LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

MENINGKATKAN KEAMANAN INFORMASI GUNA MEWUJUDKAN KEWASPADAAN NASIONAL

Oleh :

Dr. Ridwan, S.Sos, M.Si

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN (PPRA) LXVI
LEMBAGA KETAHANAN NASIONAL RI
TAHUN 2024

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

KATA PENGANTAR

Assalamualaikum Wr. Wb,
Salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur kehadirat Allah SWT - Tuhan Yang Maha Esa serta atas segala rahmat dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) LXVI Tahun 2024 telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Ilmiah Perseorangan (Taskap) dengan judul: "**MENINGKATKAN KEAMANAN INFORMASI GUNA MEWUJUDKAN KEWASPADAAN NASIONAL"**

Penentuan Judul dan Tutor Taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor : 71 Tahun 2024 tanggal 28 Maret 2024, tentang Penetapan Judul Taskap Peserta PPRA LXVI Tahun 2024 Lemhannas RI.

Pada kesempatan ini, perkenankanlah Penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA LXVI di Lemhannas RI Tahun 2024. Ucapan yang sama juga disampaikan kepada Pembimbing atau Tutor Taskap kami yaitu Ibu Prof. Dr. Ir. Reni Maryeni, M.P. 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 Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu, dengan segala kerendahan hati mohon adanya masukan guna penyempunaan naskah ini.

Besar harapan saya agar Taskap ini dapat bermanfaat sebagai sumbangan pemikiran penulis kepada Lemhannas RI, termasuk bagi siapa saja yang membutuhkannya.

Semoga Allah 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, 9 Juli 2024

Penulis

Dr. Ridwan, S.Sos, .M.Si

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini :

   Nama : Dr. Ridwan, S.Sos, M.Si
   Pangkat : -
   Jabatan : Kepala Pusat Kajian Bela Negara
   Instansi : Universitas Pembangunan Nasional Veteran Jakarta
   Alamat : Jl. RS. Fatmawati no 1, Cilandak, Jakarta Selatan 12450

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) ke XLVI tahun 2024 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, 9 Juli 2024
Penulis Taskap

Dr. Ridwan, S.Sos, .M.Si

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LEMBAR PERSETUJUAN TUTOR TASKAP

Yang bertanda tangan di bawah ini Tutor Taskap dari :

Nama	:	Dr. Ridwan, S.Sos, M.Si
Peserta	:	Program Pendidikan Reguler Angkatan (PPRA) LXVI
Judul Taskap	:	Meningkatkan Keamanan Informasi Guna Mewujudkan Kewaspadaaan Nasional.

Taskap tersebut di atas telah ditulis “sesuai/tidak sesuai” dengan Petunjuk Teknis tentang Penulisan Ilmiah Peserta Pendidikan Lemhannas RI Tahun 2022, karena itu “layak/tidak layak” dan “disetujui/tidak disetujui” untuk diuji.

“”coret yang tidak diperlukan

Jakarta, 9 Juli 2024

Tutor Taskap

Prof. Dr. Ir. Reni Maryeni, M.P.

DAFTAR ISI

Daftar Tabel

Daftar Gambar

BAB I
PENDAHULUAN

1. Latar Belakang

Kewaspadaan Nasional, sikap dalam nasionalisme dari rasa peduli, tanggung jawab warga negara terhadap kelangsungan hidup masyarakat, bangsa, bernegara dari potensi ancaman[1]. Kewaspadaan Nasional Indonesia untuk mendeteksi, mengantisipasi, dan mencegah berbagai potensi ancaman terhadap NKRI. Kesiapsiagaan dalam menghadapi ancaman untuk melindungi kedaulatan negara[2]. Konsepsi kewaspadaan nasional harus diimplemetasikan dalam kehidupan bermasyarakat, berbangsa dan bernegara dengan pendekatan kesejahteraan dan keamanan. Perkembangan lingkungan strategis yang bergerak sangat dinamis sehingga ancamanpun berubah dari ancaman yang bersifat konvensional menjadi ancaman yang bersifat multidimensional. Salah satu ancaman yang patut diperhitungkan adalah ancaman keamanan informasi diera transformasi digital.

Transformasi digital merupakan penggunaan teknologi informasi dan komunikasi digital ke dalam berbagai aspek kehidupan masyarakat pada era modern yang melampaui literasi dan kompetensi digital. Penerapan transformasi digital berkaitan dengan kemampuan pemerintah dalam mengimplementasikan teknologi dan cara kerja baru untuk meningkatkan kinerja pemerintahan[3]. Teknologi Informasi dan komunikasi digital berfokus pada perubahan cara kerja dan budaya yang ada di dalam pemerintah untuk mempermudah pekerjaan, mempercepat proses kebijakan, serta meningkatkan kolaborasi dan inovasi.

Era digitalisasi merupakan era dimana kehidupan masyarakat berkembang secara pesat dan segala akivitas dapat dilakukan secara digital. Digitalisasi telah memberi kemudahkan dalam berbagai aspek kehidupan manusia baik pekerjaan dan aktivitas lainnya. Saat ini, masyarakat dapat

---

[1] Triwidodo dkk (2024). Kewaspadaan Nasional. Lembaga Ketahanan Nasional RI.
[2] Riyanto (2017). Kewaspadaan Nasional, Bela Negara dan Integrasi Nasional. Puskom Publik Kemhan
[3] Sari, D. C., Purba, D. W., & Hasibuan, M. S. (2019). Inovasi Pendidikan Lewat Transformasi Digital. Yayasan Kita Menulis.

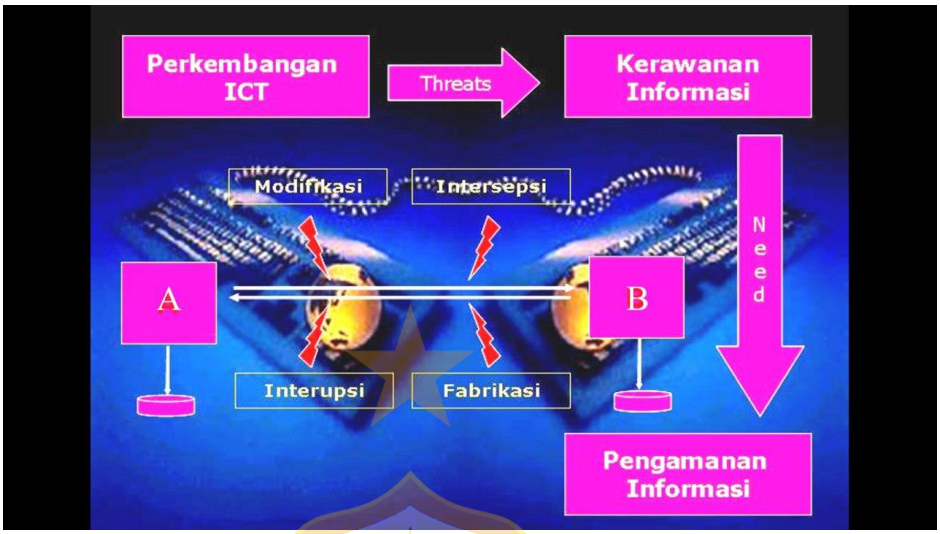
mencari dan memperoleh informasi secara mudah dan cepat. Kemudahan mengakses informasi akan meningkatkan literasi digital dan kesadaran masyarakat untuk meninjau kembali informasi sebelum diterima dan disebarkan kepada orang lain. Seluruh aktivitas dapat dilakukan hanya dengan perangkat digital dan koneksi internet yang dimiliki. Kebutuhan masyarakat akan ketersediaan informasi meningkat dan menuntut adanya kemudahan dan kebebasan dalam mendapatkan informasi. Melalui teknologi informasi dan komunikasi digital, pemerintah dengan mudah menyebarkan berbagai informasi seperti penanaman karakter dan semangat nilai-nilai bela negara kepada masyarakat, yang tertuang dalam Rencana Induk Kesadaran Bela Negara[4].

Kebutuhan masyarakat akan informasi yang transparan mendorong tuntutan akan kebebasan dan kemudahan akses informasi. Transparansi krusial dalam good governance, memastikan keterbukaan dalam penyelenggaraan pemerintahan dan akses informasi yang luas bagi publik. Pentingnya keterbukaan informasi penting untuk mencegah ketidak jelasan (*opacity*) dan keterbatasan (*secrecy*) dalam pelaksanaan pemerintahan. Keterbukaan mendukung partisipasi masyarakat dalam pengawasan dan pembangunan negara[5].

Namun, tidak semua informasi dapat diungkapkan ke publik secara keseluruhan. Terdapat informasi yang dikecualikan (informasi yang berklasifikasi rahasia) milik pemerintah yang tidak dapat diakses oleh orang yang tidak berkepentingan untuk mengetahuinya. Apabila informasi tersebut tersebar, dapat menghambat proses penegakkan hukum, mengganggu kepentingan perlindungan hak kekayaan intelektual dan persaingan usaha yang tidak sehat, serta membahayakan kepentingan nasional[6]. Upaya pemerintah dalam mengamankan informasi yang dikecualikan sangat mendesak untuk diterapkan pada semua lini pemerintahan.

[4] Peraturan Presiden Nomor 115 Tahun 2022 tentang Kebijakan Pembinaan Kesadaran Bela Negara
[5] Lenon, Michael dan Gary Berg-Cross, 2010. *Toward a High Performing Open Government* : *The Public Manager*. Winter 2010
[6] Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Gambar 1.1



Sumber : Data yang diolah

Perkembangan sistem informasi yang pesat juga menimbulkan masalah seperti pencurian dan pengrusakan informasi, mengakibatkan ketidakdekatan informasi dengan tujuan dan ketidakterkirimannya ke alamat yang benar. W. Stallings mengidentifikasi beberapa jenis serangan terhadap informasi, seperti intersepsi (akses aset oleh pihak tidak berwenang, contohnya *wiretapping*), modifikasi (mengubah informasi, contohnya merusak isi website), interupsi (mengganggu ketersediaan sistem), dan fabrikasi (menyisipkan objek palsu ke sistem, misalnya email palsu). Selain itu, ada model serangan lainnya terhadap keamanan informasi yang harus diperhatikan. Pencurian dan pengrusakan informasi mendorong pentingnya perlindungan informasi dalam era digital yang semakin kompleks.[7].

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), kejahatan siber terhadap sistem IT pelaku usaha dan Lembaga negara semakin meningkat. Pada tahun 2021, lebih dari 5 ribu kasus kejahatan siber terjadi di Indonesia[8]. Laporan *Fortinet* pada Quartal IV tahun 2022 menunjukkan lebih dari satu juta serangan berupa virus dan *botnets* yang terjadi setiap hari. Selain itu, pada Desember tahun 2020, total jumlah

[7] Sumarkidjo, 2006. Jelajah Kriptografi. Lembaga Sandi Negara
[8] Sari, R.P. (2024, Januari 27). Ancaman Siber Meningkat, Pemerintah dan Korporasi Diminta Bersatu. Sumber [online]

serangan mencapai angka tertinggi, yaitu sebesar 7.311.606 serangan siber. Serangan siber menjadi ancaman yang semakin besar bagi negara Indonesia. Bahkan, ancaman siber tidak hanya terjadi di Indonesia, serangan ini terjadi di tingkat internasional. Kurang lebih sebanyak 500 website militer milik Rusia dilumpuhkan oleh *hacker* yang meretas sistem keamanan.[9] Diluar banyaknya manfaat yang didapat dari era digitalisasi, terdapat masalah yang dapat membuat keamanan sistem informasi menjadi rentan baik terhadap kegiatan intersepsi, modifikasi, fabrikasi dan interupsi.

Pusat Operasi Keamanan Siber Nasional (Pusopskamsibnas), BSSN merilis telah terjadi 72 juta serangan siber yang masuk ke Indonesia. Amerika Serikat sebagai negara dengan anomali trafik tertinggi ke Indonesia[10]. Jumlah anomali tertinggi terjadi pada tanggal 30 Agustus 2023 dengan mencapai angka 13.937.677 anomali trafik. Tentunya angka tersebut memberikan gambaran adanya ancaman serius terhadap kehidupan bermasyarakat, berbangsa, dan bernegara yang harus diwaspadai karena dapat mengganggu ketahanan nasional.

Beberapa peristiwa kebocoran informasi yang pernah terjadi termasuk kebocoran percakapan antara Presiden BJ Habibie dan Jaksa Agung Andi Galib, kebocoran data-data masyarakat di Dinas Kependudukan dan Catatan Sipil, serta temuan alat-alat penyadap di beberapa KBRI di luar negeri. Tentunya dengan masih banyaknya kebocoran informasi milik pemerintah dan informasi publik lain yang belum terungkap dan terdeteksi, menambah permasalahan yang memerlukan solusi terbaik.

Perkembangan teknologi dan informasi menyebabkan kerawanan informasi yang memerlukan pengamanan informasi. Keamanan informasi menurut G. J Simons merupakan sebuah upaya untuk dapat mengantisipasi atau mencegah adanya penipuan yang terjadi pada sistem berlandaskan informasi, dimana informasi tersebut tidak mempunyai makna fisik. Aspek-aspek yang perlu dimiliki sebuah sistem agar keamanan informasi terjamin adalah informasi yang dikirim harus lengkap dan valid (*right information*), informasi disimpan oleh pihak yang memiliki kewenangan akan informasi

[9] Putra, D. (2023, Februari 20). Hati-hati, Serangan Siber di Indonesia Capai 1,65 Juta. Sumber [online].
[10] Laporan Bulan Desember tahun 2020, Pusat Operasi Keamanan Siber Nasional, BSSN.

tersebut (*right people*), informasi dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan informasi diberikan dalam format yang tepat (*right form*)[11]. Seluruh instansi pemerintah seharusnya memiliki fasilitas persandian untuk berkomunikasi maupun berkirim terima informasi yang berklasifikasi rahasia/ yang dikecualikan. Namun faktanya, baru 65% yang sudah terpenuhi, artinya masih ada 35% peluang terjadinya kebocoran informasi yang dikecualikan.

Ancaman lainnya yang harus diwaspadai adalah serangan siber terhadap mental dan karakter bela negara anak bangsa. Serangan ini pernah dilakukan terhadap Mesir dengan menghembuskan isu domokrasi versus otoriter melalui sosial media yang mengakibatkan jatuhnya rezim Husni Mubarak. Disisi lain, pada tahun 1998, Indonesia juga pernah diguncang dengan isu serupa yang berdampak pada jatuhnya rezim orde baru dan Presiden Suharto. Peristiwa tersebut menjadi perhatian serius bagi Pemerintah, yang kemudian mengeluarkan Peraturan Presiden Nomor 115 Tahun 2022 tentang kebijakan pembinaan kader bela negara.

2. Rumusan Masalah

Berdasarkan latar belakang serta fakta kondisi yang terjadi, maka rumusan masalah yang akan dibahas dalam Taskap ini adalah sebagai berikut :

Bagaimana upaya pemerintah dalam meningkatkan keamanan informasi khususnya informasi berklasifikasi rahasia milik pemerintah guna mewujudkan kewaspadaan nasional?

Guna menjawab permasalahan diatas, maka diperlukan adanya pertanyaan kajian sebagai berikut:

a. Bagaimana implementasi keamanan informasi yang ada di Indonesia?
b. Mengapa implementasi keamanan informasi belum optimal?
c. Bagaimana upaya pemerintah dalam mengatasi kebocoran informasi dan serangan siber yag terjadi di Indoensia.

[11] Prinsip Keamanan Informasi. Sumber [online]

3. Maksud dan Tujuan.

a. Maksud

Penulisan kertas karya ilmiah ini bertujuan untuk menyajikan gambaran, analisis, dan rekomendasi strategi kepada pemerintah dalam upaya meningkatkan keamanan informasi guna memperkuat kewaspadaan nasional. Karya ini diharapkan dapat memberikan kontribusi pada pemahaman dan langkah-langkah yang tepat dalam menghadapi tantangan keamanan informasi demi melindungi kedaulatan negara.

b. Tujuan

Tujuan dari penulisan kertas karya ilmiah perseorangan ini adalah untuk memberikan sumbangan pemikiran kepada pemerintah dalam menemukan solusi untuk meningkatkan keamanan informasi demi mencapai kewaspadaan nasional yang lebih baik. Karya ini diharapkan dapat memberikan pandangan dan rekomendasi yang berguna bagi kebijakan pemerintah dalam mengatasi permasalahan yang terkait dengan keamanan informasi guna melindungi kepentingan nasional.

4. Ruang Lingkup dan Sistematika.

a. Ruang Lingkup

Kertas karya ilmiah perseorangan ini membatasi ruang lingkupnya pada upaya pemerintah dalam meningkatkan keamanan informasi di era digitalisasi, dengan tujuan mewujudkan kewaspadaan nasional. Fokus utama penulisan kertas karya ini adalah memberikan analisis mendalam mengenai langkah-langkah dan kebijakan yang dapat diambil oleh pemerintah dalam menghadapi tantangan keamanan informasi di tengah perkembangan teknologi digital. Rekomendasi strategis yang disusun diharapkan dapat menjadi panduan bagi pemerintah dalam melindungi kepentingan nasional dari ancaman keamanan informasi.

b. Sistematika

Penulisan naskah ini disusun berdasarkan tata urut sebagai berikut:

1) BAB I : PENDAHULUAN

Pada Bab ini akan dijelaskan mengenai latar belakang, rumusan masalah, maksud dan tujuan penulisan Taskap, ruang lingkup sistematika penulisan, metode dan pendekatan yang digunakan, serta pengertian-pengertian terkait istilah yang digunakan dalam penulisan Taskap. Bab ini akan menjelaskan secara komprehensif elemen-elemen tersebut untuk memberikan pemahaman yang jelas mengenai konteks dan kerangka kerja penulisan Taskap secara keseluruhan.

2) BAB II : TINJAUAN PUSTAKA

Bab ini membahas mengenai paradigma nasional, peraturan perundang-undangan, landasan teori, perkembangan lingkungan strategis, dan kondisi tantangan dalam meningkatkan keamanan informasi; dan hasil analisisnya.

3) BAB III : PEMBAHASAN

Dalam bab ini akan diuraikan mengenai peningkatan keamanan informasi guna mewujudkan kewaspadaan nasional. Bab ini berisikan analisis mengenai semua pertanyaan yang tertulis pada Bab I dengan menggunakan kerangka teoretis serta dikaitkan dengan fakta-fakta empiris yang ada. Pada bab ini juga dianalisis pemecahan permasalahan tantangan transformasi digital guna meningkatkan keamanan informasi disertai dengan fakta yang diperoleh melalui referensi terkait.

4) BAB IV : PENUTUP

Sebagai Bab penutup, bab ini terdiri dari simpulan yang menjelaskan hasil analisa pada rumusan masalah yang dipaparkan dalam pertanyaan kajian Taskap dan rekomendasi atau saran yang dapat digunakan pemerintah sebagai bahan pertimbangan dalam meningkatkan keamanan informasi guna mewujudkan kewaspadaan nasional.

5. Metode dan Pendekatan

a. Metode

Penulisan ini mengadopsi metode analisis kualitatif deskriptif. Dalam metode ini, pengumpulan dan analisis data dilakukan melalui studi kepustakaan dan pengumpulan data sekunder dari referensi yang relevan dengan masalah yang dibahas dalam penulisan Taskap. Pendekatan ini akan digunakan sebagai kerangka strategis untuk menyajikan analisis mendalam mengenai topik yang dibahas dalam penulisan Taskap. Metode analisis kualitatif deskriptif dipilih untuk memberikan pemahaman yang komprehensif dan detail mengenai isu yang diteliti.

b. Pendekatan

Pendekatan yang digunakan dalam penulisan Taskap ini adalah perspektif kewaspadaan nasional melalui analisis multidisiplin yang sesuai dengan landasan teori yang digunakan. Pendekatan ini memungkinkan untuk menjelajahi isu keamanan informasi dan kewaspadaan nasional dari berbagai sudut pandang disiplin ilmu yang relevan, sehingga memberikan pemahaman yang holistik dan mendalam terhadap kompleksitas permasalahan yang dibahas. Dengan menggabungkan perspektif kewaspadaan nasional dan pendekatan multidisiplin, diharapkan penulisan Taskap dapat memberikan kontribusi yang berharga dalam analisis dan rekomendasi strategis terkait keamanan informasi.

6. Pengertian

a. Keamanan Informasi

Keamanan informasi menurut G. J Simons merupakan sebuah usaha untuk dapat memprediksi atau mencegah adanya penipuan yang terjadi pada sistem berlandaskan informasi, dimana informasi tersebut tidak mempunyai makna fisik. Aspek-aspek yang harus dimiliki sebuah sistem agar keamanan informasi terjamin adalah informasi yang ditransfer harus lengkap dan valid (*right information*), informasi disimpan oleh seseorang yang memiliki kewenangan akan informasi tersebut (*right people*), informasi dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan

informasi diberikan dalam format yang tepat (*right form*). Pencanangan program keamanan informasi memiliki prinsip-prinsip dasar yang harus dipenuhi agar kehandalan sistem tersebut dapat dipercaya. Prinsip-prinsip dasar tersebut adalah:

1) Kerahasiaan, informasi dijamin hanya disediakan bagi orang yang memiliki kewenangan, sehingga pihak yang tidak terlibat tidak berhak mengetahui informasi tersebut. Kerahasiaan harus menjamin data-data pribadi yang perlu dilindungi dalam hal penggunaan maupun penyebarannya.

2) Integritas, informasi harus dijaga agar selalu akurat dengan tidak memperbolehkan siapapun mengubah, kecuali atas izin pemilik informasi. Integritas informasi dapat dijaga dengan melakukan enkripsi data atau menciptakan tanda tangan dijital (*digital signature*).

3) Ketersediaan, dimana adanya jaminan informasi dapat diakses saat pihak yang berwenang membutuhkan informasi tersebut.[12]

b. Digitalisasi

Digitalisasi merupakan proses media yang bermula dari bentuk cetak, audio, video menjadi bentuk digital (Sukmana, 2005)[13]. Menurut Brennen & Kreiss, digitalisasi diartikan sebagai peningkataan ketersediaan data dalam bentuk digital yang disebabkan oleh kemajuan dalam membuat, memindahkan, menyimpan, dan menganalisis data digital serta berpotensi untuk merancang, menciptakan, dan mempengaruhi dunia kontemporer[14]. Secara umum, istilah “digitalisasi” dapat dilihat dari dua sudut pandang (Petry, 2016). Di satu sisi, secara teknis dapat dipahami sebagai konversi data analog menjadi informasi digital. Secara holistik, perkembangan masyarakat secara keseluruhan dapat dilihat sebagai hasil dari kemajuan teknologi pengolahan data elektronik. Perkembangan teknologi pengolahan data elektronik menimbulkan tantangan dan peluang baru karena memicu perubahan besar di semua tingkat perekonomian dan masyarakat, dimana

[12] Siregar, R. (2020, Mei 20). Prinsip Keamanan Informasi Sumber [online]
[13] Sukmana, Ena. (2005). Digitalisasi Pustaka. Sumber [online]
[14] Brennen, S.& Kreiss, D. (2016). Digitalization and Digitization. Sumber [online]

secara mendasar dapat mengubah cara orang berkomunikasi dan berinteraksi satu sama lain serta cara perusahaan beroperasi di pasar.[15].

c. Kepemimpinan Digital

Strategi yang dilakukan pemerintah harus mencerminkan transformasi digital saat ini. Diperlukan kepemimpinan digital (*digital leadership*) yang dibangun oleh pemerintah. Kepemimpinan digital merupakan perpaduan budaya digital dan kemampuan digital. Kepemimpinan digital termasuk ke dalam gaya kepemimpinan yang memiliki fokus pada penerapan transformasi digital di dalam sebuah lembaga atau organisasi[16]. Pemimpin digital merupakan seseorang yang visioner, berperan sebagai motivator perubahan, mampu membangun jaringan kemitraan melalui peluang-peluang baru yang tercipta dan bentuk kolaborasi lainnya (Fisk, 2002)[17].

d. Teknologi Digital

Teknologi berasal dari Bahasa Yunani, yaitu Technologia. Techne sebagai kata dasar dari teknologi yang berarti kemampuan, keterampilan, dan ilmu. Menurut Roger dalam Fatah (2008), teknologi merupakan sebuah rancangan yang digunakan sebagai alat bantu sebuah tindakan untuk mencapai hasil yang diinginkan[18]. Teknologi digital diartikan sebagai sebuah teknologi informasi yang lebih mementingkan kegiatan yang dilakukan melalui perangkat digital, komputer dll, dibandingkan kegiatan yang dilakukan dengan tenaga manusia (Danuri, 2019)[19]. Pemerintah harus mampu memimpin dan mengatur strategi yang didorong oleh teknologi digital. Tantangan digitalisasi diiringi dengan tanggung jawab besar para pemimpin digital terhadap masyarakat, organisasi, perusahaan, karyawan, dan pemangku kepentingan. Pemerintah harus memberikan perhatian

---

[15] Petry, T. (2016). *Digital Leadership* : *Erfolgreiches Fiihren in Zheiten der Digital Economy.* Freiburg : haufe-Lexware

[16] E.E.W. Tulungen., J.B. Maramis., D.P.E. Saerang. (2022). Transformasi Digital: Peran Kepemimpinan Digital. *Jurnal EMBA*. 10 (2).

[17] Fisk, P. (2002). The making of a digital leader. Business Strategy Review, 13(1), 43–50. Sumber [online]

[18] Fatah Syukur NC. (2008). *Teknologi Pendidikan*. Semarang: Rasai Media Group.

[19] Danuri, M. (2019). Perkembangan dan Transformasi Teknologi Digital. *Jurnal Ilmiah Infokam*. 15(2).

serius dan membuat strategi terbaik guna meniptakan keunggulan kompetitif di era digitalisasi (Kollmann & Schmidt, 2016)[20].

[20] Kollmann, T., & Hensellek, S. (2016). *The E-Business Model Generator*. In I. Lee (Ed.), *Encyclopedia of E-Commerce Development, Implementation, and Management* (pp. 26–36). IL: IGI Global.

BAB II
LANDASAN PEMIKIRAN

7. Umum

Transformasi digital, yang didorong oleh pemanfaatan teknologi dan digitalisasi, merupakan suatu fenomena yang mengubah tata cara kehidupan manusia dalam berbagai aspek. Transformasi digital tidak hanya mempengaruhi individu, tetapi juga instansi pemerintah, bisnis, pendidikan, dan masyarakat secara keseluruhan[21]. Digitalisasi di era ini mengubah sektor publik dengan memengaruhi penerapan, proses, budaya, struktur, dan tanggung jawab pemerintahan secara signifikan[22]. Namun, perubahan tersebut membawa dampak bagi kehidupan. Tindak kriminal juga terjadi di dunia digital, dan kehadirannya mengancam ketahanan nasional karena dapat menyerang mental dan karakter bela negara generasi muda. Meskipun digitalisasi membawa kemudahan, ancaman siber yang meningkat membuat informasi rahasia semakin mudah diretas dan disebarkan. Oleh karenanya, dalam rangka menghadapi tantangan dan ancaman dari transformasi digital, Pemerintah perlu mengimplementasikan kebijakan dan aturan yang tepat. Langkah-langkah implementasi tersebut harus melingkupi pencegahan dengan memprediksi segala kemungkinan yang akan terjadi untuk melindungi masyarakat dan menjaga keamanan nasional. Pada bab ini akan dideskripsikan mengenai peraturan dan perundang-undangan, kerangka teoretis, dan perkembangan lingkungan strategis yang mempengaruhi tingkat keamanan informasi dan hasil analisisnya guna mewujudkan kewaspadaan nasional.

8. Peraturan Perundang-Undangan

Terdapat beberapa peraturan perundang-undangan yang digunakan dalam meningkatkan keamanan informasi guna mewujudkan kewaspadaan nasional, yaitu sebagai berikut:

---

[21] E.E.W. Tulungen., J.B. Maramis., D.P.E. Saerang. (2022). Transformasi Digital: Peran Kepemimpinan Digital. *Jurnal EMBA*. 10 (2).

[22] Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. International Journal of Information Management, 60(April).

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

Penyelenggaraan negara yang terbuka sangat penting dalam mendukung transparansi dan akuntabilitas pemerintahan. Hak publik untuk memperoleh informasi sesuai dengan peraturan perundang-undangan merupakan salah satu aspek penting dalam mewujudkan negara yang terbuka. Undang-undang tentang Keterbukaan Informasi Publik menjadi landasan hukum yang esensial terkait dengan berbagai hal, seperti hak setiap individu untuk memperoleh informasi, kewajiban bagi badan publik untuk menyediakan informasi dengan cepat, tepat waktu, biaya yang proporsional, serta praktis, pengecualian informasi yang bersifat ketat dan terbatas, dan tanggung jawab badan publik untuk meningkatkan sistem dokumentasi dan layanan informasi. Adanya undang-undang ini juga mengharuskan setiap badan publik untuk memberikan akses terhadap informasi publik yang terkait dengan lembaga tersebut kepada seluruh masyarakat, sehingga meningkatkan transparansi dan partisipasi publik dalam pengawasan terhadap pemerintah. Seperti yang tertera pada pasal 7 ayat 1 “Badan Publik wajib menyediakan, memberikan dan/atau menerbitkan Informasi Publik yang berada di bawah kewenangannya kepada Pemohon Informasi Publik, selain informasi yang dikecualikan sesuai dengan ketentuan”. Informasi yang dikecualikan tersebut dapat dilihat pada pasal 17. Pada pasal 21 juga dijelaskan mengenai mekanisme untuk mendapatkan Informasi Publik didasarkan pada prinsip cepat, tepat waktu, dan biaya ringan.

Dengan dibukanya akses publik akan Informasi, diharapkan bahwa badan publik memiliki motivasi yang kuat untuk menjalankan tanggung jawabnya dan berfokus pada pelayanan publik yang terbaik. Dengan demikian, dapat mempercepat pencapaian pemerintahan yang terbuka sebagai strategi untuk mencegah praktik korupsi, kolusi, dan nepotisme (KKN), serta mempromosikan terciptanya tata kelola pemerintahan yang baik (good governance). Dengan adanya komitmen dan kinerja yang berkualitas dari badan publik dalam memberikan pelayanan yang transparan, akuntabel, dan responsif kepada masyarakat, diharapkan dapat memperkuat kepercayaan publik terhadap institusi pemerintah dan membangun fondasi yang kokoh untuk menjaga

integritas dan efektivitas pemerintahan. Kolaborasi aktif antara pemerintah dan masyarakat dalam mewujudkan prinsip-prinsip tata kelola yang baik akan menjadi kunci utama dalam menciptakan lingkungan yang bersih dan bebas dari korupsi.

b. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara

Dasar hukum dari Peraturan Presiden ini adalah UUD NKRI 1945 Pasal 4 ayat (1), Undang-Undang Nomor 36 Tahun 1999 dan Undang-Undang Nomor 11 Tahun 2008 mengatur mengenai kedudukan, tugas, dan fungsi Badan Siber dan Sandi Negara (BSSN), susunan organisasi BSSN, tata kerja BSSN, jabatan, pengangkatan, dan pemberhentian pejabat di BSSN, serta pendanaan BSSN. Menurut Pasal 1, BSSN adalah lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden, yang dipimpin oleh seorang Kepala. Sedangkan Pasal 2 menjelaskan tugas BSSN, yaitu melaksanakan tugas pemerintahan dalam bidang keamanan siber dan sandi untuk membantu Presiden dalam menjalankan pemerintahan. Seluruh pendanaan yang diperlukan untuk menjalankan tugas dan fungsi BSSN ditanggung oleh Anggaran Pendapatan dan Belanja Negara (APBN). Dengan regulasi ini, diharapkan BSSN dapat berperan penting dalam memperkuat keamanan informasi dan sistem dalam lingkup pemerintahan Indonesia.

c. Peraturan Presiden Nomor 115 Tahun 2022 tentang Kebijakan Pembinaan Kesadaran Bela Negara

Dasar hukum dari Peraturan Presiden ini adalah Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 4 ayat (1) dan Undang-Undang Nomor 23 Tahun 2019. Pasal 2 Peraturan Presiden ini mengatur mengenai kebijakan Pembinaan Kesadaran Bela Negara (PKBN) yang mencakup perencanaan, program kegiatan, pelaksanaan, pengawasan, dan evaluasi. Dengan adanya regulasi ini, diharapkan pembinaan kesadaran bela negara dapat dilaksanakan secara terarah dan efektif sesuai dengan prinsip-prinsip yang diatur dalam UUD 1945 dan undang-undang terkait. Melalui pelaksanaan PKBN yang baik, diharapkan

masyarakat dapat lebih memahami dan menerapkan nilai-nilai bela negara dalam kehidupan sehari-hari, serta terlibat aktif dalam upaya menjaga kedaulatan negara dan keutuhan wilayah Indonesia. Peran pemerintah dalam membina kesadaran bela negara menjadi semakin penting untuk menjaga keutuhan dan keamanan Indonesia di era yang terus berkembang ini. Sesuai dengan pasal 10 dalam perpres ini, Kebijakan PKBN didukung dengan membentuk forum komunikasi dan koordinasi. Tujuan dari Rencana Induk PKBN Tahun 2020-2044 adalah untuk membentuk sikap mental dan perilaku warga negara yang memiliki kesadaran dan kesiapan untuk mewujudkan nilai-nilai dasar Bela Negara dalam kehidupan berkelompok, berbangsa, dan bernegara. Dengan terbentuknya sikap mental dan perilaku tersebut, diharapkan masyarakat dapat aktif dalam mempromosikan persatuan, kesatuan, dan pemertahankan kedaulatan negara. Selain itu, pembinaan kesadaran bela negara juga bertujuan untuk membentuk sistem Pembinaan Kesadaran Bela Negara (PKBN) yang merata di seluruh wilayah Indonesia, sehingga setiap warga negara dapat terlibat aktif dalam menjaga keamanan dan ketertiban negara. Dengan demikian, diharapkan masyarakat Indonesia dapat memiliki sumber daya manusia yang unggul, memiliki kesadaran, dan kemampuan untuk melakukan tindakan nyata dalam mendukung serta memperkuat kedaulatan negara. Pada pasal 15 menjelaskan sumber dana pelaksanaan kebijakan PKBN adalah APBN dan APBD.

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

Peraturan Presiden ini memiliki dasar hukum yang tertuang dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 4 ayat (1) dan Peraturan Pemerintah Nomor 71 Tahun 2019. Pasal 2 Peraturan Presiden ini mengatur tentang ruang lingkup yang mencakup Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Sedangkan pada Pasal 3 dijelaskan bahwa strategi keamanan siber nasional dan manajemen krisis siber menjadi pedoman bagi instansi penyelenggara negara dan pemangku kepentingan untuk memperkuat kekuatan dan kapabilitas siber guna mencapai stabilitas keamanan siber. Pendanaan penyelenggaraan strategi

keamanan siber nasional dan manajemen krisis siber, sebagaimana diatur dalam Pasal 34, berasal dari Anggaran Pendapatan dan Belanja Negara (APBN), Anggaran Pendapatan dan Belanja Daerah (APBD), serta sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan. Dengan adanya regulasi ini, diharapkan upaya dalam memperkuat keamanan siber nasional dapat dilaksanakan dengan terkoordinasi dan terarah dalam rangka meningkatkan ketahanan dan keamanan informasi negara.

e. **Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional**

Perpres mengatur percepatan transformasi digital dan keterpaduan layanan digital nasional dengan menetapkan batasan istilah dalam pengaturannya. Pada pasal 2 Perpres ini menjelaskan aplikasi sistem pemerintahan berbasis elektronik prioriras untuk mewujudkan layanan digital nasional yang terpadu. Pasal tersebut berisi "Pemerintah melakukan percepatan transformasi digital melalui penyelenggaraan Aplikasi SPBE Prioritas dengan mengutamakan integrasi dan interoperabilitas. Aplikasi SPBE Prioritas dapat berupa:

1) Aplikasi SPBE yang baru akan beroperasi atau akan dibangun, dan
2) Aplikasi SPBE yang telah beroperasi atau akan dikembangkan, yang memiliki minimal 200.000 (dua ratus ribu) pengguna SPBE atau target pengguna SPBE". Pada pasal 3 dalam Perpres ini menjelaskan bahwa pemerintah menugaskan Perum Peruri untuk menyelenggarakan Aplikasi SPBE Prioritas.

9. Data/Fakta

Perkembangan sistem informasi yang pesat juga membawa berbagai permasalahan seperti pencurian dan kerusakan informasi, menyebabkan informasi tidak sampai atau tidak tepat waktu. Menurut W. Stallings, serangan terhadap informasi dapat berupa intersepsi (akses tidak sah), modifikasi (perubahan informasi), interupsi (gangguan sistem), dan fabrikasi (penyisipan

informasi palsu). Ada juga model serangan lain terhadap keamanan informasi yang perlu diwaspadai[23].

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), kejahatan siber terhadap sistem IT pelaku usaha dan Lembaga negara semakin meningkat. Pada tahun 2021, lebih dari 5 ribu kasus kejahatan siber terjadi di Indonesia[24]. Menurut laporan Fortinet pada Kuartal IV tahun 2022, lebih dari satu juta serangan berupa virus dan botnets terjadi setiap hari. Selain itu, pada Desember tahun 2020, total jumlah serangan mencapai angka tertinggi, yaitu sebesar 7.311.606 serangan siber. Serangan siber menjadi ancaman yang semakin besar bagi negara Indonesia. Bahkan, ancaman siber tidak hanya terjadi di Indonesia, serangan ini terjadi di tingkat internasional. Kurang lebih sebanyak 500 website militer milik Rusia dilumpuhkan oleh *hacker* yang meretas sistem keamanan.[25] Diluar banyaknya manfaat yang didapat dari era digitalisasi, terdapat masalah yang dapat membuat keamanan sistem informasi menjadi rentan baik terhadap kegiatan intersepsi, modifikasi, fabrikasi dan interupsi.

Pusat Operasi Keamanan Siber Nasional (Pusopskamsibnas), BSSN merilis telah terjadi 72 juta serangan siber yang masuk ke Indonesia. Amerika Serikat sebagai negara dengan anomali trafik tertinggi ke Indonesia[26]. Jumlah anomali tertinggi terjadi pada tanggal 30 Agustus 2023 dengan mencapai angka 13.937.677 anomali trafik, dimana angka tersebut memberikan informasi terhadap adanya ancaman serius terhadap kehidupan bermasyarakat, berbangsa, dan bernegara yang harus diwaspadai karena berpotensi mengganggu ketahanan nasional.

Beberapa peristiwa kebocoran informasi terjadi seperti kebocoran percakapan Presiden BJ Habibie dengan Jaksa Agung Andi Galib, kebocoran data-data masyarakat di Dinas Kependudukan dan Catatan Sipil, temuan alat-alat penyadap di beberapa KBRI diluar negeri. Tentunya, dengan masih

[23] Sumarkidjo, 2006. Jelajah Kriptografi. Lembaga Sandi Negara

[24] Sari, R.P. (2024, Januari 27). Ancaman Siber Meningkat, Pemerintah dan Korporasi Diminta Bersatu. Sumber [online]

[25] Putra, D. (2023, Februari 20). Hati-hati, Serangan Siber di Indonesia Capai 1,65 Juta. Sumber [online]

[26] Laporan Bulan Desember tahun 2020, Pusat Operasi Keamanan Siber Nasional, BSSN.

banyaknya kebocoran informasi milik pemerintah dan publik yang belum terungkap dan terdeteksi, memerlukan solusi perbaikan berkelanjutan.

Perkembangan teknologi dan informasi menyebabkan kerawanan informasi yang memerlukan pengamanan informasi. Keamanan informasi menurut G. J Simons (1984) merupakan sebuah upaya untuk dapat mengantisipasi atau mencegah adanya penipuan yang terjadi pada sistem berlandaskan informasi, dimana informasi tersebut tidak mempunyai makna fisik. Aspek-aspek yang perlu dimiliki sebuah sistem agar keamanan informasi terjamin adalah informasi yang dikirim harus lengkap dan valid (*right information*), informasi disimpan oleh pihak yang memiliki kewenangan akan informasi tersebut (*right people*), informasi dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan informasi diberikan dalam format yang tepat (*right form*)[27]. Seluruh instansi pemerintah seharusnya memiliki fasilitas persandian untuk berkomunikasi maupun berkirim terima informasi yang berklasifikasi rahasia/ yang dikecualikan. Namun faktanya, baru 65% yang sudah terpenuhi, artinya masih ada 35% peluang terjadinya kebocoran informasi yang dikecualikan[28].

Kasus Bjorka yang mencuat di penghujung tahun 2022, mengklaim bertanggung jawab dalam mencuri sejumlah informasi pribadi dan rahasia yang dimiliki oleh masyarakat dan pemerintah. Dari NIK hingga dokumen rahasia Presiden Republik Indonesia, seperti data pelanggan indihome, data registrasi *sim card*, data KPU, surat/dokumen rahasia ke presiden dan *doxing* pejabat publik. Klaim atas keberhasilan Bjorka dalam mendapatkan informasi tersebut telah menimbulkan kekhawatiran akan keamanan data dan privasi[29]. Aksi tersebut menimbulkan ketidakpastian bagi banyak pihak, terutama terkait dengan potensi penyalahgunaan informasi yang telah dicuri oleh Bjorka. Langkah-langkah pencegahan dan perlindungan data yang lebih ketat perlu segera diimplementasikan untuk mengatasi ancaman serius terhadap keamanan informasi. Kejadian ini juga menekankan pentingnya kesadaran akan perlindungan data pribadi dan kebijakan cyber security yang kuat dalam

[27] Prinsip Keamanan Informasi. Sumber [online]
[28] Ridwan, 2016. Implementasi Kebijakan Keamanan Informasi di Provinsi Sulawesi Tengah. Jurnal Ilmu Administrasi Universitas Subang Vol. 15 no 2
[29] Hacker Bjorka is Back, Data Apa saja yang Pernah dibocorkan? Sumber [online].

menjaga integritas dan privasi informasi yang sangat bernilai bagi individu dan negara.

Ancaman lainnya yang harus diwaspadai adalah serangan siber terhadap mental dan karakter bela negara anak bangsa. Serangan serupa pernah terjadi di Mesir, di mana isu demokrasi versus otoriter yang disebarkan melalui media sosial menyebabkan jatuhnya rezim Husni Mubarak. Di Indonesia, kejadian serupa terjadi pada tahun 1998, yang mengakibatkan runtuhnya rezim orde baru dan Presiden Suharto. Situasi ini mendapat perhatian serius dari pemerintah, yang kemudian mengeluarkan Peraturan Presiden Nomor 115 Tahun 2022 tentang Kebijakan Pembinaan Kader Bela Negara.

Menurut Masyarakat Telematika Indonesia (Mastel) dan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), kurangnya pemahaman tentang cara memverifikasi informasi yang diterima dapat menyebabkan penyebaran berita palsu yang merugikan individu maupun masyarakat luas. Meningkatkan literasi digital serta memberikan pemahaman tentang pentingnya sumber informasi yang dapat dipercaya dapat membantu mengurangi dampak dari penyebaran berita palsu. Oleh karena itu, penting untuk menerapkan pembelajaran literasi digital dalam kurikulum pendidikan di semua jenjang agar manfaat dari literasi digital tertanam sejak dini dan masyarakat dapat memahami pentingnya penggunaan teknologi dan literasi digital di era transformasi digital.

10. Kerangka Teoretis.

Untuk dapat melakukan analisa dan pembahasan strategi pemerintah dalam meningkatkan keamanan informasi guna mewujudkan kewaspadaan nasional**,** maka digunakan pendekatan teori transformasi digital, teori implementasi kebijakan, dan teori kewaspadaan nasional, sebagai berikut:

a. Teori Transformasi Digital

Transformasi Digital merupakan organisasi transformasi yang mengintegrasikan teknologi digital dan proses bisnis dalam ekonomi digital[30].

[30] Liu, D.-Y., Chen, S.-W. & Chou, T.-C., (2011). *Resource fit in digital transformation: Lessons learned from the CBC Bank global e-banking project. Management Decision*, 49(10), pp.1728–1742.

Sedangkan, Hess dkk. (2016) menyatakan digitalisasi atau transformasi digital berkaitan dengan perubahan yang dapat dilaksanakan oleh teknologi digital dengan membuat model bisnis organisasi, produk, proses, dan struktur di dalam organisasi. Transformasi digital merujuk pada penggunaan teknologi informasi dan komunikasi untuk mengubah secara radikal cara kerja dan proses suatu perusahaan. Transformasi digital ini melibatkan penggunaan teknologi untuk meningkatkan kinerja perusahaan, memperbaiki hubungan dengan konsumen, memodernisasi proses internal, dan mengubah nilai proposisi perusahaan agar lebih relevant dalam era digital[31]. Transformasi digital dapat diartikan sebagai adaptasi dari model bisnis yang dilakukan oleh suatu organisasi sebagai respons terhadap perubahan dinamis dalam kemajuan teknologi dan inovasi. Perubahan ini dapat memengaruhi perilaku konsumen dan sosial, sehingga organisasi harus mampu menyesuaikan diri dengan perubahan tersebut agar tetap relevan dan kompetitif[32].

Transformasi digital melibatkan kolaborasi antara berbagai inovasi dan teknologi digital yang bekerja bersama untuk menciptakan kerangka baru, praktik, nilai-nilai, regulasi, dan keyakinan yang dapat mengubah, menggantikan, atau melengkapi aturan yang ada dalam organisasi, ekosistem, atau industri tertentu. Transformasi digital melibatkan perubahan yang mendalam dalam cara kerja, berinteraksi, dan bernilai bagi stakeholders seperti karyawan, pelanggan, mitra bisnis, dan masyarakat luas[33]. Transformasi digital sangat penting bagi lembaga pemerintahan yang mengandalkan sistem, teknologi informasi, strategi, dan sumber daya manusia untuk menjalankan tugas-tugasnya secara efisien dan efektif. Dalam pemerintahan, transformasi digital berarti memanfaatkan teknologi informasi untuk meningkatkan layanan publik, transparansi, akuntabilitas, dan partisipasi masyarakat dalam proses pengambilan keputusan.[34].

---

[31] Westerman, G., Calméjane, C., & Bonnet, D., Ferraris, P., & McAfee, A. (2011). *Digital Transformation: A roadmap for billion-dollar organizations*. MIT Center for Digital Business and Capgemini Consulting, 1(1–68).

[32] Kotarba, M. (2018). Digital transformation of business models. Foundations of Management, 10(1), 123–142. https://doi.org/10.2478/fman-2018-0011

[33] Westerman, G., Bonnet, D., & Mcafee, A. (2014). The Nine Elements of Digital Transformation Opinion & Analysis. MIT Sloan Management Review, 55(3), 1–6.

[34] Hasiono, K & Santi, RCN. (2020). Menyongsong Transformasi Digital. Proceeding SENDIU. ISBN: 978-979-3649-72-6.

Terdapat empat faktor pendorong yang dapat memicu munculnya transformasi digital dalam suatu organisasi. Keempat faktor tersebut antara lain : perubahan regulasi, perubahan lanskap persaingan, pergeseran/perubahan dari industri ke bentuk digital, perubahan perilaku dan harapan konsumen[35]. Tujuan utama diterapkannya transformasi digital oleh sebuah lembaga adalah untuk meningkatkan kesiapan digital lembaga tersebut. Transformasi digital bertujuan untuk membawa perubahan yang signifikan dalam cara lembaga bekerja, menggunakan teknologi, dan berinteraksi dengan berbagai stakeholders [36]. Bukti kesiapan lembaga dalam menghadapi dunia digital adalah menciptakan inovasi kebijakan atau strategi yang diterapkan untuk menghadapi ancaman yang juga dibawa oleh digitalisasi.

b. Teori Implementasi Kebijakan

Implementasi Kebijakan Publik melibatkan aspek konflik, keputusan, dan manfaat kebijakan. Grindle menyatakan bahwa langkah awal implementasi adalah spesialisasi tujuan, program tindak, dan alokasi dana. Syarat-syarat ini penting dalam kebijakan publik. Keberhasilan implementasi dipengaruhi isi kebijakan dan konteks implementasi. Namun, kedua faktor ini juga dapat menyebabkan kegagalan implementasi. Perencana kebijakan harus memperhatikan aspek isi kebijakan dan konteks implementasi untuk mencapai tujuan yang diinginkan[37].

Pengukuran keberhasilan implementasi kebijakan dapat dilihat dari dua aspek, yaitu proses dan hasil. Aspek proses melibatkan pertanyaan apakah pelaksanaan kebijakan sesuai dengan yang telah ditetapkan dan apakah tujuan kebijakan tercapai dengan baik. Selain itu, keberhasilan implementasi kebijakan publik juga sangat ditentukan oleh tingkat keterlaksanaan kebijakan itu sendiri yang terdiri dari :

---

[35] K. Osmundsen, J. Iden, and B. Bygstad, “Digital Transformation: Drivers, Success Factors, and Implications,” Mediterr. Conf. Inf. Syst. Proc., vol. 12, pp. 1–15, 2018.
[36] *Ibid*.
[37] *Grindle*, Merilee S. *1980*. Politics and Policy Implementation in the Third World. New. Jersey : Princeton University Press

Isi Kebijakan (*Content of Policy*):

1) Pengaruh Kepentingan (Interest Effected) berkaitan dengan berbagai kepentingan yang mempengaruhi pelaksanaan suatu kebijakan.
2) Jenis Manfaat (*Type of Benefits*). Isi kebijakan ditujukan untuk menunjukkan atau menjelaskan bahwa suatu kebijakan harus mencakup berbagai jenis manfaat yang menunjukkan dampak positif.
3) Tingkat Perubahan yang Diinginkan (*Extent of Change Envision*). Setiap kebijakan memiliki target yang ingin dicapai. Isi kebijakan yang dijelaskan harus memiliki skala perubahan yang jelas.
4) Letak Pengambilan Keputusan (*Site of Decision Making*). Proses pengambilan keputusan dalam sebuah kebijakan memiliki peran penting dalam pelaksanaan kebijakan tersebut.
5) Pelaksana Program (*Program Implementer*). Dalam menjalankan suatu kebijakan atau program, kehadiran pelaksana kebijakan yang kompeten dan kapabel sangat penting untuk kesuksesan suatu kebijakan.
6) Sumber Daya yang Digunakan (Resources Committed). Pelaksanaan kebijakan harus didukung oleh sumber daya yang memadai agar pelaksanaan berjalan sesuai rencana. Sumber daya tersebut dapat berupa personil, keuangan, bakat manajerial, keterampilan, dan kemampuan fungsional.

Konteks Implementasi (*Context of Implementation*),

1) *Power, Interest, and Strategy of Actors Involved* (Kekuasaan, Kepentingan, dan Strategi dari Aktor yang Terlibat). Dalam pelaksanaan kebijakan, penting untuk mempertimbangkan kekuatan, kepentingan, dan strategi politik dari pihak-pihak yang terlibat agar implementasi kebijakan dapat berjalan lancar. Mengabaikan faktor-faktor tersebut dapat menyebabkan kebijakan tidak berjalan sesuai rencana bahkan dapat gagal sepenuhnya.

2) Karakteristik Institusi dan Rezim yang Berkuasa (*Institution and Regime Characteristics*). Keberhasilan sebuah kebijakan juga dipengaruhi oleh lingkungan di mana kebijakan tersebut diimplementasikan. Memahami karakteristik institusi dan rezim yang berkuasa sangat penting karena hal tersebut dapat memengaruhi pelaksanaan kebijakan.
3) Tingkat Kepatuhan dan Responsivitas dari Pelaksana (Compliance and Responsiveness). Tingkat kepatuhan terhadap kebijakan yang direncanakan dan respons yang tepat dari para pelaksana sangat menentukan keberhasilan implementasi suatu kebijakan[38].

Dengan demikian, secara umum dapat dipahami bahwa tugas implementasi adalah untuk membangun hubungan yang mendukung tercapainya tujuan dari kebijakan publik melalui aktivitas pemerintahan.

c. Teori Kewaspadaan Nasional

Kewaspadaan Nasional adalah sikap yang terkait dengan nasionalisme, yang dibangun dari rasa peduli, tanggung jawab, dan perhatian seorang warga negara terhadap kelangsungan hidup masyarakat, keberbangsaan, dan kebernegaraannya dari potensi ancaman[39]. Kewaspadaan Nasional merupakan kesiapsiagaan yang dimiliki bangsa Indonesia untuk mendeteksi dini, mengantisipasi, dan melakukan tindakan pencegahan terhadap berbagai bentuk potensi ancaman terhadap Negara Kesatuan Republik Indonesia (NKRI)[40]. Seiring dengan perubahan lingkungan strategis yang dinamis, ancaman telah berkembang dari yang bersifat konvensional menjadi bersifat multidimensional. Salah satu ancaman yang perlu diperhatikan adalah ancaman keamanan informasi dalam era transformasi digital. Kewaspadaan Nasional atau Padnas merupakan sikap

[38] Fajarwati, A & Rahmadilla, U. (2022). Model Implementasi Kebijakan Merilee Grindle Studi Kasus Penyerapan Tenaga Kerja Lokal pada PT. Meiji Rubber Indonesia Kabupaten Bekasi. *Jurnal Dialog*. 7(1).
[39] Triwidodo dkk (2024). Kewaspadaan Nasional. Lembaga Ketahanan Nasional RI.
[40] Riyanto (2017). Kewaspadaan Nasional, Bela Negara dan Integrasi Nasional. Puskom Publik Kemhan

yang terkait dengan nasionalisme, yang terbentuk dari rasa peduli dan tanggung jawab seorang warga negara terhadap kelangsungan hidup nasional, kehidupan bersosial, kehidupan berbangsa, dan bernegara dari potensi ancaman. Padnas juga merupakan sebuah kualitas kesiapan dan kesiagaan yang harus dimiliki oleh bangsa Indonesia untuk dapat memprediksi, mencegah secara dini, dan melaksanakan tindakan pencegahan terhadap berbagai macam bentuk dan sifat potensi ancaman terhadap NKRI.

Kewaspadaan Nasional dapat juga dijelaskan sebagai ekspresi kepedulian dan rasa tanggung jawab bangsa Indonesia terhadap keamanan dan integritas bangsa serta NKRI. Konsep ini terkait dengan Paradigma Nasional yang merupakan landasan berpikir untuk menjalankan sistem di suatu negara. Paradigma tersebut mencakup UUD 1945, Pancasila, Ketahanan Nasional, dan Wawasan Nusantara. Di dalam paradigma nasional terdapat nilai-nilai kebangsaan, kesadaran kebangsaan, dan pemahaman serta semangat kebangsaan. Oleh karena itu, kewaspadaan nasional harus didasari oleh keyakinan ideologis dan nasionalisme yang kuat serta didorong oleh upaya pemantauan secara proaktif dan berkesinambungan terhadap segala implikasi dari kondisi dan situasi yang terjadi, baik di dalam maupun di luar negeri.

Fungsi dari Kewaspadaan Nasional yang berkaitan dengan sistem Keamanan Nasional adalah sebagai berikut:

1) Memastikan Kepastian Hukum
2) Menjaga Ketenteraman dan Ketertiban Masyarakat
3) Menegakkan Hukum dan Keadilan
4) Memperkuat Kemampuan Pertahanan
5) Melindungi Rakyat dari Berbagai Bencana (Alam, Kejahatan, Kelalaian) dan Menjamin Perlindungan Hak-Hak Rakyat[41].

[41] Kementerian Pertahanan. (2017). Kewaspadaan Nasional, Bela Negara, dan Integrasi Nasional. WIRA. Vol. 67 (51).

d. Teori Keamanan Informasi

Keamanan informasi merupakan "aset berharga" yang mencakup data atau informasi yang direkam, disimpan, diproses, atau dikirim baik melalui media elektronik maupun non-elektronik. Keamanan informasi berkaitan dengan perlindungan aset berharga dari kerusakan, kehilangan, dan penyalahgunaan. Langkah-langkah perlindungan aset berharga diperlukan untuk memastikan kelangsungan bisnis, mengurangi risiko yang mungkin terjadi, serta maksimalkan keuntungan dari investasi dan peluang bisnis. Dalam usaha menangani dan mengendalikan keamanan informasi, terdapat tiga aspek utama yang harus dipertimbangkan, yaitu :

1) Kerahasiaan (Confidentiality), dimana aspek ini memastikan bahwa informasi tersebut hanya dapat diakses dan diketahui oleh pihak yang memiliki kewenangan akan informasi tersebut.
2) Integritas (Integrity), aspek ini menjamin bahwa tidak ada data yang dirubah selain izin dari pihak yang berwenang, aspek ini juga menjaga keakuratan data dan keutuhan informasi.
3) Ketersediaan (Availability), aspek ini memberikan jaminan atas ketersediaan data saat diperlukan kapan saja dan dimana saja[42].

Terdapat Indeks Kesiapan Keamanan Informasi (IKKI) sebagai alat evaluasi yang dikembangkan oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika. IKKI bertujuan untuk memberikan gambaran kondisi kesiapan (tingkat kematangan dan kelengkapan) kerangka kerja keamanan informasi atau Sistem Manajemen Keamanan Informasi (SMKI) kepada pimpinan Instansi pemerintahan. Evaluasi dilakukan terhadap berbagai area yang menjadi fokus penerapan keamanan informasi, dengan mencakup seluruh aspek keamanan yang diatur dalam standar ISO/IEC 27001.

Menurut ISO/IEC 27002:2013 tentang Sistem Manajemen Keamanan Informasi, kontrol keamanan berfungsi sebagai langkah-langkah perlindungan informasi dari potensi ancaman, menjaga

[42] Information Security Management System (ISMS). Sumber [online]

kelangsungan bisnis, mengurangi risiko, serta meningkatkan keuntungan dari investasi dan peluang bisnis. Berikut adalah contoh dari tinjauan keamanan informasi, yaitu :

1) Keamanan Fisik, strategi untuk melindungi anggota organisasi, aset fisik, dan tempat kerja dari ancaman seperti akses tidak sah, kebakaran, dan bencana alam lainnya.
2) Keamanan Personal, perlindungan bagi individu-individu yang berada di dalam instansi atau lembaga.
3) Keamanan Operasional, strategi untuk melindungi keahlian atau kemampuan instansi dalam melaksanakan tugasnya tanpa gangguan atau hambatan.
4) Keamanan Komunikasi, untuk melindungi media komunikasi, teknologi komunikasi, dan kemampuan memanfaatkan peralatan agar tujuan organisasi dapat tercapai.
5) Network Security, merupakan pengamanan yang dilakukan untuk peralatan jaring dan data organisasi, beserta isinya, serta kemampuan untuk memanfaatkan alat agar tujuan organisasi dapat tercapai[43].

Seluruh komponen tersebut turut berkontribusi dalam menjaga keamanan infromasi. Keamanan infromasi berarti melindungi informasi, termasuk perangkat dan sistem yang dipakai untuk menyimpan dan mentransfer informasi tersebut. Berbagai ancaman yang dapat mengancam keamanan informasi harus dapat diprediksi, diantisipasi, dan diminimalisir agar dapat tercipta keberlanjutan usaha dan mempercepat keuntungan dari peluang usaha.

e. Teori Perubahan

Menurut Henry, perubahan sosial mencakup semua perubahan pada lembaga-lembaga kemasyarakatan di suatu masyarakat yang memengaruhi sistem sosialnya, termasuk nilai-nilai, sikap-sikap, dan pola perilaku antar kelompok masyarakat.

Unsur utama perubahan sosial :

[43] Salazar (2005) dalam Riadi, Muchlisin. (2022). *Keamanan Informasi.* Sumber [online]

1) Terkait dengan jumlah populasi dan unsur sosial tertentu, seperti proporsi dalam kelompok penduduk.
2) Perilaku penduduk dalam periode waktu tertentu.
3) Struktur sosial dan pola interaksi antar individu.
4) Pola kebudayaan, termasuk nilai-nilai dalam masyarakat.

Faktor-faktor yang mempengaruhi perubahan sosial:

1) Kondisi struktural yang memungkinkan perubahan.
2) Motivasi untuk mengubah.
3) Upaya untuk mendorong perubahan.
4) Implementasi kontrol sosial[44].

Dalam transformasi digital, masyarakat akan mengalami perubahan sosial dengan hadirnya digitalisasi. Transformasi digital mendorong masyarakat untuk melakukan perubahan ke arah digital.

f. Teori Inovasi

Secara etimologi, inovasi berasal dari bahasa Latin "innovatio" yang berarti pembaharuan dan perubahan. Kata kerja dari inovasi adalah "innovo" yang artinya mengubah atau memperbaharui. Inovasi merupakan suatu upaya perubahan baru yang mengarah pada peningkatan[45]. Menurut Zaltman dan Duncan, inovasi adalah ide atau praktik yang dianggap baru oleh unit yang relevan. Inovasi merupakan perubahan objek yang diinterpretasikan sebagai sesuatu yang baru sesuai dengan kondisi dan situasi yang ada. Namun, tidak semua penemuan baru dapat disebut sebagai inovasi karena tidak semua orang menganggap perubahan terhadap penemuan tersebut sebagai sesuatu yang baru.

Menurut Everett Rogers, inovasi adalah ide, praktik, atau objek yang dianggap baru oleh individu atau kelompok pengadopsi. Sebuah ide dianggap baru secara objektif dan diukur berdasarkan waktu penggunaan atau penemuan ide tersebut[46]. Tahapan dari inovasi terdiri dari:

1) Pengetahuan, tahap di mana seseorang memiliki kesadaran atau pengetahuan tentang keberadaan inovasi.

---

[44] Hilmi, M. (2020). *Modul Teori Perubahan Sosial*. Universitas Jember
[45] Nur Kholifah, dkk. (2021). *Inovasi Pendidikan*. Medan: Yayasan Kita Menulis.
[46] Muhammad Kristiawan, dkk, (2018). *Inovasi Pendidikan*. Ponorogo : Wade Group

2) Bujukan, tahap di mana individu menghadapi persuasi atau pengaruh yang mendorong atau menghambat adopsi inovasi.
3) Keputusan, tahap di mana individu membuat keputusan untuk menerima atau menolak inovasi berdasarkan informasi dan persepsi yang dimilikinya.
4) Implementasi, tahap di mana individu mulai menerapkan atau menggunakan inovasi dalam kehidupan sehari-hari.
5) Konfirmasi, tahap di mana individu mencari konfirmasi atau konfirmasi dari orang lain tentang keputusan yang telah diambil terkait inovasi.

Inovasi merupakan gagasan, praktik, metode, cara, atau produk buatan manusia yang dianggap baru oleh individu atau kelompok. Dimana dalam keamanan informasi, inovasi mengacu pada upaya untuk meningkatkan keamanan informasi dengan melakukan perubahan atau optimisasi pada hal-hal yang dianggap perlu diperbaiki.

g. Teori Organisasi

Teori organisasi menurut Hodge dan Anthony adalah kumpulan konsep, prinsip, dan asumsi yang digunakan untuk menjelaskan struktur organisasi, fungsi, dan perilaku komponen-komponen di dalamnya[47]. Menurut Jones, teori organisasi adalah penelitian mengenai fungsi-fungsi organisasi dan interaksi antara organisasi dengan lingkungannya, baik dalam hal bagaimana organisasi mempengaruhi lingkungan maupun bagaimana organisasi dipengaruhi oleh lingkungannya[48]. Menurut pemahaman saya, Rubah: Teori Organisasi adalah suatu kerangka konsep, pandangan, argumen, atau pendekatan yang digunakan untuk memahami dan memecahkan masalah dalam organisasi, dengan tujuan agar organisasi dapat mencapai sasaran yang telah ditetapkan.

Organisasi adalah tempat di mana pekerjaan dilaksanakan. Organisasi merupakan sistem struktur yang memuat orang-orang dengan fungsi dan tugas masing-masing, yang bekerja sama untuk mencapai tujuan organisasi.

---

[47] Hodge, BJ. & Anthony, William P. (1988). *Organization Theory*. 3rd edition. Massachusetts, Allyn and Bacon Inc.
[48] Jones, Gareth R. (1997). *Organizational Theory: Text and Cases*. 2nd edition. Reading: Addison Wesley Longman Publishing Company.

Tujuan organisasi menggambarkan keadaan yang diinginkan, diwujudkan oleh organisasi sebagai arah yang diharapkan di masa depan. Organisasi adalah entitas sosial yang disengaja untuk bekerja bersama dengan koordinasi yang jelas untuk mencapai tujuan bersama atau serangkaian tujuan tertentu.[49]. Teori organisasi terdiri dari struktur organisasi, budaya organisasi, dan desain organisasi.

Dalam hal ini, pemerintah menjadi sebuah organisasi yang menjalankan tugasnya untuk mencapai tujuan nasional. Tujuan dari peningkatan keamanan informasi yang dilakukan pemerintah adalah untuk mewujudkan kewaspadaan nasional.

11. Lingkungan Strategis

Perkembangan lingkungan strategis mempengaruhi tingkat keamanan informasi suatu negara. Teknologi yang semakin maju menuntut adanya keamanan informasi yang lebih kuat untuk menghadapi ancaman cyber yang semakin komplekas. Dengan demikian upaya pemerintah dalam meningkatkan keamanan informasi guna mewujudkan kewaspadaan nasional tetap mempertimbangkan perkembangan lingkungan strategis mengenai ancaman global dan perkembangan transformasi digital. Upaya meningkatkan keamanan informasi sesuai dengan gatra keamanan dan pertahanan yang merupakan kemampuan negara dalam menjaga kedaulatan, keutuhan wilayah, dan keselamatan bangsa dari ancaman baik dari dalam maupun luar negeri dari serangan siber.

a. Perkembangan Lingkungan Strategis

1) Faktor Global.

Kejahatan siber adalah salah satu bentuk tindakan kriminal dalam dunia digital yang menjadi perhatian dunia. Seluruh negara yang ada di dunia tidak terlepas dari ancaman kejahatan siber yang terus menerus berkembang. *Internet Crime Complaint Center* (IC3) atau Pusat Pengaduan Kejahatan Internet yang merupakan pusat pelaporan kejahatan dunia maya. IC3 dijalankan oleh FBI sebagai lembaga yang menyelediki kejahatan siber, dimana di situs web tersebut masyarakat dapat melindungi dunia digital dan

[49] Husin, I. (2022). Teori Organisasi. *Jurnal GERBANG STMIK Bani Saleh*. Vol 12 (2).

keamanannya sendiri. Fokus dan prioritas utama dari FBI adalah melindungi dunia yang terhubung secara digital[50]. IC3 menjelaskan fakta pada tahun 2021, kerugian yang disebabkan oleh kejahatan siber yang berhasil dilaporkan warga negara Amerika Serikat berjumlah US$ 6,9 miliar atau setara dengan Rp 100 triliun. Jumlah kerugian tersebut mengalami kenaikan 5,7% persen tiap tahunnya selama lima tahun terakhir.

Dana Moneter Internasional (IMF) yang merupakan lembaga keuangan dunia mengungkapkan perkiraan total kerugian yang dialami oleh sektor keuangan di dunia akibat kejahatan siber tiap tahunnya mencapai US$ 100 miliar atau setara dengan Rp 1.450 triliun. Sektor perbankan menjadi sektor kedua yang paling rawan diincar oleh para penjahat siber. Menurut statistik kejahatan dunia maya global, Polandia menjadi negara yang memiliki keamanan siber terkuat menurut Keamanan Siber Nasional. NCSI (*National Cyber Security Index*) mengukur kemampuan suatu negara dalam menangani permasalahan kejahatan siber. Berikut adalah lima negara dengan skor NCSI tertinggi per Desember 2023 :

Tabel. 1 Negara Tertinggi Dalam Penanganan Kejahatan Siber

Nomor Urut	Negara	Presentase
1	Polandia	90,83 %
2	Estonia	85,83 %
3	Ukraina	80,83 %
4	Latvia	79.17 %
5	Inggris Raya	75.00 %

Sumber NCSI

Selain itu, organisasi yang paling berisiko terhadap kejahatan siber adalah organisasi-organisasi di Asia yang mengalami serangan siber paling banyak di seluruh dunia pada tahun 2021. Berikut adalah besar persentase serangan yang dialami oleh organisasi berdasarkan benua:

[50] *Internet Crime Complaint Center* . Sumber [online]

Tabel. 1 Benua yang paling banyak mengalami serangan siber

Nomor Urut	Benua	Presentase
1	Asia	26 %
2	Eropa	24 %
3	Amerika Utara	23 %
4	Timur Tengah dan Afrika	14 %
5	Amerika Latin	13 %

Sumber NCSI[51]

2) Faktor Regional

Asia Tenggara memiliki kasus kejahatan siber yang cukup kompleks karena mencakup populasi pelaku kejahatan lokal maupun asing. Salah satu kasus kejahatan dunia maya yang menarik adalah yang terjadi pada negara Malaysia dan Vietnam. Kasus yang terjadi di Malaysia adalah penjahat asing yang memanfaatkan negara Malaysia sebagai basis operasinya. Banyak penipu yang berasal dari Nigeria menetap di wilayah Malaysia. Penipuan tersebut meliputi penyusupan email bisnis, meskipun kejahatannya relatif menggunakan teknologi rendah, efek yang diberikan dapat sangat merusak. Kejahatan yang dilakukan oleh penipu tersebut berusaha untuk melibatkan masyarakat Malaysia ke dalam aksinya. Salah satu strategi yang sangat umum di seluruh dunia adalah berusaha mendekati orang lokal dan menggunakan wawasan, bahasa, dan aksennya untuk melancarkan aksi tersebut.

Selain itu, di Vietnam, bentuk kejahatan dunia maya yang banyak terjadi adalah peretasan. Kejahatan siber di Vietnam lebih dominan terjadi terkait penyusupan. Berdasarkan standar regional, lokasi kejahatan siber Vietnam cukup signifikan. Walaupun beberapa faktor menunjukkan Indonesia berpeluang menjadi pusat kejahatan siber internasional, terdapat faktor-faktor lain yang menjadi hambatan bagi penyebaran kejahatan siber. Seperti keahlian yang dimiliki masih tergolong rendah dibandingkan pusat

[51] Global Cyber Crime Statistics Sumber [online]

kejahatan siber lainnya, contohya beberapa negara bekas Uni Soviet[52]. Ancaman siber yang terjadi di Asia Tenggara dapat diminimalisir bahkan dicegah melalui kerja sama yang dilakukan negara-negara dengan ASEAN. Kerja sama tersebut dapat dilakukan dengan menerapkan knowledge transfer dari negara-negara di ASEAN yang memiliki kemampuan teknologi lebih tinggi. Berbagi pengetahuan ini dikoordinasikan oleh pemerintah Indonesia dan Malaysia dengan menerapkan sistem pengamanan siber MyCERT. Dengan adanya kerja sama regional melalui partisipasi aktif antar negara di wilayah Asia Tenggara, penanggulangan kejahatan dunia maya dapat ditingkatkan guna mewujudkan kewaspadaan masing-masing negara melalui mekanisme regional ASEAN[53].

3) Faktor Nasional

Berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet Indonesia diperkirakan mencapai 221.563.479 jiwa dari total populasi 278.696.200 penduduk Indonesia pada tahun 2024. Dengan demikian, tingkat penetrasi internet di Indonesia mencapai 79,5%, yang mengalami peningkatan sebesar 1,4% dari periode sebelumnya[54]. Pengguna internet di Indonesia semakin meningkat tiap tahunnya, semakin banyaknya masyarakat Indonesia yang menggunakan internet, maka harus semakin tinggi kesadaran untuk meningkatkan keamanan digital agar terhindar dari ancaman kejahatan siber.

Undang-Undang Perlindungan Data Pribadi yang telah disahkan pada tahun 2022 menunjukkan bahwa pemerintah peduli terhadap kerentanan sistem keamanan informasi yang dimiliki Indonesia. Meskipun telah terdapat payung hukum yang mengatur permasalahan perlindungan data pribadi, tindak pidana kejahatan dunia maya mengalami kenaikan signifikan pada tahun 2022. Menurut data dari Bareskrim Polri, pihak kepolisian menangani

[52] Cybercrime in Southeast Asia. Sumber [online]
[53] Penanggulangan Kejahatan Siber di ASEAN, 2023. Sumber [online]
[54] APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang, 2024. Sumber [online]

8.831 kasus kejahatan dunia maya pada tahun 2022, meningkat dibandingkan dengan 612 kasus yang ditangani pada tahun 2021[55].

b. Peluang dan Kendala

1) Peluang. Penerapan transformasi digital memiliki potensi untuk meningkatkan efisiensi operasional dan mengubah budaya sebuah organisasi menjadi lebih baik. Transformasi digital menandai perubahan yang terkait dengan pemanfaatan teknologi digital dalam berbagai aspek kehidupan. Di Indonesia, transformasi digital sedang mengalami pertumbuhan signifikan. Data dari Kementerian Keuangan menunjukkan bahwa nilai industri digital Indonesia mengalami peningkatan yang pesat, dari 41 miliar dolar pada tahun 2019, meningkat menjadi 77 miliar dolar pada tahun 2022, dan diprediksi akan mencapai 130 miliar dolar pada tahun 2025.[56]. Selain itu, era digitalisasi berpotensi memudahkan pekerjaan manusia. Saat ini, masyarakat dapat mencari dan memperoleh informasi secara mudah dan cepat. Kemudahan mengakses informasi akan meningkatkan literasi digital dan kesadaran masyarakat untuk meninjau kembali informasi sebelum diterima dan disebarkan kepada orang lain. Seluruh aktivitas dapat dilakukan hanya dengan perangkat digital dan koneksi internet yang dimiliki. Kebutuhan masyarakat akan ketersediaan informasi meningkat dan menuntut adanya kemudahan dan kebebasan dalam mendapatkan informasi.

2) Kendala. Selain manfaat yang diperoleh dari penerapan transformasi digital, terdapat dampak negatif terhadap keamanan siber di Indonesia. Kejahatan siber terus meningkat, dengan beberapa contoh kasus seperti keterlambatan, penyadapan, pencurian, dan perusakan informasi. Contohnya termasuk pembobolan situs-situs resmi pemerintah seperti situs Komisi Pemilihan Umum, Departemen Pertahanan, dan Departemen Luar Negeri, serta kasus penyadapan percakapan

[55] Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. *Sumber [online]*
[56] Kementerian Keuangan RI. 2023. Transformasi Digital untuk Masa Depan Ekonomi dan Bisnis di Indonesia. Kementerian Keuangan Republik Indonesia. Sumber [online]

Presiden oleh pihak Australia, dan penyadapan pembicaraan antara Presiden B.J. Habibie dengan Jaksa Agung Andi Ghalib, serta keterlambatan informasi yang sampai ke Gubernur. Tidak hanya dampak positif yang diberikan oleh dunia digital, tetapi ada juga ancaman dan tantangan di dalamnya. Kecanggihan sebuah sistem juga membuka jalan bagi pihak lain untuk membobol sistem tersebut. Semakin aman sebuah sistem dibangun, maka akan semakin tidak aman pula keberadaan dan keakuratan sistem tersebut. Meskipun akan tetap ada berbagai macam kendala di dalam sebuah sistem, pemerintah harus dapat mengantisipasi dan meminimalisir risiko penyadapan, mengurangi risiko ancaman, dan melindungi kerentanan sistem.

BAB III
PEMBAHASAN

12. Umum

Globalisasi menegaskan perlunya perhatian yang serius terhadap kebijakan keamanan informasi, sebab infrastruktur teknologi informasi yang bersifat publik dan global cenderung tidak aman. Ketika data dikirim melalui jaringan publik, ada risiko pihak ketiga dapat menyadap atau memanipulasi data tersebut. Dalam proses pertukaran data, ada kemungkinan orang lain ikut mengakses dan mengetahui informasi tersebut. Kebijakan keamanan informasi bertujuan untuk mengelola dan mengklasifikasikan tingkat kerahasiaan informasi sesuai dengan posisi jabatan. Informasi yang lebih sensitif akan diatur dengan lebih ketat, sesuai dengan tingkat strategisnya.

Globalisasi adalah serangkaian fenomena kompleks yang berdampak pada berbagai aspek kehidupan masyarakat. Pertumbuhan ekonomi yang cepat, pengurangan tingkat kemiskinan, kemajuan teknologi seperti internet, komunikasi, dan transportasi yang efisien merupakan sebagian dari dampak positif globalisasi. Banyak pakar meyakini bahwa globalisasi merupakan proses yang penuh misteri yang terus memicu diskusi yang berkelanjutan. Pendapat George Lodge dari Harvard Business School menyatakan bahwa tidak ada seorang pun di dunia yang dapat dengan pasti meramalkan arah globalisasi, kecuali ia diutus dari surga. Pernyataan tersebut memberikan gambaran yang disebabkan oleh dampak globalisasi yang mencakup berbagai level mulai dari lokal, regional, hingga internasional[57].

Globalisasi membuat dinamika perkembangan lingkungan strategis berkembang dengan cepat, membuka ruang banyak dimensi yang tidak hanya menawarkan peluang dan manfaat saja, tetapi juga tantangan dan tuntutan. Demikian pula, ancaman yang terus muncul menampilkan beragam varian di spektrum yang baru, yang terkadang sulit untuk dikejar dan diantisipasi, bahkan oleh hukum. Dinamika globalisasi membuat perkembangan internet

[57] Lembaga Ketahanan Nasional Republik Indonesia. (2024). Bidang Studi: Kewaspadaan Nasional.

semakin pesat. Digitalisasi yang meluas keberbagai sendi kehidupan dan menghilangkan batas-batas wilayah menjadi salah satu bukti hadirnya globalisasi. Dunia digital berpotensi membuka berbagai peluag dan kemajuan namun disisi lain dapat menjadi ancaman terhadap ketahanan nasional, seperti penyadapan informasi rahasia/ informasi yang dikecualikan milik pemerintah, menyebar berita palsu dan ujaran kebencian, isu SARA dan intoleransi, masuknya budaya asing yang dapat mempengaruhi generasi muda sehingga mengikis rasa nasionalisme, serangan siber, dan berbagai ancaman lainnya yang tidak sesuai dengan prinsip dan nilai-nilai yang ada di Pancasila sebagai pedoman hidup bangsa[58]. Masyarakat dinilai memiliki rasa aman yang rendah dalam berinternet. Banyaknya kasus pencurian data pribadi hingga data korporasi, tidak sedikit yang terjadi dan kemudian dijual ke pasar gelap. Selain itu, data kependudukan yang dipegang oleh instansi pemerintah yang melakukan kerja sama dengan pihak ketiga memiliki risiko yang tinggi untuk disalahgunakan. Para pembuat regulasi di Indonesia kurang memperhatikan situasi Indonesia yang semakin darurat kejahatan siber.

Untuk menghadapi perubahan yang disebabkan oleh globalisasi, kewaspadaan nasional (Padnas) menjadi solusi utama untuk tetap menjaga persatuan dan kesatuan bangsa, kedaulatan serta martabat nasional, dan dalam menghadapi derivasi berbagai ancaman global. Untuk menjamin kelangsungan hidup bangsa, kewaspadaan nasional wajib tertanam di benak segenap bangsa Indonesia sejak dini, sehingga dapat menangkal segala bentuk ancaman, gangguan, hambatan, dan tantangan (AGHT) dalam bermasyarakat, berbangsa, dan bernegara. Perjalanan bangsa Indonesia akan terus mengalami perubahan seiring dengan adanya dinamika internal dan eksternal.

Kewaspadaan Nasional (Padnas) adalah sikap yang terkait dengan semangat nasionalisme. Kewaspadaan nasional timbul dari kesadaran, tanggung jawab, dan perhatian masyarakat Indonesia terhadap keberlangsungan kehidupan bersama sebagai bangsa dan negara, dengan tujuan untuk mencegah potensi ancaman. Padnas juga merupakan kemampuan kesiapan dan kewaspadaan yang dimiliki oleh bangsa Indonesia untuk meramalkan, mengantisipasi sejak dini,

[58] Kansong, Usman. Relevansi Nilai-Nilai Pancasila dalam Kehidupan Berbangsa dan Bernegara para Era Teknologi Informasi. Dirjen Informasi dan Komunikasi Publik Kementerian Komunikasi dan Informatika

dan mengambil langkah-langkah pencegahan terhadap berbagai bentuk ancaman terhadap Negara Kesatuan Republik Indonesia (NKRI). Oleh karena itu, Padnas harus bersumber dari keyakinan ideologis dan cinta tanah air yang kuat, serta didorong oleh upaya pemantauan yang terus-menerus terhadap berbagai implikasi dari situasi dan kondisi yang berkembang baik di dalam maupun di luar negeri.Berdasarkan definisi di atas, mewujudkan kewaspadaan nasional di era digitalisasi menjadi sebuah hal yang sangat penting. Kita perlu peduli dan menerapkan rasa nasionalisme yang tinggi agar dapat memprediksi dan mencegah segala bentuk ancaman, hakikat ancaman yang kita hadapi, serta prosedur mengimplementasikan kewaspadaan nasional tersebut dalam kaitannya dengan ancaman.

Pembentukan rumusan kewaspadaan nasional merupakan hal yang penting dalam menentukan langkah untuk sedini mungkin mengantisipasi implikasi ancaman maupun kendala yang mungkin muncul ke dalam berbagai aspek di era globalisasi. Eratnya rasa peduli dan tanggung jawab akan memotivasi terbentuknya kewaspadaan di dalam setiap interaksi sosial masyarakat, sehingga setiap ancaman yang akan muncul dalam menjaga ketahanan nasional dapat diantisipasi sejak awal. Untuk mendapatkan kewaspadaan nasional yang berkualitas, dibutuhkan kemampuan dalam mengetahui berbagai macam bentuk ancaman, gangguan, hambatan, dan tantangan di era globalisasi. Hal tersebut mengacu pada peristiwa dan pengalaman di masa lalu, meskipun terdapat perubahan dalam pola, metode, dan modus ancaman.

Kewaspadaan nasional merupakan serangkaian tindakan yang bertujuan untuk mencegah berbagai potensi ancaman, tantangan, hambatan, dan gangguan (ATHG). Kewaspadaan nasional berakar pada semangat nasionalisme yang tumbuh dari rasa peduli dan tanggung jawab seluruh masyarakat Indonesia terhadap keberlangsungan hidup bersama sebagai bangsa dan negara. Dengan kewaspadaan nasional yang kuat, negara mampu meramalkan, mencegah, dan mengatasi berbagai potensi ancaman yang dapat mengancam persatuan negara Indonesia. Oleh karenanya, dalam mewujudkan kewaspadaan nasional, perlu adanya peran yang kesinambungan antara pemangku kepentingan yang terlibat langsung dalam pemerintahan[59]. Adapun dalam rangka mencapai tujuan

[59] Lembaga Ketahanan Nasional Republik Indonesia. (2024). Bidang Studi: Kewaspadaan Nasional.

dimaksud, beberapa upaya antisipasi yang dapat dilakukan guna meningkatkan keamanan informasi salah satunya adalah melalui adaptasi dalam hal kesiapan, kualitas dan tanggungjawab akan peran kesediaan Sumber Daya di Indonesia. Oleh karenanya, strategi yang dapat dipersiapkan dalam menghadapi era digital sebagai bentuk respons terhadap dinamika global guna meminimalisir dampak berbagai aspek kehidupan bangsa dan negara adalah melalui kesiapan atas sumber daya yang memiliki kecakapan dalam menghadapi tantangan serta ancaman yang mungkin akan timbul.

13. Implementasi Keamanan Informasi di Indonesia

Era globalisasi menjadi sebuah titik awal yang sangat penting sebagai bentuk upaya dalam memahami berbagai perkembangan dan kemajuan yang terjadi di era saat ini. Dalam era globalisasi, kehidupan manusia mengalami perubahan yang besar ditandai dengan meningkatnya pertumbuhan penduduk dan menyusutnya pangan serta energi. Hal tersebut membutuhkan perhatian dan kewaspadaan nasional yang terus menerus dan dilakukan secara serius, sehingga kepentingan nasional Indonesia tidak terganggu. Di era globalisasi yang ditandai dengan kemajuan teknologi informasi dan komunikasi, terbuka peluang bagi individu dan organisasi untuk berinteraksi secara instan meskipun berada pada jarak yang sangat jauh.

Indonesia berada di peringkat keenam terbesar di dunia dalam hal jumlah pengguna internet, di mana setiap individu yang mengakses internet setidaknya sekali tiap bulan. Menurut eMarketer pada tahun 2017, diprediksi jumlah pengguna internet di Indonesia akan mencapai 112 juta orang, melebihi Jepang yang berada di peringkat kelima, namun dengan pertumbuhan jumlah pengguna internet yang lebih lambat. Pada tahun 2015, jumlah pengguna internet global telah mencapai 3 miliar orang, dan diproyeksikan akan mencapai 3,6 miliar orang yang menggunakan internet setidaknya sekali tiap bulan pada tahun 2018[60]. Bahkan pada tahun 2023, pengguna internet di Indonesia mencapai 78,19%, dengan 167 juta pengguna aktif media sosial. Artinya, sekitar 60,4% dari total populasi telah memiliki dan menggunakan media sosial. Tentunya, semakin banyaknya pengguna dunia digital ekses positifnya adalah mempermudah

[60] Lembaga Ketahanan Nasional Republik Indonesia. (2024). Bidang Studi: Kewaspadaan Nasional.

aktivitas manusia, dan membawa mempermudah penyebaran kampanye kemanusiaan, pembentukan komunitas di tengah budaya individualis, penggalangan dana secara besar-besaran, serta konten edukatif yang memotivasi para pengguna.

Kemajuan teknologi informasi memberikan kebebasan bagi individu untuk mengakses, mengetahui, menyebarkan, dan memanfaatkan informasi tanpa batas. Namun, di sisi lain, kelimpahan informasi yang tersebar melalui internet tidak hanya mempermudah akses informasi yang dibutuhkan, tetapi juga dapat menimbulkan disinformasi dan kekacauan, terutama dalam kehidupan sosial masyarakat. Menurut data dari Detik News pada bulan Mei 2019, Kementerian Komunikasi dan Informatika (Kominfo) berhasil mengidentifikasi 30 berita palsu atau hoax yang disebarkan melalui media sosial pada tanggal 21-22 Mei 2019. Penyebaran berita palsu ini menjadi kekhawatiran bagi pemerintah karena dapat menimbulkan dampak negatif pada individu, kelompok masyarakat, serta kehidupan berbangsa dan bernegara. Ancaman di dunia digital semakin meningkat, dan masyarakat sebagai pengguna internet harus memiliki kecerdasan multiperspektif dan keberanian untuk memverifikasi informasi yang diterima atau menyaringnya agar tidak mudah terpengaruh oleh berita yang tendensius[61]. Maraknya berita palsu (*hoax*) dan informasi yang menyesatkan (*misleading*) dapat membawa masyarakat ke arah perilaku yang tidak etis dan dapat meningkatkan tingkat kriminalitas di dunia digital (*cybercrime*).

Terhubung menjadi suatu kewajiban yang tak dapat dihindari bagi manusia di zaman globalisasi dan industry 4.0. Kemudahan akses informasi dan kemajuan teknologi menjadi faktor utama dalam menciptakan koneksi komunikasi antara individu di seluruh dunia. Di satu sisi, informasi akan mudah tersebar dan diakses, termasuk informasi faktual maupun hoaks. Dalam berkomunikasi harus bijak, baik dalam hal pribadi maupun pekerjaan, karena kelalaian dalam berkomunikasi tidak hanya akan mengancam kerahasiaan dan keamanan informasi pribadi, tetapi juga kerahasiaan dan keamanan informasi yang berklasifikasi rahasia milik negara.

[61] Menghalau Hoaks Melalui Peningkatan Literasi Digital. Sumber [online]

Menurut data Threat Exposure Rate (TER), yang merupakan parameter untuk mengukur persentase komputer yang terkena malware, Indonesia memiliki persentase serangan malware sebesar 23,54%**.** Angka ini menunjukan bahwa hampir satu dari empat komputer di Indonesia rentan atau telah terkena serangan malware. Angka ini menunjukkan tingkat kerentanan yang cukup tinggi dibandingkan dengan negara-negara lain di kawasan Asia, seperti China yang memiliki persentase 21,36% dan Thailand dengan 20,78%**.** Persentase yang lebih tinggi terjadi di Indonesia mengindikasikan bahwa infrastruktur keamanan siber di negara tersebut mungkin masih lemah atau kurang efektif dalam mencegah serangan malware dibandingkan negara-negara lain.[62]

Faktor-faktor yang dapat menyebabkan tingginya angka serangan malware adalah :

a. Kesadaran Keamanan Siber yang Rendah: Banyak pengguna komputer di Indonesia mungkin tidak sepenuhnya menyadari pentingnya perlindungan terhadap malware dan praktik keamanan siber yang baik.
b. Penggunaan Perangkat Lunak Bajakan: Penggunaan perangkat lunak bajakan yang tidak mendapatkan pembaruan keamanan reguler dapat membuat sistem lebih rentan terhadap serangan.
c. Keterbatasan Infrastruktur Teknologi: Infrastruktur teknologi informasi dan komunikasi (TIK) di Indonesia mungkin belum sepenuhnya mendukung sistem pertahanan siber yang kuat.

Menteri Komunikasi dan Informatika periode 2014-2019, Rudiantara, menyoroti rendahnya tingkat kesadaran masyarakat Indonesia terhadap keamanan siber. Menurut Rudiantara, budaya kesadaran terhadap keamanan siber tidak harus terkait dengan penggunaan teknologi canggih secara berlebihan, namun bisa dimulai dari setiap individu[63]. Rudiantara menggarisbawahi pentingnya meningkatkan kesadaran akan ancaman keamanan digital di tengah pesatnya perkembangan teknologi informasi. Beliau menekankan bahwa setiap individu memiliki peran yang vital dalam menjaga keamanan siber, baik dalam kehidupan sehari-hari maupun di ranah digital

[62] Ashari, 2020. Keamanan Informasi : sudah saatnya kita peduli. Sumber [online]
[63] Ayuwuragil, 2017. Kesadaran Keamanan Siber Indonesia Peringkat Ke – 70 Dunia. CNN Indonesia Sumber [online]

Rendahnya *security awereness* pejabat publik untuk menyadari pentingnya keamanan informasi tercermin dari berbagai peristiwa kebocoran data yang terjadi di Indonesia. Contohnya, kebocoran percakapan antara Presiden BJ Habibie dengan Jaksa Agung Andi Galib, kebocoran data masyarakat di Dinas Kependudukan dan Catatan Sipil, dan temuan alat penyadap di beberapa KBRI di luar negeri. Implikasi kebocoran data sangat serius, dapat dibayangkan jika informasi perbankan diretas oleh pihak yang tidak bertanggung jawab, hal itu dapat menimbulkan kekacauan. Peristiwa tersebut menunjukkan bahwa masih diperlukan peningkatan kesadaran akan keamanan informasi bagi pejabat publik. Seharsnya seluruh instansi pemerintah dilengkapi dengan peralatan keamanan informasi yang terkoneksi dengan Jaring Komunikasi Sandi Nasional, sehingga dapat berkomunikasi dan bertukar informasi yang bersifat rahasia atau terklasifikasi secara aman dan terjamin.

Data dari Lembaga Sandi Negara (Lemsaneg) yang kini menjadi Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa baru 64% jaringan Komunikasi Sandi Nasional yang sudah terpenuhi[64]. Artinya, masih terdapat 36% peluang terjadinya kebocoran informasi yang berpotensi menimbulkan dampak yang merugikan. Dalam menghadapi ancaman keamanan siber, penting bagi pemerintah dan seluruh pihak terkait untuk meningkatkan investasi dalam keamanan informasi serta melakukan tindakan preventif yang tepat guna melindungi data sensitif dan informasi pribadi masyarakat.

Rendahnya literasi digital masyarakat terkait keamanan informasi menjadi masalah serius dalam era digital saat ini. Banyak individu yang kurang memahami pentingnya melindungi informasi pribadi dan sensitif dari ancaman keamanan siber. Akibatnya, masyarakat rentan menjadi korban kejahatan cyber seperti pencurian identitas, phishing, malware, dan lain sebagainya. Ketidakpahaman masyarakat dalam hal keamanan informasi juga dapat menyebabkan penyebaran informasi hoaks dan disinformasi yang merugikan. Dengan minimnya pengetahuan tentang cara memverifikasi informasi yang diterima secara online, masyarakat cenderung mudah terpengaruh dan tersebar luasnya berita palsu.

[64] Ridwan, 2018. Implementasi Kebijakan Keamanan Informasi di Provinsi Sulawesi Tengah. Jurnal Ilmu Administrasi. Universitas Subang.

14. Implementasi Keamanan Informasi di Indonesia Belum Optimal

a. Konten Kebijakan yang ambigu

Dewasa ini, semakin berkembang pandangan bahwa dalam era keterbukaan informasi publik, tidak ada yang seharusnya disembunyikan. Transparansi dianggap sebagai prinsip utama yang harus diterapkan dalam berbagai aspek kehidupan, termasuk dalam hal pengelolaan informasi. Masyarakat memandang bahwa segala hal haruslah terbuka dan dapat diketahui oleh publik.

Namun, di balik dorongan untuk menjadi lebih transparan, terdapat beberapa pertimbangan yang perlu diperhatikan. Beberapa informasi perlu dirahasiakan untuk menjaga kepentingan nasional, keamanan publik, dan privasi individu. Keterbukaan informasi yang berlebihan dapat memberikan celah bagi pihak yang tidak bertanggung jawab untuk memanfaatkannya dengan cara yang merugikan.

Penting untuk menemukan keseimbangan antara transparansi dan kerahasiaan dalam hal pengelolaan informasi. Proses pengambilan keputusan mengenai apa yang boleh dan tidak boleh diungkapkan kepada publik harus dilakukan secara bijaksana, dengan memperhatikan dampak dan konsekuensi dari setiap keputusan tersebut. Dengan demikian, prinsip keterbukaan informasi publik dapat dijalankan secara efektif dan bertanggung jawab. Asas manfaat (*type of benefits*)[65] dari kebijakan keamanan informasi dan siber yang tidak jelas/ambigu berdampak belum optimalnya implementasi keamanan informasi.[66]

Implementasi keamanan informasi di Indonesia masih belum optimal akibat regulasi yang ambigu dan kurang memberikan sanksi yang tegas terhadap pelanggaran keamanan data. Saat ini, regulasi terkait keamanan informasi cenderung hanya sebatas menghimbau tanpa memberikan ketegasan atau pengawasan yang memadai terhadap penggunaan persandian dalam berkomunikasi informasi rahasia di institusi pemerintah. Dalam konteks keamanan informasi, pentingnya penggunaan persandian untuk menjaga kerahasiaan dan integritas informasi yang berklasifikasi rahasia tidak boleh

---

[65] *Grindle*, Merilee S. *1980*. Politics and Policy Implementation in the Third World. New. Jersey : Princeton University Press

[66] Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara

diabaikan. Namun, tanpa adanya regulasi yang jelas dan sanksi yang tegas, implementasi keamanan informasi di sektor pemerintah bisa terbengkalai.

Regulasi yang ada saat ini tidak memberikan wewenang yang cukup luas kepada Badan Siber dan Sandi Negara (BSSN) dalam menjalankan tugasnya sebagai lembaga yang bertanggung jawab atas merumuskan dan melaksanakan kebijakan pengamanan informasi di Indonesia. Hal ini menjadi hambatan dalam menjaga keamanan informasi negara secara efektif. Selain itu, Rancangan Undang-Undang tentang rahasia negara juga masih tertunda dalam proses persetujuan hingga saat ini.

Dengan keterbatasan wewenang yang dimiliki BSSN dan belum disahkannya RUU tentang rahasia negara, perlindungan informasi negara menjadi rentan terhadap ancaman keamanan cyber yang semakin canggih. Oleh karena itu, diperlukan langkah-langkah untuk memperkuat peran dan wewenang BSSN serta segera menyelesaikan pembahasan RUU tentang rahasia negara agar keamanan informasi negara dapat terjaga dengan baik.

b. Jaring Komunikasi Sandi Nasional yang belum utuh

Menyelenggarakan Jaring Komunikasi Sandi Nasional (JKSN) yang hanya mencakup 64% dari total instansi pemerintah yang seharusnya terfasilitasi menjadi permasalahan yang krusial. Kondisi ini menunjukkan bahwa masih terdapat 36% potensi kebocoran informasi yang dapat terjadi di instansi pemerintah yang belum terintegrasi dengan JKSN[67]. Masalah ini menjadi poin kritis yang perlu segera diatasi guna menjaga keamanan informasi pemerintah yang merupakan aset penting negara.

Keterbatasan sumber daya, baik dari segi anggaran, sumber daya manusia, maupun peralatan sandi, menjadi faktor utama yang menghambat implementasi JKSN secara menyeluruh. Dari segi anggaran, diperlukan investasi yang lebih besar untuk menjangkau semua instansi pemerintah yang membutuhkan fasilitas JKSN[68]. Sumber daya manusia yang berkualitas dan berjumlah memadai juga diperlukan untuk mengoperasikan dan memelihara

[67] Ridwan, 2018. Implementasi Kebijakan Keamanan Informasi di Provinsi Sulawesi Tengah. Jurnal Ilmu Administrasi Universitas Subang Vol. 15 no 2
[68] Miller, 2017. *Performance-Based Budgeting: Concepts and Examples.* Routledge

sistem ini dengan baik. Selain itu, ketersediaan peralatan sandi yang memadai juga menjadi faktor penentu dalam keberhasilan implementasi JKSN.

Alokasi anggaran untuk melengkapi seluruh instansi pemerintah belum terintegrasi dengan JKSN. Pengadaan peralatan sandi dan perangkat lunak pendukung belum tersedia guna menunjang keberhasilan JKSN. Kurangnya sumber daya manusia yang berkualitas dan terlatih dalam bidang persandian serta keamanan informasi. Pelatihan dan peningkatan kompetensi bagi personel yang bertugas dalam operasional JKSN menjadi hal yang sangat penting untuk menjaga keberlangsungan system penyandian ini. Belum terbetuknya kerjasama antara lembaga terkait[69], baik pemerintah maupun swasta, untuk mendukung implementasi JKSN yang lebih luas. Kolaborasi antara berbagai instansi dan lembaga dapat mempercepat proses integrasi JKSN pada tingkat yang lebih tinggi.

c. Security Awareness Pejabat Publik Rendah

Masalah sosialisasi keamanan informasi yang tidak tepat sasaran oleh implementor kebijakan[70] menjadi perhatian penting dalam menjaga keamanan informasi di berbagai instansi. Hal ini disebabkan oleh kurangnya partisipasi dan kehadiran pejabat yang berwenang atau pimpinan instansi dalam kegiatan sosialisasi mengenai pentingnya persandian untuk menjaga keamanan informasi dari berbagai ancaman seperti intersepsi, fabrikasi, modifikasi, dan interupsi.

Kegiatan sosialisasi terkait keamanan informasi seringkali hanya diikuti oleh staf dan level pimpinan terendah, seperti eselon 4, sementara pejabat yang memiliki kekuasaan dan wewenang yang lebih tinggi jarang hadir atau bahkan tidak hadir sama sekali. Hal ini dapat menimbulkan dampak negatif dalam upaya menjaga keamanan informasi.

Ketidakhadiran pejabat atau pimpinan instansi dalam kegiatan sosialisasi keamanan informasi mengirimkan sinyal yang buruk kepada bawahan, yaitu kurangnya keseriusan dan prioritas terhadap keamanan informasi. Selain itu,

---

[69] Holmberg, Susanne & Buhl, H., 2020. *Organizing Interorganizational Collaboration: Theory and Method.* Edward Elgar Publishing

[70] *Grindle*, Merilee S. *1980*. Politics and Policy Implementation in the Third World. New. Jersey : Princeton University Press

tanpa partisipasi aktif dari pejabat yang berwenang, implementasi kebijakan keamanan informasi menjadi terhambat dan dapat meningkatkan risiko terhadap kebocoran atau penyalahgunaan informasi sensitif.

Seharusnya pimpinan instansi dan pejabat yang berwenang memberikan perhatian dan dukungan penuh terhadap kegiatan sosialisasi keamanan informasi. Pucuk Pimpinan sebagai pemegang kebijakan tertinggi memahami dan menginternalisasi pentingnya persandian dalam menjaga keamanan informasi serta mengambil langkah-langkah konkret untuk melibatkan diri secara aktif dalam program sosialisasi tersebut.

d. Ego Sektoral antar Instansi Pemerintah

Ego sektoral antar instansi pemerintah sering kali menjadi penghambat utama dalam upaya mengoptimalkan keamanan informasi di tingkat nasional. Dalam konteks ini, ego sektoral merujuk pada kecenderungan masing-masing instansi untuk mempertahankan otonomi, wewenang, dan kepentingan sendiri[71]. Ego sektoral bisa berdampak negatif pada tujuan negara, seperti keamanan informasi.

Setiap instansi pemerintah memiliki mandat dan tanggung jawab khusus yang sering kali menyebabkan instansi pemerintah lebih fokus pada pencapaian tujuan internal daripada pada kolaborasi lintas instansi. Dalam hal keamanan informasi, instansi yang memiliki tanggung jawab langsung terhadap pengelolaan data dan informasi lebih mementingkan prosedur internalnya daripada berbagi informasi atau bekerja sama dengan instansi lain untuk menciptakan sistem yang lebih terintegrasi dan aman.

Salah satu dampak nyata dari ego sektoral ini adalah adanya kesenjangan dalam pertukaran informasi antar instansi. Misalnya, jika satu instansi memiliki informasi kritis mengenai potensi ancaman keamanan siber, tetapi enggan berbagi informasi tersebut dengan instansi lain yang mungkin memiliki kapasitas untuk menanggulangi ancaman tersebut, maka celah dalam keamanan informasi dapat terbuka. Hal ini sering kali diperparah oleh perbedaan standar operasional dan kebijakan keamanan yang diterapkan

[71] Scott, Richard. 2020. *Institutions and Organizations: Ideas, Interests, and Identities*. SAGE Publications, Inc.

oleh masing-masing instansi, yang menyebabkan tidak adanya keselarasan dalam pendekatan terhadap ancaman keamanan informasi.

Selain itu, ego sektoral juga dapat menyebabkan lambatnya respons terhadap insiden keamanan informasi. Ketika suatu insiden terjadi, instansi yang terlibat mungkin lebih fokus pada upaya untuk melindungi citra dan reputasi instansi sendiri daripada segera berkoordinasi dengan instansi lain untuk memitigasi dampak insiden tersebut. Akibatnya, penanganan insiden menjadi kurang efisien dan berpotensi memperburuk situasi.

Pendekatan yang lebih kolaboratif dan terkoordinasi antar instansi pemerintah belum terbangun[72]. Mengembangkan kerangka kerja bersama untuk keamanan informasi, yang mengintegrasikan kebijakan, prosedur, dan standar operasional lintas instansi belum terjadi. Seharusnya antar instansi membangun budaya yang mendorong kerjasama dan saling percaya antar instansi, sehingga ego sektoral dapat diminimalisir dan tujuan keamanan informasi nasional dapat dicapai secara lebih efektif.

e. Literasi Digital Masyarakat Rendah

Tingkat literasi digital yang masih rendah di kalangan masyarakat turut berkontribusi pada rendahnya tingkat keamanan informasi secara keseluruhan. Masih banyak masyarakat yang kurang paham akan pentingnya keamanan informasi dan belum memahami dengan baik ancaman yang mungkin dihadapi saat berselancar di dunia maya[73]. Keadaan ini semakin diperparah dengan belum adanyaperan pemerintah daerah yang bertugas sebagai garda terdepan untuk memberikan sosialisasi dan edukasi mengenai ancaman informasi serta risiko yang dapat timbul saat beraktivitas di ruang digital.

Belum adanya peran pemerintah daerah yang mengedukasi masyarakat mengenai keamanan informasi menyebabkan minimnya pemahaman dan kesadaran akan pentingnya perlindungan data pribadi dan informasi sensitif di lingkungan cyber. Hal ini membuka celah bagi berbagai potensi ancaman seperti peretasan data, penipuan online, dan serangan malware yang dapat

[72] Holmberg, Susanne & Buhl, H., 2020. *Organizing Interorganizational Collaboration: Theory and Method.* Edward Elgar Publishing
[73] Jones, S. 2019. *Digital Literacy for Teachers: A Critical Guide*. Routledge

merugikan individu maupun lembaga. Tanpa pemahaman yang memadai, masyarakat rentan menjadi korban kejahatan cyber dan kerugian finansial yang tak terduga.

Oleh karena itu, diperlukan langkah-langkah konkret untuk meningkatkan literasi digital masyarakat serta memperkuat keamanan informasi secara keseluruhan. Instansi di level bawah perlu diberdayakan sebagai agen sosialisasi serta edukasi yang bertugas menyebarkan informasi terkait ancaman dan resiko di dunia siber. Penyuluhan mengenai tindakan preventif yang harus diambil untuk melindungi diri dari potensi bahaya cyber juga perlu ditingkatkan guna menciptakan lingkungan digital yang lebih aman dan terpercaya bagi seluruh masyarakat. Dengan upaya kolaboratif antarinstansi dan keterlibatan aktif masyarakat, diharapkan tingkat keamanan informasi dapat ditingkatkan secara signifikan.

Secara umum dakat disimpulkan bahwa kondisi keamanan informasi di Indonesia saat ini dinilai belum optimal. Masih terdapat kendala pada anggaran, dukungan politik, payung hukum RUU Rahasia Negara yang belum tersedia hingga saat ini. Regulasi dan peraturan mengenai keamanan siber di Indonesia masih lemah. Menurut Laporan National Cyber Security Index (NCSI) pada tahun 2022, Indonesia berada pada posisi ke-3 terendah antara negara G20 dalam indeks keamanan siber[74]. Selain itu, pejabat publik sering kali menggunakan telepon biasa atau komunikasi terbuka untuk menyampaikan pesan yang bersifat rahasia. Tindakan ini menunjukkan rendahnya kesadaran keamanan di kalangan pejabat publik, sehingga kebocoran informasi dapat terjadi akibat kesalahan manusia, kerentanan sistem, atau serangan siber. Akibatnya, data sensitif seperti informasi keuangan atau data pribadi dapat menjadi diketahui oleh publik. Dengan meningkatkan kesadaran keamanan informasi, individu dan organisasi dapat serta merta meminimalisir risiko keamanan informasi, melindungi data yang bersifat rahasia atau sensitif, dan mengurangi potensi kerugian. Oleh karena itu, penting bagi setiap individu dan organisasi untuk mengedepankan kesadaran keamanan informasi dalam era perkembangan teknologi informasi dan keamanan siber yang sangat pesat[75].

[74] Annur, Cindy M. (2022, September 13). Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20. Sumber [online]
[75] Pentingnya IT Security Awareness dan Risiko dari Keamanan Informasi. Sumber [online]

15. Upaya Pemerintah dalam Mengatasi Kebocoran Informasi dan Serangan Siber di Indonesia

Sebagai pemimpin, pemerintah memiliki peran penting dalam menjaga dan meningkatkan keamanan informasi negara, terutama informasi yang bersifat khusus dan rahasia. Informasi merupakan aset berharga yang harus dijaga demi keutuhan NKRI. Pemerintah harus aktif dalam meningkatkan keamanan informasi untuk melindungi data sensitif dan infrastruktur negara dari ancaman digital. Upaya yang tepat diperlukan untuk mencapai tujuan tersebut. Kepentingan nasional, termasuk kewaspadaan nasional Indonesia, dapat terwujud apabila pemerintah mampu memprediksi dan mengantisipasi ancaman digital dengan memanfaatkan segala peluang yang ada. Pemerintah memiliki tanggung jawab besar untuk melindungi keamanan informasi negara.

Dampak globalisasi terhadap kehidupan sosial, bangsa, dan negara mendorong perlunya adaptasi dan penyesuaian yang berkelanjutan. Persiapan, kualitas, dan tanggung jawab dalam menghadapi tantangan dan ancaman global sangat penting untuk keberhasilan dalam menghadapi dinamika global. Keberlangsungan eksistensi suatu negara menjadi hal yang vital dalam globalisasi. Pemenuhan kepentingan nasional merupakan kunci utama dalam menjaga serta mengembangkan kehidupan negara dalam hubungan dengan negara lain. Konsep kepentingan nasional menjadi landasan dalam kebijakan politik luar negeri, pertahanan, dan kebijakan lainnya. Pemahaman akan kepentingan nasional menjadi penting dalam menganalisis hubungan antar negara di dunia, terutama dalam dominasi negara bangsa dalam hubungan internasional.

Ancaman nyata adalah ancaman yang terus-menerus muncul, baik dari dalam maupun luar negeri, yang dapat mengancam kedaulatan, integritas wilayah, dan keamanan bangsa. Penanganan ancaman nyata menjadi prioritas utama pemerintah dalam menjaga keamanan negara. Contohnya, melakukan langkah-langkah preventif, memperkuat pertahanan, dan meningkatkan kerjasama internasional untuk mengatasi ancaman tersebut. Penting bagi setiap negara untuk terus memantau, mengidentifikasi, dan merespons ancaman nyata dengan

cepat dan efektif demi menjaga stabilitas dan keamanan dalam negeri serta hubungan dengan negara lain. Bentuk ancaman yang menjadi perioritas dalam penanganannya meliputi :

1) Terorisme dan radikalisme;
2) Separatisme dan pemberontakan bersenjata;
3) Bencana alam;
4) Pelanggaran wilayah perbatasan;
5) Perompakan dan pencurian sumber daya alam;
6) Wabah penyakit;
7) Serangan siber dan spionase;
8) Peredaran dan penyalahgunaan narkoba.[76].

Serangan siber merupakan ancaman nyata yang menuntut prioritas penanganan yang serius. Pemerintah perlu memberi perhatian pada masalah ini dan mengambil langkah-langkah yang tepat untuk menjaga keamanan informasi serta kewaspadaan nasional. Dalam keamanan informasi di Indonesia, terdapat berbagai isu dan fakta terkait permasalahan ini. Untuk mengatasi tantangan ini, pemerintah dapat melakukan langkah-langkah seperti peningkatan kesadaran masyarakat terhadap keamanan cyber, meningkatkan kerjasama internasional dalam pertukaran informasi, pengembangan kebijakan dan regulasi yang lebih ketat terkait keamanan siber, serta penguatan infrastruktur dan teknologi keamanan informasi di tingkat nasional. Berikut adalah upaya yang dapat dilakukan pemerintah untuk mengatasi permasalahan mengenai keamanan informasi:

a. Membuat Regulasi Keamanan Informasi yang Komprehensif.

Pentingnya membuat regulasi keamanan informasi yang komprehensif menjadi kunci dalam upaya mencegah kebocoran informasi yang sensitif. Dengan adanya regulasi yang kuat, dilengkapi dengan memperkuat wewenang Badan Siber dan Sandi Negara (BSSN), instansi pemerintah di seluruh tingkatan baik pusat maupun daerah akan diperintahkan untuk

[76] Lembaga Ketahanan Nasional Republik Indonesia. (2024). Bidang Studi: Kewaspadaan Nasional.

menggunakan persandian sebagai langkah pengamanan yang efektif terhadap informasi yang memiliki tingkat kerahasiaan tertentu.

Regulasi yang mengatur penggunaan persandian dalam pengelolaan informasi rahasia merupakan langkah yang strategis untuk melindungi data sensitif dari akses yang tidak sah dan ancaman keamanan cyber lainnya. Dengan memaksa seluruh instansi pemerintah untuk tunduk pada aturan tersebut, diharapkan tingkat keamanan informasi negara dapat ditingkatkan secara signifikan.

BSSN sebagai lembaga yang bertanggung jawab dalam merumuskan kebijakan keamanan informasi akan memainkan peran yang semakin penting dalam menjalankan tugasnya dengan wewenang yang lebih kuat. Langkah ini akan memberikan landasan hukum yang jelas bagi penerapan persandian dalam berbagai aktivitas pemerintah, baik di tingkat pusat maupun daerah.

Asas manfaat (*type of benefits*) dengan adanya regulasi yang komprehensif dan penguatan wewenang BSSN, diharapkan akan tercipta lingkungan kerja yang lebih aman dan terjamin dari ancaman kebocoran informasi sensitif[77]. Melalui langkah-langkah proaktif ini, diharapkan bahwa keamanan informasi negara bisa terjaga dengan baik, serta masyarakat dapat yakin bahwa data dan informasi yang mereka miliki akan dikelola dengan standar keamanan yang tinggi demi kepentingan bersama.

b. Meningkatkan Jaring Komunikasi Sandi Nasional (JKSN)

Jaring Komunikasi Sandi Nasional (JKSN) merupakan infrastruktur yang dibentuk dalam rangka memberikan layanan pertukaran informasi yang aman berupa akses internet, aplikasi hosting, *e-mail* dan menjadi perantara bagi komunikasi digital antara titik JKSN dengan Pusat Komando dan Kendali Komunikasi (Communication and Command Center – C3) yang berada di Kantor BSSN Ragunan, ataupun komunikasi antar titik JKSN.

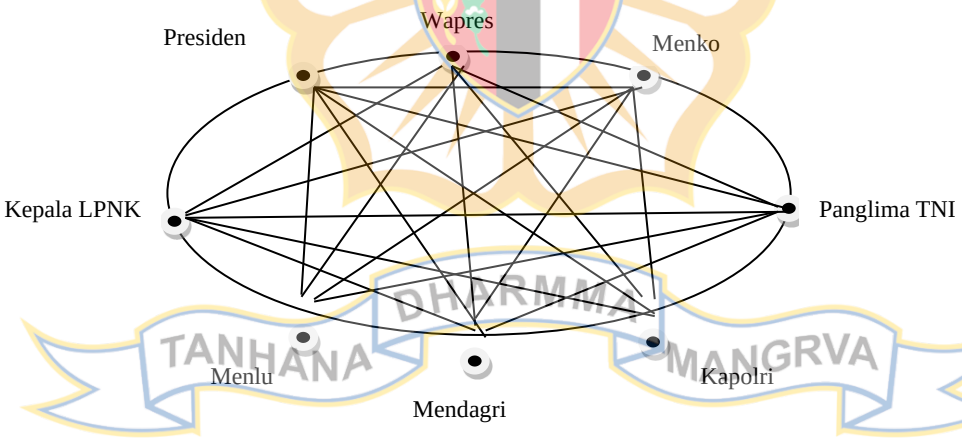
Jaring Komunikasi Sandi Nasional (JKSN) sebagai insfrastruktur perlu dipelihara dan dijaga kualitasnya agar dapat menyumbangkan performa yang maksimal, sehingga layanan pengamanan informasi dapat berjalan optimal.

[77] Grindle, Merilee S. *1980. Politics and Policy Implementation in the Third World*. New. Jersey : Princeton University Press

Sebagai lembaga pemerintah yang berada di bawah dan bertanggung jawab langsung kepada Presiden, Badan Siber dan Sandi Negara (BSSN) melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi. Persandian merupakan elemen penting dalam mewujudkan keamanan informasi pada penyelenggaraan pemerintahan, terutama dalam Sistem Pemerintahan Berbasis Elektronik (SPBE). Direktorat Operasi Sandi yang berada dalam Deputi Bidang Operasi Keamanan Siber dan Sandi, BSSN memiliki tugas melaksanakan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi sandi. Tugas tersebut meliputi bidang kriptografi, steganografi, pengamanan informasi berklasifikasi, analisis sandi, kontra penginderaan, analisis sinyal, pengamanan sinyal, dan komunikasi sandi. Direktorat Operasi Sandi diharapkan mampu memberikan kontribusi besar dalam mewujudkan keamanan informasi nasional[78].

Berikut adalah klasifikasi level keamanan informasi yang dijelaskan dalam gambar di bawah ini:

Gambar 1.2 Contoh Jaring Keamanan Informasi VVIP



Gambar di atas menjelaskan jaring komunikasi Very Very Important Person (VVIP) antara Presiden, Wakil Presiden, para Menteri, Panglima TNI, Kapolri dan Kejagung. Jaring komunikasi tersebut dilindungi dengan teknologi keamanan informasi sehingga komunikasi Presiden beserta pejabat VVIP

[78] Badan Siber dan Sandi Negara. *Laporan Kinerja Direktorat Operasi Sandi 2023*. Deputi Bidang Operasi Keamanan Siber dan Sandi

lainya terjaga dari upaya penyadapan dan pencurian informasi dari pihak-pihak yang tidak memiliki kewenangan untuk mengetahuinya.

Perkembangan teknologi dalam skala global telah membawa dampak yang sangat pesat bagi umat manusia. Perkembangan teknologi juga membawa konsekuensi negatif, terutama terkait dengan keamanan informasi. Ancaman terhadap keamanan informasi semakin meningkat seiring dengan kemajuan teknologi, terutama melalui metode penyadapan yang semakin berkembang. Ancaman keamanan informasi dengan menggunakan metode penyadapan mulai terarah langsung kepada pengguna akhir (end user) dengan memanfaatkan sistem komunikasi yang biasa digunakan oleh masyarakat. Hal ini tentu memberikan dampak yang serius terhadap privasi dan keamanan data pribadi pengguna. Informasi sensitif dan rahasia dapat dengan mudah diretas dan disalahgunakan oleh pihak yang tidak bertanggung jawab.

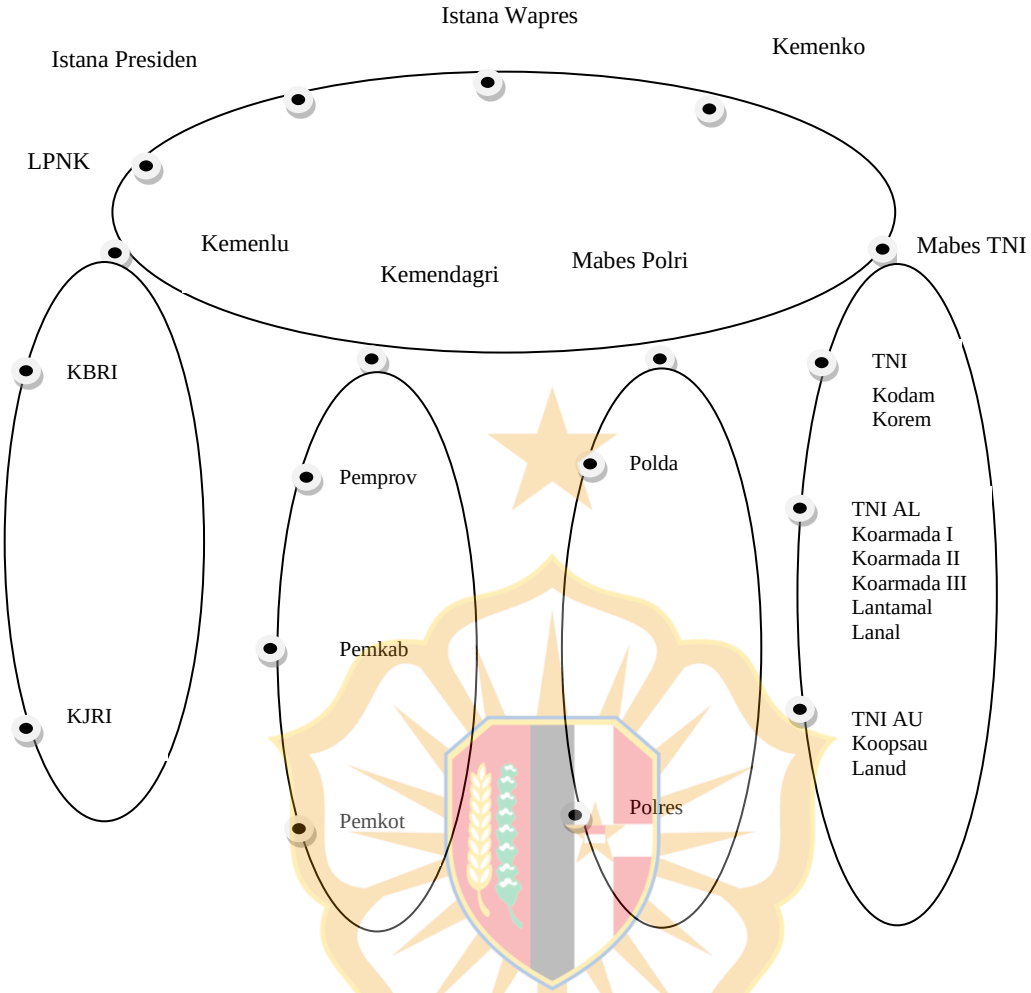
Berbagai teknik penyadapan telah dikembangkan, mulai dari peretasan password, malware, hingga social engineering. Metode penyadapan semakin canggih dan sulit dideteksi, menyebabkan kerentanan yang semakin besar terhadap keamanan informasi. Masyarakat perlu meningkatkan kesadaran akan pentingnya menjaga keamanan informasi pribadi serta melindungi diri dari ancaman cyber yang semakin canggih.

Bentuk layanan yang dilakukan BSSN dalam rangka pengamanan VVIP merupakan bentuk pengamanan dari ancaman penyadapan dan kebocoran informasi. Terdapat 8 (delapan) dokumen yang mengatur prosedur maupun teknis mengenai pelaksanaan Operasi Pengamanan Sinyal, yaitu:

- SOP Permohonan Layanan Kontra Penginderaan;
- SOP Pelaksanaan Layanan Kontra Penginderaan;
- SOP Pembuatan Surat Jawaban Permohonan Layanan Kontra Penginderaan;
- SOP Penyiapan Peralatan Kontra Penginderaan Fisik;
- SOP Operasi Kontra Penginderaan Fisik;
- SOP Analisis dan Mitigasi Indikasi Penyadapan;
- SOP Kontra Penginderan Jaring; dan
- SOP Pelaporan Kontra Penginderaan[79]

[79] Badan Siber dan Sandi Negara. *Laporan Kinerja Direktorat Operasi Sandi 2023*. Deputi Bidang Operasi Keamanan Siber dan Sandi

Gambar 1.3 Contoh Jaring Keamanan Informasi antar dan internal instansi



Berdasarkan gambar di atas, jaring komunikasi internal dan eksternal instansi dimana setiap instansi memiliki struktur yang berisi Kamar Sandi (Kasa), yaitu tempat dimana aktivitas pengamanan informasi dilaksanakan.. Pada gambar tersebut terlihat bahwa masing-masing instansi dapat saling berkomunikasi secara aman dan terlindungi dengan teknologi pengamanan informasi seperti komunikasi Markas Besar Tentara Nasional Indonesia (Mabes TNI) dengan Kementerian Koordinator, Kementerian Dalam Negeri dengan Kementerian Luar Negeri, Istana Presiden dengan Mabes TNI.

Selain komunikasi antar instansi, komunikasi juga berlangsung di internal instansi seperti di lingkungan Kementerian Dalam Negeri, contoh komunikasinya adalah komunikasi atau kirim terima informasi yang dikecualikan / rahasia antara Kementerian Dalam Negeri dengan Pemerintah Provinsi, Pemerintah Provinsi dengan Pemerintah kabupaten dan Pemerintah Kabupaten dengan Pemerintah Kota. Dari kedua gambar tersebut terlihat

perbedaan level pengamanan informasi. Pada gambar 1.2 menjelaskan pengamanan informasi milik personal (pejabat tinggi), sedangkan gambar 1.3 menjelaskan pengamanan informasi yang dimiliki institusi.

Sesuai dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Susunan Organisasi dan Tata Kerja Badan Siber dan Sandi Negara tentang Perubahan atas Peraturan Badan Nomor 6 Tahun 2021 tentang Susunan Organisasi dan Tata Kerja Badan Siber dan Sandi Negara, Direktorat Operasi Sandi merupakan satuan unit kerja yang berada di bawah naungan Deputi Bidang Operasi Keamanan Siber dan Sandi. Direktorat Operasi Sandi memiliki tugas untuk melakukan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi sandi, fokus pada kriptografi, steganografi, komunikasi sandi, dan pengamanan informasi berklasifikasi. Fungsi tersebut adalah hal yang sangat penting sebagai salah satu bentuk penjamin keamanan informasi, terutama di tengah semakin meningkatnya pemakaian teknologi informasi dan komunikasi[80].

Pemanfaatan Jaring Komunikasi Sandi Nasional yang utuh akan mampu melindungi dan menjaga kerahasiaan komunikasi pejabat tinggi negara yang berada didalam jaring VVIP. Sementara kirim terima informasi yang dikecualikan milik pemerintah / informasi rahasia terjaga keuntuhan dan keaslian informasi yang dikirim melalui jarring VIP antar instansi dan internal instansi masing-masing. Jaring Komunikasi Sandi Nasional harus utuh dan digunakan secara penuh oleh instansi pemerintah. Jika satu saja jaringan terputus, dengan kata lain, ada instansi pemerintah tidak menggunakan menggunakan peralatan sandi yang tergabung dalam Jaring Komunikasi Sandi Nasional, dipastikan keamanan informasi akan terancam dan akan berdampak kepada ketahanan nasional.

Dalam menghadapi tantangan keamanan informasi yang semakin kompleks di era transformasi digital, meningkatkan pengelolaan keamanan informasi guna melindungi kepentingan nasional menjadi prioritas utama. Untuk mencapai tujuan tersebut, perlu diimplementasikan sistem keamanan informasi yang komprehensif dan terintegrasi. Dimana langkah tersebut dapat

[80] Badan Siber dan Sandi Negara. *Laporan Kinerja Direktorat Operasi Sandi 2023*. Deputi Bidang Operasi Keamanan Siber dan Sandi

meliputi pembentukan kebijakan keamanan informasi yang jelas dan sesuai dengan standar, serta prosedur-prosedur yang dapat diterapkan secara konsisten di berbagai instansi pemerintah. Salah satu upaya keamanan informasi adalah membangun Jaring Komunikasi Sandi Nasional yang utuh dengan mengimplementasi teknologi keamanan informasi yang mutakhir, seperti enkripsi data, *firewall*, dan sistem keamanan lainnya guna melindungi data dan informasi yang dikecualikan milik pemerintah / informasi rahasia, termasuk dari serangan siber yang semakin canggih.

c. Meningkatkan *Security Awareness* Pejabat Publik Akan Pentingnya Keamanan Informasi

Perkembangan digitalisasi membawa dampak baru bagi pemimpin politik, ekonomi, dan masyarakat secara keseluruhan. Tidak hanya dibutuhkan kemahiran teknis dalam mengelola teknologi digital, digitalisasi juga mengharuskan para pengambil keputusan memiliki pemahaman pola pikir digital agar dapat mengidentifikasi dan mengevaluasi dengan akurat peluang dan tantangan yang ada. Konsep kepemimpinan digital menjadi kunci penting di era digital, di mana pejabat publik dihadapkan dengan peluang dan tantangan yang berkaitan dengan digitalisasi. Tentunya, konsep kepemimpinan digital memerlukan pemahaman betapa vitalnya kemampuan seorang pemimpin digital dalam mewujudkan tujuan guna mendukung keberhasilan transformasi digital dalam perekonomian dan masyarakat. Oleh karena itu, pelatihan dan pengembangan kemampuan kepemimpinan digital menjadi sangat penting agar pemimpin dapat menghadapi tantangan yang kompleks di era digital.[81].

Pemerintah berperan penting dalam menciptakan keunggulan kompetitif yang berkelanjutan, dan harus mencerminkan transformasi digital. Kepemimpinan digital pejabat publik dibangun untuk memimpin upaya teknologi digital, sambil menghadapi ancaman keamanan informasi. Tanggung jawab besar terhadap masyarakat, organisasi, perusahaan, karyawan, dan pemangku kepentingan harus diemban. Diperlukan perhatian serius dari

[81] Hensellek, Simon. (2020). *Digital Leadership : A Framework for Successful Leadership in the Digital Age.* Journal of Madia Management and Entrepreurship Vol.2

pemerintah dalam merancang strategi terbaik guna menciptakan keunggulan kompetitif di era digitalisasi. (Kollmann & Schmidt, 2016)[82].

Meningkatkan kesadaran keamanan (*security awareness*) pejabat publik merupakan hal yang sangat penting dalam upaya mewujudkan kewaspadaan nasional. Sebagai pihak yang memiliki akses dan tanggung jawab terhadap informasi penting negara, pejabat publik perlu diberikan pemahaman dan pelatihan yang memadai mengenai ancaman keamanan informasi serta praktik-praktik praktis untuk melindungi informasi tersebut. Pelatihan mencakup pengenalan dan pemahaman akan berbagai jenis ancaman keamanan informasi, cara mengidentifikasi tanda-tanda serangan siber, dan praktik-praktik yang dapat dilakukan untuk mencegah serangan siber.

Pejabat publik memiliki kewenangan untuk mengakses informasi yang sensitif dan mungkin bersifat pribadi, sehingga perlu dibekali pengetahuan mengenai pentingnya menjaga keamanan informasi. Oleh karenanya, para pejabat publik harus memiliki sikap yang tegas dan kebijakan yang tepat untuk melindungi data tersebut. Upaya ini dapat diwujudkan dengan menerapkan sistem keamanan yang efektif, seperti penggunaan algoritma enkripsi yang kuat, antivirus, dan *firewall*. Selain itu, pejabat publik harus menerapkan langkah-langkah dan prosedur yang ketat agar sistem dapat dikontrol secara efektif, misalnya pengawasan terhadap kontrol akses, pengawasan kontrol input, dan pengawasan kontrol output. Pejabat publik juga harus melakukan pemantauan terhadap aktivitas yang berhubungan dengan informasi sensitif yang mereka kelola agar dapat mencegah kebocoran oleh pihak yang tidak berwenang. Upaya pencegahan kebocoran informasi dapat dilakukan dengan menerapkan sistem monitoring yang efektif, seperti pengawasan log aktivitas dan pengawasan aktivitas pengguna. Selain itu, pejabat publik wajib melakukan pengujian terhadap keamanan informasi yang dimiliki. Langkah monitoring dapat diwujudkan melalui pelaksanaan sistem pengujian yang komprehensif, seperti pengujian kekuatan sandi, pengujian kekuatan *firewall*, dan pengujian kekuatan antivirus.

[82] Kollmann, T., & Hensellek, S. (2016). *The E-Business Model Generator*. In I. Lee (Ed.), *Encyclopedia of E-Commerce Development, Implementation, and Management* (pp. 26–36). IL: IGI Global.

Security awareness merupakan kemampuan individu atau organisasi untuk memahami dan mengetahui berbagai risiko keamanan informasi, serta tindakan yang perlu diambil untuk mengurangi risiko tersebut. Pentingnya keamanan informasi dibutuhkan karena kegagalan sistem dan perangkat keras, serangan siber, kegagalan perangkat keras, dan kejahatan siber dapat mengakibatkan kerugian, penipuan, maupun kerusakan data. Keamanan informasi meliputi perlindungan informasi atau data dari berbagai ancaman yang mengikutsertakan akses, penggunaan, perubahan, atau penghapusan yang tidak sah. Hal tersebut memiliki tujuan untuk memelihara kerahasiaan, integritas, dan ketersediaan informasi yang dimiliki oleh organisasi, institusi, atau individu.

Tujuan dari security awareness adalah untuk meningkatkan pemahaman seluruh pejabat publik tentang pentingnya keamanan informasi dan kesadaran akan tanggung jawab mereka terhadap keamanan informasi. Security awareness bukan hanya menjadi tanggung jawab Top Management, Tim TIK, dan Tim Keamanan Informasi semata, tetapi juga menjadi tanggung jawab setiap pejabat publik. Menurut Badan Siber dan Sandi Negara (BSSN), pada tahun 2021 tercatat lebih dari 1,6 miliar anomali lalu lintas atau serangan siber yang terjadi di berbagai wilayah Indonesia. Oleh karena itu, peningkatan kesadaran keamanan informasi menjadi hal yang vital untuk melindungi data dan sistem informasi dari ancaman cyber[83]. Penting untuk menerapkan *security awareness* pejabat publik agar mereka dapat terlindungi dari sasaran para peretas.

Pertama, security awareness menjadi penting karena memenuhi persyaratan ISO 27001 (2013). ISO 27001 merupakan standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) yang memberikan panduan mengenai langkah-langkah yang harus diterapkan oleh sebuah organisasi untuk menjaga keamanan informasi.

Kedua, kesadaran keamanan sangat penting karena dapat membantu organisasi menghadapi ancaman keamanan informasi yang terus berkembang dengan cepat, serta menjaga nilai dan reputasi organisasi. Ancaman

[83] Sukseskan Implementasi Security Awareness Melalui MONICA. Sumber [online].

keamanan informasi selalu berubah dan semakin kompleks, oleh karena itu, seluruh anggota organisasi perlu memiliki security awareness yang baik untuk mengidentifikasi, mencegah, dan menanggulangi berbagai ancaman tersebut.

Ketiga, kesadaran keamanan memiliki peran penting dalam mencegah serangan siber. Dalam kondisi ini, pencegahan serangan siber bertujuan untuk meningkatkan kesadaran para pejabat publik akan pentingnya perlindungan informasi yang bersifat sensitif dan rahasia. Dengan security awareness yang baik, para pejabat publik akan lebih waspada dan proaktif dalam menangani informasi dengan aman, serta memahami risiko-risiko yang terkait dengan kelalaian dalam penanganan informasi. Selain itu, kesadaran keamanan juga membantu individu maupun organisasi untuk memahami konsekuensi dari penanganan informasi sensitif yang kurang aman.

Keempat, kesadaran keamanan sangat penting karena merupakan program yang berkelanjutan. Program berkelanjutan mengacu pada upaya yang tidak hanya dilaksanakan sebagai kegiatan tahunan, tetapi juga diterapkan secara konsisten untuk mempertahankan dan meningkatkan kesadaran keamanan setiap saat. Kesadaran keamanan yang terus menerus ditingkatkan akan membantu individu maupun organisasi untuk selalu siap menghadapi berbagai ancaman keamanan informasi yang terus berkembang. Selain itu, kesadaran keamanan juga menjadi landasan bagi lembaga untuk merancang program-program kesadaran keamanan yang efektif

Restia Moegiono memaparkan langkah-langkah perumusan program security awareness sebagai berikut : menciptakan tim yang bertanggung jawab atas pengembangan dan pemeliharaan program *security awareness*, pembuatan program *security awareness* yang didasarkan pada peran masing-masing individu dalam organisasi, membangun tingkat kesadaran minimum terkait *security awareness* di seluruh lapisan organisasi, menentukan konten-konten yang relevan untuk program *security awareness*, memilih media yang efektif sebagai sarana penyampaian program *security awareness*[84].

[84] Pentingnya Security Awareness dalam Perusahaan, Berikut Poin Penting Pembuatannya. Sumber [online]

d. Meningkatkan literasi digital masyarakat guna membangun kewaspadaan nasional

Pada era modern ini, kemajuan teknologi informasi berkembang dengan pesat dan menjadi sesuatu yang tidak dapat dielakkan, sehingga seluruh masyarakat perlu menerimanya. Dengan demikian, perlu untuk menekankan pentingnya literasi digital yang dilakukan oleh masyarakat. Tidak dapat dipungkiri, teknologi informasi memberikan banyak perkembangan dan kemajuan bagi keberlangsungan hidup manusia. Penggunaan komputer dan internet semakin dimanfaatkan untuk membantu mempermudah berbagai macam aktivitas manusia. Perangkat komputer dan digital lainnya terus berkembang sebagai produk yang semakin canggih, termasuk berbagai perangkat gawai, sehingga memungkinkan segala macam informasi untuk diakses dan disebarkan secara mudah melalui jaringan internet. Namun, tidak semua informasi yang tersebar di internet memiliki karakter yang positif dalam perkembangannya. Banyak informasi lain yang bersifat negatif dan membawa dampak buruk bagi masyarakat, seperti ujaran kebencian, penipuan, berita palsu, radikalisme, dan kejahatan siber lainnya. Dibutuhkan kebijakan dan kemampuan dari pengguna *gadget* dalam mengontrol informasi yang diterimanya dari jaring internet.

UNESCO, sebagai organisasi internasional yang fokus pada bidang pendidikan, ilmu pengetahuan, dan kebudayaan, menyatakan bahwa literasi digital memiliki kaitan erat dengan kemampuan hidup para pengguna. Literasi digital tidak hanya melingkupi penggunaan teknologi, tetapi juga keterampilan pengguna dalam menggunakan teknologi, berpikir kritis, kreatif, dan inovatif, serta keinginan untuk belajar guna mengembangkan kompetensi digital.[85].

Istilah literasi digital (*digital literacy*) pertama kali diperkenalkan oleh Paul Glitser pada tahun 1997. Paul menyatakan bahwa literasi digital adalah kemampuan untuk menggunakan teknologi dan informasi dari perangkat digital secara efektif dan efisien dalam berbagai konteks seperti pendidikan, pekerjaan, dan kehidupan sehari-hari. Bawden (2001) juga menjelaskan bahwa literasi digital merupakan konsep yang berdasarkan pada literasi

[85] Indeks Literasi Digital Indonesia Kembali Meningkat Tahun 2022. Sumber [online]

komputer dan informasi. Beliau menyebutkan ada tujuh aspek di dalam literasi digital, yakni:

1) Kemampuan merumuskan pengetahuan, yaitu kemampuan untuk mengembangkan informasi dari berbagai sumber yang valid.
2) Kemampuan menyajikan informasi dengan berpikir kritis, dengan memahami informasi dan memastikan keakuratan serta kelengkapan sumber informasi dari internet.
3) Kemampuan membaca dan memahami informasi yang terus berkembang.
4) Pemahaman akan pentingnya media konvensional dan hubungannya dengan media internet.
5) Kesadaran terhadap pentingnya akses individu dalam menyediakan referensi informasi.
6) Kemampuan menyaring informasi yang diterima.
7) Keterasaan nyaman dan aman dalam mengakses serta menyebarkan informasi.[86].

Menurut AJ. Bellshaw, terdapat delapan unsur penting yang dapat meningkatkan literasi digital masyarakat, yaitu unsur Kultural, Kognitif, Konstruktif, Komunikatif, Kepercayaan diri, Kreatif, Kritis, dan Tanggung jawab sosial. Artinya, diperlukan pendekatan multi-dimensi dalam proses pembelajaran masyarakat agar mereka dapat memiliki pemahaman digital yang baik, mampu menggunakan teknologi, serta memiliki kecerdasan, kreativitas, dan keberbudayaan dalam penggunaan teknologi[87]. Maraknya penyebaran informasi melalui media digital menuntut masyarakat untuk memiliki kemampuan literasi digital yang patut dikembangkan dan menjadi pembelajaran seumur hidup. Dengan pemahaman yang baik akan literasi digital, masyarakat akan lebih selektif dalam memilah informasi, tidak mudah terpengaruh, dan mencari kembali kebenaran dari setiap informasi yang

[86] Kurnianingsih, I, dkk. (2017). Upaya Peningkatan Kemampuan Literasi Digital bagi Tenaga Perpustakaan Sekolah dan Guru di Wilayah Jakarta Pusat Melalui Pelatihan Literasi Informasi. *Jurnal Pengabdian kepada Masyarakat*, Vol. 3(1).

[87] Menghalau Hoax Melalui Peningkatan Literasi Digital. Sumber [online].

diterima, baik yang berasal dari media cetak maupun elektronik. Hal yang terpenting dalam peningkatan literasi digital adalah meningkatnya kualitas hidup dan kesejahteraan masyarakat. Dengan literasi digital yang baik, masyarakat dapat memanfaatkan teknologi dengan lebih efektif untuk meningkatkan pengetahuan, keterampilan, akses informasi, serta berpartisipasi dalam kehidupan sosial dan ekonomi secara lebih baik sehingga mendorong kesejahteraan dan perkembangan yang berkelanjutan.

Meningkatnya literasi digital masyarakat merupakan hal yang penting guna memastikan bahwa masyarakat dapat beradaptasi dengan dunia digital dan dapat menggunakan teknologi secara aman dan bertanggung jawab. Langkah-langkah yang dapat dilakukan untuk meningkatkan literasi digital masyarakat adalah dengan mengadakan program pelatihan dan edukasi mengenai pentingnya literasi digital dan bahayanya berita palsu yang perlu ditingkatkan dan disosialisasikan secara merata. Masyarakat perlu diberikan pengetahuan dan pemahaman yang baik mengenai ancaman serta risiko di dunia digital, seperti *phishing*, *malware*, dan hoaks, serta cara mengidentifikasi dan menghindari berbagai ancaman tersebut. Pelatihan ini dapat dilakukan melalui *workshop*, seminar, atau kampanye literasi digital di berbagai komunitas maupun *platform* media sosial.

Selain itu, kolaborasi yang dilakukan antara institusi pendidikan dan lembaga swadaya masyarakat juga dapat memperkuat upaya peningkatan literasi digital bagi masyarakat. Materi literasi digital dapat diterapkan ke dalam kurikulum pendidikan formal, baik mulai dari tingkat sekolah dasar hingga perguruan tinggi. Sementara lembaga swadaya masyarakat dapat menyelenggarakan seminar atau pelatihan literasi digital bagi masyarakat umum. Masyarakat juga harus mau menerima pengetahuan dan menjalankan materi yang sudah diberikan. Masyarakat harus peduli dan ikut serta terlibat dalam meningkatkan keamanan informasi dengan meningkatkan literasi digital.

BAB IV

PENUTUP

16. SIMPULAN

Dalam era transformasi digital yang semakin maju seperti sekarang ini, keamanan informasi menjadi sangat krusial untuk diperhatikan. Bukan hanya untuk melindungi data pribadi, namun juga untuk menjaga keamanan nasional secara keseluruhan. Melalui langkah-langkah yang tepat, kita dapat meningkatkan keamanan informasi guna mewujudkan kewaspadaan nasional yang lebih baik.

1. Implementasi keamanan informasi di Indonesia masih belum optimal, indikatornya adalah :
   a. Penyelenggaraan Jaring Komunikasi Sandi Nasional (JKSN) baru mencakup 64% dari total instansi pemerintah yang seharusnya terfasilitasi. Artinya, masih terdapat 36% potensi kebocoran informasi yang dapat terjadi di instansi pemerintah yang belum terintegrasi dengan JKSN. Masalah ini merupakan poin kritis yang perlu segera diatasi untuk menjaga keamanan informasi pemerintah yang merupakan aset penting negara.
   b. Rendahnya kesadaran akan keamanan informasi di kalangan pejabat publik. Mereka cenderung lebih nyaman menggunakan alat komunikasi konvensional ketimbang peralatan sandi yang canggih seperti *Cryptophone*. Meskipun *Cryptophone* menawarkan keamanan yang tinggi dengan sinkronisasi yang cepat, namun pejabat publik lebih memilih faktor kecepatan dalam menggunakan alat komunikasi. Prioritas ini menyebabkan risiko kebocoran informasi yang tinggi karena keamanan tidak diutamakan.
   c. Tingkat pemahaman masyarakat mengenai keamanan informasi juga masih rendah, terutama dalam hal berselancar di dunia maya. Banyak masyarakat yang belum memahami resiko dan ancaman keamanan yang dapat terjadi saat beraktivitas online.

2. Penyebab belum optimalnya implementasi keamanan informasi adalah:
   a. Konten dari regulasi yang ambigu, dimana regulasi hanya sebatas menghimbau namun tidak memaksa apalagi memberikan sanksi jika pejabat publik dan instansi pemerintah tidak menggunakan persandian dalam mengkomunikasikan informasi-informasi yang dikecualikan atau yang rahasia.
   b. Terbatasnya sumber daya, baik anggaran, sumber daya manusia sandi baik dari aspek kualitas maupun kuantitas, peralatan sandi guna menunjang Jaring Komunikasi Sandi Nasional.
   c. Sosialisasi keamanan informasi yang tidak tepat sasaran. Pejabat yang berwenang atau pimpinan instansi tidak menghadiri kegiatan sosialisasi pentingnya persandian guna menjaga keamanan Informasi dari berbagai ancaman seperti intersepsi, fabrikasi, modifikasi dan interupsi. Kegiatan sosialisasi cenderung diikuti oleh staf dan level pimpinan terendah dalam hal ini eselon 4. Sehingga *security awearness* pejabat publik rendah. Dampaknya pejabat publik lebih nyaman menggunakan alat komunikasi konvensional ketimbang peralatan sandi yang canggih seperti *Cryptophone.*
   d. Ego sektoral antar instansi pemerintah sehingga belum terbentuk interoperabilitas diantara instansi pemerintah. Banyak instansi pemerintah tidak mau menggunakan peralatan sandi atau peralatan keamanan informasi karena mengganggap itu tugas Badan Siber dan Sandi Negara.
   e. Kurangnya literasi digital, edukasi dan sosialisasi mengenai keamanan informasi, menjadi faktor utama rendahnya pemahaman masyarakat dalam menghadapi risiko siber di era transformasi digital.

3. Upaya pemerintah dalam mengatasi kebocoran informasi dan serangan siber yang terjadi di Indoensia.
   a. Membuat regulasi seperti undang-undang rahasia negara guna memperkuat wewenang Badan Siber dan Sandi Negara dan memaksa seluruh instansi pemerintah untuk menggunakan persandian dalam kirim terima dan berkomunikasi rahasia.

b. Membangun Jaring Komunikasi Sandi Nasional yang utuh di seluruh instansi pemerintah baik dalam maupun luar negeri serta menambah pendidikan tenaga ahli dalam bidang siber dan sandi guna memenuhi kebutuhan sumber daya manusia.
c. Memerintahkan pejabat publik untuk mengikuti kursus singkat tentang keamanan informasi dan ancaman serta tantangan yang dihadapi kedepan di era transformasi digital dengan regulasi yang mewajibkan setiap pejabat publik untuk mengikutinya.
d. Membangun interoperabilitas instansi pemerintah. Jaring Komunikasi Sandi Nasional dapat terwujud sepenuhnya dengan dukungan dari semua instansi pemerintah. Membangun interoperabilitas instansi pemerintah penting untuk memastikan komunikasi yang aman dan efektif antar instansi pemerintah serta menjaga keamanan informasi yang bersifat rahasia dan sensitif. Interoperabilitas yang baik akan memungkinkan pertukaran data yang lancar dan terjamin antar instansi pemerintah, sehingga kerja sama dan koordinasi dalam berbagai bidang dapat berjalan dengan lebih efisien dan efektif.
e. Melakukan literasi digital, edukasi dan sosialisasi kepada masyarakat mengenai pentingnya keamanan informasi dan risiko cyber di era transformasi digital. Kampanye sosial, seminar, dan pelatihan secara rutin dapat meningkatkan kesadaran masyarakat akan risiko cyber yang mungkin mengancam keamanan informasi pribadi dan institusi.

Dengan langkah-langkah preventif dan proaktif yang terkoordinasi dengan baik, diharapkan implementasi keamanan informasi di Indonesia dapat meningkat, baik di tingkat institusi pemerintah maupun kesadaran masyarakat luas, sehingga keberlangsungan informasi negara dapat terjaga dengan baik.

17. REKOMENDASI

Rekomendasi untuk meningkatkan keamanan informasi guna mewujudkan kewaspadaan nasional adalah :

1. Kepada Pemerintah dan DPR, agar
   a. Menyusunan Kebijakan Keamanan Informasi Nasional yang komprehensif dan mengikat untuk mengatur perlindungan data dan informasi sensitif secara menyeluruh. Kebijakan ini harus mencakup regulasi yang jelas, sanksi yang tegas bagi pelanggar, serta mekanisme pengawasan dan evaluasi yang efektif. Kebijakan ini memberi wewenang kepada BSSN untuk memaksa seluruh instansi pemerintah untuk menggunakan persandian dan memberikan sanksi jika instansi pemerintah tidak melaksanakannya. Kebijakan keamanan informasi harus di evaluasi secara periodik satu tahun sekali dengan memonitor perkembangan ancaman keamanan informasi.
   b. Mengalokasikan anggaran yang memadai untuk membangun infrastruktur keamanan informasi yang tangguh serta mendukung riset dan pengembangan solusi keamanan informasi yang inovatif. Kemenkominfo membangun infrastruktur jaringan dan BBSN membuat arsitektur Jaring Komunikasi Sandi Nasional, mengadakan pelatihan bagi tenaga ahli keamanan informasi, dan pengembangan sistem keamanan yang handal.
   c. Menempatan posisi jabatan strategis yang menangani keamanan informasi di instansi pemerintah pada level eselon I, supaya lebih mudah dalam pengambilan keputusan mengingat ancaman keamanan informasi dan siber sangat membahayakan ketahanan nasional.

2. Kepada Kementerian Komunikasi dan Informasi dan Pemerintah Daerah, agar :
   a. Melakukan penguatan kerjasama lintas sektor antara pemerintah, swasta, dan masyarakat guna menyediakan infrastruktur jaringan yang komprehensif.

b. Menyediakan jaringan khusus untuk kirim terima dan komunikasi rahasia negara guna menjaga keamanan informasi secara holistik sehingga informasi sensitif dapat lebih mudah dilindungi dari serangan pihak-pihak yang tidak bertanggung jawab.
c. Berkolaborasi dengan pemerintah daerah, mengedukasi masyarakat betapa pentingnya keamanan informasi, melalui program edukasi dan sosialisasi kepada masyarakat mengenai resiko keamanan informasi yang mungkin terjadi dan langkah-langkah yang dapat diambil untuk melindungi informasi pribadi. Semakin tinggi tingkat kesadaran masyarakat, semakin sulit pula bagi pihak-pihak jahat untuk melakukan serangan terhadap informasi sensitif.
d. Melaksanakan monitoring terpadu terhadap lalu lintas informasi di dunia siber dengan memfilter dan memblokir konten-konten yang dapat merugikan masyarakat serta merusak persatuan dan kesatuan berbangsa dan bernegara.

3. Kepada Badan Siber dan Sandi Negara, agar :
   a. Mendidik sumber daya manusia siber dan sandi yang memadai baik dari aspek kualitas dan kuantittas.
   b. Membuat peralatan keamanan informasi yang mandiri dan tangguh serta algorithma yang *unbreakable.*
   c. Membangun arsitektur Jaring Komunikasi Sandi Nasional yang interoperabilitas antar instansi pemerintah pusat dan daerah.
   d. Melakukan kerjasama internasional dalam bidang keamanan informasi sangat penting mengingat sifat serangan cyber yang tidak mengenal batas wilayah. Dengan menjalin kerjasama dengan negara-negara lain, Indonesia dapat memperoleh informasi dan dukungan dalam menangani ancaman keamanan informasi secara global.

4. Kepada akademisi, agar melakukan Riset dan kajian yang inovasi dalam bidang keamanan informasi guna mengantisipasi perkembangan teknologi dan tren serangan yang terus berkembang.

DAFTAR PUSTAKA

BUKU

Badan Siber dan Sandi Negara. *Laporan Kinerja Direktorat Operasi Sandi 2023*. Deputi Bidang Operasi Keamanan Siber dan Sandi

Fatah Syukur NC. (2008). *Teknologi Pendidikan*. Semarang: Rasai Media Group.

Grindle, Merilee S. *1980*. Politics and Policy Implementation in the Third World. New. Jersey : Princeton University Press

Hilmi, M. (2020). *Modul Teori Perubahan Sosial*. Universitas Jember

Hodge, BJ. & Anthony, William P. (1988). *Organization Theory*. 3rd edition. Massachusetts, Allyn and Bacon Inc.

Holmberg, Susanne & Buhl, H., 2020. *Organizing Interorganizational Collaboration: Theory and Method.* Edward Elgar Publishing

Jones, Gareth R. (1997). *Organizational Theory: Text and Cases*. 2nd edition. Reading: Addison Wesley Longman Publishing Company.

Jones, Susan. 2019. *Digital Literacy for Teachers: A Critical Guide*. Routledge

Kansong, Usman. Relevansi Nilai-Nilai Pancasila dalam Kehidupan Berbangsa dan Bernegara para Era Teknologi Informasi. Dirjen Informasi dan Komunikasi Publik Kementerian Komunikasi dan Informatika.

Laporan Bulan Desember tahun 2020, Pusat Operasi Keamanan Siber Nasional, BSSN.

Lembaga Ketahanan Nasional Republik Indonesia. (2024). Bidang Studi: Kewaspadaan Nasional.

Lenon, Michael dan Gary Berg-Cross, 2010. *Toward a High Performing Open Government* : *The Public Manager*. Winter 2010.

Miller, Gerald. 2017. *Performance-Based Budgeting: Concepts and Examples.* Routledge

Muhammad Kristiawan, dkk, (2018). *Inovasi Pendidikan*. Ponorogo : Wade Group

Nur Kholifah, dkk. (2021). *Inovasi Pendidikan*. Medan: Yayasan Kita Menulis.

Petry, T. (2016). *Digital Leadership* : *Erfolgreiches Fiihren in Zheiten der Digital Economy.* Freiburg : haufe-Lexware.

Ridwan. 2016. Implementasi Kebijakan Keamanan Informasi di provinsi Sulawesi Tengah.

Riyanto (2017). Kewaspadaan Nasional, Bela Negara dan Integrasi Nasional. Puskom Publik Kemhan.

Sari, D. C., Purba, D. W., & Hasibuan, M. S. (2019). Inovasi Pendidikan Lewat Transformasi Digital. Yayasan Kita Menulis.

Scott, Richard. 2020. *Institutions and Organizations: Ideas, Interests, and Identities*. SAGE Publications, Inc.

Sumarkidjo, 2006. Jelajah Kriptografi. Lembaga Sandi Negara.

Triwidodo dkk (2024). Kewaspadaan Nasional. Lembaga Ketahanan Nasional RI.

JURNAL

Danuri, M. (2019). Perkembangan dan Transformasi Teknologi Digital. *Jurnal Ilmiah Infokam*. 15(2).

E.E.W. Tulungen., J.B. Maramis., D.P.E. Saerang. (2022). Transformasi Digital: Peran Kepemimpinan Digital. *Jurnal EMBA*. 10 (2).

Fajarwati, A & Rahmadilla, U. (2022). Model Implementasi Kebijakan Merilee Grindle Studi Kasus Penyerapan Tenaga Kerja Lokal pada PT. Meiji Rubber Indonesia Kabupaten Bekasi. *Jurnal Dialog*. 7(1).

Fisk, P. (2002). The making of a digital leader. Business Strategy Review, 13(1), 43–50.

Hasiono, K & Santi, RCN. (2020). Menyongsong Transformasi Digital. Proceeding SENDIU. ISBN: 978-979-3649-72-6.

Hensellek, Simon. (2020). *Digital Leadership : A Framework for Successful Leadership in the Digital Age.* Journal of Madia Management and Entrepreurship Vol.2

Husin, I. (2022). Teori Organisasi. *Jurnal GERBANG STMIK Bani Saleh*. Vol 12 (2).

Kementerian Pertahanan. (2017). Kewaspadaan Nasional, Bela Negara, dan Integrasi Nasional. WIRA. Vol. 67 (51).

Kollmann, T., & Hensellek, S. (2016). *The E-Business Model Generator*. In I. Lee (Ed.), *Encyclopedia of E-Commerce Development, Implementation, and Management* (pp. 26–36). IL: IGI Global.

K. Osmundsen, J. Iden, and B. Bygstad, "Digital Transformation: Drivers, Success Factors, and Implications," Mediterr. Conf. Inf. Syst. Proc., vol. 12, pp. 1–15, 2018.

Kotarba, M. (2018). Digital transformation of business models. Foundations of Management, 10(1), 123–142.

Kurnianingsih, I, dkk. (2017). Upaya Peningkatan Kemampuan Literasi Digital bagi Tenaga Perpustakaan Sekolah dan Guru di Wilayah Jakarta Pusat Melalui Pelatihan Literasi Informasi. *Jurnal Pengabdian kepada Masyarakat*, Vol. 3(1).

Liu, D.-Y., Chen, S.-W. & Chou, T.-C., (2011). *Resource fit in digital transformation: Lessons learned from the CBC Bank global e-banking project. Management Decision*, 49(10), pp.1728–1742.

M. Jusuf, M., Y. Tampanguma, M., & Mewengkang, F. (2022). Tindak Pidana Intersepsi (Penyadapan) diluar Penegak Hukum Teknologi Informasi dan Komunikasi di Indonesia. *Jurnal Unsrat*.

Ridwan, 2018. Implementasi Kebijakan Keamanan Informasi di Provinsi Sulawesi Tengah. Jurnal Ilmu Administrasi Universitas Subang Vol. 15 no 2

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. International Journal of Information Management, 60(April).

Westerman, G., Calméjane, C., & Bonnet, D., Ferraris, P., & McAfee, A. (2011). *Digital Transformation: A roadmap for billion-dollar organizations*. MIT Center for Digital Business and Capgemini Consulting, 1(1–68).

Westerman, G., Bonnet, D., & Mcafee, A. (2014). The Nine Elements of Digital Transformation Opinion & Analysis. MIT Sloan Management Review, 55(3), 1–6.

PERATURAN PERUNDANGAN

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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

Undang-Undang Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara.

Peraturan Presiden Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara

Peraturan Presiden Nomor 115 Tahun 2022 tentang Kebijakan Pembinaan Kesadaran Bela Negara.

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

Peraturan Presiden Nomor 82 Tahun 2023 Tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional.

WEBSITE

Annur, Cindy M. (2022, September 13). Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20. https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20 . Diakses 16 Maret Pukul 13.00 WIB

APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang, 2024. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20mengumumkan%20jumlah%20pengguna%20internet,jiwa%20penduduk%20Indonesia%20tahun%202023. Diakses 14 Maret 2024 pukul 20.43 WIB

Ashari, 2020. Keamanan Informasi : sudah saatnya kita peduli Sumber https://www.djkn.kemenkeu.go.id/artikel/baca/13113/Keamanan-Informasi-Sudah-Saatnya-Kita-Peduli.html diakses 13 Agustus 2024 pukul 19.45 wib

Ayuwuragil, 2017. Kesadaran Keamanan Siber Indonesia Peringkat Ke – 70 Dunia. https://www.cnnindonesia.com/teknologi/20171206162248-185-260555/kesadaran-keamanan-siber-indonesia-peringkat-ke-70-dunia diakses 13 Agustus 2024 pukul 2020 wib

Brennen, S.& Kreiss, D. (2016). Digitalization and Digitization. Available online: http://culturedigitally.org/2014/09/digitalization-and-digitization Diakses 5 Maret 2024 pukul 20.0 wib.

CISSReC Lembaga Riset Keamanan Siber. Diakses pada 14 Maret 2024 pukul 13.05 wib.

Cybercrime in Southeast Asia. https://www.aspi.org.au/report/cybercrime-southeast-asia Diakses pada 14 Maret 2024 pukul 20.40 WIB

Diskominfo provsu. (2017, Desember 7). Pentingnya Pengamanan Informasi di Instansi Pemerintah. https://diskominfo.sumutprov.go.id/artikel-686-pentingnya-pengamanan-informasi-di-instansi-pemerintah.html Diakses pada 14 Maret 2024 pukul 15.15 WIB

Global Cyber Crime Statistics. https://aag-it.com/the-latest-cyber-crime-statistics/. Diakses pada 14 Maret 2024 pukul 20.35 wib.

Hacker Bjorka is Back, Data Apa saja yang Pernah dibocorkan?. https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka-is-back-data-apa-saja-yang-pernah-dibocorkan Diakses 7 Juni 2024. Pkul 20.59. WIB.

Indeks Literasi Digital Indonesia Kembali Meningkat Tahun 2022. https://www.kominfo.go.id/content/detail/39858/literasi-digital-masyarakat-indonesia-membaik/0/artikel. Diakses 15 Maret 2024 Pukul 15.00 WIB

Information Security Management System (ISMS). https://www.djkn.kemenkeu.go.id/kanwil-jakarta/baca-artikel/16304/Information-Security-Management-System-ISMS.html#:~:text=Keamanan%20Informasi%20DASAR%20TEORI%20Keamanan,media%20elektronik%20atau%20non%20elektronik. Diakses 15 Maret pukul 13.25 WIB

Internet Crime Complaint Center. https://www.ic3.gov/. Diakses 14 Maret 2024 pukul 20.30 WIB.

Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat Diakses pada 14 Maret 2024 pukul 20.45 WIB

Kementerian Keuangan RI. 2023. Transformasi Digital untuk Masa Depan Ekonomi dan Bisnis di Indonesia. Kementerian Keuangan Republik Indonesia. https://djpb.kemenkeu.go.id/porta l/id/berita/berita/nasional/4074-transformasi-digital-untuk-masadepan-ekonomi-dan-bisnis-diindonesia.html diakses 14 maret 2024 pukul 21.00 wib.

Menghalau Hoaks Melalui Peningkatan Literasi Digital. https://dkpus.babelprov.go.id/content/menghalau-hoax-melalui-peningkatan-literasi-digital?qt-artikel=1. Diakses pada 15 Maret 2024 pukul 16.00 WIB.

Pemkot Jogja Gelar Jarring Komunikasi Sandi Internal. https://warta.jogjakota.go.id/detail/index/3867 Diakses pada 14 Maret 2024 pukul 15.10 WIB.

Penanggulangan Kejahatan Siber di ASEAN, 2023. https://sin.do/u/ioshttps://nasional.sindonews.com/read/1175677/18/penanggulangan-kejahatan-siber-di-asean-1692007731/30 Diakses 14 Maret 2024 pukul 20.42 WIB.

Pentingnya Security Awareness dalam Perusahaan, Berikut Poin Penting Pembuatannya. https://kliklegal.com/pentingnya-security-awareness-dalam-perusahaan-berikut-poin-penting-pembuatannya/. Diakses 16 Maret 2024 Pukul 13.40 WIB.

Pentingnya IT Security Awareness dan Risiko dari Keamanan Informasi. https://www.ad-ins.com/id/our-story/kisah-adins/pentingnya-it-security-awareness-dan-risiko-dari-keamanan-informasi/. Diakses 16 Maret 2024 Pukul 13.00 WIB.

Prinsip Keamanan Informasi. https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/13120/Keamanan-Informasi.html. Diakses 20 Pebruari 2024 Pukul 19.00 WIB

Putra, D. (2023). Hati-hati, Serangan Siber di Indonesia Capai 1,65 Juta. https://www.cnbcindonesia.com/tech/20230221220938-37-415809/hati-hati-serangan-siber-di-indonesia-capai-165-juta diakses 20 Pebruari 2024 pukul 19.00 wib.

Rendahnya Literasi Digital Indonesia. https://binus.ac.id/character-building/2023/02/rendahnya-literasi-digital-indonesia/ Diakses pada 14 Maret 2024 pukul 15.20 wib.

Salazar (2005) dalam Riadi, Muchlisin. (2022). *Keamanan Informasi.* https://www.kajianpustaka.com/2022/10/keamanan-informasi.html. Diakses pada 15 Maret 2024 Pukul 13.40 wib.

Sari, R.P. (2024). Ancaman Siber Meningkat, Pemerintah dan Korporasi Diminta Bersatu. https://www.cloudcomputing.id/berita/ancaman-siber-meningkat diakses 27 Januari 2024 pukul 19.00 wib.

Siregar, R. (2020, Mei 20). Prinsip Keamanan Informasi. https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/13120/Keamanan-Informasi.html. Diakses pada tanggal 20 Mei 2024 pukul 17.00 wib.

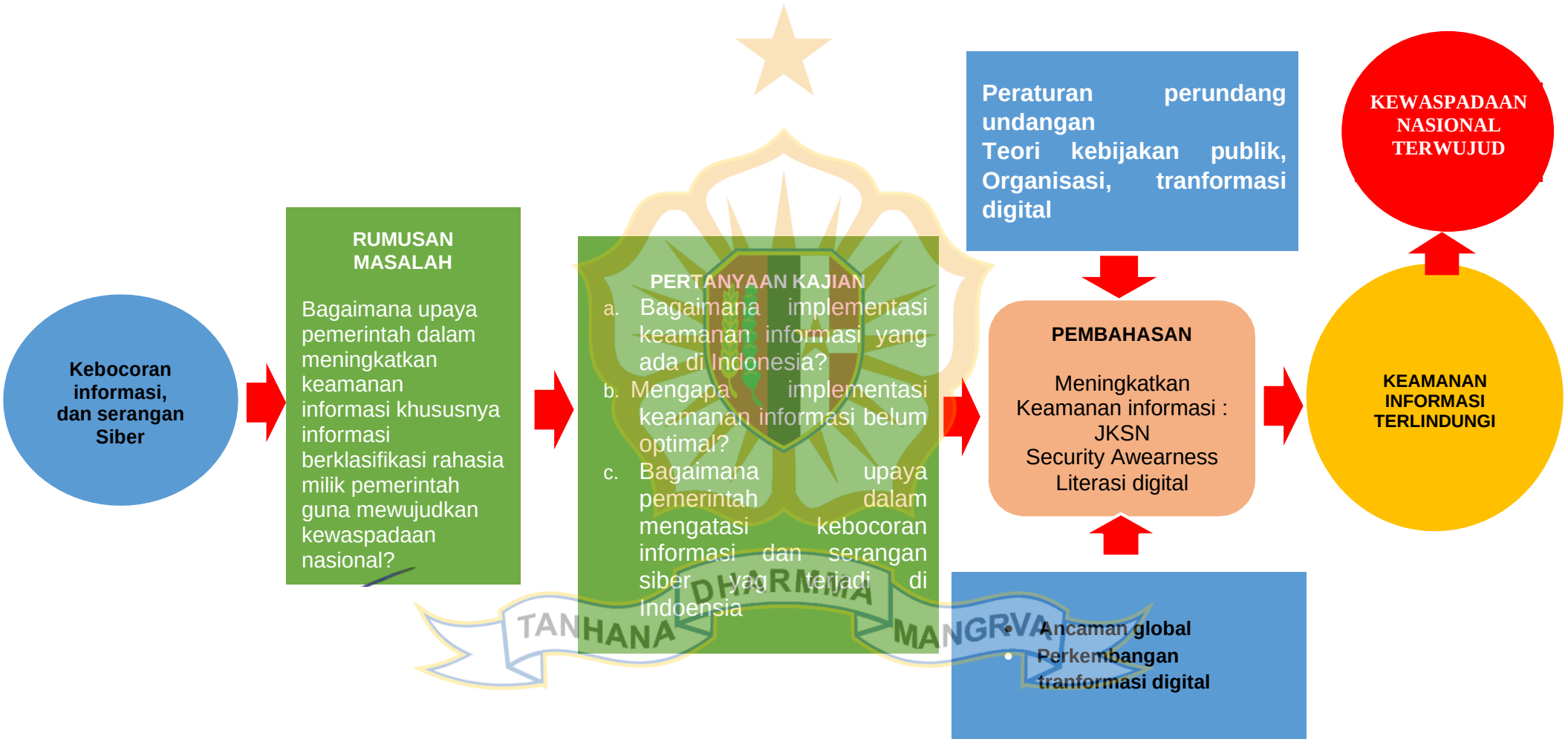
Sukseskan Implementasi Security Awareness Melalui MONICA. https://bcperak.beacukai.go.id/berita/sukseskan-implementasi-security-awareness-melalui-monica. Diakses 16 Maret 2024 Pukul 13.30 WIB.

Sukmana, Ena. (2005). Digitalisasi Pustaka. https://www.researchgate.net/publication/236965703_DIGITALISASI_PUSTAKA. Diakses 5 Maret 2024 pukul 19.30 wib.


DHARMMA
TANHANA
MANGRVA

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

MENINGKATKAN KEAMANAN INFORMASI GUNA MEWUJUDKAN KEWASPADAAN NASIONAL



LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

RIWAYAT HIDUP

NAMA	: DR. RIDWAN, S.SOS, M.SI
TEMPAT LAHIR	: PADANG PANJANG, 10 AGUSTUS 1974
JABATAN	: KEPALA PUSAT KAJIAN BELA NEGARA UPN VETERAN JAKARTA DIREKTUR UTAMA ELESEM JAYA ABADI
SUKU BANGSA	: MINANG
AGAMA	: ISLAM

PENDIDIKAN UMUM

S1 ADM NEGARA STIA	: 2005
S2 ADM PUBLIK STIA	: 2007
S3 ADM PUBLIK UNIV. PADJADJARAN	: 2016

PENDIDIKAN KEDINASAN

SEKOLAH INTELIJEN STRATEGIS BAIS TNI	: 1993
AKADEMI SANDI NEGARA	: 1996
MILS MAIL AND MILS FILE TRAINING	: 2005
NUSANTARA CRYPTO SMS TRAINING	: 2006
RANCANG BANGUN KURIKULUM	: 2009
TRAINING OF COURSE LAN	: 2010
TRAINING OF TRAINER LAN	: 2011
PELATIHAN PENGEMBANGAN FASILITATOR DKLAT	: 2011
PELATIHAN KRIPTOGRAFI MODERN	: 2011
SEA SURVIVAL TRAINING	: 2011
PELATIHAN EVALUASI DAN PENGMBANGAN KURIKULUM DAN PENYUSUNAN RPS	: 2020
TOT BELA NEGARA	: 2021
TOT PANCASILA	: 2021
PEKERTI	: 2022
TOT TAPLAI LEMHANNAS	: 2023
APPLY APPROACH	: 2023
PPRA LXVI LEMHANNAS	: 2024

RIWAYAT PEKERJAAN
BADAN SIBER DAN SANDI NEGARA
POLHUKAM
PASPAMPRES
BADAN KEAMANAN LAUT/BAKAMLA
PEMPROV. SULAWESI TENGAH
UNIVERSITAS SUBANG
UPN VETERAN JAKARTA
ELESEM JAYA ABADI

PENGALAMAN OPERASI
SATGAS INTEL DI PAPUA, ACEH, AMBON
OPERASI GURITA HIU MACAN 003 PERAIRAN TIMUR INDONESIA
OPERASI SEPANJANG TAHUN KRI CUCUT PERAIRAN BARAT INDONESIA

PENGALAMAN MENGAJAR
SAT INDUK BAIS TNI
PUSDIKLAT BADAN SIBER DAN SANDI NEGARA
SEKOLAH TINGGI SANDI NEGARA
BANDIKLAT JAWA BARAT
BANDIKLAT JAWA TIMUR
SESKOAD
SEKKAU
UNIVERSITAS SUBANG
UNIVERSITAS PERTAHANAN
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

PENGHARGAAN
PIAGAM TANDA PEGHARGAAN DHARMA PERSANDIAN X TAHUN
PIAGAM TANDA KEHORMATAN SATYALANCANA KARYA SATYA X TAHUN

PENGALAMAN PENELITIAN
AKTIF MENULIS BUKU, JURNAL NASIONAL DAN INTERNASIONAL SERTA KEGIATAN PROFESIONAL/PENGABDIAN KEPADA MASYARAKAT