan regulasi lain seperti UU ITE dan UU PDP, tugas BSSN yang tumpang tindih dengan lembaga lain di mana BSSN memiliki berbagai fungsi terkait dengan keamanan siber, seperti identifikasi, deteksi, proteksi, dan penanggulangan serangan siber, kemudian adanya potensi tumpang tindih aplikasi digital dalam Sistem Pemerintahan Berbasis Elektronik (SPBE). Dalam hal ini, BSSN sangat mendukung penerapan efisiensi aplikasi berdasarkan Perpres RI Nomor 132 Tahun 2022 tentang Arsitektur SPBE Nasional untuk meminimalkan kemungkinan tumpang tindih atau duplikasi aplikasi. Karena dalam domain keamanan, simplikasi aplikasi akan memudahkan dalam penerapan keamanan SPBE, juga penanganan insiden siber. Apabila aplikasi tersebut tumpang tindih maka dapat menghambat efektivitas dan efisiensi kinerja pemerintah pusat dan daerah dalam memberikan pelayanan publik. Sedangkan dari segi keamanannya, terlalu rentan dan berisiko terhadap kejahatan siber[46].

4) **Kompleksitas Sistem Hukum**. Regulasi dan kebijakan di bidang keamanan siber harus sesuai dengan sistem hukum yang ada. Tantangan keempat adalah menghadapi kompleksitas sistem hukum, terutama dalam menghadapi aspek internasional dari ancaman siber, seperti sumber serangan dari luar negeri atau serangan yang melibatkan negara lain.

5) **Pengawasan dan Penegakan Hukum**. Implementasi dan penegakan kebijakan keamanan siber memerlukan sistem pengawasan dan penegakan hukum yang kuat. Tantangan kelima adalah memastikan ada mekanisme yang efektif untuk mengawasi dan menegakkan kepatuhan terhadap kebijakan dan regulasi keamanan siber. Selain itu, juga diperlukan kemampuan untuk menyelidiki dan mengatasi insiden keamanan secara tuntas.

[46] https://bssn.go.id/kepala-bssn-berikan-masukan-pada-rapat-koordinasi-tingkat-menteri-bahas-potensi-tumpang-tindih-aplikasi-spbe/ Diunduh pada tanggal 6 Agustus 2023 pukul 12:29 WIB

6) **Belum adanya Regulasi yang Secara Khusus Mengatur tentang Keamanan Siber**. Pemerintah memang telah mengesahkan dan memberlakukan UU Perlindungan Data Pribadi dan UU ITE untuk mengatasi permasalahan terkait dengan keamanan siber saat ini, akan tetapi kedua UU tersebut masih belum cukup mengingat perkembangan lingkungan strategis saat ini yang berubah dengan cepat, tidak ada kepastian, dan perlu adaptasi.

14. Dampak yang disebabkan oleh Serangan Siber di Kementerian dan Lembaga

Serangan siber dapat memiliki dampak yang serius pada kementerian dan lembaga di Indonesia, baik dari segi operasional, reputasi, maupun keamanan data. Terdapat beberapa serangan siber pada situs resmi pemerintahan di Indonesia, diantaranya kasus peretasan akun YouTube DPR RI yang menampilkan tayangan judi *online* secara *live* dalam dua tayangan pada tanggal 6 September 2023, selain itu foto profil *channel* YouTube DPR juga diganti dengan gambar disertai tulisan 'slot baris'[47]. Kasus peretasan situs resmi pemerintahan lainnya antara lain peretasan situs BPJS kesehatan pada tahun 2021, kebocoran data asuransi BRI Life tahun 2021, serangan *deface website* Sekretariat Kabinet RI tahun 2021, serangan DDoS terhadap situs DPR RI tahun 2020, Kebocoran data e-HAC Kemenkes tahun 2021, kebocoran data pengguna Tokopedia tahun 2020, pembobolan database Polri tahun 2021, Peretasan *channel* YouTube BNPB tahun 2021, dan *Defacing* Situs Telkomsel tahun 2017[48]. Berdasarkan data yang diperoleh dari Badan Intelijen Negara (BIN) di mana BIN melalui Deputi-VI bidang Intelijen Siber telah menempatkan perangkat sensor untuk mendeteksi serangan siber di Kementerian dan Lembaga, pada semester I tahun 2023 jumlah serangan siber yang terjadi sebanyak 121.196.623 serangan. Selama periode enam bulan pertama tahun 2023, serangan siber tertinggi terjadi pada bulan Maret

[47] https://news.detik.com/berita/d-6915636/youtube-dpr-ri-di-hack-tampilkan-live-judi-online Diunduh pada tanggal 27 September 2023 pukul 12:21 WIB
[48] Shinta, Amelia. 2022. *10 Kasus Serangan Hacker yang Pernah Terjadi di Indonesia*. Url: https://www.dewaweb.com/blog/kasus-hacker-di-indonesia/. Diunduh pada tanggal 6 Agustus 2023 pukul 12:34 WIB

sebanyak 24.726.465 serangan, kemudian pada bulan April mengalami penurunan. Pada bulan Mei 2023 serangan siber kembali mengalami peningkatan karena pelaksanaan KTT ASEAN di Labuan Bajo. Sedangkan pada bulan Juni 2023, tren serangan siber kembali menurun dengan jumlah 14.440.709 serangan (BIN, 2023). Jenis serangan siber yang terjadi di Kementerian dan Lembaga di Indonesia antara lain eksploitasi kerentanan sistem keamanan siber dan serangan *malware* (lihat gambar 1 dan 2 Lampiran 3).

Dengan menggunakan analisis PESTLE (*Political, Economic, Social, Technological, Legal, Environmental*), yaitu suatu pendekatan analisis yang digunakan untuk mengidentifikasi dan mengevaluasi faktor-faktor makro lingkungan eksternal yang dapat memengaruhi organisasi maupun bisnis, maka diharapkan Kementerian dan Lembaga di Indonesia dapat mengidentifikasi dampak yang ditimbulkan dari serangan siber. Analisis ini membantu dalam pengembangan strategi yang efektif untuk memperkuat ketahanan nasional terhadap ancaman siber. Serangan siber membawa berbagai dampak pada Kementerian dan Lembaga, berdasarkan analisis PESTLE, dampak-dampak tersebut antara lain sebagai berikut:

a. **Politik**. Serangan siber dapat memiliki dampak yang signifikan pada bidang politik di Indonesia. Beberapa dampak yang mungkin terjadi antara lain:

   1) **Manipulasi Opini Publik**. Serangan siber dapat digunakan untuk menyebarkan informasi palsu, berita hoaks, ataupun propaganda politik yang dapat memengaruhi opini publik. Hal ini dapat mengganggu pandangan masyarakat terhadap isu-isu politik dan elektabilitas kandidat tokoh politik.

   2) **Mengganggu Pertahanan dan Keamanan**. Serangan siber yang menargetkan lembaga pemerintah yang memiliki peran dalam pertahanan atau keamanan nasional memiliki potensi untuk membahayakan kedaulatan dan keamanan suatu negara. Lembaga tersebut memiliki akses terhadap informasi strategis dan rahasia negara yang sangat penting bagi pertahanan dan keamanan nasional. Serangan yang berhasil terhadap lembaga

pertahanan atau keamanan dapat mengakibatkan pencurian informasi rahasia seperti rencana pertahanan, strategi militer, atau rencana taktis. Informasi semacam ini, jika jatuh ke tangan pihak yang tidak sah, dapat membahayakan kemampuan pertahanan nasional. Serangan siber juga dapat memungkinkan penyerang untuk memanipulasi informasi dalam sistem lembaga pertahanan.

3) **Pencurian Data Politik**. Serangan siber yang berhasil dapat mencuri data politik yang sensitif, termasuk strategi kampanye, rencana politik, dan komunikasi internal partai politik. Data ini dapat digunakan untuk merusak reputasi dan mempengaruhi dinamika politik.
4) **Gangguan Pemilihan Umum.** Serangan siber dapat mengganggu integritas dan keamanan pemilihan umum dengan mendistorsi sistem pemilihan elektronik, menyebarkan informasi palsu tentang proses pemilihan, atau mencoba memanipulasi hasil suara.
5) **Polarisasi Politik**. Manipulasi informasi dan opini publik melalui serangan siber dapat menguatkan polarisasi politik dengan memperdalam perpecahan di antara kelompok-kelompok politik.
6) **Ketegangan antar Partai Politik**. Serangan siber yang dilakukan oleh kelompok atau individu yang berafiliasi dengan partai politik tertentu dapat memperburuk ketegangan antarpartai dan meningkatkan konflik politik sehingga berpengaruh pada stabilitas politik nasional.
7) **Gangguan terhadap Komunikasi Pemerintah**. Serangan siber yang mengganggu sistem komunikasi pemerintah dapat menghambat penyampaian kebijakan pemerintah kepada masyarakat.
8) **Ketidakstabilan Pemerintahan**. Serangan siber yang berhasil dapat mempengaruhi operasional pemerintah dan kebijakan publik, selain itu juga mengganggu stabilitas pemerintahan dan penerapan program-program penting.
9) **Ketidakpercayaan pada Institusi Pemerintah**. Serangan siber yang mengungkapkan atau mengganggu praktik korupsi atau

kecurangan dalam politik dapat menurunkan kepercayaan publik terhadap institusi politik dan pemerintahan.

10) **Penggunaan Teknologi untuk Kampanye Negatif**. Serangan siber dapat digunakan untuk kampanye negatif atau serangan personal terhadap kandidat atau pejabat politik, serta mengubah persepsi publik terhadap tokoh politik tersebut.

11) **Ketegangan Internasional**. Serangan siber yang dilakukan dari luar negeri atau terhadap target dengan dampak internasional memiliki potensi besar untuk mengubah hubungan diplomatik dan keamanan nasional. Serangan semacam ini dapat memicu ketegangan diplomatik, merusak hubungan bilateral, mempengaruhi pertimbangan keamanan nasional, memicu respons militer atau keamanan, mengubah dinamika kerjasama internasional dalam bidang keamanan siber, dan bahkan mempengaruhi opini publik serta tindakan politik di negara yang menjadi target.

b. **Ekonomi**. Terhadap aspek ekonomi, insiden serangan siber memiliki dampak signifikan yang dapat mengganggu sistem perekonomian di Indonesia. Dampak tersebut antara lain:

1) **Penghentian Layanan Infrastruktur Vital**. Serangan siber mampu menciptakan dampak serius dengan mengakibatkan gangguan pada layanan infrastruktur vital. Tindakan ini bisa mengacaukan sektor-sektor penting seperti sistem keuangan, transportasi, energi, dan komunikasi, yang menyebabkan terhentinya layanan yang fundamental bagi perekonomian suatu negara.

2) **Gangguan Layanan Publik**. Gangguan pada infrastruktur vital berpotensi merugikan industri, bisnis, dan masyarakat secara keseluruhan, mengganggu aliran perdagangan, menghambat pertumbuhan ekonomi, dan memicu dampak negatif jangka panjang pada stabilitas ekonomi nasional.

3) **Kerugian Finansial**. Terjadinya insiden penipuan *online*, *phishing*, pencurian data nasabah, dan akses ilegal ke rekening perbankan

dapat merugikan masyarakat dalam hal keuangan dan mengganggu aktivitas bisnis.

4) **Kehilangan Data**. Dalam kasus serangan seperti pencurian data atau *ransomware*, baik perusahaan maupun individu berpotensi mengalami kehilangan data berharga. Data tersebut bisa termasuk data pelanggan, informasi rahasia bisnis, dan data pribadi. Kehilangan data tersebut dapat mengganggu operasional jangka panjang dan merusak reputasi.

5) **Penurunan Kepercayaan Publik**. Serangan siber yang berhasil dapat merusak kepercayaan masyarakat terhadap perusahaan, layanan, dan penggunaan *platform online*. Kekhawatiran terhadap keamanan data dapat menghambat adopsi teknologi digital dan e-*commerce*. Lebih lanjut dapat menghambat proses digitalisasi perekonomian.

6) **Penambahan Anggaran untuk Biaya Pemulihan.** Usaha untuk memulihkan suatu kerusakan dari serangan siber membutuhkan biaya yang signifikan. Biaya tersebut meliputi biaya untuk mengamankan sistem kembali, mengembalikan data, membayar tebusan (dalam kasus *ransomware*), dan investasi dalam perangkat keamanan tambahan.

7) **Kerugian Kekayaan Intelektual**. Suatu organisasi dapat mengalami pencurian atau kerusakan pada kekayaan intelektualnya, seperti hak cipta, hak paten, ataupun rahasia dagang. Di mana hal ini dapat menghambat inovasi dan memberikan keuntungan kompetitif kepada pesaing.

8) **Penurunan Investasi Asing**. Serangan siber yang terjadi berulang kali atau membawa dampak besar dapat mengurangi minat investor asing untuk menanamkan modal di Indonesia. Ketidakpastian keamanan siber dapat membuat lingkungan bisnis menjadi kurang menarik dan tidak dapat dikembangkan.

c. **Sosial**. Pada aspek sosial, serangan siber dapat menimbulkan perubahan perilaku sosial dan budaya baik individu maupun organisasi

dalam hal ini Kementerian dan Lembaga. Dampak yang terjadi antara lain:

1) **Kehilangan Reputasi**. Serangan siber yang berhasil dapat merusak reputasi Kementerian atau Lembaga dengan cara menyebabkan kebocoran data atau informasi. Dampak dari kebocoran ini dapat mengakibatkan penurunan kepercayaan publik dan segala bentuk layanannya, serta merusak citra dan integritas yang telah dibangun selama bertahun-tahun.
2) **Ketidakpastian dan Ketidakpercayaan**. Serangan siber memiliki potensi untuk menciptakan ketidakpastian dan ketidakpercayaan di kalangan masyarakat, terutama jika data pribadi warga negara menjadi obyek serangan. Apabila data pribadi berhasil dicuri dalam serangan siber, dapat memengaruhi kepercayaan masyarakat dalam menggunakan teknologi digital.
3) **Penyebaran Hoaks**. Serangan siber dapat digunakan untuk menyebarkan informasi palsu atau hoaks yang dapat mempengaruhi persepsi masyarakat terhadap berbagai isu sosial budaya. Hal ini kemudian berpotensi menyebabkan konflik sosial.
4) **Penyebaran Konten Merugikan**. Serangan siber seperti penyebaran foto atau informasi pribadi yang merugikan dapat merusak reputasi individu atau kelompok dalam skala besar. Hal ini kemudian dapat menyebabkan stigmatisasi sosial dan dampak emosional yang serius.
5) **Gangguan pada Interaksi Sosial**. Serangan siber pada *platform* media sosial atau komunikasi *online* dapat mengganggu interaksi sosial dan budaya yang semakin bergantung pada teknologi digital. Hal tersebut selanjutnya dapat mengurangi hubungan antarindividu secara langsung dan berdampak pada komunikasi budaya.
6) **Polarisasi dan Konflik *Online***. Serangan siber dapat digunakan untuk menguatkan polarisasi dan konflik dalam masyarakat dengan memperbesar prasangka buruk, perbedaan pandangan dan menciptakan ketegangan antar kelompok sosial atau budaya.

7) **Kekhawatiran pada Keamanan Data Pribadi**. Seringnya terjadi insiden serangan siber karena sistem keamanan siber yang lemah dapat membuat masyarakat menjadi lebih waspada terhadap penggunaan teknologi digital dan berbagi informasi pribadi secara *online*. Budaya tersebut dapat mengurangi adopsi teknologi baru dan berdampak pada perkembangan digitalisasi.
8) **Gangguan pada Edukasi *Online***. Serangan siber dapat mengganggu *platform* pendidikan *online* yang semakin penting dalam era digital sehingga berdampak pada akses pendidikan dan pembelajaran masyarakat terhadap teknologi.
9) **Ancaman terhadap Warisan Budaya Digital**. Ancaman tersebut termasuk pada integritas warisan budaya digital, situs-situs bersejarah, arsip digital, dan konten budaya yang penting bagi identitas nasional.
10) **Penurunan Partisipasi Publik dalam Aktivitas Budaya**. Serangan siber yang mengganggu acara budaya atau *platform online* untuk berbagi kreativitas dapat mengurangi partisipasi publik dalam kegiatan budaya.

d. **Teknologi.** Terhadap aspek teknologi, serangan siber dapat mengganggu operasional Kementerian dan Lembaga yang sudah maupun akan menerapkan digitalisasi dalam sistem internalnya. Dampak tersebut antara lain:
1) **Gangguan Ketersediaan Layanan**. Serangan DDoS (*Distributed Denial of Service*) dapat menyebabkan *server* atau situs web menjadi tidak responsif, sehingga layanan yang biasanya tersedia untuk pengguna menjadi tidak dapat diakses.
2) **Kekacauan pada Sistem**. Serangan *malware* atau *ransomware* seperti virus, *worm*, trojan, dan *spyware*, dapat mencuri informasi pribadi pengguna tanpa sepengetahuannya, mengenkripsi data pada sistem komputer atau jaringan, dan kemudian meminta tebusan agar data dapat diakses kembali. Serangan *ransomware* memiliki dampak global, merusak berbagai organisasi dan institusi,

termasuk rumah sakit, perusahaan besar, dan lembaga pemerintah.

3) **Gangguan Komunikasi**. Serangan siber dapat mengganggu kemampuan komunikasi dalam jaringan internal atau eksternal Kementerian dan Lembaga. Komunikasi yang efektif menjadi kunci dalam menjalankan operasional harian karena banyak proses tergantung pada pertukaran informasi yang cepat dan akurat.
4) **Kerusakan Infrastruktur Teknologi.** Serangan siber yang merusak atau menghancurkan sistem komputer dan infrastruktur teknologi dapat mengganggu operasional organisasi, perusahaan, atau lembaga pemerintah. Ini dapat mengakibatkan gangguan signifikan dalam penyediaan layanan teknologi.
5) **Gangguan terhadap Aktivitas Penelitian dan Inovasi.** Serangan siber yang mengincar akademik, laboratorium riset, atau organisasi inovatif dapat menghambat penelitian dan pengembangan teknologi baru sehingga berdampak negatif pada kemajuan ilmiah dan teknologi di Indonesia.
6) **Ketidakstabilan Sistem dan Jaringan.** Serangan siber yang berhasil dapat menyebabkan ketidakstabilan dalam sistem dan jaringan komunikasi, termasuk internet yang dapat memperlambat atau bahkan menghentikan akses *online*, mengganggu aktivitas bisnis dan komunikasi.
7) **Penurunan Inovasi Start-Up dan Perusahaan Teknologi**. Start-up dan perusahaan teknologi sangat rentan terhadap serangan siber, sehingga serangan yang berhasil dapat merusak reputasi, menyebabkan kehilangan pelanggan, dan menghambat pertumbuhan perusahaan baru di bidang teknologi.
8) **Ancaman terhadap Teknologi Transformasional.** Teknologi seperti *Internet of Things* (IoT), kecerdasan buatan (AI), dan kendaraan otonom dapat menjadi target serangan siber yang berpotensi mengancam keamanan dan fungsionalitasnya.
9) **Gangguan terhadap Layanan Publik Digital.** Serangan terhadap layanan publik digital, seperti layanan pemerintah online, dapat

mengganggu akses masyarakat terhadap layanan penting seperti kesehatan, pendidikan, dan administrasi.

e. ***Legal (*Hukum)**. Serangan siber terhadap kementerian dan lembaga di Indonesia memiliki dampak mencakup beberapa dimensi hukum yang melibatkan tanggung jawab, regulasi, dan perlindungan terhadap privasi serta data. Dampak serangan siber dalam aspek hukum antara lain:

1) **Mendorong Penguatan Regulasi Keamanan Siber**. Serangan siber dapat mendorong pemerintah untuk memperkuat kerangka regulasi siber, yang meliputi undang-undang dan peraturan baru yang mengatur perlindungan data dan keamanan siber. Regulasi semacam ini dapat membawa konsekuensi bagi lembaga-lembaga pemerintah.
2) **Pelanggaran Hukum**. Serangan siber yang mencakup pencurian data pribadi, pencurian kekayaan intelektual, atau akses ilegal ke sistem dapat melanggar hukum hak kekayaan intelektual, hukum perlindungan data, dan UU terkait kejahatan siber.
3) **Penyalahgunaan Informasi.** Serangan siber dapat menimbulkan pencurian data yang nantinya dapat disalahgunakan untuk kegiatan ilegal, termasuk identitas palsu, pencurian identitas, atau penipuan *online* di mana hal ini menyebabkan pelanggaran hukum yang serius.
4) **Kewajiban dan Tuntutan Hukum**. Pihak yang terkena dampak serangan siber, baik itu individu atau perusahaan, dapat mengajukan tuntutan hukum terhadap pelaku serangan atau pihak yang dianggap bertanggung jawab terhadap keamanan sistem yang rentan.
5) **Sengketa Kontrak**. Serangan siber yang mengganggu operasional bisnis atau layanan yang diberikan oleh perusahaan dapat mengakibatkan sengketa kontrak antara pihak yang terlibat, baik itu perusahaan dengan pelanggan atau dengan penyedia layanan.
6) **Pengembangan Hukum Kejahatan Siber**. Dampak serangan siber dapat mempercepat perkembangan dan penyesuaian hukum

terkait kejahatan siber di Indonesia. Hukum yang lebih tegas dapat diperlukan untuk menangani ancaman yang berkembang di dunia siber.

7) **Tindakan Investigasi**. Pasca terjadinya serangan siber, tindakan investigasi akan diperlukan untuk mengidentifikasi sumber serangan, menilai dampaknya, dan mengumpulkan bukti. Di mana hal ini melibatkan kerjasama antara sektor publik dan swasta serta penegak hukum.

f. ***Environment*** **(Lingkungan)**. Serangan siber terhadap aspek Lingkungan, tidak memberikan dampak secara langsung. Dampak tersebut antara lain:

1) **Gangguan lingkungan fisik dan infrastruktur**. Serangan semacam ini dapat merusak atau mengganggu infrastruktur teknologi yang mendukung operasional pemerintahan, Dampaknya bisa meluas ke sektor lingkungan fisik seperti penggunaan sumber daya energi yang lebih besar untuk mengatasi dampak serangan dan pemulihan sistem yang terkena dampak, yang pada gilirannya dapat meningkatkan jejak karbon.

2) **Memicu Penggunaan Sumber Daya yang Tidak Efisien dan Berdampak pada Lingkungan**. Serangan siber yang mengganggu sistem informasi dan komunikasi yang digunakan untuk mengelola lingkungan, dapat mengganggu pengambilan keputusan yang berhubungan dengan keberlanjutan lingkungan.

3) **Dampak pada Riset Lingkungan.** Lembaga penelitian dan pengembangan yang menjadi target serangan siber dapat mengalami gangguan pada riset lingkungan dan kehilangan data yang diperlukan untuk memahami tentang perubahan lingkungan guna penyusunan kebijakan terkait lingkungan hidup.

4) **Dampak pada Teknologi Lingkungan.** Serangan terhadap teknologi lingkungan yang digunakan untuk pemantauan, pemrosesan data, atau penilaian dampak lingkungan dapat

menghambat kemampuan untuk merencanakan dan mengelola pengelolaan lingkungan dengan efektif.

5) **Hambatan terhadap Sistem Peringatan Bencana.** Sistem peringatan dini bencana alam yang berhubungan dengan keselamatan masyarakat dapat terganggu dengan insiden serangan siber, sehingga menghambat kemampuan untuk memberikan peringatan yang cepat dan akurat kepada masyarakat.

6) **Terhambatnya Pertumbuhan Teknologi Hijau.** Serangan siber yang mengganggu perkembangan dan implementasi teknologi hijau seperti penggunaan energi baru terbarukan (EBT atau solusi ramah lingkungan dapat menghambat transisi energi pada masyarakat secara berkelanjutan.

Tabel V. Analisis PESTLE Dampak Serangan Siber pada Kementerian dan Lembaga

Politik	Ekonomi	Sosial	Teknologi	Hukum	Lingkungan
• Manipulasi opini publik • Mengganggu pertahanan dan keamanan • Pencurian Data Politik • Gangguan Pemilu • Polarisasi Politik • Ketegangan antar Parpol • Gangguan komunikasi pemerintah • Ketidakstabilan pemerintahan • Ketidakpercaya-an pada institusi pemerintah • Kampanye negatif • Ketagangan internasional	• Layanan infrastruktur Vital berhenti • Gangguan layanan publik • Kerugian finansial • Kehilangan data • Penurunan kepercayaan publik • Penambahan anggaran untuk biaya pemulihan • Kerugian kekayaan intelektual • Penurunan investasi asing	• Kehilangan Reputasi • Ketidakpastian dan Ketidak percayaan • Penyebaran hoaks • Penyebaran konten merugikan • Gangguan pada interaksi sosial • Polarisasi dan Konflik *Online* • Kekhawatiran keamanan data pribadi • Gangguan edukasi *online* • Ancaman warisan budaya digita • Penurunan partisipasi publik dalam aktivitas budaya	• Gangguan ketersediaan layanan • Kekacauan sistem • Gangguan komunikasi • Kerusakan infrastruktur teknologi • Gangguan aktivitas penelitian dan inovasi • Ketidak stabilan sistem dan jaringan • Penurunan inovasi start-up dan perusahaan teknologi • Ancaman teknologi transforma sional • Gangguan layanan publik digital	• Mendorong penguatan regulasi kamsiber • Pelanggaran hukum • Penyalah-gunaan informasi • Kewajiban dan tuntutan hukum • Sengketa kontrak • Pengemba ngan hukum kejahatan siber • Tindakan investigasi	• Gangguan lingkungan fisik dan infrastruktur • Memicu penggunaan SD yang tidak efisien dan berdampak pada lingkungan • Dampak pada riset lingkungan • Dampak pada teknologi lingkungan • Hambatan pada sistem peringatan dini • Hambatan pertumbuhan teknologi hijau

15. Strategi dan Upaya untuk Meningkatkan Pertahanan Siber pada Kementerian dan Lembaga dalam Rangka Mendukung Ketahanan Nasional.

Hasil analisis dampak serangan siber terhadap Kementerian dan Lembaga di Indonesia dengan menggunakan pendekatan PESTLE secara jelas memberikan gambaran mendalam tentang kerentanannya dari berbagai sudut pandang. Dari situ, Kementerian dan Lembaga di Indonesia kemudian perlu mengarahkan upaya mereka dalam membangun pertahanan siber yang efektif. Dalam merumuskan strategi pertahanan siber, penting bagi Kementerian dan Lembaga untuk memperhitungkan perubahan regulasi hukum yang mungkin diperlukan untuk melindungi data dan privasi serta menentukan tanggung jawab hukum dalam skenario serangan siber. Selain itu, strategi pertahanan siber harus mencakup penguatan aspek teknologi untuk menghadapi risiko teknologi yang semakin maju, serta upaya dalam menciptakan kebijakan internal yang mendukung kesadaran dan pelatihan terkait keamanan siber bagi karyawan. Analisis dampak dari berbagai dimensi dalam kerangka PESTLE memberikan panduan yang komprehensif bagi Kementerian dan Lembaga dalam merancang pendekatan yang holistik dan adaptif untuk menjaga integritas dan keamanan sistem digital mereka dalam menghadapi ancaman siber yang terus berkembang.

Selanjutnya, dilihat dari kemampuan pertahanan siber, Kementerian dan Lembaga di Indonesia saat ini masih rentan terhadap serangan siber. Kerentanan digambarkan dengan data dan fakta terkait rendahnya berbagai indeks siber secara global dan terjadinya insiden sebagai dampak dari serangan siber. Kerentanan pertahanan siber dipengaruhi oleh tiga aspek dominan, yaitu SDM, teknologi dan regulasi. Untuk meningkatkan kemampuan pertahan siber diperlukan berbagai stategi dan upaya dengan merujuk kerangka teoretis yang terdiri dari teori penerimaan teknologi, konsep pertahanan siber, konsep pertahanan mendalam, konsep *pentahelix* dan konsep ketahanan nasional. Selain itu juga dengan mempertimbangkan data dan fakta serta kemampuan pertahanan siber Kementerian dan Lembaga saat ini. Strategi dan Upaya juga mempertimbangkan dampak dari serangan siber serta perkembangan lingkungan strategis dengan memanfaatkan peluang dan

menghadapi kendala dalam meningkatkan kemampuan pertahan siber. Strategi dan upaya tersebut disusun berdasarkan aspek, SDM, teknologi dan regulasi.

Peluang yang dapat dimanfaatkan dari perkembangan lingkungan strategis antara lain modernisasi pertahanan siber setiap negara, kerjasama bilateral terkait pengembangan teknologi siber dan pencegahan serangan siber, pesatnya perkembangan ilmu pengetahuan dan teknologi dalam bidang siber, tren pertumbuhan teknologi konektivitas yang cepat sehingga dapat memberikan peluang dalam inovasi teknologi siber, serta ketersediaan SDM usia produktif yang dapat diberdayakan untuk menjadi tenaga ahli bidang siber. Sedangkan kendala yang harus dihadapi antara lain intensitas kejahatan siber yang semakin meningkat dan beragam, penyalahgunaan teknologi AI, penguasaan dan pemahaman teknologi siber di setiap negara yang berbeda-beda, keterbatasan literasi digital, infrastruktur digital dan pemerataan akses teknologi digital.

Peningkatan kemampuan pada aspek SDM, teknologi dan regulasi akan meningkatkan kemampuan pertahanan siber di Kementerian dan Lembaga, selanjutnya pertahanan siber yang kuat akan mendukung ketangguhan ketahanan nasional. Strategi dan upaya yang dapat diimplementasikan dalam meningkatkan kemampuan pertahan siber di Kementerian dan Lembaga dijelaskan sebagai berikut:

a. **Aspek Sumber Daya Manusia.** Peningkatan pertahanan siber untuk mendukung ketahanan nasional di Indonesia memerlukan strategi dan upaya yang kokoh dalam aspek SDM. Aspek SDM memiliki peran untuk meningkatkan indeks global terkait keamanan siber, indeks inovasi global, indeks kesiapan digital, mengantisipasi terjadinya serangan siber dan tren anomali trafik. Sesuai implementasi teori penerimaan teknologi informasi, aspek SDM memegang peranan penting. SDM juga berperan pada konsep pertahanan siber, konsep pertahanan mendalam, konsep *pentahelix* dan konsep ketahanan nasional. Strategi dan upaya yang perlu dilakukan untuk meningkatkan kemampuan pertahanan siber yaitu meningkatkan pemahaman tentang risiko keamanan siber dan praktik keamanan *online*, meningkatkan keterampilan keamanan siber dan

memenuhi kebutuhan SDM yang memiliki keahlian siber serta meningkatkan literasi digital. Strategi dan upaya pada aspek SDM tersebut dapat dijelaskan sebagai berikut:

1) **Rekrutmen dan Seleksi**. Kementerian dan Lembaga bersama dengan BSSN dan BKN melakukan perekrutan yang selektif dan tepat sasaran untuk mengidentifikasi individu dengan potensi dalam bidang keamanan siber. Proses seleksi yang ketat akan membantu memastikan bahwa hanya individu yang berkualitas dan memiliki komitmen terhadap ketahanan siber yang diterima.
2) **Pendidikan dan Pelatihan**. Kementerian Komunikasi dan Informatika (Kemenkominfo) bekerjasama dengan BSSN serta penanggung jawab pertahanan dan keamanan siber di masing-masing Kementerian dan Lembaga dapat melaksanakan pendidikan dan pelatihan untuk meningkatkan kapasitas SDM bidang Siber sebagai langkah kritis dalam memperkuat pertahanan siber. Hal ini meliputi pelatihan dalam deteksi serangan siber, kesadaran keamanan siber, penanganan insiden keamanan siber, penggunaan keamanan perangkat lunak, pengelolaan akses dan kata sandi, pengujian keamanan (*security testing*) dan teknik-teknik keamanan terbaru. Dalam lingkup keamanan siber, SDM mencakup seluruh personel yang terlibat dalam penggunaan teknologi informasi, dari tingkat manajemen hingga level karyawan. Pendidikan dan pelatihan SDM dapat dilakukan dengan memastikan bahwa seluruh personel memiliki pemahaman yang baik tentang ancaman siber dan praktik keamanan yang efektif, meningkatkan pemahaman tentang risiko keamanan siber dan praktik keamanan *online*, meningkatkan keterampilan keamanan siber di kalangan karyawan Kementerian dan Lembaga, serta menambah ketersediaan SDM yang memiliki keahlian di bidang siber.
3) **Mendirikan Sekolah Siber**. KemenPUPR bersama Kemendikbudristek dan BSSN mendirikan sekolah khusus dalam bidang siber yang bertujuan untuk memberikan pemahaman dan

pengajaran guna mencetak SDM yang menguasai segala hal yang berkaitan dengan dunia siber.

4) **Kurikulum Keamanan Siber**. Kemendikbudristek dapat mengintegrasikan konsep dan pengetahuan keamanan siber ke dalam kurikulum pendidikan formal, terutama di institusi pendidikan teknologi informasi. Hal tersebut dapat dijadikan upaya untuk memastikan bahwa para lulusan memiliki pemahaman dasar tentang risiko siber dan praktik terbaik dalam menghadapi ancaman tersebut. Pada kegiatan pendidikan dan pelatihan di Kementerian dan Lembaga perlu disusun kurikulum yang sesuai sehingga dapat menghasilkan SDM yang berkualitas dan dapat menjalankan tugas sesuai harapan.

5) **Sertifikasi Keamanan Siber**. Pemerintah melalui BSSN dan Badan Sertifikasi Nasional (BSN) melakukan sertifikasi keamanan siber bagi para profesional IT, seperti sertifikasi CISSP (*Certified Information Systems Security Professional*) maupun CISM (*Certified Information Security Manager*). Sertifikasi ini akan membantu memastikan bahwa para tenaga profesional memiliki pemahaman dan keterampilan yang diperlukan dalam mengelola keamanan siber. Sertifikasi juga perlu diberikan kepada personel di Kementerian dan Lembaga yang membidangi siber. SDM yang mengawaki organisasi siber harus memiliki kompetensi yang telah dilakukan sertifikasi.

6) **Penyiapan Struktur Jabatan dan Tim Ahli terkait keamanan siber**. Kementerian dan Lembaga dapat menyiapkan struktur jabatan di level Eselon I yang membidangi terkait siber dan merekrut ahli siber untuk mengawaki struktur jabatan tersebut sebagai program jangka pendek. Selain itu juga dapat membentuk tim ahli keamanan siber dengan pendampingan dari BSSN dan Kemenkominfo yang memiliki pengetahuan khusus dalam menghadapi ancaman siber. Tim ini harus siap merespons insiden keamanan dan mengembangkan strategi pertahanan yang efektif. Penyiapan struktur jabatan dan tim ahli terkait keamanan siber

pada Kementerian dan Lembaga diharapkan dapat meningkatkan kemampuan dalam mengatisipasi dan memitigasi serangan siber.

7) ***Reward* dan Pengakuan**. Pimpinan di masing-masing Kementerian dan Lembaga dapat memberikan penghargaan dan pengakuan kepada individu atau tim yang berhasil mencegah atau merespons serangan siber dengan efektif. Upaya ini dapat memotivasi profesional keamanan siber untuk terus berkinerja tinggi dan optimal.

8) **Bekerjasama dengan Sektor Industri, Perguruan Tinggi, dan Institusi Pendidikan**. Langkah strategis ini merupakan implementasi konsep ***Pentahelix***, di mana sektor industri diibatkan dalam pengembangan program pelatihan dan sertifikasi keamanan siber. Hal ini akan memastikan bahwa tenaga kerja yang dihasilkan sesuai dengan kebutuhan industri dan mampu mengatasi ancaman siber yang semakin berkembang. Selain itu juga dilakukan pembinaan hubungan timbal balik antara pemerintah dalam hal ini Kemenkominfo dan BSSN, sektor industri, dan institusi pendidikan lainnya untuk memastikan bahwa kurikulum yang diberikan mengikuti perkembangan terkini dalam teknologi dan keamanan siber. Hal ini sebagai upaya untuk mempersiapkan lulusan dengan pengetahuan yang relevan dan siap untuk berkontribusi dalam pertahanan siber. Kerjasama dengan sektor industri, perguruan tinggi, dan institusi pendidikan tersebut diharapkan dapat meningkatkan pemahaman tentang risiko keamanan siber dan praktik keamanan *online*, meningkatkan ketrampilan keamanan siber dan memenuhi kebutuhan SDM yang memiliki keahlian siber.

9) **Kerjasama dan Kolaborasi Internasional**. Kementerian dan Lembaga bersama dengan Kemenlu dapat berpartisipasi dalam kerjasama internasional untuk bertukar informasi, pelatihan, dan pengalaman dalam menghadapi ancaman siber. Hal ini akan membantu memperluas wawasan dan meningkatkan kemampuan pertahanan siber nasional. Berpartisipasi dalam kerja sama internasional dalam bidang keamanan siber, baik dengan negara

lain maupun organisasi internasional dapat membuka pintu untuk pertukaran pengetahuan, pelatihan bersama, dan respons bersama terhadap ancaman siber lintas negara. Kerjasama dan kolaborasi Kementerian dan Lembaga dengan negara lain dan Lembaga internasional diharapkan dapat meningkatkan pemahaman tentang risiko keamanan siber, meningkatkan pemahaman tentang praktik keamanan *online*, meningkatkan keterampilan keamanan siber dan memenuhi kebutuhan SDM yang memiliki keahlian siber.

10) **Monitoring dan Evaluasi**. Kemenkominfo, BSSN, serta Kementerian dan Lembaga terus melakukan pemantauan dan mengevaluasi efektivitas program-program yang telah diimplementasikan dalam mengembangkan SDM dalam bidang keamanan siber secara berkala. Pengembangan berkelanjutan tersebut diperlukan untuk menghadapi ancaman yang terus berkembang di dunia siber.
11) **Melakukan simulasi Serangan (*Penetration Testing* atau *Ethical Hacking*)**. Simulasi serangan, juga dikenal sebagai pengujian penetrasi atau *ethical hacking*, sebagai bentuk latihan yang didesain khusus untuk mensimulasikan serangan siber oleh pihak yang berwenang dengan tujuan mengidentifikasi kerentanan dalam sistem dan infrastruktur organisasi. Dalam latihan ini, sekelompok ahli keamanan siber akan mencoba mengeksploitasi kerentanan yang ada dalam lingkungan organisasi seperti sistem, jaringan, dan aplikasi. Tujuan dari simulasi serangan adalah untuk mengidentifikasi kerentanan dan celah keamanan yang mungkin ada dalam sistem organisasi, menilai kemampuan deteksi dan respons tim keamanan dalam menghadapi serangan yang sedang berlangsung, menguji efektivitas langkah-langkah keamanan yang telah diimplementasikan, dan mengukur tingkat keamanan dan ketahanan organisasi terhadap serangan dari pihak luar.
12) **Kampanye Kesadaran dan Edukasi**. Melalui peran Kemenkominfo, BSSN, BIN, dan penanggung jawab pertahanan dan keamanan siber di masing-masing Kementerian dan Lembaga

baik di pusat maupun daerah dapat melaksanakan kampanye kesadaran dan edukasi terhadap ancaman siber dan praktik keamanan. Kampanye kesadaran dan edukasi mengenai ancaman siber dan praktik keamanan yang tepat merupakan salah satu langkah penting dalam membangun budaya tanggap terhadap keamanan siber yang kuat di suatu organisasi atau masyarakat. Tujuan dari kampanye ini adalah untuk meningkatkan pemahaman dan kesadaran tentang ancaman siber yang ada, serta memberikan pengetahuan dan keterampilan yang diperlukan untuk melindungi diri dan sistem dari serangan siber. Kampanye kesadaran dan edukasi dalam keamanan siber sangat penting karena *pertama* kesadaran terhadap potensi ancaman siber dan risiko yang dihadapi oleh organisasi dan individu masih minim sehingga kampanye kesadaran membantu meningkatkan pemahaman tentang jenis-jenis serangan siber yang ada, seperti *phishing*, *malware*, peretasan, dan lainnya, sehingga individu lebih waspada dan berhati-hati dalam berinteraksi di dunia digital. *Kedua*, dengan meningkatkan pemahaman tentang praktik keamanan yang benar, orang dapat mengurangi risiko dan kerentanan keamanan yang dapat dimanfaatkan oleh penyerang. Hal ini mencakup praktik penggunaan kata sandi yang kuat, pembaruan perangkat lunak secara teratur, dan pemahaman tentang taktik penipuan yang umum digunakan oleh penjahat siber. *Ketiga*, kampanye kesadaran dan edukasi membantu menciptakan budaya keamanan di mana setiap individu menganggap keamanan siber sebagai tanggung jawab pribadi. Dengan memahami pentingnya tindakan keamanan, individu lebih cenderung untuk mengadopsi praktik keamanan yang baik secara konsisten.

Pelaksanaan kampanye kesadaran dan edukasi keamanan siber dapat dilakukan melalui pelibatan pemerintah, industri swasta/dunia usaha, universitas/akademisi, kelompok masyarakat, dan media sebagaimana implementasi **konsep *Pentahelix***. Pemerintah dalam hal ini Kementerian dan Lembaga terkait dengan

leading sector Kemenkominfo dan BSSN mensosialisasikan regulasi dan kebijakan pemerintah dalam Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber serta regulasi lain yang berhubungan dengan pertahanan siber. Industri swasta/dunia usaha sebagai penyedia jasa layanan siber yang berkontribusi terhadap ekosistem digital, membantu pemerintah dalam kampanye kesadaran dan edukasi keamanan siber. Peran universitas/akademisi sebagai penyedia SDM dan hasil riset yang berguna untuk disosialisasikan kepada masyarakat luas. Komunitas masyarakat berkontribusi dalam pengambilan keputusan dan memperoleh manfaat langsung dari kampanye kesadaran dan edukasi keamanan siber sehingga literasi digitalnya meningkat. Sedangkan peran media baik media *offline* maupun media *online* berkontribusi sebagai sarana media komunikasi untuk penyebarluasan informasi untuk keberhasilan kampanye kesadaran dan edukasi keamanan siber yang menjadi program pemerintah, penyerbarluasan informasi tersebut dapat menyamakan persepsi terhadap keamanan siber dan perlindungan terhadap lingkungan digital.

Aspek SDM memiliki peran penting dalam meningkatan kemampuan pertahanan siber untuk mendukung ketahanan nasional di Indonesia. Melalui strategi dan upaya tersebut diatas dengan tujuan meningkatkan pemahaman tentang praktik keamanan *online*, meningkatkan keterampilan keamanan siber dan memenuhi kebutuhan SDM yang memiliki keahlian siber serta meningkatkan literasi digital. Strategi dan upaya pada aspek SDM tersebut diatas dapat meningkatkan indeks global terkait keamanan siber, indeks inovasi global, indeks kesiapan digital, mengantisipasi terjadinya serangan siber dan tren anomali trafik

b. **Aspek Teknologi**. Langkah strategis dalam aspek teknologi memainkan peran yang sangat penting dalam peningkatan pertahanan siber untuk mendukung ketahanan nasional di Indonesia. Dengan berkembangnya

ancaman siber yang semakin canggih dan kompleks, penggunaan teknologi yang tepat menjadi kunci dalam melindungi infrastruktur dan informasi negara yang bersifat sensitif dan rahasia. Aspek teknologi memiliki peran penting untuk meningkatkan indeks global terkait keamanan siber, indeks inovasi global, indeks kesiapan digital, mengantisipasi terjadinya serangan siber dan tren anomali trafik. Sesuai **teori penerimaan teknologi informasi**, aspek teknologi memegang peranan penting. Aspek teknologi juga berperan pada konsep pertahanan siber, konsep pertahanan mendalam, konsep *pentahelix* dan konsep ketahanan nasional. Strategi dan upaya aspek teknologi yang perlu dilakukan untuk meningkatkan kemampuan pertahanan siber antara lain membangun infrastruktur digital, meningkatkan keamanan jaringan, meningkatkan keamanan perangkat keras dan perangkat lunak, meningkatkan kemampuan identifikasi dan deteksi dini, meningkatkan kecepatan tanggapan dan penanganan keamanan siber, meningkatkan perlindungan data dan informasi dan meningkatkan inovasi teknologi. Strategi dan upaya pada aspek teknologi dapat dijelaskan sebagai berikut:

1) **Pengembangan infrastruktur, Peralatan Keamanan Fisik dan Jaringan.** Kemenkominfo Bersama-sama dengan BSSN dan Kementerian dan Lembaga membangun infrastrukur digital di wilayah terpencil dan tertinggal, menginvestasikan teknologi dalam infrastruktur keamanan jaringan yang tangguh, termasuk *firewall*, IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System*), dan teknologi segmentasi jaringan. Hal ini akan membantu mengisolasi potensi serangan dan mencegah penyebarannya. Penggunaan teknologi perangkat keras yang aman dibutuhkan untuk melindungi peralatan fisik dan jaringan yang penting. Selain itu juga diperlukan implementasi teknologi sensor dan pemantauan keamanan untuk mendeteksi perubahan atau gangguan pada infrastruktur fisik.
2) **Pengembangan Sistem Keamanan Siber**. Untuk meningkatkan pertahanan siber, Kementerian dan Lembaga di Indonesia perlu

membangun dan mengimplementasikan sistem keamanan siber yang kuat dan terintegrasi untuk melindungi infrastruktur kritis, jaringan komunikasi, dan sistem penting lainnya, serta menggunakan berbagai teknologi pertahanan dan keamanan yang canggih. Berikut adalah beberapa teknologi keamanan siber yang perlu diterapkan oleh Kementerian dan Lembaga dengan pengawasan dari Kemenkominfo, BSSN dan BIN:

a) Menerapkan dan selalu meng*update* *Firewall*. *Firewall* berfungsi sebagai penghalang yang melindungi jaringan dari akses yang tidak sah atau lalu lintas berbahaya. *Firewall* yang terkonfigurasi dengan baik dapat membantu melindungi jaringan dari serangan luar dan mencegah penyebaran *malware*.

b) Analisis Data dan *Threat Intelligence*. Analisis data dan *threat intelligence* dapat digunakan untuk mengidentifikasi tren ancaman siber yang baru dan berkembang. Dengan memantau aktivitas siber secara terus-menerus, pihak berwenang di masing-masing Kementerian dan Lembaga dapat lebih cepat merespons serangan dan mengambil tindakan preventif.

c) Keamanan Jaringan dan Pemantauan (*Security Information and Event Management* - SIEM). SIEM membantu mendeteksi aktivitas mencurigakan atau serangan dalam lalu lintas jaringan dan memberikan informasi tentang insiden keamanan yang sedang berlangsung.

e) Penilaian Rentang Ancaman dan Kelemahan Keamanan (*Vulnerability Assessment and Threat Intelligence*). Teknologi ini membantu dalam mengidentifikasi dan mengatasi kerentanan keamanan serta memberikan wawasan tentang ancaman siber yang sedang berkembang.

f) Teknologi Persandian Tingkat Lanjut (*Advanced Encryption Technology*). Penggunaan teknologi enkripsi yang kuat membantu melindungi data saat berada dalam penyimpanan

atau transit, sehingga hanya pihak yang berwenang yang dapat mengaksesnya.

g) Penerapan *security awareness. Security awareness* dapat diterapkan di masing-masing instansi pemerintah dengan dukungan literasi dalam isu siber.

Penerapan teknologi keamanan siber ini harus didukung oleh kebijakan, regulasi, dan SDM yang tepat agar dapat memberikan tingkat perlindungan yang maksimal. Selain itu, Kementerian dan Lembaga juga harus melakukan pembaruan teknologi secara berkala dan melakukan uji coba serta evaluasi untuk memastikan efektivitasnya dalam menghadapi ancaman siber yang terus berkembang.

3) **Melakukan Deteksi Dini dan Respon Cepat.** Hal ini dapat dilakukan dengan menggunakan teknologi analitik canggih dan kecerdasan buatan untuk mendeteksi serangan secara dini dan mengidentifikasi pola perilaku aneh yang mengindikasikan serangan. Sebagai contoh Sistem Deteksi Intrusi (*Intrusion Detection System* - IDS) dan Sistem Pencegahan Intrusi (*Intrusion Prevention System* - IPS). IDS dan IPS membantu mendeteksi dan mencegah serangan siber dengan memonitor dan mengawasi lalu lintas jaringan serta mengambil tindakan pencegahan secara otomatis untuk menghentikan serangan yang mencurigakan. Kemudian teknologi kecerdasan buatan (*Artificial Intelligence - AI*) dan Analisis Big Data yang dapat digunakan untuk mengidentifikasi pola serangan yang kompleks dalam lalu lintas jaringan dan perilaku pengguna yang dapat mengindikasikan serangan dan tidak terlihat oleh metode tradisional. Teknologi ini dapat membantu dalam deteksi dini dan respons yang cepat terhadap serangan.

Selain itu dapat dilakukan pengembangan kapabilitas respons yang cepat dengan memanfaatkan teknologi otomasi dan orkestrasi untuk mengisolasi serangan dan memulihkan sistem dengan cepat dengan mengembangkan model prediktif untuk mengidentifikasi ancaman potensial dan mengambil tindakan pencegahan.

4) **Pengembangan Teknologi dan Keamanan Aplikasi**. Hal ini dapat dilakukan untuk memastikan bahwa perangkat lunak dan aplikasi yang digunakan di berbagai sektor telah mengikuti praktik pengembangan aman dan diuji secara menyeluruh untuk mengidentifikasi kerentanannya. Teknologi analisis statis dan dinamis dapat diterapkan untuk mengidentifikasi kerentanan perangkat lunak secara otomatis. Penerapan teknologi keamanan pada perangkat keras dan perangkat lunak meliputi enkripsi data, solusi deteksi intrusi, pembaruan rutin untuk perangkat lunak, dan penggunaan solusi keamanan untuk perangkat *mobile* dan *endpoint.*

5) **Kriptografi dan Keamanan Data**. Teknologi kriptografi yang kuat digunakan untuk melindungi data penting selama penyimpanan dan transmisi, serta mengembangkan sistem otentikasi ganda dan teknologi identifikasi yang canggih untuk mencegah akses yang tidak sah. Teknologi yang digunakan contohnya Sistem Manajemen Identitas dan Akses (*Identity and Access Management* - IAM). IAM dapat memastikan bahwa hanya orang yang berwenang yang memiliki akses ke sistem dan data tertentu, membantu mencegah akses yang tidak sah dan melindungi informasi sensitif.

6) **Kolaborasi dan Kerjasama dengan Industri Teknologi**. Kementerian dan Lembaga dapat berkolaborasi dengan industri swasta dalam pengembangan dan implementasi solusi keamanan canggih. Banyak perusahaan teknologi memiliki pengetahuan dan sumber daya yang diperlukan untuk membantu meningkatkan pertahanan siber. Membangun hubungan Kerjasama dengan industri teknologi dilakukan untuk mengadopsi solusi keamanan terbaru dan memanfaatkan pengetahuan dan teknologi terkini dalam pertahanan siber, serta mendorong inovasi dalam teknologi keamanan siber melalui kerja sama dengan perusahaan teknologi lokal maupun global.

7) **Kerjasama Internasional**. Kementerian dan Lembaga bersama dengan Kemenlu dapat melakukan hubungan Kerjasama baik

bilateral maupun multilateral dengan negara-negara yang telah mengimplementasikan teknologi pertahanan dan keamanan siber yang canggih dan terbukti mampu mengatasi serangan siber dengan optimal, untuk kemudian diterapkan di Indonesia.

8) **Penggunaan *Open Source* (Sumber Daya Terbuka).** Penanggung jawab pertahanan dan keamanan siber di masing-masing Kementerian dan Lembaga baik di pusat maupun daerah perlu menggunakan *Open source* atau sumber daya yang terbuka dalam mengembangkan teknologi pertahanan sibernya. *Open source* atau sumber daya terbuka merujuk pada perangkat lunak, perangkat keras, atau sumber daya lain yang kode sumbernya (*source code*) tersedia untuk umum dan dapat diakses, dipelajari, dimodifikasi, dan didistribusikan secara bebas oleh siapa saja. Artinya, perangkat lunak *open source* dikembangkan dengan lisensi yang memungkinkan para pengguna untuk melihat kode sumbernya, mengubahnya, dan berbagi kembali hasil modifikasi tersebut dengan masyarakat. Menerapkan *open source* sangat membantu pertahanan siber bagi Kementerian dan Lembaga karena:

   a) Dengan akses terbuka ke kode sumber, para ahli keamanan siber dapat memeriksa dengan cermat perangkat lunak atau sistem yang digunakan. Mereka dapat mengidentifikasi potensi kerentanan keamanan dan secara proaktif dapat memperbaikinya.

   b) *Open source* memberikan transparansi yang tinggi karena siapapun dapat melihat dan memahami bagaimana perangkat lunak atau sistem beroperasi.

   c) Responsivitas terhadap Kerentanan. Jika suatu kerentanan keamanan teridentifikasi, komunitas *open source* dapat segera merespons dan merilis pembaruan keamanan.

   d) Dukungan Komunitas. *Open source* sering kali didukung oleh komunitas yang luas dan beragam dari para pengembang,

ahli keamanan, dan pengguna yang saling berkolaborasi untuk mengidentifikasi dan memperbaiki masalah keamanan.

e) Biaya Implementasi. Tidak adanya biaya lisensi atau biaya penggunaan, sehingga Kementerian dan Lembaga dapat menggunakan solusi *open source* dengan biaya yang lebih rendah.

f) Dukungan Komunitas Global. *Open source* berarti bahwa komunitas global dapat bersama-sama berkontribusi dalam meningkatkan keamanan dan fungsionalitas. Jika suatu masalah diidentifikasi di satu negara, solusi dan pengetahuan tersebut dapat dengan cepat menyebar ke negara-negara lain melalui kolaborasi internasional.

Dengan mengadopsi strategi dan upaya dalam aspek teknologi ini, Indonesia dapat mengembangkan kemampuan pertahanan siber yang lebih kuat dan adaptif dalam menghadapi ancaman siber yang terus berkembang. Kombinasi antara teknologi keamanan yang canggih, analisis data cerdas, dan tindakan preventif akan membantu melindungi infrastruktur digital negara dan mendukung ketahanan nasional.

c. **Aspek Regulasi dan Kebijakan**. Regulasi dan kebijakan yang kuat dapat membentuk kerangka kerja hukum yang memadai untuk mengatasi ancaman siber, mendorong kerjasama, serta memastikan bahwa tindakan yang diambil selaras dengan tujuan strategis negara. Aspek regulasi dan kebijakan diperlukan untuk meningkatkan indeks global terkait keamanan siber, indeks inovasi global, indeks kesiapan digital, serta untuk mengantisipasi terjadinya serangan siber dan tren anomali trafik. Aspek regulasi dan kebijakan mengimplementasikan konsep pertahanan siber, konsep pertahanan mendalam, konsep *pentahelix* dan konsep ketahanan nasional dalam mencegah dan menghadapi serangan siber. Strategi dan upaya aspek regulasi dan kebijakan yang perlu dilakukan untuk meningkatkan kemampuan pertahanan siber antara lain dijelaskan sebagai berikut:

1) **Pembentukan Hukum dan Regulasi Kebijakan Keamanan Siber Nasional**. Dalam hal ini diperlukan peran KemenkumHAM, Kemenkominfo, BSSN, BIN, dan BRIN untuk menyusun regulasi dan kebijakan keamanan siber khusus yang komprehensif dan sesuai dengan perkembangan teknologi serta tren ancaman siber setingkat Undang-undang (UU). UU tersebut kemudian dimasukkan dalam prolegnas untuk kemudian disahkan di DPR RI. Aspek-aspek yang dapat dimasukkan dalam kebijakan dan regulasi keamanan siber antara lain:
   a) Perlindungan Data dan Informasi. Mencakup langkah-langkah enkripsi, pengaturan akses yang tepat, dan pengaturan retensi data yang dapat mengacu pada UU PDP dan UU ITE.
   b) Tindakan Pencegahan. Meliputi kebijakan pembaruan perangkat lunak secara rutin, konfigurasi keamanan yang tepat, pelatihan keamanan bagi personel, serta kebijakan pengelolaan hak akses pengguna dengan cermat.
   c) Penanganan Insiden. Termasuk pelaporan insiden, respons cepat, isolasi dan pemulihan sistem, serta penyelidikan dan analisis insiden untuk mencegah kejadian serupa di masa depan.
   d) Sanksi dan Konsekuensi. Hal ini bertujuan untuk mendorong kesadaran dan kepatuhan terhadap kebijakan keamanan serta memberikan efek pencegahan.
   e) Pelatihan dan Kesadaran. Kebijakan harus menetapkan pentingnya pelatihan keamanan siber bagi seluruh personel dan pengguna teknologi informasi. Kampanye kesadaran juga perlu diadakan secara berkala untuk meningkatkan pemahaman tentang ancaman siber dan praktik keamanan yang tepat.
   f) Pengelolaan Risiko. Mencakup penilaian risiko berkala, identifikasi dan penanganan kelemahan, serta perencanaan dan implementasi tindakan pencegahan dan mitigasi risiko.

g) Kerjasama Lintas Sektor. Kebijakan dapat memperkuat kerjasama lintas sektor, khususnya dengan lembaga keamanan siber nasional, sektor swasta, dan lembaga penegak hukum, untuk pertukaran informasi tentang ancaman dan penanganan keamanan.

2) **Penilaian Risiko dan Identifikasi Keamanan**. Kemenkominfo, BSSN, BIN, dan lembaga audit pertahanan dan keamanan siber di masing-masing Kementerian dan Lembaga baik di pusat maupun daerah dapat melakukan penilaian risiko secara berkala untuk mengidentifikasi kelemahan dan kerentanan dalam infrastruktur yang digunakan. Beberapa langkah yang biasa dilakukan dalam penilaian risiko sebagai berikut:

a) Identifikasi Aset dan Nilai. Dalam hal ini ditentukan aset yang akan dievaluasi, seperti infrastruktur IT, data sensitif, dan proses bisnis kritis serta menilai nilai dan kepentingannya terhadap kelangsungan tugas Kementerian dan Lembaga.

b) Identifikasi Ancaman dan Rentang Ancaman (*Threat Identification and Landscape*). Dengan mengidentifikasi ancaman yang mungkin dihadapi, organisasi dapat mengetahui berbagai jenis serangan yang mungkin terjadi. Sedangkan dengan mengevaluasi rentang ancaman yang ada, organisasi dapat menilai tingkat keamanan yang diperlukan untuk melindungi aset mereka secara efektif. Dengan mengidentifikasi ancaman dan rentang ancaman dengan baik, organisasi dapat meningkatkan tingkat kesiapan mereka dalam menghadapi serangan siber dan memastikan bahwa langkah-langkah keamanan yang diambil sesuai dengan risiko yang ada.

c) Identifikasi kerentanan (*Vulnerability Identification*). Hal ini merupakan langkah penting dalam pertahanan siber karena membantu Kementerian dan Lembaga untuk mengetahui kelemahan yang ada dalam sistem, perangkat lunak, atau infrastruktur yang dapat dieksploitasi oleh para pelaku

kejahatan siber. Dengan mengidentifikasi kerentanan yang ada dalam sistem, organisasi dapat mengetahui area-area yang rentan terhadap serangan siber. Dengan mengetahui risiko yang ada, mereka dapat mengambil tindakan pencegahan dan mitigasi yang tepat untuk mengurangi potensi risiko keamanan. Kemudian, identifikasi kerentanan memungkinkan Kementerian dan Lembaga untuk melakukan pemantauan yang lebih efektif terhadap area-area yang memiliki risiko tinggi. Hal ini memungkinkan deteksi dini terhadap potensi serangan sebelum kerentanan dapat dieksploitasi. Selanjutnya, dengan mengetahui kerentanan, Kementerian dan Lembaga dapat melakukan perbaikan keamanan yang diperlukan untuk mengatasi kelemahan tersebut. Tindakan perbaikan dapat mencakup pembaruan perangkat lunak, pengaturan konfigurasi yang lebih ketat, atau penghapusan kerentanan yang tidak perlu.

d) Analisis Dampak (*Impact Analysis*). Dalam hal ini yaitu menganalisis potensi dampak dari ancaman yang terjadi pada aset, termasuk dampak finansial, operasional, hukum, dan reputasi. Analisis Dampak sangat penting dalam pertahanan siber karena membantu Kementerian dan Lembaga untuk memahami potensi konsekuensi dari serangan keamanan atau insiden yang mungkin terjadi. Serangan keamanan dapat berdampak pada reputasi dan kepercayaan Kementerian dan Lembaga. Dengan analisis dampak, Kementerian dan Lembaga dapat memahami bagaimana serangan tersebut dapat memengaruhi persepsi pelanggan, mitra, dan pemangku kepentingan lainnya. Analisis dampak juga membantu Kementerian dan Lembaga dalam mengantisipasi dampak finansial dari serangan keamanan. Biaya pemulihan, kerugian pendapatan, dan biaya reputasi dapat diestimasi lebih awal untuk membantu perencanaan anggaran keamanan yang tepat.

e) Pengukuran Probabilitas. Mengukur probabilitas terjadinya ancaman atau pengeksploitasi kerentanan tertentu. Pengukuran probabilitas adalah langkah penting dalam pertahanan siber karena membantu Kementerian dan Lembaga untuk memahami tingkat risiko yang terkait dengan potensi serangan atau insiden keamanan. Dengan mengukur probabilitas, Kementerian dan Lembaga dapat mengidentifikasi ancaman yang memiliki kemungkinan terbesar untuk terjadi. Ini memungkinkan Kementerian dan Lembaga untuk memprioritaskan upaya keamanan pada area-area yang memiliki risiko yang paling tinggi. Pengukuran probabilitas juga membantu Kementerian dan Lembaga dalam mengalokasikan sumber daya dan anggaran keamanan dengan bijaksana. Area dengan probabilitas tinggi dapat menerima prioritas dalam alokasi sumber daya untuk meningkatkan pertahanan.

3) **Penyusunan Rencana Tanggap Keamanan (*Incident Response Plan*).** Kementerian dan Lembaga harus membuat dan melakukan pengujian terhadap rencana tanggap keamanan yang jelas dan terstruktur, termasuk prosedur untuk mengidentifikasi, melaporkan, dan menangani insiden keamanan dengan cepat dan efektif. Pendampingan dari Kemenkominfo dan BSSN diperlukan untuk implementasi di masing-masing Kementerian, Lembaga, dan Pemerintah Daerah. Rencana ini harus didesain dengan jelas dan terstruktur untuk memberikan panduan yang jelas kepada tim keamanan dalam menghadapi insiden keamanan dengan cepat dan efektif. Berikut adalah beberapa langkah untuk membuat dan menguji rencana tanggap keamanan:

a) Pembentukan tim tanggap keamanan yang terdiri dari personel yang terlatih dan berpengalaman dalam keamanan siber. Selanjutnya menentukan peran dan tanggung jawab setiap anggota tim, termasuk koordinator, penangan insiden, analis, dan komunikasi publik.

b) Menentukan jenis insiden keamanan yang mungkin terjadi dan mengklasifikasikan kejadian berdasarkan tingkat keparahan dan dampaknya. Misalnya, serangan DDoS, peretasan data, *malware*, dan lain-lain.

c) Menetapkan prosedur untuk melaporkan insiden keamanan secara cepat dan akurat. Selanjutnya menentukan juga mekanisme eskalasi jika insiden memerlukan perhatian lebih lanjut dari pihak yang lebih tinggi di dalam organisasi atau otoritas eksternal.

d) Merencanakan cara untuk mendeteksi dini insiden keamanan dan memastikan respons yang cepat dari tim tanggap keamanan, termasuk penerapan sistem deteksi intrusi (IDS), pemantauan jaringan yang efektif, dan tindakan pencegahan otomatis (IPS).

e) Menetapkan langkah-langkah untuk mengisolasi dan memitigasi dampak insiden keamanan. Hal ini dapat mencakup pembatasan akses, pemutusan koneksi, atau penonaktifan sementara sistem terdampak.

f) Memastikan rencana termasuk prosedur untuk mengumpulkan dan menyimpan bukti terkait insiden keamanan. Ini akan membantu dalam analisis forensik dan investigasi lebih lanjut setelah insiden selesai.

g) Merencanakan komunikasi yang akan dilakukan selama dan setelah insiden dengan menetapkan saluran komunikasi baik internal maupun eksternal.

h) Menentukan langkah-langkah pemulihan setelah insiden selesai dan evaluasi respons tim tanggap keamanan untuk meningkatkan tanggap keamanan di masa depan.

i) Melakukan pengujian terhadap rencana tanggap keamanan secara berkala untuk memastikan kesiapan dan efektivitasnya.

j) Memastikan rencana tanggap keamanan harus selalu diperbarui dan disempurnakan secara berkala berdasarkan

pelajaran dari insiden keamanan dan perubahan dalam lingkungan teknologi dan ancaman siber.

Dengan memiliki Rencana Tanggap Keamanan yang jelas dan terstruktur, Keamanan dan Lembaga dapat meningkatkan kemampuan mereka dalam menghadapi insiden keamanan dan mengurangi dampak negatif yang dapat ditimbulkan oleh ancaman siber. Selain itu, pengujian dan latihan secara berkala akan membantu memastikan bahwa tim keamanan memiliki kesiapan yang tepat dan terlatih dalam menghadapi situasi keamanan yang darurat.

4) **Kerjasama Lintas Sektoral**. Meningkatkan kerjasama antara pemerintah, sektor swasta, lembaga pendidikan, masyarakat, dan memberdayakan peran media dalam Kerjasama ***Pentahelix*** sebagai langkah kunci dalam memperkuat pertahanan siber. Kerjasama lintas sektoral ini memungkinkan semua pihak yang terlibat untuk berbagi informasi, pengalaman, dan sumber daya dalam menghadapi ancaman siber yang semakin kompleks dan lebih luas. Untuk mencapai keberhasilan kerjasama lintas sektoral maka diperlukan komitmen dari semua pihak yang terlibat. Berdasarkan analisis **konsepsi Pentahelix**, Pemerintah harus menyediakan kebijakan dan regulasi yang memfasilitasi kolaborasi tersebut sebagai payung hukum, sementara sektor swasta dan lembaga pendidikan aktif berkontribusi dengan berbagi informasi dan sumber daya. Kelompok masyarakat juga perlu didorong untuk dapat melaporkan dan berpartisipasi dalam upaya keamanan siber baik secara langsung maupun melalui media. Kerjasama lintas sektoral yang efektif, maka ancaman siber dapat dihadapi secara lebih komprehensif dan potensi dampak negatif dapat diminimalisir. Selain itu, kolaborasi ini akan membantu mengidentifikasi tren ancaman yang lebih luas dan mendalam, sehingga semua pihak dapat bersama-sama bekerja menuju pertahanan siber yang lebih tangguh.

5) **Keterlibatan Keamanan Siber dalam Proses Pengadaan Teknologi**. Keterlibatan keamanan siber dalam proses pengadaan teknologi sangat penting untuk memastikan bahwa setiap solusi teknologi yang diadopsi oleh suatu organisasi telah melalui penilaian keamanan yang ketat. Langkah ini merupakan bagian dari praktik keamanan siber yang disebut "*secure by design*" atau "keamanan sejak awal," yang bertujuan untuk mengidentifikasi dan mengatasi potensi risiko keamanan sejak tahap awal perencanaan dan pengadaan teknologi. Dalam penerapannya, apabila teknologi dibeli dari vendor atau pemasok, maka Kementerian dan Lembaga harus melakukan penilaian keamanan terhadap vendor tersebut. Selanjutnya Kementerian dan Lembaga memastikan bahwa dokumen kontrak antara organisasi dan vendor atau pemasok mencakup persyaratan keamanan yang cukup jelas. Termasuk dalam kontrak pernyataan tentang kewajiban vendor untuk melindungi data dan informasi organisasi dengan tingkat keamanan yang sesuai. Langkah selanjutnya adalah melakukan uji penetrasi dan pengujian keamanan untuk menguji keamanan solusi teknologi secara langsung yang melibatkan simulasi serangan untuk mengidentifikasi kerentanan dan melihat sejauh mana solusi dapat bertahan terhadap serangan nyata. Selain itu, penyelenggara wajib memastikan bahwa solusi teknologi dapat diintegrasikan dengan infrastruktur keamanan yang sudah ada di organisasi. Integrasi yang baik memastikan keseluruhan keamanan organisasi ditingkatkan dengan adopsi teknologi baru.

   Regulasi terkait penggunaan teknologi asing juga perlu diperhatikan terutama yang berpotensi mengancam keamanan nasional, hal ini untuk memastikan bahwa teknologi yang digunakan oleh pemerintah dan sektor swasta memenuhi standar keamanan yang diperlukan.

6) **Audit Keamanan Secara Berkala**. Audit keamanan secara berkala merupakan proses evaluasi yang dilakukan untuk menilai efektivitas sistem keamanan, kepatuhan terhadap kebijakan dan

standar keamanan, serta menemukan area-area yang memerlukan perbaikan lebih lanjut. Audit keamanan bertujuan untuk mengidentifikasi potensi risiko keamanan, mengukur kinerja sistem keamanan, dan menilai kepatuhan terhadap kebijakan dan regulasi yang berlaku. Dalam kegiatan ini, tim auditor Kementerian dan Lembaga mengevaluasi apakah sistem dan infrastruktur telah sesuai dengan kebijakan keamanan yang telah ditetapkan oleh organisasi. Dengan melakukan audit keamanan secara berkala, Kementerian dan lembaga dapat meningkatkan tingkat keamanan dan mengidentifikasi potensi risiko keamanan yang dapat diatasi sebelum menyebabkan masalah yang lebih serius. Audit keamanan juga membantu memastikan bahwa sistem dan infrastruktur terus berada dalam kepatuhan terhadap kebijakan dan standar keamanan yang berlaku, sehingga pertahanan siber Kementerian dan Lembaga menjadi lebih tangguh.

Merujuk pada **konsep Ketahanan Nasional**, dengan mengimplementasikan strategi dan upaya tersebut, Kementerian dan Lembaga di Indonesia dapat menciptakan kerangka kerja hukum dan regulasi yang kokoh, serta kebijakan yang mendukung untuk memperkuat pertahanan siber dan mendukung ketahanan nasional. Kombinasi antara pendekatan regulasi, kebijakan, dan penegakan hukum yang efektif akan membantu melindungi negara dari berbagai ancaman siber yang ada. Strategi dan upaya yang dilakukan oleh Kementerian dan Lembaga dalam meningkatkan pertahanan siber tersebut sebagai rangkaian strategi dan taktik yang digunakan untuk melindungi sistem, jaringan, perangkat, dan data dari serangan siber yang merugikan, merupakan implementasi dari **konsep Pertahanan Siber**. Apabila strategi dan upaya guna meningkatkan pertahanan siber dapat dilakukan dengan optimal oleh Kementerian dan Lembaga di Indonesia, maka serangan siber dalam bentuk apapun dapat dicegah, diantisipasi, dan diatasi dengan baik. Lebih lanjut, sebagai implementasi **konsep Pertahanan Mendalam**, Kementerian dan Lembaga dapat mengembangkan pertahanan sibernya pada posisi yang terintegrasi,

meningkatkan kekuatan pertahanan siber di setiap lapisan, penggunaan wilayah tertentu sebagai pertahanan dalam hal ini Kementerian dan Lembaga khususnya yang berada di sektor krusial untuk mampu menangkal serangan siber, serta meningkatkan kemampuan komunikasi dalam Kerjasama lintas sektoral.

BAB IV
PENUTUP

16. Simpulan

Seiring dengan perkembangan ruang siber yang semakin pesat saat ini, serangan siber juga mengalami peningkatan yang signifikan, bentuknya semakin beragam, dan memiliki dampak destruktif yang cukup membahayakan. Hampir semua sektor mengalami serangan siber, salah satunya di sektor Pemerintahan khususnya dalam lingkup Kementerian dan Lembaga. Kemampuan pertahanan siber pada Kementerian dan Lembaga dapat dilihat dari aspek Sumber Daya Manusia (SDM), aspek teknologi, serta aspek kebijakan dan regulasi. Kondisi kemampuan pertahanan siber pada Kementerian dan Lembaga dari aspek SDM, antara lain kurangnya pemahaman tentang risiko keamanan siber, kurangnya pemahaman tentang praktik keamanan *online,* kurangnya keterampilan keamanan siber, minimnya ketersediaan SDM yang memiliki keahlian di bidang siber, dan rendahnya literasi digital. Kondisi kemampuan pertahanan siber pada Kementerian dan Lembaga dari aspek teknologi yaitu masih belum meratanya infrastruktur digital, keamanan jaringan, keamanan perangkat keras dan perangkat lunak yang rentan terhadap serangan siber, kurangnya kemampuan identifikasi dan deteksi dini, lambatnya tanggapan dan penanganan keamanan siber, minimnya perlindungan data dan informasi, serta rendahnya inovasi teknologi. Sedangkan kondisi kemampuan pertahanan siber pada Kementerian dan Lembaga dari aspek regulasi, meliputi ketertinggalan regulasi terhadap perkembangan teknologi, kurangnya koordinasi, regulasi dan kebijakan keamanan siber yang saling tumpang tindih, kompleksitas sistem hukum, lemahnya sistem pengawasan dan penegakan hukum, serta belum adanya regulasi yang secara khusus mengatur tentang keamanan siber.

Serangan siber yang terjadi dapat memiliki dampak yang serius pada Kementerian dan Lembaga baik dari segi operasional, reputasi, maupun keamanan data. Berbagai dampak serangan siber tersebut dapat ditemukan dengan menggunakan analisis PESTLE. Dampak-dampak yang disebabkan oleh serangan siber di Kementerian dan Lembaga dapat menyebabkan

gangguan yang signifikan secara langsung baik dalam bidang politik, ekonomi, sosial, teknologi, hukum maupun pada aspek lingkungan.

Melihat kondisi kemampuan pertahanan siber dari aspek SDM, teknologi, serta kebijakan dan regulasi, kemudian dampak yang disebabkan oleh serangan siber terhadap Kementerian dan Lembaga, maka dalam meningkatkan pertahanan siber pada Kementerian dan Lembaga di Indonesia dalam rangka mendukung ketahanan nasional, dibutuhkan berbagai strategi dan upaya yang dapat diimplementasikan pada ketiga aspek yang menjadi pokok pembahasan yaitu SDM, teknologi, serta kebijakan dan regulasi. Strategi dan upaya tersebut antara lain *pertama* pada aspek SDM dengan melaksanakan rekrutmen dan seleksi, pendidikan dan pelatihan, mengintegrasikan konsep dan pengetahuan keamanan siber ke dalam kurikulum pendidikan formal, terutama di institusi pendidikan teknologi informasi, sertifikasi keamanan siber, penyiapan struktur jabatan dan tim ahli terkait keamanan siber, memberikan penghargaan dan pengakuan kepada individu atau tim yang berhasil mencegah atau merespons serangan siber dengan efektif, bekerjasama dengan sektor industri, perguruan tinggi, dan institusi pendidikan, kerjasama dan kolaborasi internasional, melakukan monitoring dan evaluasi, melakukan simulasi serangan, serta kampanye kesadaran dan edukasi.

Kedua pada aspek Teknologi, dapat dilakukan pengembangan infrastruktur, peralatan keamanan fisik dan jaringan, pengembangan sistem keamanan siber, melakukan deteksi dini dan respon cepat, pengembangan teknologi dan keamanan aplikasi, kriptografi dan keamanan data, kolaborasi dan kerjasama dengan industri teknologi, kerjasama internasional dengan negara-negara yang telah mengimplementasikan teknologi pertahanan dan keamanan siber yang canggih dan terbukti mampu mengatasi serangan siber dengan optimal, dan penggunaan *open source* (sumber daya terbuka).

Ketiga pada aspek Kebijakan dan Regulasi antara lain pembentukan hukum dan regulasi kebijakan keamanan siber nasional, melakukan penilaian risiko dan identifikasi keamanan, penyusunan rencana tanggap keamanan, melakukan kerjasama lintas sektoral, melibatkan keamanan siber dalam proses pengadaan teknologi untuk memastikan bahwa setiap solusi teknologi

yang diadopsi oleh suatu organisasi telah melalui penilaian keamanan yang ketat, dan melaksanakan audit keamanan secara berkala sebagai proses evaluasi pertahanan siber.

17. Rekomendasi

Dalam rangka penguatan pertahanan siber guna mendukung ketangguhan ketahanan nasional diperlukan adanya *political will* dari Pemerintah untuk mempercepat, mengeksekusi dan menjalankan strategi serta upaya pada pembahasan. Dengan demikian rekomendasi yang dapat diusulkan antara lain:

a. DPR RI bersama dengan KemenkumHAM, Kemenkominfo dan BSSN, memasukan RUU Keamanan dan Pertahanan Siber dalam prolegnas, sehingga dapat segera diberlakukan. Beberapa substansi utama dalam UU tersebut adalah perlindungan data pribadi, keamanan siber, regulasi platform *online*, pemberantasan kejahatan digital, kolaborasi dan kemitraan, pendidikan dan kesadaran serta penegakan hukum. Tujuan utama dari UU Siber adalah untuk menciptakan lingkungan digital yang aman, etis, dan teratur.

b. KemenkumHAM dan BSSN menyusun Peraturan Pemerintah (PP) terkait Penguatan BSSN untuk disahkan oleh Presiden RI. Penguatan BSSN mencakup berbagai langkah untuk memastikan bahwa lembaga ini dapat beroperasi dengan optimal dalam mengatasi ancaman siber meliputi penyediaan sumber daya, pembentukan kebijakan dan pedoman keamanan siber, pengawasan dan pengendalian, serta pelatihan dan peningkatan kapabilitas personel serta memiliki kewenangan untuk mengkoordinasikan Kementerian dan Lembaga apabila terjadi serangan siber.

c. Pemerintah melalui Kemenkominfo, Kemendikbudristek, BSSN dan BRIN, serta industri teknologi dalam negeri bekerja sama dalam mendorong kemandirian teknologi di bidang siber. *Stakeholder* terkait harus bekerja sama untuk menggalakkan pembuatan, pengembangan, dan pengelolaan teknologi digital, termasuk perangkat keras, aplikasi dan perangkat lunak, oleh industri dalam negeri. Tujuannya untuk

mengurangi ketergantungan pada teknologi luar, meningkatkan kontrol atas sistem teknologi informasi, dan merangsang pertumbuhan industri teknologi di dalam negara, serta memperkuat keamanan siber nasional dengan memiliki kendali lebih besar terhadap infrastruktur teknologi kritis.

d. Kemenhan dan Panglima TNI memprioritaskan penguatan keamanan dan pertahanan siber di lingkungan TNI. Penguatan tersebut dilakukan dengan pengembangan organisasi, peningkatan SDM yang memadai, pembaruan alutsista serta teknologi untuk menghadapi spektrum ancaman siber dalam konteks pertahanan nasional. Penguatan keamanan dan pertahanan siber di lingkungan TNI sebagai embrio Pembentukan TNI Angkatan Siber, hal ini sebagai langkah antisipasi spektrum ancaman pertahanan dan keamanan di bidang siber serta perang siber di masa mendatang. Angkatan Siber tersebut untuk melengkapi ketiga matra pertahanan di Indonesia yang khusus untuk mengantisipasi dan mengatasi segala bentuk ancaman siber. Dalam hal ini perlu dipersiapkan *roadmap*, dasar hukum, personel dan anggaran yang memadai.

Peserta PPSA XXIV,

Indan Gilang Buldansyah, S.Sos.
No. Peserta 046

DAFTAR PUSTAKA

Buku dan Jurnal Penelitian

Christmartha, Gultom, Aritonang. (2020). *Strategi Pengembangan Sumber Daya Manusia Siber Nasional Guna Mendukung Pertahanan Negara*. Jurnal Pemikiran dan Penelitian Manajemen Pertahanan. Unhan

Farizy, Salman. 2020. *Keamanan Sistem Informasi*. Unpam Press. Jakarta

Frost and Sullivan. 2018. *Cybersecurity in ASEAN: An Urgent Call to Action*, ATKearney

Muhammad Yaumi. 2018. *Media Dan Teknologi Pembelajaran*, Cetakan Pertama. Jakarta: Prenadamedia Group

Stalling, Williams. 2015. *Computer Security (Principles and Practices)*. Pearson. New Jersey

Siti Paramadita et.al. 2020. *Analisis PESTLE Terhadap Penetrasi Gojek Di Indonesia*. Jurnal Pengabdian dan Kewirausahaan- Vol. 4 No. 1 2020

Tim Pokja Geostrategi Indonesia dan Ketahanan Nasional. 2023. *Bahan Ajar Bidang Studi Geostrategi Indonesia dan Ketahanan Nasional*. Jakarta: Lemhannas RI

BPS. 2022. *Laju Pertumbuhan Penduduk Tahun 2020-2022*. Jakarta: BPS RI

BSSN. 2020. *Laporan Hasil Monitoring Keamanan Siber Tahun 2020*. Jakarta: BSSN RI

Ditjen Strahan Kementerian Pertahanan. 2021. *Perkembangan Lingkungan Stategis Tahun 2021*. Jakarta: Kementerian Pertahanan RI

Tanya Sammut-Bonnici and David Galea. 2015. *PEST Analysis.* Wiley Encyclopedia of Management, edited by Professor Sir Cary L Cooper

Tzeng, Yusio. 2022. *China's Military Modernization in Autonomous, Cyber, and Space Weapons*. Meeting China's Emerging Capabilities Countering Advances in Cyber, Space, And Autonomous Systems. The National Bureau of Asian Research

Peraturan Perundang-undangan

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara

Undang-Undang RI nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam Undang-Undang RI nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang RI nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang RI Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP)

Peraturan Presiden RI Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN)

Peraturan Presiden RI Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital

Peraturan Presiden RI Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

Peraturan Menteri Pertahanan RI Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber

Paparan Narasumber

Dr. Rudi Rusdiah BE, M.A. 2023. *Geopolitik Digital: Implikasi & Tantangan Keamanan Big Data dalam era Transformasi Digital 2045*. Paparan disampaikan pada Seminar Ketahanan Nasional Transformasi Digital Indonesia 2045 Lemhannas RI tanggal 7 Agustus 2023

Dr. Sulistyo. 2023. *Strategi Mewujudkan Ketahanan Siber Nasional*. Paparan disampaikan pada Seminar Ketahanan Nasional Transformasi Digital Indonesia 2045 Lemhannas RI tanggal 24 Agustus 2023

Prof. Ir. Teddy Mantoro, MSc, PhD, SMIEEE. 2023. *Akselerasi Transformasi Digital, Infrastruktur Digital, dan Ekosistem Digital Dalam Mewujudkan Transformasi Digital Indonesia*. Disampaikan pada Diskusi Panel BS Strategi dengan tema Strategi Percepatan Transformasi Digital untuk Pembangunan Nasional yang Berkelanjutan, PPSA XXIV Lemhannas RI tanggal 6 Juli 2023

Rujukan *Online*

https://datareportal.com/reports/digital-2023-indonesia. Diunduh tanggal 12 Juni 2023 pukul 21:13 WIB

https://bssn.go.id/annualreport2022/ Diunduh tanggal 10 Juni 2023 pukul 10:14 WIB

https://swa.co.id/swa/trends/technology/waspada-tren-serangan-siber-di-2023-lebih-mutakhir Diunduh tanggal 10 Juni 2023 pukul 10:23 WIB

https://kbbi.web.id/tingkat Diunduh tgl 10 Juni 2022 pukul 13:46 WIB

https://aws.amazon.com/id/what-is/cybersecurity/ Diunduh tgl 10 Juni 2022 pukul 13:51 WIB

https://jdih.kemenkeu.go.id/fulltext/2010/479~KMK.01~2010KepLamp.pdf https://indonesiabaik.id/infografis/pengguna-internet-di-indonesia-makin-tinggi Diunduh pada 11 Juni 2023. Pukul 09:46 WIB

https://www.bbc.com/indonesia/articles/cn01gdr7eero Diunduh tanggal 4 Juli 2023 pukul 15:26 WIB

https://hypernet.co.id/id/2023/03/09/cybercrime-dan-6-fakta-menariknya/, Diunduh tanggal 5 Juni 2023 pukul 20.15 WIB

https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan, Diunduh tanggal 5 Juni 2023 pukul 20.45 WIB

https://www.dw.com/id/perang-siber-infrastruktur/a-64063719 Diunduh tanggal 7 Juni 2023 pukul 18.28 WIB

https://www.antaranews.com/berita/2737877/mewaspadai-dampak-serangan-siber-perang-rusia-ukraina Diunduh tanggal 10 Juni 2023 pukul 09.21 WIB

https://www.bps.go.id/indicator/12/1976/1/laju-pertumbuhan-penduduk.html, Diunduh tanggal 20 Juni 2023 pukul 09.57 WIB.

https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62 Diunduh tanggal 5 Juli 2023 pukul 19:24 WIB

https://www.republika.id/posts/20379/urgensi-sdm-keamanan-siber Diunduh tanggal 11 Juli 2023 pukul 16:09 WIB

https://www.medcom.id/nasional/politik/8Kyzja2N-bssn-dibutuhkan-18-ribu-personel-sdm-untuk-keamanan-siber Diunduh tanggal 11 Juli 2023 pukul 17:01 WIB

https://news.detik.com/berita/d-6770000/mahfud-kutip-data-pemenuhan-literasi-digital-di-indonesia-sangat-rendah Diunduh tanggal 13 Juli 2023 pukul 15:10 WIB

https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62 Diunduh tanggal 13 Juli 2023 pukul 15:16 WIB

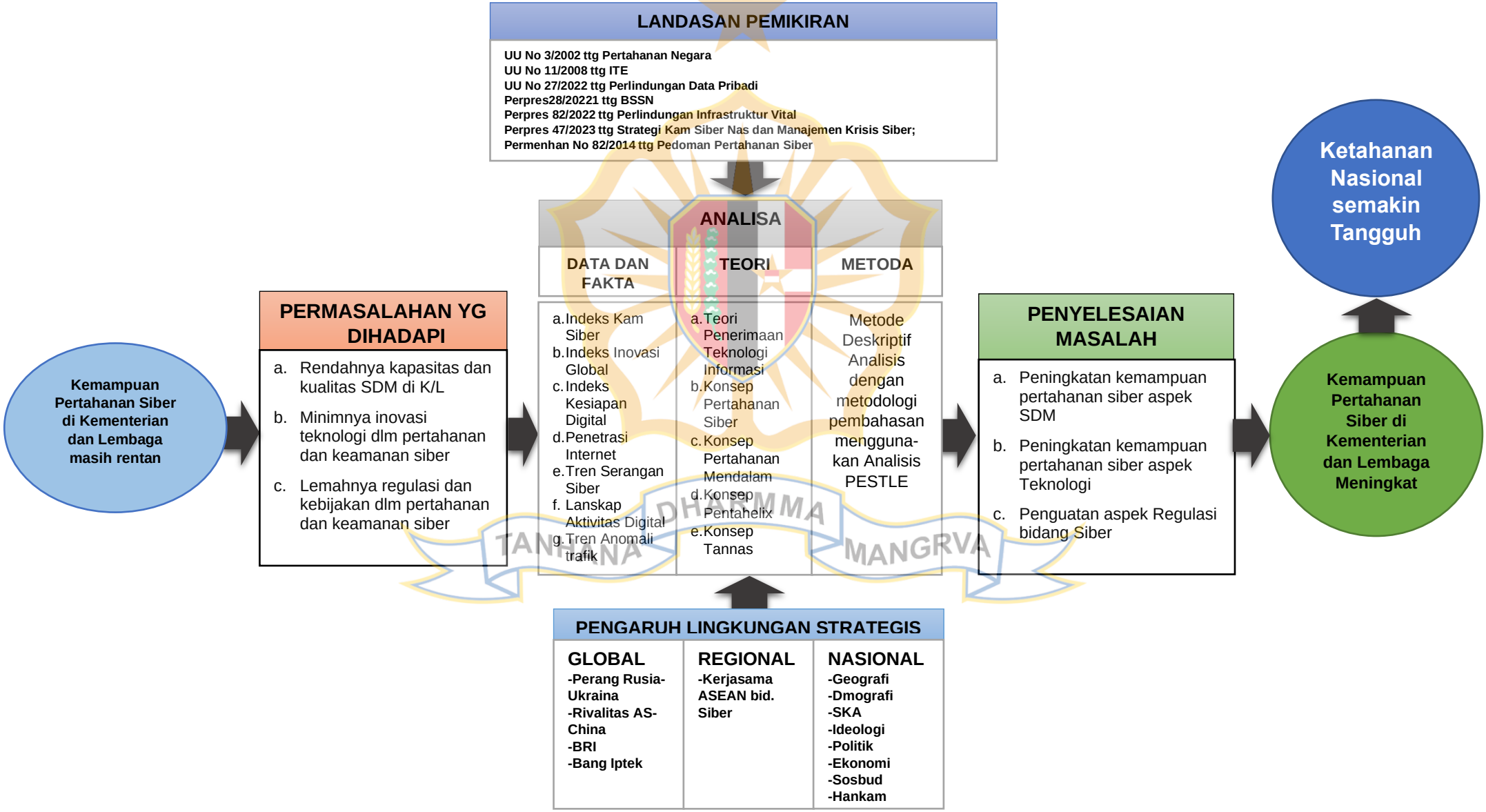
https://www.trade.gov/market-intelligence/indonesia-digital-economy-opportunities Diunduh tanggal 15 Juli 2023 pukul 20:06 WIB

https://bssn.go.id/kepala-bssn-berikan-masukan-pada-rapat-koordinasi-tingkat-menteri-bahas-potensi-tumpang-tindih-aplikasi-spbe/ Diunduh tanggal 15 Juli 2023 pukul 22:34 WIB

Shinta, Amelia. 2022. *10 Kasus Serangan Hacker yang Pernah Terjadi di Indonesia*. Url: https://www.dewaweb.com/blog/kasus-hacker-di-indonesia/. Diunduh pada tanggal 6 Agustus 2023 pukul 12:56 WIB

ALUR PIKIR **LAMPIRAN 1**

PENINGKATAN PERTAHANAN SIBER
DALAM RANGKA MENDUKUNG KETAHANAN NASIONAL



LAMPIRAN 2

DAFTAR RIWAYAT HIDUP

DATA POKOK

a. NAMA : INDAN GILANG BULDANSYAH
b. PANGKAT / NRP : MARSEKAL PERTAMA TNI
c. NO HP/EMAIL : 081221111195/indan_gilang@yahoo.com

PENDIDIKANUMUM

a. SDN1 CIMAHI : 1980 – 1986
b. SMPN 1 CIMAHI : 1986 – 1989
c. SMAN 2 BANDUNG : 1989 – 1992
d. S1 Administrasi Niaga : 2004

PENDIDIKAN MILITER

AKADEMI ANGKATAN UDARA	ANGKATAN 1995
SEKBANG LIV	TAHUN 1997
SEKKAU	ANGKATAN KE 75 TAHUN 2004
IMAA	TAHUN 2004
SIP	ANGKATAN KE 56 TAHUN 2006
SESKOAU	ANGKATAN KE 46 TAHUN 2009
SESKO TNI	ANGKATAN KE 46 TAHUN 2019

PENGANGKATAN/ KENAIKAN PANGKAT

LETNAN DUA	TMT 27 JULI 1995
LETNAN DUA PENERBANG	TMT 24 JUNI 1997
LETNAN SATU PENERBANG	TMT 1 OKTOBER 1998
KAPTEN PENERBANG	TMT 1 OKTOBER 2001
MAYOR PENERBANG	TMT 1 APRIL 2007
LETKOL PENERBANG	TMT 1 OKTOBER 2011
KOLONEL PENERBANG	TMT 1 OKTOBER 2015
MARSEKAL PERTAMA	TMT NOVEMBER 2020

PENGALAMAN JABATAN

PA PNB SKD 6 LANUD ATS	TMT 1 JULI 1998
KOMANDAN SKADIK 104 WINGDIK TERBANG	TMT 13 MARET 2010
DANLANUD WIRIADINATA TASIKMALAYA	TMT 23 JULI 2012
PABANDYA-2/DALOPS SPABAN IV/OPS SOPS MABES TNI	TMT 27 MARET 2014
ASPERS KOSEKHANUDNAS I	TMT 10 APRIL 2015
KADISOPS LANUD ADISUTJIPTO	TMT 29 APRIL 2016
KSD MINPA DISMINPERSAU	TMT APRIL 2017

DANLANUD ADI SOEMARMO	TMT FEBRUARI 2017
ASREN KOOPSAU I	TMT DESEMBER 2019
PABAN IV RENPROGAR SRENUM TNI	TMT JULI 2020
KADISPENAU	TMT 27 NOV 2020

TANDA JASA/KEHORMATAN

GOM IX RAKSAKA DHARMA
GOM IX RAKSAKA DHARMA ULANGAN 1
GOM IX RAKSAKA DHARMA ULANGAN 2
KESETIAAN VIII TAHUN
KESETIAAN XVI TAHUN
KESETIAAN XXIV TAHUN
DHARMA NUSA
DHARMA NUSA ULANGAN 1
SATYA LENCANA DWIDYA SISTHA
SATYA LENCANA DWIDYA SISTHA ULANGAN 1
SATYA LENCANA WIRA KARYA
SBP NARARYA
SATYA LENCANA YUDHA DHARMA

PENGHARGAAN

PENGHARGAAN GUBERNUR AAU LULUSAN TERBAIK AAU 1995 JURUSAN TEKNIK INDUSTRI
PENGHARGAAN DANSEKKAU LULUSAN TERBAIK SEKKAU A-75 TAHUN 2004
PENGHARGAAN DANSESKOAU LULUSAN TERBAIK SESKOAU A-46 TAHUN 2009
PENGHARGAAN DARI MENLU RI DLM RANGKA MISI EVAKUASI WNI DARI NEPAL TAHUN 2015

PENGALAMAN PENERBANGAN

INSTRUKTUR PENERBANG
PENERBANG UJI FUNGSI AS-202 BRAVO, S-58 T TWINPAC, NAS-332 SUPER PUMA.
CAPTAIN PILOT S-58 T TWINPAC, NAS-332 SUPER PUMA (MILITARY DAN VVIP), BO-105 BOLCOW.
PIC AS-202 BRAVO, T-34 CHARLE, KT-1 WOONG BEE.

RIWAYAT PENUGASAN OPERASI

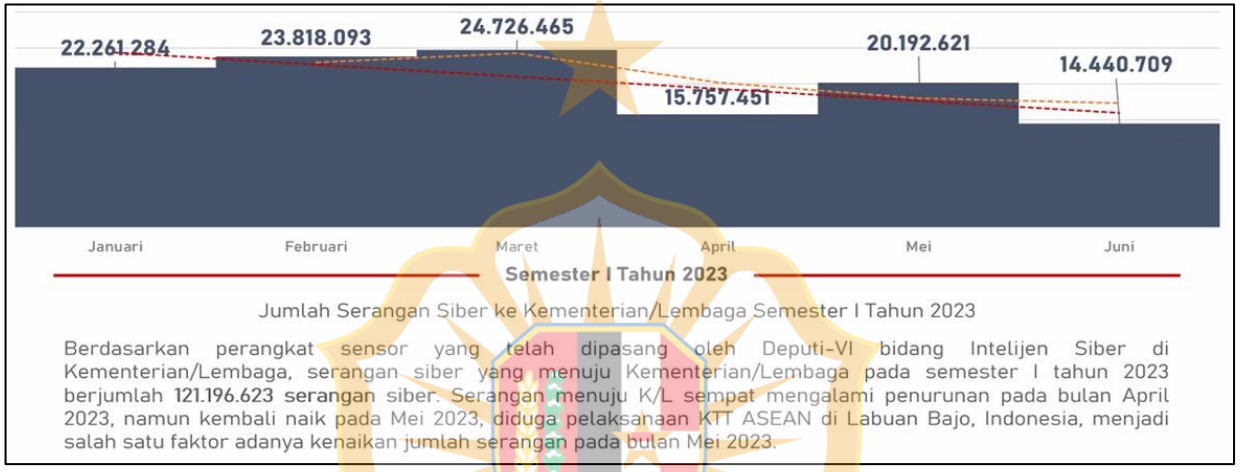
OPS CENDRAWASIH/RAJAWALI DI IRJA/PAPUA
OPS DHARMA NUSA (NAD)
OPS LIMKAM NAD
OPS BHAKTI TNI TSUNAMI NAD DAN NIAS

PENUGASAN LUAR NEGERI

LATMA ELANG MALINDO KUANTAN MALAYSIA	TAHUN 2004
AS 332 SUPER PUMA SIMULATOR EXC DI SINGAPURA	TAHUN 2004
JUNIOR OFFICER EXCHANGE VISIT DI SINGAPURA	TAHUN 2009
EIS OFFICER KUALA LUMPUR MALAYSIA	TAHUN 2010
TIM RECCE VISIT SATGAS HELI TNI DI MINUSMA MALI AFRIKA BARAT	TAHUN 2014
AGG DELEGASI BASARNAS PADA PERANCANGAN LATIHAN SAR BASARNAS – SAR MALAYSIA	TAHUN 2014
AGG DELEGASI NEGOISASI SATGAS HELI TNI DI MINUSMA DENGAN UN DI UN HEADQUARTERS NEW YORK USA	TAHUN 2014
EIS OFFICER THAILAND	TAHUN 2014
SUPERVISOR EVAKUASI WNI DARI YAMAN	TAHUN 2015
KOMANDAN MISI PENCARIAN DAN EVAKUASI WNI DARI NEPAL	TAHUN 2015

LAMPIRAN 3

SERANGAN SIBER DI KEMENTERIAN DAN LEMBAGA DI INDONESIA



Jumlah Serangan Siber ke Kementerian/Lembaga Semester I Tahun 2023

Berdasarkan perangkat sensor yang telah dipasang oleh Deputi-VI bidang Intelijen Siber di Kementerian/Lembaga, serangan siber yang menuju Kementerian/Lembaga pada semester I tahun 2023 berjumlah **121.196.623 serangan siber**. Serangan menuju K/L sempat mengalami penurunan pada bulan April 2023, namun kembali naik pada Mei 2023, diduga pelaksanaan KTT ASEAN di Labuan Bajo, Indonesia, menjadi salah satu faktor adanya kenaikan jumlah serangan pada bulan Mei 2023.

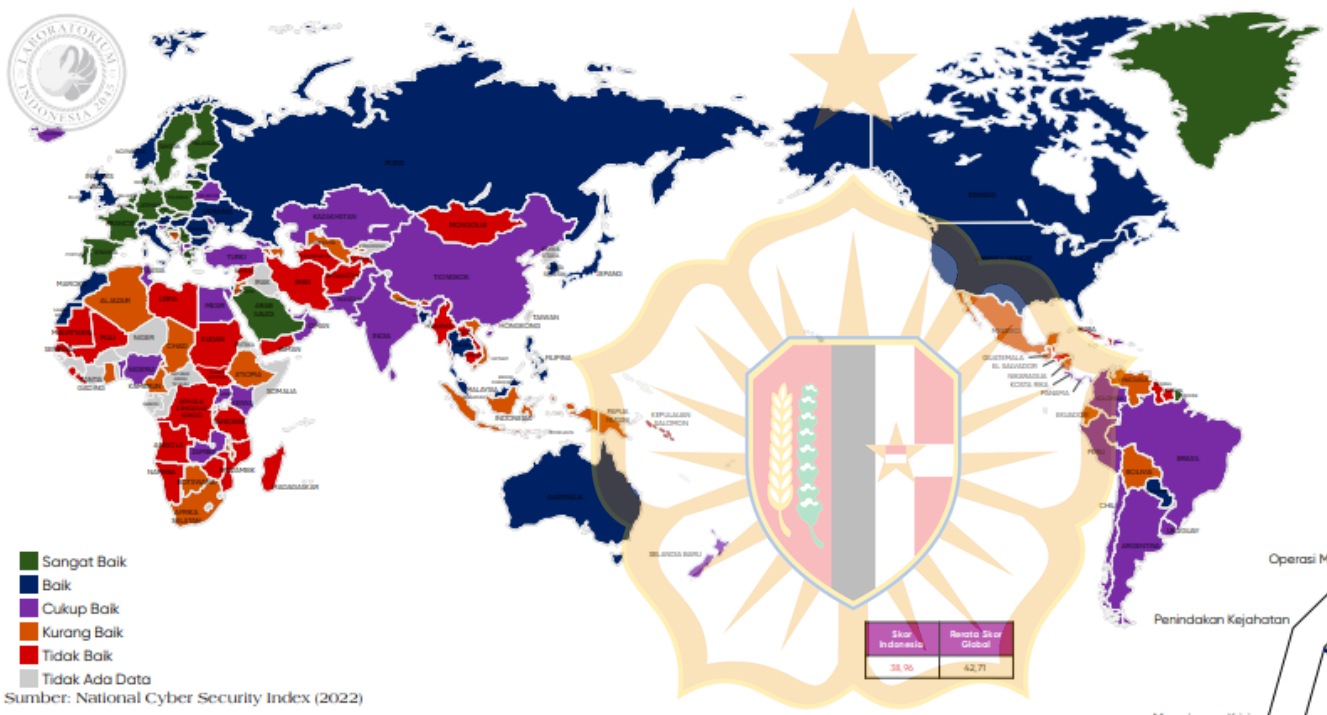
LAMPIRAN 4

CAPAIAN INDONESIA DALAM BIDANG SIBER

Indeks	Variabel	Skor Indonesia terhadap Rerata Global	Posisi Indonesia	Indikator
National Cyber Security Index	E-ID & TS	89 (IDN); 52 (GLB)	Sangat Baik	*Implementasi unique persistent identifier*; protokol *cryptosystem*; *e-Identification*; tanda tangan elektronik; *timestamping*; sistem logistik teregistrasi elektronik; kompetensi otoritas terkait
National Cyber Security Index	Penindakan Kejahatan	78 (IDN); 59 (GLB)	Baik	Kriminalisasi kejahatan siber; Operasional unit penindakan kejahatan siber; unit forensik digital; 24/7 hotline kejahatan siber
	Respons Insiden	67 (IDN); 51 (GLB)	Baik	Operasional unit pengelolaan insiden siber; pelaporan penanggulangan siber rutin; unit tunggal untuk koordinasi insiden siber global
	Operasi Militer	33 (IDN); 27 (GLB)	Baik	Operasional unit militer siber; Pelaksanaan latihan militer siber; partisipasi dalam latihan siber pertahanan siber internasional
Global Innovation Index	Kepuasan Pasar	48,5 (IDN); 47,6 (GLB)	Baik	Kredit; Investasi; Perdagangan, Diversifikasi, dan Skala Pasar
National Cyber Security Index	Pendidikan	44 (IDN); 50 (GLB)	Buruk	Pendidikan kompetensi siber di sekolah; Ketersediaan program sarjana-master-doktoral siber; Asosiasi keamanan siber
	Data Pribadi	25 (IDN); 64 (GLB)	Buruk	Regulasi perlindungan data pribadi; Kompetensi otoritas terkait
	Manajemen Krisis	20 (IDN); 25 (GLB)	Buruk	Penetapan Rencana mitigasi krisis siber; Latihan krisis siber nasional; Partisipasi dalam latihan krisis siber internasional
	Layanan Digital	20 (IDN); 27 (GLB)	Buruk	Operasional layanan publik keamanan siber; Protokol ; Kompetensi otoritas
	Ancaman	20 (IDN); 38 (GLB)	Buruk	Mekanisme analisis ancaman siber rutin; publikasi laporan ancaman siber berkala; operasional kanal informasi ancaman siber
	Kontribusi Global	17 (IDN); 30 (GLB)	Buruk	Partisipasi dalam perumusan konvensi keamanan siber; Kehadiran di forum internasional; Tuan rumah kegiatan internasional; Melaksanakan kegiatan capacity building keamanan siber untuk negara lain
Global Innovation Index	Infrastruktur	41,4 (INA); 41,48 (GLB)	Buruk	Teknologi Informasi dan Komunikasi (TIK); Infrastruktur umum; Keberlanjutan ekologi
	SDM dan Penelitian	22,4 (INA); 32,7 (GLB)	Buruk	Pendidikan; Pendidikan tersier; pengembangan dan riset
	Pengetahuan dan Keluaran Teknologi	16,3 (INA); 24,06 (GLB)	Buruk	Penciptaan pengetahuan; Dampak pengetahuan; Difusi pengetahuan
	Keluaran Kreatif	18,3 (INA); 26,51 (GLB)	Buruk	Aset tak berwujud; Jada dan produk kreatif; Kreativitas online
National Cyber Security Index	Layanan Esensial	0 (IDN); 29 (GLB)	Sangat Buruk	Identifikasi operator; Protokol operator; Kompetensi otoritas pengawas; Pemantauan reguler
	Kebijakan	0 (IDN); 40 (GLB)	Sangat Buruk	Operasional unit kerja; forum koordinasi; strategi nasional; rencana aksi keamanan siber
Global Innovation Index	Institusi	51,2 (INA); 64,94 (GLB)	Sangat Buruk	Lingkungan politik; Lingkungan regulasi; Lingkungan Bisnis
	Kepuasan Bisnis	17,5 (INA); 29,76 (GLB)	Sangat Buruk	Pengetahuan pekerja; Keterkaitan inovasi; Penyerapan pengetahuan

LAMPIRAN 5

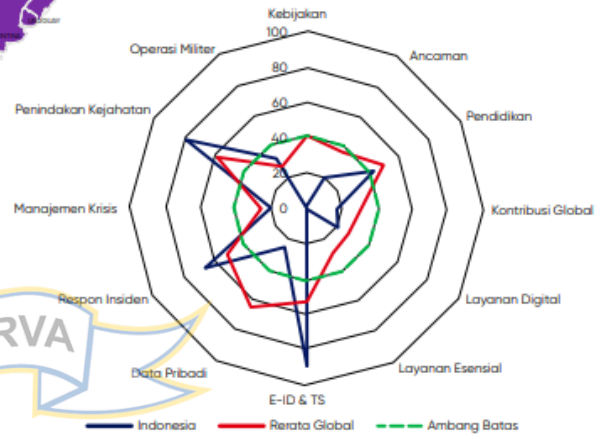
INDEKS KEAMANAN SIBER NASIONAL (2022)



Menurut penilaian *National Cyber Security Index* (NCSI), kapasitas keamanan siber **Indonesia** berada di kategori **kurang baik**.

Indonesia memiliki skor NCSI 38,96 yang berada di bawah rerata global.

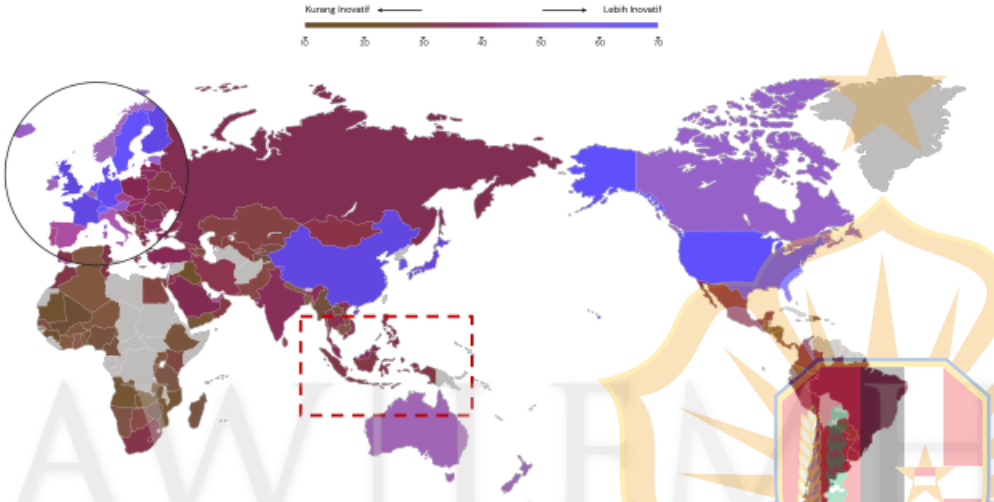
Indonesia memiliki skor di bawah rerata global pada



delapan kapasitas keamanan siber, yakni Kebijakan, Ancaman, Pendidikan, Kontribusi Global, Layanan Digital, Layanan Esensial, Data Pribadi, dan Manajemen Krisis. Di sisi lain, Indonesia memiliki skor di atas rerata global untuk empat kapasitas, yakni Identitas Digital dan Layanan Kepercayaan (E-ID & TS), Respons Insiden, Penindakan Kejahatan, dan Operasi Militer.

LAMPIRAN 6

INDEKS INOVASI GLOBAL INDONESIA (2022)



Indonesia menempati peringkat **87** dari 132 negara pada *Global Innovation Index* (GII). Nilai rata-rata agregat Indonesia (55,3) di bawah rata-rata global (58,2). Negara yang memiliki peringkat dekat dengan Indonesia adalah Uzbekistan dan Paraguay.

Penilaian ini menunjukkan Indonesia belum mampu menunjang dan memproduksi aktivitas atau produk inovatif. Terdapat enam variabel dari Indonesia yang harus diperbaiki antara lain: 1) Kepuasan bisnis; 2) Pengetahuan dan keluaran teknologi; 3) Keluaran kreativitas; 4) Institusi; 5) Penelitian dan SDM; dan 6) Infrastruktur.

Dengan membandingkan skor Indonesia dengan rata-rata global, **hanya variabel kepuasan pasar (48,5) yang mampu melampaui skor rata-rata dunia** (47,6). Variabel Institusi menempati skor tertinggi, namun aspek tersebut memiliki rentangan terjauh dengan rata-rata dunia dibandingkan lainnya. Variabel **keluaran kreatif menjadi aspek dengan skor terendah** dengan nilai 17,5.

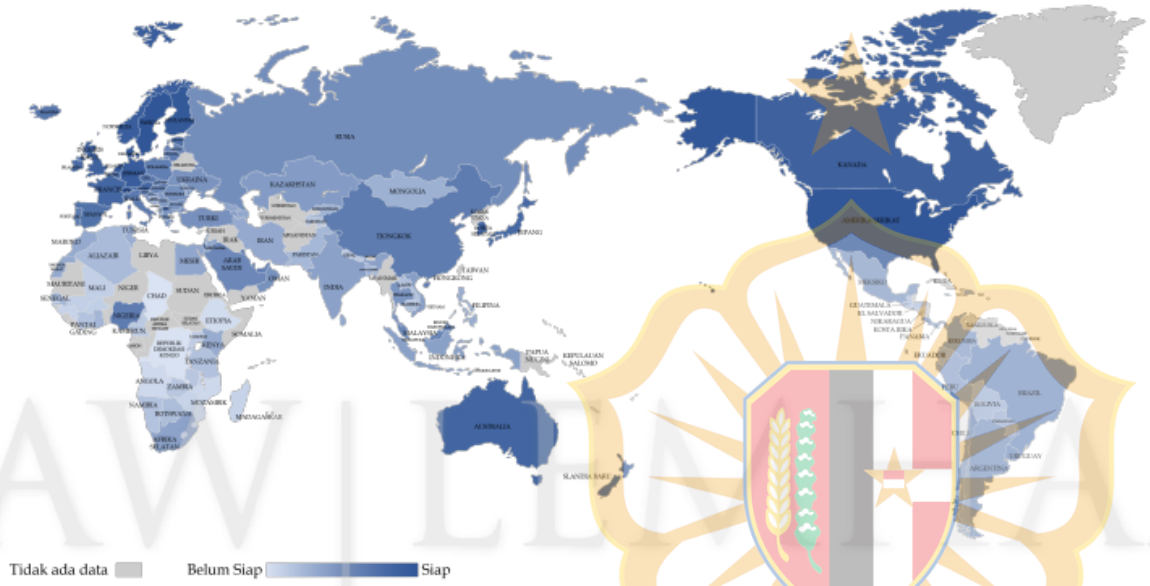
No	Variabel	Indonesia	Rata-Rata Global
1	Kepuasan Pasar	48,50	47,60
2	Kepuasan Bisnis	17,50	29,76
3	Pengetahuan dan Keluaran Teknologi	18,30	24,06
4	Keluaran Kreativitas	17,30	26,51
5	Institusi	51,20	64,94
6	Penelitian dan SDM	22,40	64,94
7	Infrastruktur	41,40	41,48

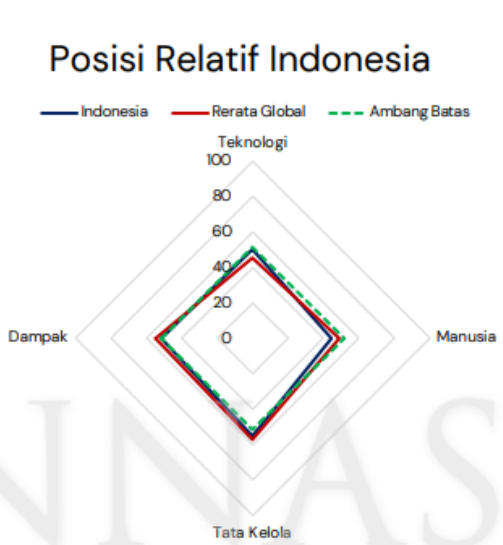
> Rerata Global < Rerata Global

Sumber: WIPO Global Innovation Index (2022)

LAMPIRAN 7

INDEKS KESIAPAN DIGITAL INDONESIA (2021)





Berdasarkan NRI, Indonesia dinilai masih belum sepenuhnya siap mengeksploitasi kesempatan yang ditawarkan teknologi informasi dan komunikasi. Indonesia menduduki peringkat ke-66 dari 130 negara dengan skor 50,37 yang berada di bawah rerata global 52,22. Negara yang memiliki peringkat dekat dengan Indonesia adalah Kolombia (65) dan India (67). Sementara itu, Belanda (82,06) menjadi negara dengan skor NRI terbaik dan Chad (21,85) menduduki posisi terendah.

Indonesia memiliki skor di bawah rerata global pada tiga variabel NRI. Variabel manusia, khususnya terkait kesiapan sektor bisnis dalam memanfaatkan teknologi informasi dan komunikasi, memiliki skor terendah. Indonesia memiliki skor di atas rerata global untuk variabel teknologi. Indonesia cukup unggul dalam dimensi akses. Harga data di Indonesia relatif terjangkau, masyarakat cukup aktif mengirimkan pesan pendek, serta cakupan jaringan 3G di Indonesia juga relatif mumpuni.

No	Variabel	Indonesia	Rerata Global
1	Teknologi	50,07	45,23
2	Manusia	44,69	48,75
3	Tata Kelola	55,02	57,20
4	Dampak	51,70	54,98

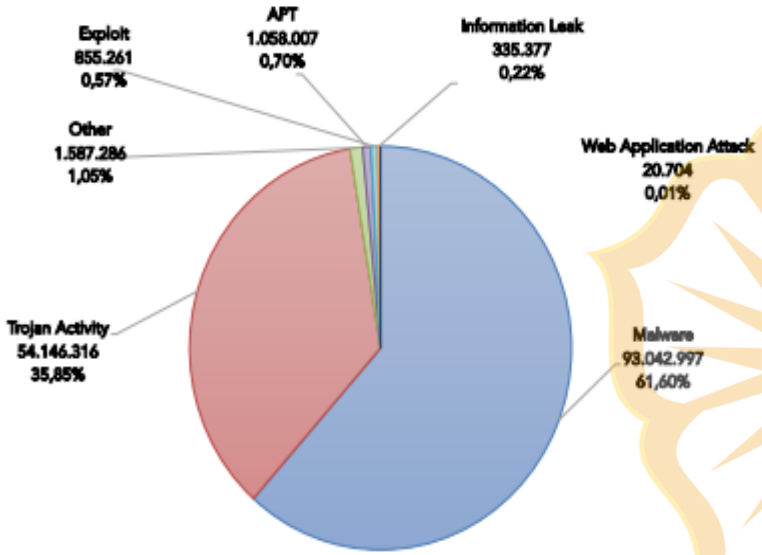
> Rerata Global < Rerata Global

Sumber: Portulans Academy (2022)

LAMPIRAN 8

KATEGORI ANOMALI TRAFIK (2023)

Pada periode 1 Januari – 22 Juni 2023, terdapat **190.064.862** anomali dengan **148.495.076** anomali diindikasikan berhasil menginfeksi *(Compromise)* dan **2.550.872** anomali dengan status serangan berhasil *(Attack Successful)*.



Anomali dengan status *compromise* dan *attack successful* berasal dari kategori *Malware* (61,60%), *Trojan Activity* (35,85%), *Other* (1,05%), APT (0,70%), *Exploit* (0,57%), *Information Leak* (0,22%), dan *Web Application Attack* (0,01%).

Berikut daftar 3 anomali tertinggi dari setiap klasifikasi yang diindikasikan *compromise* dan *attack successful*.

KLASIFIKASI	THREAT NAME	TOTAL
Malware	PhishingSite Other Malware activity	27.395.839
	MiningPool Mining Virus activity	13.564.323
	fakeTelegram Malicious Download activity	8.099.241
Trojan Activity	Generic Trojan RAT activity	41.331.939
	CobaltStrike RAT activity	3.554.442
	Emotet Stealer Trojan activity	1.246.816
Other	MSSQL database account brute force guess	763.491
	Website Automatic Directory Listing Detection	490.614
	TELNET account violence guess	102.021
Exploit	Discover out-of-band DNS requests using specific domain names	606.743
	Microsoft windows doublepulsar (double pulsar) smb remote code execution	185.165
	The site has a mining script code	61.263
APT	Kimsuky	256.225
	Winnti	121.017
	APT40	87.518
Information Leak	Plaintext password transmission found	109.615
	Find the robots.txt file	56.035
	Weak password risk detected (SMTP)	41.390
Web Application Attack	Cross-site Scripting(XSS)(Machine Learning)	11.024
	Cross-site Scripting(XSS)(Machine Learning)(mobile)	4.166
	Found to download files through httpfileserver	3.338