LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PEMBANGUNAN SISTEM KEAMANAN SIBER DAN INFRASTRUKTUR TEKNOLOGI IBU KOTA NUSANTARA DALAM RANGKA KEWASPADAAN NASIONAL

Oleh :

DR. PRATAMA DAHLIAN PERSADHA, S.SOS., MM.

KETUA BIDANG SIBER DEWAN ANALIS STRATEGIS BIN

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN SINGKAT ANGKATAN (PPSA)-XXIV
LEMHANNAS RI TAHUN 2023

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

KATA PENGANTAR

Assalammualaikum Wr Wb, salam sejahtera bagi kita semua.

Dengan memanjatkan segala puji dan syukur kehadirat Tuhan Yang Maha Esa serta atas segala rahmat dan petunjuk serta karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Singkat Angkatan (PPSA) XXIV TA 2023 telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Perorangan (Taskap) dengan judul : **"PEMBANGUNAN SISTEM KEAMANAN SIBER DAN INFRASTRUKTUR TEKNOLOGI IBU KOTA NUSANTARA DALAM RANGKA KEWASPADAAN NASIONAL".**

Penentuan Tutor dan judul taskap ini didasarkan oleh Keputusan Deputi Pendidikan Pimpinan Tingkat Nasional Lembaga Ketahanan Nasional Republik Indonesia Nomor : B/95/V/2023 tanggal 22 Mei 2023 tentang Hasil Rapat Penetapan Judul Taskap peserta PPSA XXIV tahun 2023 yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah Penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPSA XXIV di Lemhannas RI tahun 2023. Ucapan yang sama juga disampaikan kepada Pembimbing atau Tutor Taskap kami yaitu Mayjen TNI (Purn) Dr. I Putu Sastra Wingarta, S.I.P., M.Sc. dan Tim Penguji Taskap serta semua pihak yang telah membantu serta membimbing untuk membuat serta menyelesaikan taskap ini sampai terselesaikan sesuai dengan waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI. Penulis menyadari bahwa dihadapkan dengan kemampuan intelektual serta penguasaan dibidang akademis, maka kualitas dari taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon kiranya ada kritik serta masukan guna perbaikan dalam rangka penyempurnaan naskah ini.

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

yang menjadi *stake holder* atau yang membutuhkannya dalam rangka pembangunan sistem keamanan siber dan infrastruktur teknologi di Ibu Kota Nusantara sehingga kewaspadaan nasional Indonesia meningkat.

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

Sekian dan terima kasih. Wassalamualaikum Wr Wb.

Jakarta, 27 Agustus 2023

Penulis,

Dr. Pratama Dahlian Persadha, S.Sos., MM.

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini :

   Nama : Dr. Pratama Dahlian Persadha, S.Sos., MM.

   Jabatan : Ketua Bidang Siber Dewan Analis Strategis BIN

   Instansi : Badan Intelijen Negara

   Alamat : Villa Tanah Baru Blok A No. 5, Depok, Jawa Barat

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

   a. Kertas Karya Perorangan (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, 27 Agustus 2023

Penulis,

Dr. Pratama Dahlian Persadha, S.Sos., MM.

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LEMBAR PERSETUJUAN TUTOR TASKAP

Yang bertanda tangan di bawah ini Tutor pembuatan Kertas Karya Perorangan (TASKAP) Peserta Pendidikan Singkat PPSA XXIV Tahun 2023.

Nama : Dr. Pratama Dahlian Persadha, S.Sos., MM.
Peserta : Program Pendidikan Singkat Angkatan (PPSA) XXIV
Judul Taskap : **"PEMBANGUNAN SISTEM KEAMANAN SIBER DAN INFRASTRUKTUR TEKNOLOGI IBU KOTA NUSANTARA DALAM RANGKA KEWASPADAAN NASIONAL"**.

Taskap tersebut di atas telah ditulis "sesuai/~~tidak sesuai~~" dengan Juknis Taskap Peraturan Gubernur Lemhannas RI Nomor 24 Tanggal 12 Desember 2022, karena itu "layak/~~tidak layak~~" dan "disetujui/~~tidak disetujui~~" untuk diuji.
*coret yang tidak diperlukan.

Jakarta, 27 Agustus 2023
Tutor Taskap,

[ ]c.
Mayor Jenderal [illegible] (Purn).

DAFTAR ISI

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

TABEL

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1. Latar Belakang

Indonesia akan memindahkan ibukotanya ke Ibu Kota Negara Nusantara (IKN) sebagai tindak lanjut dari rencana pemerintah untuk mempercepat pembangunan dan meningkatkan kesejahteraan masyarakat Indonesia. IKN merupakan kawasan baru yang dirancang untuk menjadi pusat pemerintahan dan layanan publik, serta menjadi kawasan ekonomi terpadu dan berkelanjutan.

Isu pemindahan ibu kota negara telah menjadi perbincangan sejak lama, bahkan sejak zaman Presiden Soekarno. Hal ini disebabkan oleh berbagai faktor, salah satunya adalah tingkat kepadatan penduduk DKI Jakarta yang sangat tinggi.Menurut data BPS pada tahun 2021, DKI Jakarta memiliki tingkat kepadatan penduduk mencapai 15.978 jiwa/km[1], yang merupakan tertinggi di Indonesia. Tingkat kepadatan penduduk yang tinggi ini menjadi salah satu penyebab kemacetan dan ketimpangan ekonomi antar daerah. Pemindahan ibu kota negara diharapkan dapat mengurangi kemacetan dan ketimpangan ekonomi tersebut. Namun, pemindahan ibu kota juga memunculkan paradigma baru, yaitu perlunya infrastruktur yang memadai untuk mendukung fungsi ibu kota negara.

Alasan dari pemindahan ibukota ini adalah untuk mengurangi beban Jakarta sebagai pusat pemerintahan dan pusat bisnis nasional. Jakarta sebagai ibu kota saat ini telah mengalami berbagai masalah seperti kemacetan lalu lintas, banjir, dan polusi udara. Masalah-masalah tersebut mempengaruhi produktivitas dan kualitas hidup masyarakat serta menimbulkan berbagai masalah lingkungan dan kesehatan. Pemindahan ibukota ini juga diharapkan dapat mengurangi ketimpangan regional, meningkatkan investasi, dan mempercepat pertumbuhan ekonomi di wilayah Indonesia Timur.

Pemindahan ibu kota negara merupakan salah satu upaya pemerintah untuk memenuhi janjinya dalam melakukan pemerataan pembangunan di

[1] BPS, Kepadatan Penduduk menurut Provinsi (jiwa/km2) 2019-2021, (2023)

daerah-daerah luar Jawa. Hal ini disebabkan oleh distribusi penduduk dan ekonomi yang masih terpusat di Pulau Jawa. Dengan memindahkan ibu kota ke Kalimantan Timur, pemerintah berharap dapat mendorong pertumbuhan ekonomi di daerah tersebut dan mengurangi ketimpangan pembangunan di Indonesia. Pemindahan ibu kota juga memiliki implikasi politik bagi pemerintah. Hal ini dikarenakan ibu kota merupakan simbol negara dan pusat pemerintahan yang kuat. Dengan memindahkan ibu kota, pemerintah berharap dapat meningkatkan legitimasi mereka di luar Pulau Jawa dan memperkuat posisi mereka pada pemilu-pemilu yang akan datang.

Pemindahan ibukota ke IKN juga memberikan manfaat dalam hal pembangunan infrastruktur yang lebih modern dan terintegrasi. IKN akan dibangun dengan konsep kota pintar (*smart city*) dan dilengkapi dengan fasilitas transportasi modern seperti kereta cepat, bandara internasional, dan pelabuhan laut yang terhubung secara langsung dengan kawasan bisnis dan pusat pemerintahan. Hal ini diharapkan dapat mendukung pertumbuhan ekonomi dan meningkatkan kualitas hidup masyarakat.

Selain itu, pemindahan ibukota juga memberikan manfaat dalam hal pelestarian lingkungan dan keberlanjutan. IKN dirancang sebagai kota hijau dengan konsep ramah lingkungan yang memperhatikan aspek keberlanjutan dalam pembangunannya. Hal ini meliputi penggunaan energi terbarukan, pengolahan air limbah, dan penghijauan wilayah. Manfaat lingkungan ini juga diharapkan dapat meningkatkan kualitas hidup masyarakat dan memperkuat ketahanan lingkungan di Indonesia. Secara keseluruhan, pemindahan ibukota ke IKN diharapkan dapat memberikan manfaat dalam hal mengurangi beban Jakarta, mempercepat pembangunan infrastruktur modern, meningkatkan kualitas hidup masyarakat, dan pelestarian lingkungan. Namun, pemindahan ibukota juga membutuhkan persiapan yang matang, seperti perencanaan yang tepat, pengaturan legal dan kebijakan, serta dukungan dari berbagai pihak terkait.

Dalam era digital ini, teknologi dan informasi menjadi faktor penting dalam pemerintahan, terutama bagi negara kesatuan. Pemerintah pusat perlu memiliki akses informasi yang mudah dan cepat untuk memperkuat kendalinya. Akses listrik dan internet merupakan faktor utama yang

menentukan kemudahan akses informasi. Data menunjukkan bahwa akses terhadap aliran listrik di Pulau Kalimantan masih sangat rendah, yaitu hanya berkisar diangka 4.8%.[2] Hal ini menunjukkan bahwa masih banyak daerah di Kalimantan yang belum memiliki akses listrik. Pemerintah perlu mengembangkan infrastruktur listrik agar masyarakat dapat mengakses listrik dengan mudah dan cepat. Akses listrik yang memadai akan memungkinkan pemerintah pusat untuk menerima informasi setiap saat dan siaga dalam keadaan genting nasional. Pemerintah pusat harus selalu memperbarui informasi mengenai permasalahan yang muncul di daerah-daerah. Dengan kemudahan akses listrik, pengembangan pada bagian teknologi digital dan internet dapat didukung.

Kepindahan ibukota ke tempat baru dapat memunculkan ancaman baru, baik dari darat, laut dan udara, tetapi saat ini ada lagi ancaman nyata yang harus diperhatikan, yaitu ancaman siber. Pemindahan infrastruktur pemerintahan ke lokasi baru dapat menimbulkan risiko baru pada sistem keamanan siber. Terdapat beberapa contoh negara lain yang mengalami ancaman siber setelah memindahkan ibukotanya ke tempat baru.

Contohnya adalah Kazakhstan, negara yang memindahkan ibukotanya dari Almaty ke Nur-Sultan pada tahun 1997. Setelah pemindahan ibukota, Kazakhstan mengalami serangan siber yang signifikan pada sistem keamanan siber negara dan instansi pemerintahan. Serangan siber yang dilakukan oleh kelompok penjahat siber berhasil mencuri data penting seperti informasi paspor, sertifikat kelahiran, dan dokumen penting lainnya dari database pemerintah Kazakhstan. Meningkatnya ancaman siber terkait pemindahan ibukota baru juga terjadi di India. Pada tahun 2015, India mengumumkan rencana untuk memindahkan ibukotanya dari New Delhi ke Amaravati. Namun, rencana ini dibatalkan setelah adanya kekhawatiran tentang risiko keamanan siber pada sistem pemerintah.

Ancaman siber dapat terjadi kepada sebuah sistem dimanapun selama terhubung kepada jaringan internet. Pada pemindahan ibukota baru serangan siber dapat terjadi karena infrastruktur teknologi dan keamanan siber yang belum matang dan belum terintegrasi dengan baik. Oleh karena itu, perlu

[2] Kementerian ESDM, Statistik Ketenagalistrikan Tahun 2021, 2022

dilakukan perencanaan dan implementasi pembangunan sistem keamanan siber yang kokoh dan terintegrasi dengan baik pada seluruh sektor kehidupan di Ibu Kota Negara Nusantara (IKN). Upaya ini akan membantu mencegah ancaman siber dan melindungi data penting serta infrastruktur kritis di IKN.

Selain itu juga beberapa negara yang mengalami kerusakan atau masalah serius akibat serangan siber, di antaranya adalah :

a. Ukraina: Pada tahun 2015 dan 2017, Ukraina menjadi target serangan siber yang merusak sistem kelistrikan dan pemrosesan data. Serangan ini menyebabkan pemadaman listrik yang luas dan mengakibatkan kerugian ekonomi dan sosial yang signifikan[3]. Dan sebelum terjadi perang Rusia-Ukraina kemarin pun, negara ini juga mengalami serangan siber habis-habisan sehingga hampir semua infrastruktur kritisnya lumpuh, seperti Listrik, layanan perbankan, layanan pemerintah, transportasi dan lainnya[4].
b. Amerika Serikat: Pada tahun 2016, terjadi serangan siber terhadap sistem pemilihan presiden AS yang diyakini berasal dari pemerintah Rusia[5]. Serangan ini memicu kontroversi besar dan mempengaruhi hasil pemilihan presiden.
c. Estonia: Pada tahun 2007, Estonia menjadi target serangan siber yang dilakukan oleh kelompok aktivis Rusia setelah pemerintah Estonia menghapus patung peringatan Tentara Merah[6]. Serangan ini memicu protes massal dan merusak sistem pemerintah dan bisnis Estonia.
d. Arab Saudi: Pada tahun 2012, salah satu perusahaan minyak terbesar di dunia, Aramco, menjadi target serangan siber[7]. Serangan ini menyebabkan kerusakan sistem yang parah dan mengakibatkan 30.000 komputer milik Aramco tidak bisa digunakan.
e. Bangladesh: Pada tahun 2016, terjadi serangan siber terhadap bank sentral Bangladesh[8]. Serangan ini berhasil mencuri $ 81 juta dari rekening bank dan memicu investigasi yang luas.

---

[3] https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01
[4] https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
[5] https://www.bbc.com/indonesia/dunia/2016/10/161008_dunia_as_pemilu_rusia
[6] https://www.bbc.com/news/39655415
[7] https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html
[8] https://theonebrief.com/the-bangladesh-bank-heist-lessons-in-cyber-vulnerability/

Jumlah serangan siber di Indonesia juga masih sangat tinggi, 976.429.996 *Anomali Traffic* atau serangan siber[9]. Sebanyak 47% dari keseluruhan kasus yang terjadi merupakan serangan malware, 44% merupakan penipuan, sedangkan sisanya berbentuk kejahatan siber lainnya, seperti *website defacement*, dan aktivitas manipulasi data dan kebocoran data. Ini berarti setiap hari terjadi 2.675.151 serangan siber, umumnya dilancarkan dalam bentuk peretasan, *virus*, dan perangkat perusak lainnya (malware). Kejahatan siber, yang meliputi *phising*, *spoofing*, *cracking*, serangan *ransomware*, dan sejenisnya, telah menjadi priotitas bagi negara-negara di seluruh dunia mengingat ancaman yang terus meningkat dari waktu ke waktu.

Menurut Statista Technology Market Outlook, kerugian akibat kejahatan siber di seluruh dunia diperkirakan mencapai US$7,08 triliun atau sekitar Rp108.756 triliun (kurs Rp15.361/US$) pada tahun 2022, meningkat 29% dibanding tahun sebelumnya yang sebesar US$5,49 triliun. Proyeksi dari Statista juga menunjukkan bahwa kerugian dari kejahatan siber diperkirakan meningkat hampir tiga kali lipat menjadi US$13,82 triliun pada lima tahun mendatang atau pada tahun 2028[10].

Tingginya tingkat ketergantungan pada teknologi informasi dan komunikasi (TIK) di hampir semua sektor kehidupan, termasuk pemerintahan, ekonomi, dan sosial-budaya, menjadi salah satu faktor yang meningkatkan risiko ancaman siber di Ibu Kota Negara Nusantara (IKN). IKN sebagai ibu kota baru Indonesia yang sedang dalam tahap pembangunan perlu memperhatikan keamanan siber sebagai prioritas. Pemanfaatan teknologi informasi yang semakin pesat di IKN, seperti *Internet of Things* (IoT) dan sistem *smart city*, dapat meningkatkan risiko terhadap serangan siber karena keamanan jaringan yang belum terjamin sepenuhnya.

Terkait dengan peningkatan serangan siber di berbagai negara di dunia, termasuk Indonesia, IKN juga perlu waspada terhadap ancaman ini. Serangan siber dapat terjadi dari berbagai pihak, seperti hacker individu, kelompok kriminal, atau bahkan pemerintah asing yang mencari informasi rahasia dan

[9] BSSN, Lanskap Keamanan Siber 2022, (2023)
[10] Petrosyan, Ani, Annual cost of cybercrime worldwide 2017-2028, (2023)

data penting. IKN sebagai ibu kota baru yang sedang dalam tahap pembangunan dapat menjadi target serangan siber yang menargetkan infrastruktur kritis, seperti sistem transportasi, listrik, air bersih, dan lain sebagainya. Oleh karena itu, keamanan siber harus dianggap sebagai bagian penting dalam perencanaan pembangunan IKN.

Meskipun ada beberapa kebijakan dan peraturan terkait keamanan siber di Indonesia, namun masih banyak yang perlu ditingkatkan. Dalam hal ini, peran pemerintah dan institusi terkait sangat penting dalam meningkatkan kesadaran dan kesiapan terhadap ancaman siber di IKN. Salah satu upaya yang dapat dilakukan adalah dengan memperkuat kerjasama antar lembaga dan meningkatkan investasi pada keamanan siber. Hal ini juga perlu didukung oleh peningkatan kapasitas sumber daya manusia yang terampil dalam bidang keamanan siber.

Konsep kewaspadaan nasional merujuk pada upaya yang dilakukan oleh sebuah negara untuk melakukan peringatan dini, deteksi dini, tangkal dini, cegah dini & tangkal dini juga dapat dipergunakan mencegah ancaman dan serangan siber yang dapat membahayakan keamanan siber dan kedaulatan nasional serta membangun sistem keamanan siber dan infrastruktur teknologi yang berkelanjutan.

Berdasarkan uraian diatas, penulis merasa perlu untuk menulis Kertas Karya Ilmiah Perseorangan (Taskap) dengan Judul Pembangunan Sistem Keamanan Siber dan Infrastruktur Teknologi Ibu Kota Nusantara Dalam Rangka Kewaspadaan Nasional,

2. Rumusan Masalah

Karena begitu besarnya ancaman siber pada IKN yang perlu diperhatikan antara lain tingginya ketergantungan pada teknologi informasi dan komunikasi (TIK), peningkatan serangan siber di Indonesia, potensi serangan siber terhadap infrastruktur kritis di IKN, dan kebijakan serta peraturan terkait keamanan siber yang masih perlu ditingkatkan, sehingga yang harusnya IKN adalah konsep *Smart City*, bisa-bisa kalau tidak siap akan menjadi *Fragile City*. Oleh karena itu penulis merasa perlu untuk menulis Taskap dengan rumusan masalah ***"Bagaimana membuat dan mendesain***

pembangunan sistem keamanan siber dan infrastruktur teknologi Ibu Kota Nusantara dalam rangka kewaspadaan nasional?"

Selanjutnya supaya analisa dan pembahasan yang dilakukan lebih terstruktur dan terarah, maka kajian dari pembahasan ini dijabarkan dalam beberapa pertanyaan sebagai berikut :

a. Bagaimana potensi ancaman siber global yang dapat mengancam keamanan dan kedaulatan Indonesia dalam pengembangan Ibu Kota Nusantara (IKN)?
b. Bagaimana dampak dari potensi ancaman keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi terhadap perkembangan dan keberlangsungan IKN dan Indonesia di masa depan?
c. Bagaimana konsep pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi untuk mewujudkan kewaspadaan nasional dalam melindungi IKN dari ancaman siber global dan menjaga kedaulatan Indonesia?

3. Maksud dan Tujuan.

a. **Maksud.** Maksud dari penulisan Taskap ini adalah ~~untuk~~ memberikan gambaran, analisis~~,analisa~~ dan rekomendasi mengenai~~tentang bagaimana~~ pentingnya merancang dan mengimplementasikan langkah-langkah strategis yang bertujuan membangun sistem keamanan siber yang kuat dan infrastruktur teknologi yang handal di Ibu Kota Nusantara. Penelitian ini akan berfokus pada upaya meningkatkan kewaspadaan nasional terhadap berbagai ancaman keamanan siber yang mungkin dihadapi oleh Ibu Kota Nusantara, dengan tujuan memitigasi risiko dan menjaga keberlanjutan operasional Ibu Kota yang menjadi pusat administrasi dan kebijakan negara.
b. **Tujuan.** Tujuan dari penulisan~~Penulisan~~ Taskap ini adalah~~bertujuan untuk~~ memberikan sumbangan pemikiran dari peserta kepada para pemangku kepentingan dalam upaya mengidentifikasi,

merancang, dan melaksanakan langkah-langkah strategis guna membangun sistem keamanan siber yang tangguh dan infrastruktur teknologi yang kuat di Ibu Kota Nusantara. Dengan demikian, penelitian ini akan memberikan kontribusi penting dalam menciptakan lingkungan teknologi yang aman, handal, dan terlindungi, sehingga mendukung perkembangan dan keberlangsungan Ibu Kota Nusantara serta keselamatan dan keamanan Indonesia secara keseluruhan di era digital yang semakin kompleks ini.

4. Ruang Lingkup dan Sistematika.

a. Ruang Lingkup. Secara umum banyak sekali ancaman siber yang bisa mengganggu atau menghancurkan satu negara. Apalagi ketika ada pemindahan pusat negara dan pemerintahan yang baru. Tetapi supaya lebih fokus, maka ruang lingkup yang akan dibahas dalam tulisan ini adalah pokok-pokok permasalahan yang menyangkut apa potensi dan dampak ancaman siber global terhadap kedaulatan Indonesia serta bagaimana konsep membangun system keamanan siber dan insfrastruktur teknologi yang kokoh dan terintegrasi.

b. Sistematika. Sesuai dengan ruang lingkup pembahasan, maka penyusunan Taskap ini disusun dengan tata urut sebagai berikut:

1) **Bab I Pendahuluan**. Bab ini merupakan bagian awal penulisan yang~~dan~~ memuat ~~tentang~~ latar belakang mengenai~~yang berisikan fakta-fakta yang berkaitan dengan~~ kondisi keamanan siber yang ada di Ibu Kota Nusantara (IKN) saat ini. Selain itu, bab ini juga menjelaskan~~,~~ maksud, ~~dan~~ tujuan, ruang lingkup, ~~dan~~ sistematika, metode, dan pendekatan yang digunakan dalam penyusunan Taskap ini. Terdapat pula ~~serta~~ beberapa pengertian yang disajikan untuk memperjelas istilah-istilah ~~yang dianggap~~ penting dalam tulisan ini.

2) **Bab II Landasan Pemikiran.** Dalam Bab II, diuraikan mengenai~~tentang~~ peraturan perundang-undangan yang menjadi dasar~~sebagai landasan~~ operasional, ~~—~~data dan fakta, serta

beberapa kerangka teoritis dan tinjauan pustaka ~~yang~~ relevan yang digunakan~~dijadikan~~ sebagai referensi dalam~~bahan rujukan terkait~~ pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi. Selanjutnya, dijelaskan~~, kemudian diuraikan~~ perkembangan lingkungan strategis global, regional, dan nasional yang berpengaruh~~memberikan pengaruh~~ terhadap pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi, sehingga berdampak pada kewaspadaan nasional.

3) **Bab III Pembahasan.** Bab ini memberikan~~berisi~~ gambaran umum mengenai kondisi ancaman dan keamanan siber saat ini. Selain itu, dibahas juga~~,~~ kondisi pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi di IKN Nusantara yang dihadapkan pada tantangan dan potensi ancaman yang ada. Hal ini bertujuan untuk mengidentifikasi berbagai~~dihadapi, sehingga dapat diidentifikasikan~~ persoalan yang perlu dipecahkan dan menentukan~~persoalan, untuk kemudian ditentukan~~ konsep pemecahannya~~pemecahan persoalan~~.

4) **Bab IV Penutup.** Sebagai bagian akhir dari penyusunan Taskap, terdapat~~yang berisikan tentang~~ simpulan dari keseluruhan hasil pembahasan dan analisis. Selain itu, juga disampaikan~~analisa serta diajukan~~ saran strategis sebagai rekomendasi yang ditujukan kepada pemangku kepentingan agar pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi di IKN dapat berjalan~~terlaksanakan~~ dengan baik.

5. Metode dan Pendekatan.

a. Metode. Penulisan Taskap ini menggunakan metode penelitian kualitatif dengan pendekatan~~,~~ deskriptif-analitis. Metode ini ~~yang~~ menekankan pada pengumpulan data sekunder melalui~~berupa~~ *desk review*, kajian pustaka, dan studi dokumen yang relevan. Metodologi~~dari data, dengan metodologi~~ pembahasan yang digunakan dalam penulisan ini adalah~~menggunakan~~ *PESTL dan SWOT*.

b. **Pendekatan.** Pendekatan yang digunakan dalam penulisan Taskap ini adalah pendekatan~~menggunakan~~ perspektif kewaspadaan nasional serta pendekatan kepentingan nasional yang melibatkan ~~dengan~~ analisis multidisipliner dari berbagai~~multidisiplin~~ ilmu yang sesuai dengan kerangka teoretis dan~~,~~ fakta yang ada. Pendekatan ini juga~~, dengan~~ memperhatikan kondisi gatra dan lingkungan strategis yang relevan. Penulisan Taskap ini dilakukan~~disusun~~ secara sistematis, akurat, dan faktual dengan mendeskripsikan dua variabel yang relevan~~varibel~~.

6. **Pengertian.**

a. **Keamanan siber** adalah merujuk pada perlindungan sistem komputer, jaringan, perangkat keras, perangkat lunak, dan data dari berbagai ancaman digital. Tujuan dari keamanan siber adalah untuk mencegah akses tidak sah, penggunaan, perubahan, atau penghancuran data serta melindungi infrastruktur teknologi dari serangan siber yang dapat menyebabkan gangguan, kerugian finansial, dan bahkan ancaman terhadap keselamatan nasional.

b. **PESTL,** PESTL adalah sebuah metode analisis atau konsep dalam prinsip manajemen strateis yang diterapkan sebagai sebuah alat untuk memantau sebuah lingkungan pemerintahan serta mengantisipasi situasi makro yang dapat mempengaruhi situasi pemerintahan. PESTL merupakan singkatan yang dibentuk dari beberapa kata yaitu Politik, Ekonomi, Sosial, Teknology serta Lingkungan. Dengan mengunakan metode Analisa PESTL akan dapat memberikan pandangan baru tentang lingkungan makro dari banyak sudut pandang yang pada saat mengembangkan ide atau rencana tertentu.[11] Analisis PESTL paling efektif jika digunakan bersamaan dengan Analisis SWOT untuk memahami peluang dan ancaman seputar rencana pengembangan yang akan dilakukan.

c. ***SWOT***, *SWOT* adalah sebuah alat perencanaan untuk mengidentifikasikan *Strength* (Kekuatan), *Weakness* (Kelemahan), *Opportunity* (Peluang) serta *Threats* (Ancaman). Dengan menggunakan Analisa *SWOT* kita akan dapat memahami faktor-faktor kunci – kekuatan,

[11] https://www.cipd.org/en/knowledge/factsheets/pestle-analysis-factsheet/

kelemahan, peluang, dan ancaman – yang terlibat dalam suatu proyek atau organisasi. Hal ini melibatkan pernyataan tujuan organisasi atau proyek dan mengidentifikasi faktor internal dan eksternal yang mendukung atau tidak mendukung pencapaian tujuan tersebut. SWOT sering digunakan sebagai bagian dari proses strategis atau perencanaan, namun dapat diterapkan untuk membantu memahami suatu organisasi atau situasi, dan juga untuk pengambilan keputusan dalam berbagai skenario.[12]

d. **Infrastruktur Teknologi** adalah rangkaian perangkat keras, perangkat lunak, jaringan, dan sistem lainnya yang mendukung dan memfasilitasi pengoperasian teknologi informasi dan komunikasi (TIK) dalam suatu lingkungan. Dalam konteks penelitian ini, infrastruktur teknologi mencakup aspek-aspek seperti *server*, *router*, jaringan kabel, perangkat seluler, sistem operasi, dan aplikasi yang menjadi pondasi dan tulang punggung dalam mendukung fungsi Ibu Kota Nusantara.

e. **Ibu Kota Negara,** menurut KBBI Daring adalah tempat di manakedudukan pemerintah pusat suatu negara atau pusat pemerintahan berkedudukan. Ibu Kota Negara yang bernama Nusantara dan selanjutnya disebut sebagai Ibu Kota Nusantara, adalah sebuah wilayahsatuan pemerintahan daerah yang memiliki statusbersifat khusus setara dengan setingkat provinsi. Wilayah ini ditetapkan dan diatur sebagai yang wilayahnya menjadi tempat kedudukan Ibu Kota Negara melalui sebagaimana ditetapkan dan diatur dengan Undang-Undang ini. Dalam hal ini Kabupaten Penajam Paser Utara, yang terletak di Provinsi Kalimantan Timur, dianggap sebagai merupakan calon Ibu Kota Negara Republik Indonesia.

f. **Integrasi** adalah pembauran hingga menjadi kesatuan yang utuh atau bulat atau penggabungan aktivitas, program, atau komponen perangkat keras yang berbeda ke dalam satu unit fungsional.[13] Integrasi dalam naskah ini diartikan sebagai suatu proses menggabungkanuntuk mengoordinasikan dan mengolaborasikan berbagai fungsi, bagian, dan

---

[12] https://www.cipd.org/uk/knowledge/factsheets/swot-analysis-factsheet
[13] Badan Pengembangan dan Pembinaan Bahasa. OpCit.

tugas yang berbeda menjadi satu kesatuan fungsional yang utuh atau lengkap. Dalam konteks naskah ini, integrasi mengacu ada pada proses koordinasi dan kolaborasi berbagai elemen yang ada dalam suatu pekerjaan yaitu sistem keamanan siber IKN.

g. **Kewaspadaan Nasional** adalah langkah-langkah antisipatif yang diambil oleh suatu negara untuk mengidentifikasi, menganalisis, dan mengatasi berbagai ancaman dan risiko yang dapat mengancam keamanan, ketertiban, dan keselamatan negara secara menyeluruh. Dalam konteks penelitian ini, kewaspadaan nasional terkait dengan upaya menghadapi berbagai ancaman keamanan siber yang berpotensi merusak infrastruktur teknologi dan kesinambungan operasional Ibu Kota Nusantara serta kepentingan nasional Indonesia secara keseluruhan.

h. **Pembangunan,** menurut Wisadirana (2004), memiliki akar) pembangunan berdasarkan etimologinya berasal dari kata dari "bangun" yang mengandungmempunyai arti kata sadar, bangkit, atau berdiri, serta membuat atau membina. Secara keseluruhanDalam arti yang sepenuhnya, pembangunan adalah suatu proses perubahan yang direncanakanterencana untuk memperbaiki berbagai aspek kehidupan masyarakat. Proses pembangunan ini melibatkan berbagai bidangdemikian berlangsung dalam segala aspek kehidupan masyarakat, seperti ekonomi, sosial, budaya, dan politik, yang berlangsung pada tingkattataran makro dan mikro[14].

i. **Serangan Siber** adalah upaya yang dilakukan oleh pihak-pihak yang tidak sah untuk memasuki, merusak, mengganggu, atau mencuri informasi dari sistem komputer, jaringan, atau infrastruktur teknologi. Serangan ini dapat berupa *malware*, *ransomware*, serangan DDoS (*Distributed Denial of Service*), atau berbagai teknik peretasan lainnya yang bertujuan mencuri data sensitif atau merusak operasional sistem.

j. **Ancaman Keamanan Siber** mencakup segala potensi risiko atau bahaya yang diarahkan pada infrastruktur teknologi dan data yang terhubung dengan jaringan digital. Ancaman ini dapat berasal dari

[14] Wisadirana. Darsono. Pembanguna berdimensi kerakyatan. Yayasan Obor. 2004

berbagai pihak, seperti peretas (*hacker*), kelompok teroris siber, negara asing, atau individu yang memiliki tujuan merusak, mencuri informasi, menyebabkan gangguan operasional, atau mengganggu ketertiban umum melalui serangan siber.

k. **Memitigasi Risiko** berarti mengurangi dampak atau kemungkinan terjadinya risiko yang berkaitan dengan keamanan siber dan infrastruktur teknologi. Upaya memitigasi risiko melibatkan identifikasi potensi ancaman, evaluasi kerentanannya, serta penerapan langkah-langkah pencegahan dan tanggapan yang efektif untuk mengurangi atau menghilangkan risiko tersebut.

l. **Infrastruktur Kritis** adalah komponen-komponen penting dan vital dari suatu negara atau wilayah yang jika mengalami kerusakan atau gangguan dapat menyebabkan dampak serius terhadap keamanan nasional, perekonomian, dan kesejahteraan masyarakat. Dalam konteks penelitian ini, infrastruktur kritis terkait dengan infrastruktur teknologi yang menjadi tulang punggung Ibu Kota Nusantara dan berperan sentral dalam berbagai aspek kehidupan negara.

BAB II
LANDASAN PEMIKIRAN

7. Umum.

Ibu Kota Negara Republik Indonesia yang baru diharapkan dapat menjadi Ibu Kota Negara yang memiliki nilai-nilai identitas bangsa Indonesia yang beragam dan bersatu karen Negara Indonesia memiliki sangat banyak kekayaan serta budaya yang beragam diantaranya adalah memiliki 23 lingkungan keadatan, lebih dari 1000 suku bangsa yang tersebar diseluruh penjuru Indonesia dengan lebih dari 600 bahasa yang dipergunakan oleh warga lokal serta lebih dari 300 lagu-lagu daerah dan 200 kesenian tari. Semua keragamanan tersebut selama ini dapat hidup berdampingan karena memiliki dasar negara dan ideologi yang kuat yaitu Pancasila serta disatukan dengan Bhineka Tunggal Ika. Pemindahan Ibu Kota Negara diharapkan dapat menjadi simbol persatuan dan kesatuan bangsa Indonesia. Ibu Kota yang baru nanti diharapkan agar dapat menjadi episentrum bagi berbagai suku bangsa dan budaya di Indonesia, dan menjadi representasi dari keragaman dan kesatuan bangsa Indonesia.

Paradigma IKN sebagai sebuah kota yang modern serta berkelanjutan memiliki ikatan yang kuat, dimana pembangunan berkelanjutan merupakan sebuah proses untuk memenuhi kebutuhan saat ini namun tidak merusak sumberdaya untuk kebutuhan generasi selanjutnya. Kota yang dianggap berkelanjutan adalah sebuah kota yang proses perancangan, pembangunan, serta pengelolaanya dilakukan supaya dapat memenuhi kebutuhan warganya mulai dari aspek sosial ekonomi serta aspek lingkungan namun tidak mengganggu lingkungan yang sudah ada.

Kota cerdas atau *smart city* merupakan konsep pembangunan kota yang bertujuan untuk efisiensi pengelolaan sumber daya dan pelayanan efektif melalui informasi akurat dan infrastruktur aksesibel. Secara umum, *smart city* menggabungkan Teknologi Informasi dan Komunikasi (TIK) untuk menghubungkan, memantau, dan mengendalikan sumber daya kota dengan efisien, maksimalkan pelayanan warga, dan dukung pembangunan

berkelanjutan. Konsep ini berkembang seiring perubahan pola pikir dalam pembangunan kota yang terintegrasi dengan teknologi.

Konsep *Intelligent city*, tambahan dari *smart city*, berfokus pada transformasi komunitas menjadi lebih baik, kreatif, dan terlibat dalam proyek pengembangan pintar yang mendukung koneksi kota melalui teknologi. Contoh contohnya adalah pengembangan ibu kota Malaysia, Putrajaya, yang mengintegrasikan prinsip-prinsip Islam dan membangun infrastruktur yang seimbang dengan kebutuhan. Ini termasuk pembangunan fasilitas perkantoran dan hunian serta perhatian terhadap pelestarian alam, termasuk danau buatan yang terhubung dengan lingkungan sekitarnya.

Kepala Badan Siber dan Sandi Negara (BSSN) Republik Indonesia, Hinsa Siburian, saat berbicara dalam Seminar Ketahanan Nasional merayakan HUT ke-58 Lembaga Ketahanan Nasional (Lemhannas) RI di Hotel Borobudur, Jakarta, menjelaskan sistem keamanan siber di Ibu Kota Nusantara (IKN). Beliau membahas segala aspek, termasuk tata kelola, SDM, identifikasi, deteksi, proteksi, penanggulangan, dan pemulihan. Pembangunan sistem ini dilakukan secara berkelanjutan dengan fokus pada sumber daya manusia, tata kelola, dan teknologi.[15]

Pembangunan sistem keamanan siber dan infrastruktur teknologi di Ibu Kota Nusantara dalam rangka kewaspadaan nasional adalah suatu perwujudan strategis yang sangat penting bagi Indonesia dalam menghadapi era digital dan mengatasi ancaman keamanan siber yang semakin kompleks. Saat ini, perkembangan teknologi informasi dan komunikasi (TIK) telah menjadi pendorong utama pertumbuhan ekonomi, inovasi, dan kemajuan dalam berbagai sektor kehidupan. Namun, kemajuan ini juga membuka peluang bagi berbagai ancaman keamanan yang dapat mengancam stabilitas dan kedaulatan negara.

Kebijakan pemerintah untuk memindahkan ibu kota negara ke Kalimantan menjadi dasar bagi~~acuan~~ Pemerintah dalam~~untuk~~ menyusun strategi pertahanan udara guna melindungi dan mempertahankan IKN. Strategi keamanan siber IKN harus terintegrasi dengan semua *stakeholder*

[15] https://www.bssn.go.id/kepala-bssn-hinsa-siburian-paparkan-sistem-keamanan-siber-di-ikn-pada-seminar-ketahanan-nasional-hut-ke-58-lemhannas/

terkait. DalamBerkaitan dengan hal tersebut, pada bab II ini, dijelaskan tentang peraturan perundang-undangan, kerangka teori, fakta dan data yang relevan,ada serta hubungannyakaitannya dengan perkembangan lingkungan strategis. Hal ini menjadi landasan sebagai pisau analisis untukdalam membahas tigaketiga persoalan terkait pembangunan sistem keamanan siber dan infrastruktur teknologi IKN yang terintegrasi, dengan tujuan mencari agar dapat ditemukan jawaban dan solusi yang khusus guna khususnya untuk mewujudkan kewaspadaan nasional.

8. Peraturan Perundangan-undangan.

a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Dalam UUD NRI 1945, terdapat bukti normatif yang menjadidapat ditemukan sebagai konstitusi negara terkait dengan pertahanan yaitu pasal 27 dan pasal 30. Pasal ini yang menyatakan bahwa negara Indonesia memiliki hak untuk membela diri dan melakukan perang gunauntuk mempertahankan kemerdekaan dan keselamatan negara. Pasal 27 ayat 3 pada UUD NRI 1845 berbunyi “Setiap warga negara berhak dan wajib ikut serta dalam upaya pembelaan negara.” Pasal ini bertujuan supaya masyarakat memiliki kesadaran untuk melakukan bela negara. Kegiatan bela negara yang sebutkan pada pasal tersebut tidaklah harus bentuk ikut militer tapi bisa juga dapat berbentuk bagaimana kita secara-bersama sama mengamankan ruang siber di Indonesia dari serangan bangsa lain. Hal tersebut dikuatkan kembali dengan Pasal 30 ayat 2 yang berbunyi “Usaha pertahanan dan keamanan negara dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta oleh Tentara Nasional Indonesia dan Kepolisian Negara Republik Indonesia, sebagai kekuatan utama, dan rakyat, sebagai kekuatan pendukung.” Dimana pertahanan rakyat semesta yang perlu dilakukan saat ini tidak hanya pada kewilayahan secara fisik naum juga sudah mulai mencakup wilayah ruang siber. Selain itu,Dalam UUD NRI 1945 juga menekankanmenegaskan pentingnya menjaga kedaulatan, keutuhan wilayah, dan keamanan nasional.

b. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Undang-undang ini merupakan revisi dari UU Nomor 11 Tahun 2008 dan mengatur lebih rinci tentang perlindungan data pribadi, keamanan sistem elektronik, serta upaya pencegahan dan penanganan tindakan yang merugikan dalam transaksi elektronik. Berdasarkan UU ITE, informasi elektronik mencakup rekaman elektronik seperti tulisan, suara, gambar, dan lainnya. Transaksi elektronik adalah perbuatan hukum melalui komputer atau media elektronik, berlaku di dalam dan luar wilayah Indonesia. Ini penting dalam pembangunan sistem keamanan siber di Ibu Kota Nusantara.

c. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.

Peraturan Presiden No. 39/2019 mengenai Satu Data Indonesia adalah langkah pemerintah untuk mengatur tata kelola data demi mendukung pembangunan holistik. Prinsip-prinsip Satu Data Indonesia termasuk standar data, metadata, interoperabilitas, dan kode referensi. Saat ini, pemerintah menunjuk tiga pembina data: Kementerian Keuangan (data keuangan), BPS (data statistik), dan BIG (data geospasial). Pembina data bertugas menerapkan data leadership dan quality assurance pada penyelenggara data.

d. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Perlindungan data pribadi dijelaskan dalam penjelasan Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Bagian penjelasan ini merinci konsep perlindungan data pribadi terkait penggunaan teknologi informasi. Bagian penjelasan

mengartikan data pribadi sebagai bagian dari hak pribadi, termasuk hak privasi, bebas gangguan, komunikasi tanpa pengawasan, dan pengawasan akses informasi pribadi seseorang. Perlindungan data pribadi bertujuan melindungi hak-hak ini agar tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab

e. Undang-Undang Nomor 3 Tahun 2022 Tentang Ibu Kota Negara.

Pembentukan Undang-Undang Nomor 3 Tahun 2022 tentang Ibu Kota Negara bertujuan untuk mendukung pemindahan Ibu Kota dan perubahan tatanan pemerintahan. Tujuannya adalah memperbaiki tata kelola wilayah, menciptakan Ibu Kota yang aman, modern, berkelanjutan, dan berketahanan. Undang-Undang ini juga akan menjadi panduan dalam pembangunan dan penataan wilayah lain di Indonesia. Isi Undang-Undang ini mencakup perubahan nama, lokasi, dan luas Ibu Kota Negara. Ganti nama Ibu Kota dari Jakarta menjadi Nusantara bertujuan memperkuat identitas nasional dan persatuan. Ibu Kota baru akan dipindahkan ke Kalimantan Timur dengan luas 56.180 ha dan kawasan pengembangan 199.962 ha.

f. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat.

Yang dimaksud dengan Penyelenggara Sistem Elektronik (PSE) adalah setiap pihak baik itu perseorangan maupun lembaga negara, perusahaan, atau kelompok yang memiliki, mengelola, dan/atau mempergunakan sebuah sistem elektronik dengan tujuan untuk kepentingan pribadi ataupun pihak lainnya. Perusahaan-perusahaan yang melakukan operasional secara digital dan berada didalam wilayah di Indonesia wajib untuk melakukan pendaftaran diri kepada pemerintah melalui aturan ini. Penyelenggara Sistem Elektronik (PSE) Lingkup Privat adalah layanan serta aplikasi yang dapat dipergunakan oleh seluruh masyarakat, seperti media sosial, platform OTT, transportasi *Online* dan sebagainya.

g. **Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik**

Secara umum, "Sistem Pemerintahan Berbasis Elektronik" dapat diartikan sebagai pendekatan atau strategi dalam administrasi pemerintahan di mana teknologi informasi dan komunikasi (TIK) digunakan secara luas untuk meningkatkan efisiensi, transparansi, dan responsifitas dalam penyelenggaraan pemerintahan dan pelayanan publik. Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah implementasi pemerintahan yang menggunakan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna.

h. **Panduan Pengamanan Siber bagi Instansi Pemerintah oleh Badan Siber dan Sandi Negara (BSSN).**

BSSN, sebagai instansi pemerintah, berkomitmen untuk mewujudkan keamanan siber nasional. Untuk mencapai tujuan tersebut, BSSN berupaya untuk memastikan terjaminnya keamanan siber di berbagai sektor, termasuk sektor pemerintah, sektor infrastruktur informasi kritis nasional (IIKN), dan sektor ekonomi digital. Salah satu upaya yang dilakukan BSSN adalah dengan melaksanakan kegiatan proteksi keamanan siber dengan cara mengeluarkan berbagai panduan terkait keamanan siber. Panduan ini menyediakan petunjuk dan panduan teknis untuk meningkatkan keamanan siber pada instansi pemerintah, termasuk dalam penggunaan infrastruktur teknologi.

i. **Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)**

UU Perlindungan Data Pribadi (UU PDP) merupakan bentuk hukum normatif yang memberikan perlindungan data pribadi bagi warga Indonesia. UU PDP berlaku untuk sektor publik dan privat, serta

mengatur 10 ketentuan aturan turunan dalam bentuk aturan pelaksanaan. Beberapa contoh pasal yang mungkin diatur dalam aturan pelaksanaan UU PDP adalah pengajuan keberatan terhadap pemrosesan otomatis, pelanggaran data pribadi dan ganti rugi, hak subjek data pribadi, pemrosesan data, penilaian dampak, pemberitahuan, pelaksanaan fungsi pelindungan data pribadi, transfer data, sanksi administratif, serta wewenang lembaga dan aturan pelaksanaan UU PDP. UU PDP juga terkait dengan hal-hal seperti pelaksanaan hak subjek data pribadi, kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi, analisis dampak, koordinasi antar kementerian/lembaga atau otoritas pengawas di luar negeri.

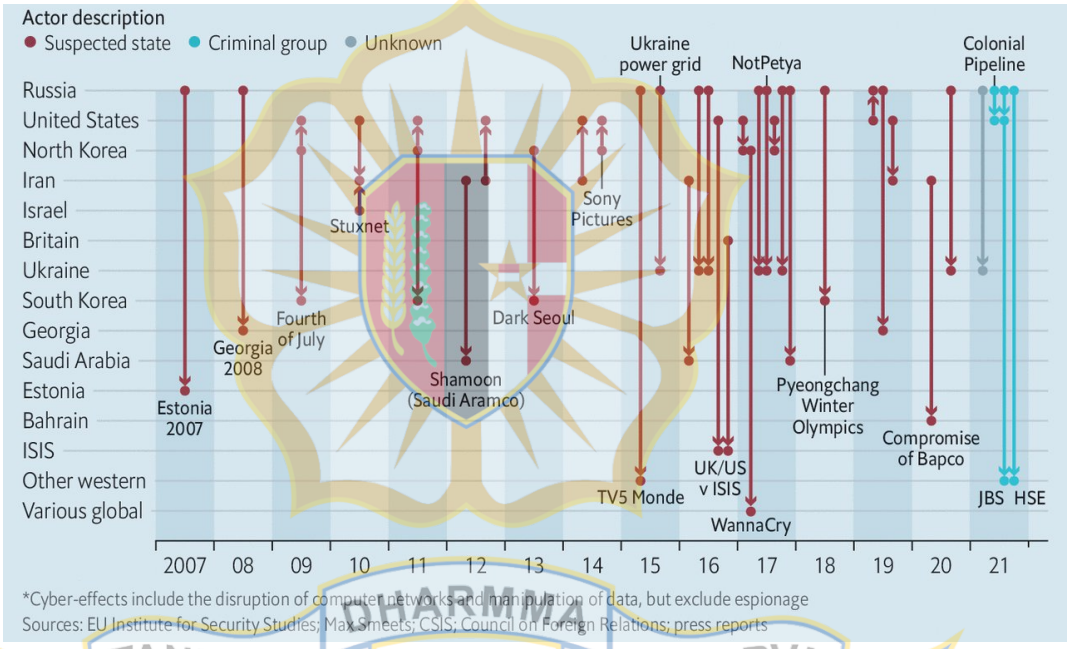
j. Rencana Pembangunan Jangka Menengah Nasional (RPJMN 2020-2024).

Saat ini keamanan siber telah menjadi salah satu prioritas nasional sesuai yang tertuang di RPJMN 2020-2024 dalam Prioritas Nasional (PN), yaitu untuk memperkuat stabilitas politik, hukum, pertahanan dan keamanan. Salah satu bentuk tindaklanjut prioritas nasional tersebut adalah pembentukan tim tanggap insiden keamanan siber atau *Computer Security Incident Response Team* (CSIRT) Dalam RPJMN 2020-2024, menjelaskan bahwa untuk menjaga stabilitas keamanan nasional, diperlukan pembangunan kemampuan pertahanan yang mampu menghadapi berbagai~~segala macam~~ ancaman, baik dari dalam negeri maupun ~~dari~~ luar negeri. Mencakup rencana pembangunan kebijakan nasional di bidang telekomunikasi dan informatika, termasuk peningkatan sistem keamanan siber dan infrastruktur teknologi.

9. Data dan Fakta.

a. Operasi *Cyber War*, juga dikenal sebagai perang siber, merujuk pada serangkaian tindakan offensif dan defensif yang dilakukan oleh negara-negara atau kelompok untuk memanipulasi, mengganggu, atau merusak sistem komputer, jaringan, dan infrastruktur digital lawan. Tujuan dari operasi cyber war dapat bervariasi, termasuk pencurian data, sabotase,

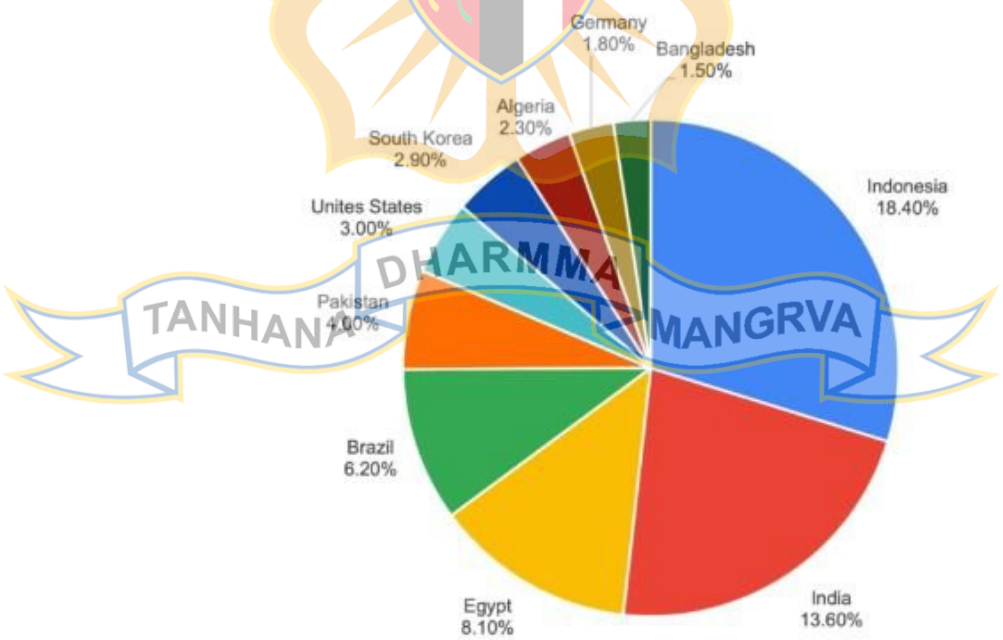
propaganda, pengintaian, dan mengacaukan sistem komunikasi. Serangan siber dapat menimbulkan kerugian finansial yang besar, mengganggu aktivitas ekonomi, atau bahkan membahayakan keselamatan Masyarakat. Operasi *Cyber War* menjadi semakin relevan dengan perkembangan teknologi informasi dan komunikasi. Negara-negara besar seperti Amerika Serikat, Rusia, Tiongkok, dan negara-negara Eropa telah dilaporkan terlibat dalam operasi *cyber war*. Beberapa operasi *cyber* terkenal termasuk Stuxnet, serangan pada sistem nuklir Iran yang diduga dilakukan oleh AS dan Israel, serta serangan siber oleh Rusia terhadap infrastruktur Ukraina.



Gambar 1. Operasi Perang Siber Yang Terjadi Di Dunia

b. *Ransomware* merupakan jenis serangan siber yang telah menimbulkan ancaman serius bagi berbagai instansi di Indonesia. Serangan *ransomware* dapat dianggap mematikan karena dapat menyebabkan kerugian finansial yang besar dan mengganggu operasi bisnis yang normal. *Ransomware* adalah jenis *malware* yang bertujuan untuk mengenkripsi atau mengunci data korban dan meminta pembayaran tebusan untuk mengembalikan data tersebut. Jika serangan *ransomware* berhasil, korban dapat mengalami kerugian finansial yang signifikan

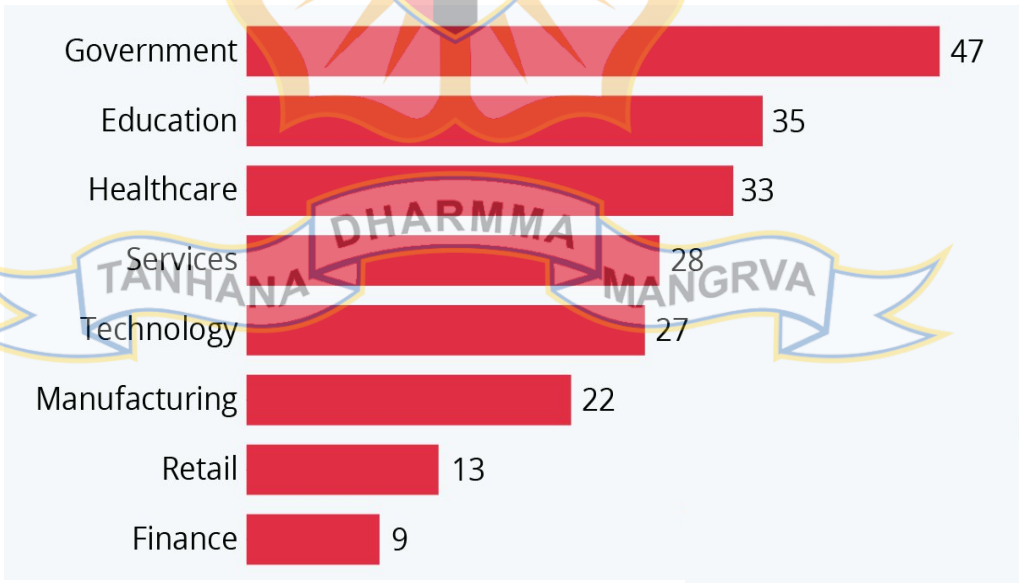
karena harus membayar tebusan yang diminta oleh penyerang. Selain itu, proses pemulihan data yang terkena serangan *ransomware* bisa memakan waktu dan memerlukan biaya tambahan. Serangan *ransomware* juga dapat mengganggu operasi bisnis secara keseluruhan. Data yang terkunci dapat menghambat akses ke informasi penting dan mengganggu proses bisnis yang normal. Hal ini dapat menyebabkan penundaan dalam pengerjaan proyek, kehilangan pelanggan, dan kerugian keuangan yang signifikan. Dalam beberapa kasus, serangan *ransomware* juga dapat menyebabkan kerugian reputasi pemerintah karena dapat mengungkapkan data rahasia. Menurut laporan dari Emisoft pada tahun 2019, 2020, dan 2021, Indonesia dan India menjadi negara-negara yang paling sering mendapatkan serangan *ransomware* secara bergantian setiap tiga bulan. Pada laporan tersebut, Indonesia menduduki posisi pertama dalam daftar ini dengan lebih dari 18% total serangan *ransomware* kemudian disusul India pada peringkat kedua dengan total lebih dari 13% total serangan *ransomware* yang terjadi di seluruh dunia.



Gambar 2.1. 10 Negara dengan Kiriman Ransomware Terbanyak Pada Q4 2021

c. Menurut data yang dikumpulkan oleh perusahaan keamanan Blackfog, terdapat 244 kasus retas *ransomware* yang dipublikasikan dari bulan

Januari hingga November pada tahun ini. Angka ini menunjukkan peningkatan sebesar 25 persen dibandingkan dengan periode yang sama pada tahun sebelumnya, yaitu tahun 2020. Salah satu penyebab meningkatnya serangan *ransomware* ini adalah beberapa geng *Ransomware* terkenal didunia menyediakan layanan *Ransomware as a Service* (RaaS) yaitu model bisnis di dunia serangan siber di mana para penyerang yang mengembangkan *ransomware* menyewakan atau menjual perangkat lunak *ransomware* mereka kepada orang lain yang ingin melancarkan serangan. Dalam model RaaS, pengembang *ransomware* menyediakan perangkat lunak ransomware yang siap digunakan, biasanya dengan antarmuka pengguna yang mudah digunakan dan fitur-fitur tertentu yang dapat disesuaikan. Dalam skenario RaaS, orang yang ingin melancarkan serangan siber tidak perlu memiliki pengetahuan teknis yang mendalam atau keahlian dalam pengembangan perangkat lunak berbahaya. Mereka dapat menggunakan perangkat lunak *ransomware* yang telah dibuat oleh pengembang RaaS dengan membayar biaya atau persentase dari hasil tebusan yang diperoleh.



Gambar 2.2. Industri yang Paling Terpengaruh oleh *Ransomware* (Nov, 2021)

d. Menurut *Global Cybersecurity Index* (GCI), terdapat sepuluh negara yang diakui memiliki pertahanan siber yang paling baik. Negara-negara ini secara konsisten menunjukkan komitmen tinggi terhadap keamanan siber dan memiliki infrastruktur serta kebijakan yang kokoh untuk melindungi diri dari ancaman siber. Mereka aktif dalam memperkuat kemampuan siber, berinvestasi dalam penelitian dan pengembangan teknologi keamanan, serta berkolaborasi dengan sektor swasta dan internasional untuk memperkuat pertahanan mereka. Sementara itu, Indonesia berada pada peringkat ke-24 dari 194 negara diseluruh dunia dengan skor nilai sebesar 94.88. Bahkan di tingkat regional Asia Pasifik, Indonesia berhasil menempati peringkat ke-6 serta peringkat ke-3 pada regional ASEAN.Hal ini merupakan sebuah peningkatan karena pada penilaian GCI sebelumnya, Indonesia hanya berhasil menempati urutan ke 41 pada tahun 2018. Meskipun menduduki peringkat yang cukup tinggi dalam daftar negara-negara dengan pertahanan siber yang dianalisis, tetapi kenyataannya keamanan siber di tanah air masih rendah, hal ini mengingatkan kita tentang pentingnya terus meningkatkan upaya dalam membangun infrastruktur dan kebijakan keamanan siber yang lebih tangguh.

Tabel 1. 10 Negara Dengan Pertahanan Siber Terbaik

10 Negara Pertahanan Siber Terbaik

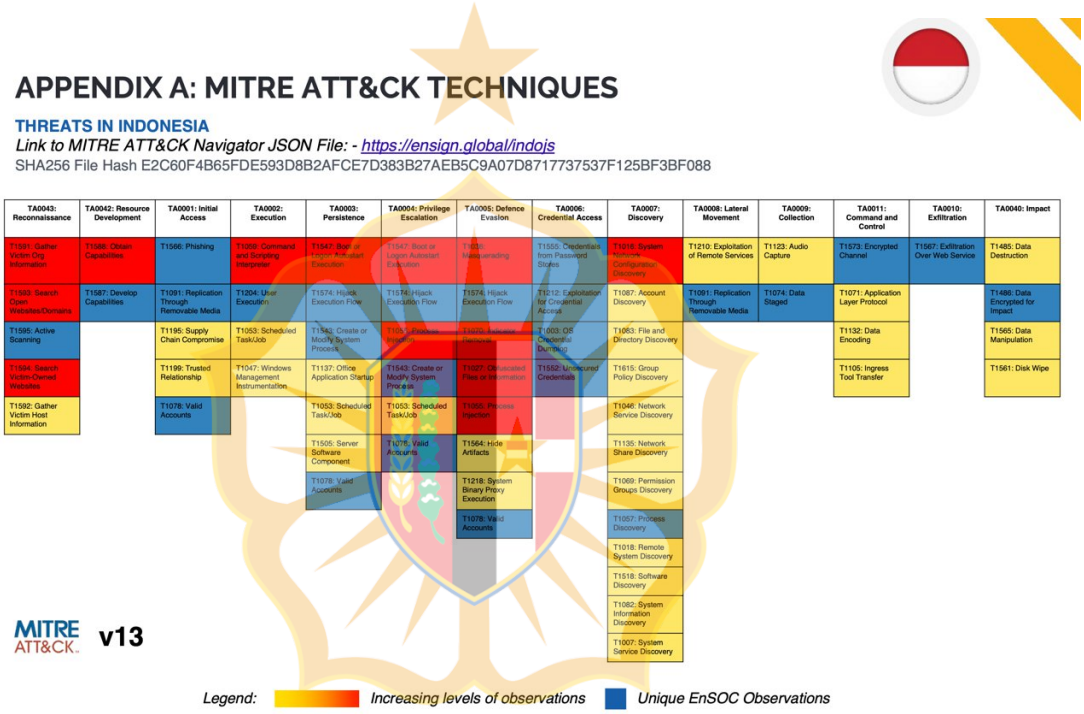
Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Indonesia	94.88	24

Wilayah Asia Pasifik

Country Name	Overall Score	Regional Rank
Korea (Rep. of)	98.52	1
Singapore	98.52	1
Malaysia	98.06	2
Japan	97.82	3
India	97.49	4
Australia	97.47	5
Indonesia	94.88	6
Viet Nam	94.55	7
China	92.53	8
Thailand	86.5	9
New Zealand**	84.04	10
Bangladesh	81.27	11

Source: Global Cybersecurity Index

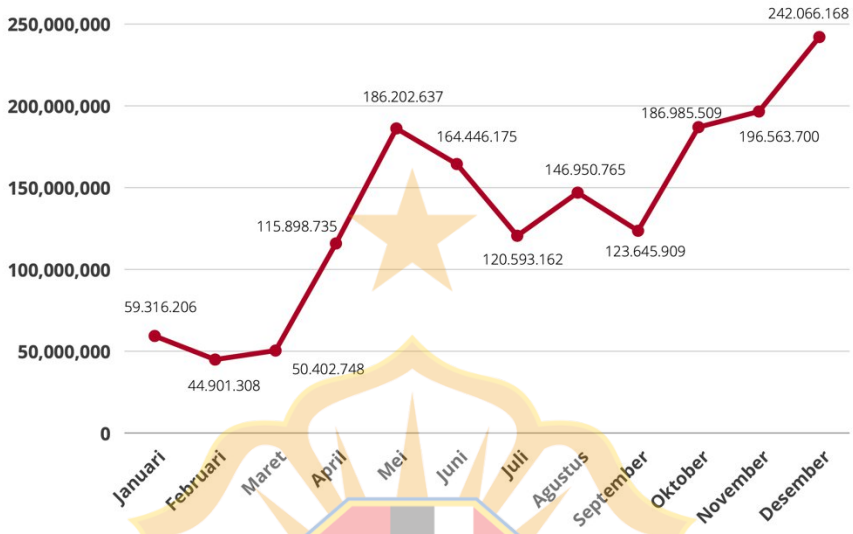
e. MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) adalah kerangka kerja yang digunakan untuk memahami taktik dan teknik yang digunakan oleh penyerang siber. Di Indonesia, ancaman siber semakin meningkat dan beragam, dengan berbagai teknik yang digunakan oleh pelaku serangan. Beberapa teknik yang sering terlihat dalam ancaman siber di Indonesia termasuk serangan *phishing*, *ransomware*, serangan DDoS, eksploitasi kerentanan perangkat lunak, dan pengintaian siber.



Gambar 2.2. Teknik Ancaman Serangan Siber Ke Indonesia

f. Kelompok Operasi Deteksi, Penanggulangan dan Pemulihan, Penanganan Insiden dan Krisis Siber Nasional BSSN melakukan pemantauan *anomaly traffic* terhadap Indonesia selama 7/24 jam (1 Januari 2021 pukul 00:00:00 hingga 31 Desember 2021 pukul 23:59:59). JUMLAH ANOMALI (Serangan Siber) NASIONAL 2021 sebesar 1.637.973.022. *Anomaly trafik* paling tinggi terjadi pada bulan Desember 2021 dengan jumlah 242.066.168 *anomaly trafik*. Dari total keseluruhan *anomaly trafik* sepanjang tahun 2021, 44.62% didominasi oleh MyloBot Botnet. Mylobot Botnet merupakan sebuah *malware* yang menargetkan system operasi Microsoft Windows. *Malware* ini menyebar melalui

lampiran yang dikirimkan pada surat elektronik atau file unduhan yang telah diinfeksi. Setelah menyerang, *malware* memungkinkan peretas untuk memiliki control penuh terhadap perangkat yang sudah terinfeksi oleh *malware* ini.



Gambar 2.3. Trafik Anomali (Serangan Siber) Nasional 2021

g. Bedasarkan anomali yang dideteksi melalui monitoring yang dilakukan oleh Direktorat Operasi Keamanan Siber, didapatkan alamat IP sumber dan tujuan anomali. Alamat IP tersebut dapat menunjukkan dari negara manakah anomali berasal dan ke negara manakah anomali ditujukan. Berikut merupakan 10 negara sumber & destinasi anomali dengan jumlah serangan tertinggi selama tahun 2021 beserta daftar IP dengan aktivitas anomali tertinggi setiap bulannya. Seperti dapat dilihat pada gambar dibawah ini, Indonesia menjadi peringkat pertama baik sebagai sumber anomali maupun tujuan anomali.

Gambar 2.4. Top 10 Negara Sumber Dan Destinasi Anomali (Serangan Siber) 2021

h. Memahami potensi risiko dari serangan siber ini akan memperkuat langkah Indonesia dalam menjaga keamanan dan kedaulatan saat mengembangkan IKN. Tanpa pemahaman yang komprehensif tentang penyerang dan permukaan serangan, negara tidak akan dapat melindungi warganya dari serangan dan negara perlu mengembangkan berbagai kemampuan baru seperti Memahami Penyerang, Memahami Korban, Memprediksi Penyebaran dan Dampak Serangan, Memahami Evolusi Permukaan Serangan[16] Sebagai contoh, Pada 2015, Ukraina mengalami serangan siber terhadap sistem grid listrik, mengakibatkan pemadaman listrik dan tindakan ini dituduh berasal dari kelompok Sandworm yang berhubungan dengan pemerintah Rusia. Ini bukan hanya serangan infrastruktur, tetapi juga tantangan terhadap kedaulatan Ukraina. Contoh lainnya adalah serangan ransomware WannaCry pada 2017 yang melumpuhkan layanan kesehatan NHS di Inggris dan organisasi lain di 150 negara, menimbulkan kerugian finansial besar dan menunjukkan bahwa infrastruktur kesehatan juga rentan terhadap serangan siber. Secara global, kerugian finansial yang diakibatkan oleh serangan siber diperkirakan adalah 6 trilyun dollar amerika, seperti pada gambar dibawah ini

[16] V.S. Subrahmanian, Michael Ovelgonne, Tudor Dumitras, B. Aditya Prakash, The Global Cyber-Vulnerability Report, Springer (2016), h. 30

Gambar 2.5. Kerugian Finansial akibat serangan siber

Negara-negara besar seperti Amerika Serikat dan Inggris telah mengalami serangan siber yang ditujukan untuk mengambil alih kontrol infrastruktur atau mencuri informasi rahasia. Contoh serangan siber yang dapat mengambil alih kontrol infrastuktur adalah *Worm* Stuxnet yang menyerang sistem kontrol Siemens yang digunakan di sejumlah fasilitas seperti pembangkit listrik, pabrik, dan pekerjaan pengolahan air. Sementara sasarannya yang jelas adalah program nuklir Iran, hal itu juga mengganggu operasi kontrol industri komputer di pabrik-pabrik di Cina, India dan Indonesia[17]

10. Kerangka Teoretis.

Dalam menganalisis data dan fakta pembangunan sistem keamanan siber dan infrastruktur teknologi ibu kota nusantara dalam rangka kewaspadaan nasional, ~~maka~~ digunakan beberapa teori guna~~untuk~~ mendukung proses pembahasan tersebut. Tujuan penggunaan teori ini adalah untuk mencapai kesesuaian ~~sehingga ditemukan kesamaan~~ antara isu inti yang dibahas~~pokok persoalan~~ dengan teori yang digunakan.

a. Metode PESTL & SWOT.

[17] Nir Kshetri - The Quest to Cyber Superiority_ Cybersecurity Regulations, Frameworks, and Strategies of Major Economies-Springer International Publishing (2016), h. 223.

Merupakan sebuah metode untuk merumuskan alternatif kebijakan/ mitigasi pada berbagai kondisi dan konteks dimana scenarios building bertujuan untuk membangun spekulasi ketidakpastian di masa depan. PESTL & SWOT bertujuan mengartikulasikan berbagai faktor dalam perencanaan organisasi yang menerapkan prinsip bukan untuk meramal masa depan, melainkan upaya mempersiapkan rencana mitigasi. Analisis PESTL adalah alat analisis strategis yang digunakan untuk mengevaluasi lingkungan secara makro. Analisis PESTLini dilakukan dengan memecah peluang dan risiko menjadi faktor-faktor berikut:

1) Politik (*Political*): Kebijakan pemerintah, stabilitas politik, dan peraturan yang berlaku.
2) Ekonomi (*Economic*): Kondisi ekonomi makro, tingkat inflasi, dan tingkat suku bunga.
3) Sosial (*Social*): Demografi, perubahan sosial, dan budaya.
4) Teknologi (*Technological*): Teknologi baru, inovasi, dan tingkat penetrasi teknologi.
5) Lingkungan (*Environmental*): Peraturan lingkungan, perubahan iklim, dan sumber daya alam.

Analisis SWOT adalah alat analisis yang digunakan untuk mengevaluasi kekuatan (*strengths*), kelemahan (*weaknesses*), peluang (*opportunities*), dan ancaman (*threats*) suatu bisnis. Analisis ini dapat membantu bisnis untuk memahami lingkungan internal dan eksternalnya, serta mengidentifikasi peluang dan risiko yang dapat mempengaruhi bisnis. Berikut adalah penjelasan singkat dari masing-masing faktor SWOT:

1) Kekuatan (*Strengths*): Faktor-faktor internal yang dapat memberikan keunggulan bagi bisnis. Contoh kekuatan antara lain: produk atau layanan yang berkualitas, reputasi yang baik, dan karyawan yang terampil.
2) Kelemahan (*Weaknesses*): Faktor-faktor internal yang dapat menjadi hambatan bagi bisnis. Contoh kelemahan antara lain: harga produk yang tinggi, distribusi yang terbatas, dan persaingan yang ketat.

3) Peluang (*Opportunities*): Faktor-faktor eksternal yang dapat menguntungkan bisnis. Contoh peluang antara lain: pertumbuhan pasar, perubahan regulasi, dan perkembangan teknologi baru.
4) Ancaman (*Threats*): Faktor-faktor eksternal yang dapat merugikan bisnis. Contoh ancaman antara lain: persaingan yang meningkat, perubahan ekonomi, dan bencana alam.

b. Teori tentang Keamanan-Siber (*CyberSecurity*).

Teori keamanan siber merupakan teori yang berhubungan dengan upaya memahami dan menganalisis masalah keamanan siber, baik dari sudut pandang teknologi, hukum, maupun politik. Teori keamanan siber mencakup berbagai aspek, mulai dari ancaman siber, kerentanan sistem teknologi informasi, hingga kebijakan dan strategi yang dapat digunakan untuk mengatasi masalah keamanan siber. Keamanan cyber yang kuat melibatkan penerapan kontrol berdasarkan tiga pilar: sumber daya manusia, proses, dan teknologi. Pendekatan tiga cabang ini membantu organisasi mempertahankan diri dari serangan terorganisir dan ancaman internal umum, termasuk pelanggaran tidak disengaja dan kesalahan manusia[18].

Teori ini berkaitan dengan upaya untuk mempertimbangkan dan memahami implikasi etika dari pengembangan dan penggunaan teknologi keamanan siber. Teori ini juga mengkaji tentang berbagai faktor etika yang perlu dipertimbangkan dalam mengembangkan dan mengimplemen-tasikan teknologi keamanan siber. Dalam praktiknya, teori-teori keamanan siber digunakan untuk mengembangkan kebijakan, strategi, dan teknologi yang efektif dalam menghadapi berbagai ancaman keamanan siber yang ada. Dalam era digital seperti sekarang ini, teori-teori keamanan siber sangat penting untuk membantu organisasi maupun negara dalam mempertahankan keamanan dan kedaulatan mereka dari ancaman siber yang semakin kompleks dan beragam.

---

[18] UK IT- Governance, What is Cybersecurity, 2019. Available at https://www.itgovernance.co.uk/what-is-cybersecurity

c. Teori tentang Kedaulatan-Siber (*Cyber Sovereignty*)

Teori kedaulatan siber menekankan pentingnya pengaturan dan pengendalian atas data dan informasi yang berada di dalam wilayah kedaulatan negara, serta pentingnya membangun infrastruktur teknologi yang dapat mengamankan akses, penggunaan, dan pengolahan data dan informasi tersebut. Konsep ini juga menekankan pentingnya hak negara untuk menentukan kebijakan dan strategi dalam pengelolaan ruang siber di dalam wilayah kedaulatan mereka.

Kedaulatan dunia maya, di negara-negara seperti Rusia, Cina, Prancis, dan Arab Saudi, mendapat pengawasan luar biasa dari NSA internasional. Dimana negara-negara tersebut mencari rujukan pembenaran untuk kegiatan yang menguntungkan negara adidaya seperti AS dengan memanfaatkan kebebasan Internet (dunia-maya/siber)[19].

d. Teori tentang Strategi Keamanan Siber Nasional (*National Cybersecurity Strategy*)

Teori tentang Strategi Keamanan Siber Nasional adalah teori yang berkaitan dengan upaya untuk mengembangkan strategi dan kebijakan yang efektif dalam menghadapi ancaman keamanan siber di tingkat nasional. Teori ini mencakup berbagai aspek, mulai dari identifikasi ancaman, penilaian risiko, pengembangan kebijakan dan strategi, hingga implementasi dan evaluasi kebijakan dan strategi tersebut. NSS ini adalah pendekatan top-down tingkat tinggi untuk keamanan siber yang menetapkan berbagai tujuan dan prioritas nasional yang harus dicapai dalam jangka waktu tertentu[20]. Teori tentang Strategi Keamanan Siber Nasional digunakan untuk mengembangkan kebijakan dan strategi yang efektif dalam menghadapi berbagai ancaman keamanan siber di tingkat nasional. Konsep ini sangat penting dalam era digital seperti sekarang

---

[19] Schneier, Bruce, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company. 2015. ISBN 978-0393244816.
[20] ENISA, National Cybersecurity Strategy, European Union Agency for Network and Information Security, 2019. Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies

ini, di mana ancaman siber semakin kompleks dan beragam, serta dapat mengancam kedaulatan negara dan keamanan nasional.

e. Konsep Kewaspadaan Nasional

Konsep kewaspadaan nasional mengacu pada upaya yang dilakukan oleh suatu negara untuk mempertahankan dan melindungi kepentingan nasionalnya dari berbagai ancaman baik yang bersifat internal maupun eksternal. Konsep ini mencakup serangkaian langkah yang dirancang untuk mengidentifikasi, menganalisis, dan mengantisipasi ancaman, serta merespons dengan cepat dan efektif ketika ancaman tersebut muncul.

Dalam konteks kewaspadaan nasional sebagai langkah antisipatif terhadap ancaman yang dihadapi Ibu Kota Nusantara, berikut adalah penjelasan tentang beberapa konsep terkait:

1) *Early Warning System* (Sistem Peringatan Dini): *Early Warning System* adalah suatu sistem yang dirancang untuk mendeteksi dan memberikan peringatan awal tentang ancaman yang mungkin timbul.
2) *Early Detection* (Deteksi Dini): *Early Detection* merujuk pada kemampuan untuk mendeteksi ancaman atau kegiatan mencurigakan sejak dini.
3) Tangkal Dini: Tangkal Dini adalah langkah-langkah yang diambil untuk menghadapi dan mengatasi ancaman sejak awal muncul.
4) Cegah Dini: Cegah Dini merupakan upaya pencegahan yang dilakukan sebelum ancaman benar-benar terjadi.
5) Tanggap Dini: Tanggap Dini adalah respons yang cepat dan efektif terhadap ancaman yang telah terdeteksi atau terjadi.

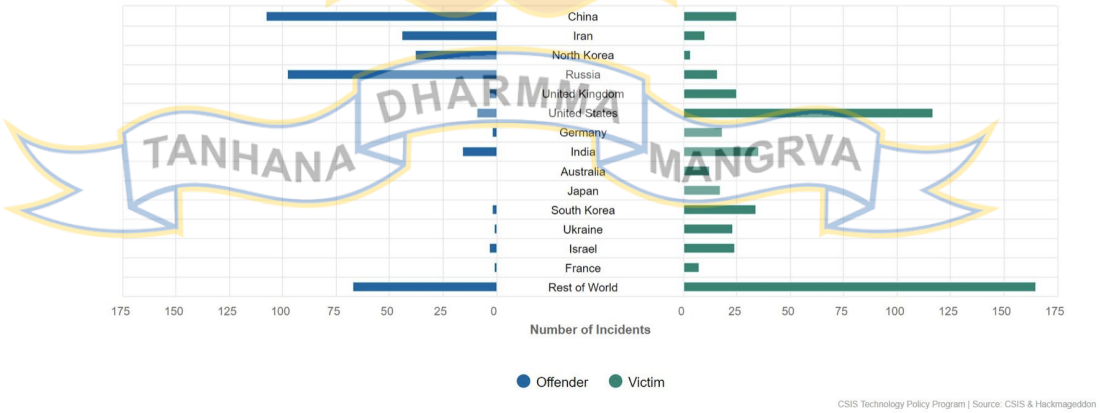
Dalam konteks kewaspadaan nasional terhadap ancaman yang dihadapi Ibu Kota Nusantara, implementasi konsep-konsep ini menjadi sangat penting. *Early Warning System* dan *Early Detection* memungkinkan pihak terkait untuk memperoleh informasi awal tentang ancaman yang mungkin terjadi, sehingga mereka dapat mengambil langkah-langkah pencegahan dan penanggulangan dengan cepat.

Tangkal Dini dan Cegah Dini bertujuan untuk meminimalkan kerugian dan dampak negatif ancaman terhadap keamanan dan stabilitas Ibu Kota Nusantara sebelum mencapai tingkat yang lebih serius.

11. Lingkungan Strategis.

a. Lingkungan Global

mencerminkan pentingnya meningkatkan kesadaran terhadap dinamika perkembangan lingkungan strategis secara global terkait keamanan siber dan infrastruktur teknologi di Indonesia. Di era yang semakin terhubung secara digital, tantangan keamanan siber semakin kompleks dan beragam. Berbagai negara dan kelompok aktor menghadapi ancaman siber yang berkembang dengan cepat, termasuk serangan siber yang menargetkan infrastruktur kritis, data sensitif, dan kepentingan nasional. Kita lihat grafik di bawah ini. Data ini dikeluarkan oleh CSIS, lembaga *think tank* AS. Terlihat bagaimana AS telah melihat ancaman siber cukup serius, menjadikan Russia dan Tiongkok sebagai ancaman serius keamanan siber. Pihak-pihak di AS berulang kali menjadi Russia sebagai "tersangka" terpilihnya Donald Trump dalam pemilu 2016, karena adanya operasi siber dari "Kremlin".



Gambar 2.6. Peta Aktor dan Korban Serangan Siber Global

Untuk menghadapi tantangan ini, Indonesia sebagai Ibu Kota Nusantara perlu menerapkan strategi yang kokoh dalam membangun sistem keamanan siber dan infrastruktur teknologi yang andal. Hal ini

mencakup pembentukan kerangka hukum yang efektif, kerja sama antara sektor publik dan swasta, serta peningkatan kapasitas sumber daya manusia dalam bidang keamanan siber.

Dinamika perkembangan lingkungan strategis global mencakup perkembangan teknologi, perubahan perilaku pelaku serangan, dan evolusi taktik keamanan siber. Oleh karena itu, pemahaman mendalam tentang perkembangan tersebut menjadi kunci untuk merancang sistem keamanan siber yang tangguh dan adaptif. Dengan mengidentifikasi tren dan ancaman terbaru, Indonesia dapat mengambil langkah-langkah proaktif untuk melindungi infrastruktur teknologi dan data vitalnya, memitigasi potensi risiko serangan siber, serta mengamankan kepentingan nasional secara holistik. Pembangunan sistem keamanan siber dan infrastruktur teknologi yang efektif di Ibu Kota Nusantara akan memberikan dampak positif bagi keamanan nasional secara keseluruhan. Dengan mengintegrasikan pendekatan multidisiplin dan berbasis data, Indonesia dapat menghadapi tantangan dan ancaman siber dengan lebih baik, sehingga menjadikan negara ini semakin kuat dan siap menghadapi dinamika perkembangan lingkungan strategis global yang tidak dapat diprediksi dengan pasti.

b. Lingkungan Regional

Dinamika lingkungan regional ditandai dengan banyaknya meningkatnya ketegangan serangan siber di ASEAN menggarisbawahi pentingnya mengidentifikasi dinamika perkembangan lingkungan strategis pada tataran regional terkait keamanan siber dan infrastruktur teknologi di Indonesia. Seiring tren dan potensi digitalisasi, Pemerintah Indonesia terus mengakselerasi agenda transformasi digital nasional, termasuk memperkuat konektivitas digital ASEAN, khususnya melalui Keketuaan ASEAN tahun 2023[21] untuk memperkuat epicentrum of growth. Lingkungan strategis regional mencakup interaksi dan hubungan antara negara-negara tetangga dan aktor-aktor regional dalam hal

[21] https://www.antaranews.com/berita/3692229/menkominfo-nyatakan-indonesia-optimalkan-konektivitas-digital-asean

keamanan siber. Di tingkat regional, tantangan keamanan siber tidak hanya dipengaruhi oleh ancaman yang datang dari negara-negara tetangga, tetapi juga oleh tindakan aktor siber regional dan transnasional yang dapat mengancam stabilitas keamanan siber Indonesia. Perkembangan teknologi yang pesat, seperti *Internet of Things* (IoT), *artificial intelligence* (AI), dan *blockchain*, membuka peluang baru bagi pelaku serangan untuk melancarkan tindakan mereka secara efisien dan tidak terdeteksi.

Berdasarkan pengamatan Ensign Infosecurity *Cyber Threat Landscape* 2023, penulis mencatat adanya representasi yang menonjol dari kejahatan terorganisir, dan kelompok ancaman yang disponsori oleh negara—berasal dari China, Korea Utara, Iran, dan Rusia—yang menargetkan wilayah-wilayah tersebut. Lotus Blossom dan Naikon adalah kelompok ancaman yang mencolok yang umumnya menargetkan Indonesia, Malaysia, dan Singapura. Dark Pink teramati menargetkan wilayah-wilayah berbahasa Melayu di Indonesia dan Malaysia. Berbeda dengan tahun-tahun sebelumnya, penulis juga melihat penurunan penargetan di wilayah-wilayah tersebut dari kelompok-kelompok ancaman yang berasal dari Rusia, dan tempat tersebut kini lebih dominan diisi oleh kelompok-kelompok ancaman yang berasal dari China. Hal ini mungkin menjadi hasil dari konflik Rusia-Ukraina yang terus berlanjut.

Tabel 2. Wilayah-Wilayah Spesifik Dan Ancaman Siber Regional.

	Agrius	APT29	Dark Pink	Desorden	FIN11	Kimsuky	Lazarus Group	Lotus Blossom, Thrip	menuPass	Naikon	Operation Dragon Castling	Roaming Mantis
Profile	Organised Crime	State-sponsored	State-sponsored	Organised Crime	Organised Crime	State-sponsored	State-sponsored	State-sponsored	State-sponsored	State-sponsored	Organised Crime	Organised Crime
Motivation	Information theft & espionage Sabotage & destruction	Information theft & espionage	Information theft & espionage	Financial gain	Financial crime Financial gain	Information theft & espionage Sabotage & destruction Financial crime	Information theft & espionage Sabotage & destruction Financial crime	Information theft & espionage	Information theft & espionage	Information theft & espionage	Information theft & espionage	Financial crime
Associated Territory	Iran	Russia	Vietnam	Unknown	Unknown	North Korea	North Korea	China	China	China	China	Unknown
Ensign TERRITORIES												
Singapore		•			•			•		•		
Malaysia			•	•				•		•		
Hong Kong	•								•		•	
South Korea						•	•					•
Indonesia			•	•				•		•		

Pembangunan sistem keamanan siber dan infrastruktur teknologi yang tangguh di Ibu Kota Nusantara harus mempertimbangkan dinamika dan tren terkini dalam ancaman siber pada tingkat regional. Kerja sama antarnegara dan kolaborasi dengan aktor regional lainnya juga menjadi penting untuk menghadapi tantangan bersama dan berbagi informasi tentang ancaman yang mungkin dihadapi. Melalui pemahaman yang mendalam tentang dinamika lingkungan strategis regional, Indonesia dapat mengidentifikasi celah keamanan yang mungkin dieksploitasi oleh para penyerang dan mengambil tindakan pencegahan yang tepat. Penyusunan kebijakan keamanan siber yang berfokus pada tingkat regional juga akan membantu Ibu Kota Nusantara menjadi pusat pertahanan siber yang efektif dan menjaga kewaspadaan nasional dengan baik. Dengan berinvestasi dalam kemampuan keamanan siber yang berbasis data dan teknologi terbaru, serta bekerja sama dengan negara-negara tetangga dan aktor regional, Indonesia dapat membangun sistem keamanan siber yang andal dan adaptif untuk menghadapi ancaman dan dinamika perkembangan lingkungan strategis di tingkat regional dengan efektif.

c. Lingkungan Nasional

Dinamika lingkungan nasional yang dapat memberikan pengaruh, baik langsung maupun tidak langsung, terhadap upaya pembangunan sistem keamanan siber dan infrastruktur teknologi ibu kota nusantara dalam rangka kewaspadaan nasional di IKN dapat diuraikan melalui aspek-aspek ~~sebagai~~ berikut:

1) Geografi.

Dinamika lingkungan nasional memiliki pengaruh baik langsung maupun tidak langsung terhadap upaya pembangunan sistem keamanan siber dan infrastruktur teknologi di Ibu Kota Nusantara (IKN) dalam rangka kewaspadaan nasional, terutama dalam aspek geografi. Pertumbuhan urbanisasi yang pesat di IKN menyebabkan kepadatan populasi dan tingginya aktivitas ekonomi,

sehingga infrastruktur teknologi menjadi lebih rentan terhadap serangan siber. Konektivitas internet yang semakin luas di IKN membuka celah bagi pelaku serangan siber untuk mencoba menembus infrastruktur dan meretas data sensitif. Selain itu, keberagaman budaya di Indonesia juga berdampak pada kerentanan terhadap serangan siber berbahasa Indonesia. Di sisi lain, keberadaan pulau-pulau terpencil menimbulkan tantangan dalam meningkatkan aksesibilitas dan keamanan jaringan di seluruh wilayah negara. Semua faktor ini harus dipertimbangkan secara holistik dalam merancang dan melaksanakan sistem keamanan siber yang efektif untuk menjaga kewaspadaan nasional dan menghadapi ancaman siber dengan baik.

2) Demografi.

Perkembangan aspek demografi Indonesia saat ini dan ke depankedepan masih menghadapi masalah pemerataan penduduk. Salah satu tujuan pembangunan IKN adalah untuk mendorong pemerataanagar penduduk lebih merata, terutama antara Pulau Jawa dan Pulau Kalimantan. Migrasi penduduk dari Jakarta menuju IKN baru telah direncanakan dalamsesuai lima tahap pembangunan IKN. Tahap pertama Migrasi penduduk dimulai dengan relokasi pelopor dari anggota TNI, Polri, dan BIN padadi tahun 2023, kemudian diikuti oleh relokasi representasi badan eksekutif, legislatif, yudikatif, dan ASN pada awal tahun 2024, dan seterusnya. Jumlahselanjutnya. Skema jumlah penduduk di IKN pada Tahap 1 dan 2 diperkirakan akan naik secara eksponensial seiring dengan rencana pemindahan anggota TNI, Polri, BIN, ASN, beserta keluarga, danserta rencana pembukaan kawasan di IKN untuk kegiatan ekonomi dan sosial. Pada Tahap 3, diperkirakan pertumbuhan penduduk akan lebih lambat, kemudian meningkat kembali pada Tahap 4 dan 5 ketika seluruh kegiatan sektor ekonomi baru mulai berkembang sesuai rencana yang direncanakan akan selesai pada tahun 2045[22].

[22] Lampiran II Undang-undang Nomor 3 tahun 2022 tentang Ibu Kota Negara, h. 99.

3) Politik.

Dinamika lingkungan nasional pada aspek politik memberikan pengaruh baik langsung maupun tidak langsung terhadap upaya pembangunan sistem keamanan siber dan infrastruktur teknologi di Ibu Kota Nusantara (IKN) dalam rangka kewaspadaan nasional. Keberadaan kebijakan keamanan siber yang jelas dan komprehensif menjadi kunci dalam menciptakan lingkungan yang aman bagi infrastruktur teknologi di Indonesia. Selain itu, keterlibatan aktif pemerintah dalam pencegahan, deteksi, dan penanggulangan serangan siber memiliki peran penting dalam menanggulangi ancaman siber yang terus berkembang di IKN.

4) Ekonomi.

Dinamika lingkungan nasional pada aspek ekonomi memiliki pengaruh baik langsung maupun tidak langsung terhadap upaya pembangunan sistem keamanan siber dan infrastruktur teknologi di Ibu Kota Nusantara (IKN) dalam rangka kewaspadaan nasional. Pertumbuhan *e-commerce* yang pesat dengan nilai transaksi mencapai lebih dari 42 miliar dolar AS pada tahun 2021 membuka peluang bagi serangan siber terhadap data konsumen dan sistem transaksi *online*. Investasi sebesar 1,2 miliar dolar AS dalam sektor teknologi di Indonesia pada tahun 2021 menandakan pentingnya menjaga keamanan siber dan melindungi aset digital dari ancaman serangan. Namun, dampak serangan siber tidak dapat diabaikan karena biaya global yang diperkirakan mencapai 6 triliun dolar AS pada tahun 2021, yang dapat menyebabkan kerugian finansial yang signifikan bagi perusahaan dan pemerintah di IKN. Terutama, sektor energi dan utilitas menjadi sasaran serangan sekitar 42% di Indonesia, menunjukkan perlunya penguatan keamanan siber untuk melindungi infrastruktur kritis yang sangat bergantung pada teknologi informasi dan internet.

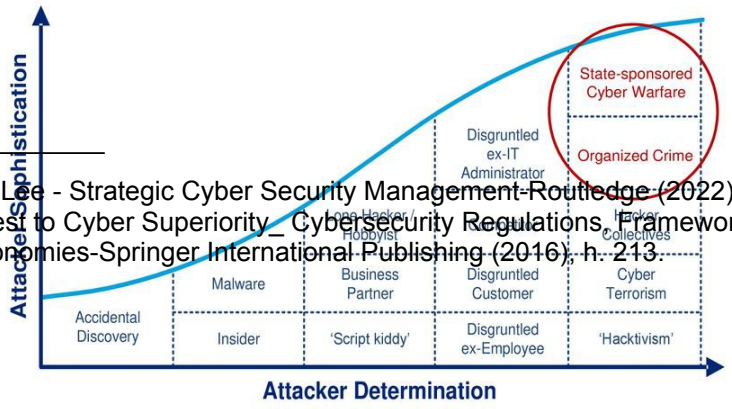
5) Pertahanan Keamanan.

Dinamika lingkungan nasional pada aspek Pertahanan Keamanan memiliki pengaruh baik langsung maupun tidak langsung terhadap upaya pembangunan sistem keamanan siber dan infrastruktur teknologi di Ibu Kota Nusantara (IKN) dalam rangka kewaspadaan nasional. Pengamanan infrastruktur kritis, terutama sektor energi dan utilitas, menjadi prioritas untuk menjaga stabilitas dan keamanan nasional. Dalam lingkungan pertahanan keamanan, peran aktif BSSN, BIN, TNI dan Polri dalam operasi siber untuk melawan ancaman menjadi krusial dalam memastikan keamanan negara.

BAB III
PEMBAHASAN

12. Umum.

Pengertian Ancaman Siber Global berkaitan dengan upaya serangan, infiltrasi, atau tindakan subversif melalui dunia maya yang dilakukan oleh aktor-aktor tak dikenal—bisa berupa individu, kelompok, atau negara—dengan tujuan merusak, mencuri data, atau menghambat operasi sistem teknologi informasi suatu entitas atau negara. Tujuan serangan dunia maya adalah untuk melumpuhkan infrastruktur negara dengan maksud menyebabkan kerusakan politik dan ekonomi dan Tindakan perang atau terorisme dunia maya dilakukan untuk menimbulkan pergolakan politik dan mengakibatkan suatu negara menjadi tidak stabil secara politik.[23] Serangan siber berusaha menghancurkan sistem komputer, mencuri intelijen, menyebarkan propaganda online, dan menyebabkan kerusakan lainnya[24]



[23] Peter Trim, Yang-Im Lee - Strategic Cyber Security Management-Routledge (2022), h. 57
[24] Nir Kshetri - The Quest to Cyber Superiority_ Cybersecurity Regulations, Frameworks, and Strategies of Major Economies-Springer International Publishing (2016), h. 213.

Gambar 3.1. Grafik klasifikasi serangan siber

Seperti tampak pada gambar 3.1, serangan siber dengan metode serangan yang rumit serta kebulatan tekat untuk melakukan serangan siber paling tinggi dilakukan oleh peretas yang dibiayai oleh negara serta kelompok kejahatan terorganisasi.

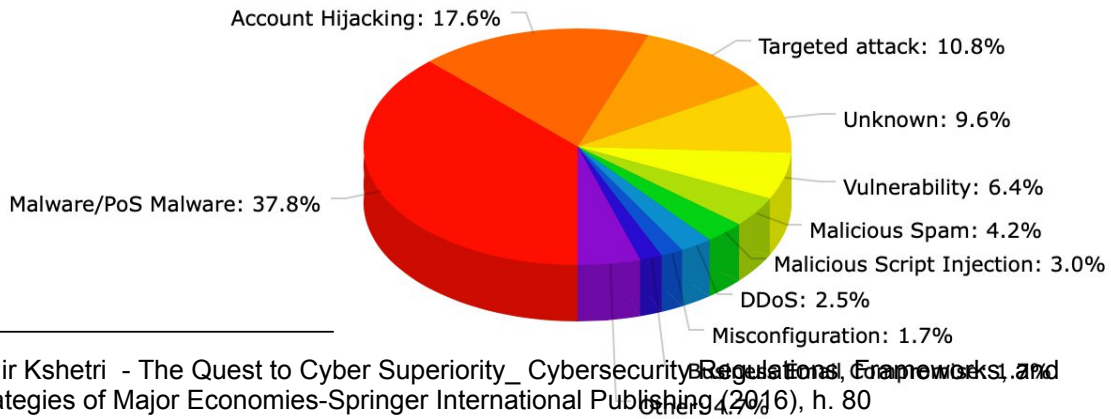
Di era digital saat ini, keamanan siber telah menjadi salah satu isu utama dalam hubungan internasional dan menjadi titik penting dalam strategi pertahanan suatu negara. Dalam konteks pengembangan Ibu Kota Nusantara (IKN) di Indonesia, ancaman siber global memegang potensi risiko yang sangat tinggi. Mengingat rencana pembangunan IKN yang akan memanfaatkan teknologi canggih, hal ini secara otomatis menarik perhatian dari berbagai pihak, baik yang memiliki niat baik maupun yang ingin mengambil keuntungan. Terlebih, kecanggihan teknologi yang diharapkan menjadi tulang punggung IKN menjadikannya target empuk bagi serangan siber.

Mengacu pada Teori Keamanan-Siber (*CyberSecurity*), terdapat beberapa poin krusial yang harus diperhatikan. Pertama, integritas dan kerahasiaan data merupakan hal yang mutlak. Jika sistem keamanan siber IKN tidak dirancang dengan baik, data sensitif pemerintah dan masyarakat bisa bocor atau disusupi, mengakibatkan kerugian materiil hingga potensi krisis keamanan nasional. Kedua, ketersediaan infrastruktur. Serangan siber seperti DDoS (*Distributed Denial of Service*) dapat menghambat akses ke sistem informasi vital, mengganggu operasional pemerintahan hingga layanan publik di IKN. Dalam teori ini juga ditekankan pentingnya pendidikan dan kesadaran masyarakat tentang keamanan siber. Masyarakat yang edukatif dan sadar akan pentingnya keamanan siber akan meminimalisir potensi risiko dari dalam, seperti kebocoran data akibat kelalaian pengguna. Potensi

ancaman siber global terhadap pengembangan IKN sangatlah nyata. Mengacu pada Teori Keamanan-Siber, penting bagi Indonesia untuk mempersiapkan diri dengan sistem pertahanan siber yang kuat, pendidikan masyarakat, serta kerjasama internasional dalam bidang keamanan siber untuk memastikan keamanan dan kedaulatan bangsa dalam era digital.

Ibu Kota Nusantara (IKN) Nusantara di Indonesia sebagai pusat pemerintahan modern sangat fokus pada infrastruktur teknologi terintegrasi. Namun, ancaman siber global yang terus berkembang menjadi isu utama. Dalam konteks ini, Teori Keamanan-Siber menunjukkan bahwa serangan siber bukan hanya masalah kejahatan digital, tetapi juga ancaman nyata terhadap kedaulatan negara. Keamanan siber global melibatkan integritas data, kerahasiaan, dan ketersediaan layanan. Kesiapan IKN Nusantara dalam menghadapi ancaman ini sangat penting, mengingat potensi kerugian bukan hanya ekonomi, tetapi juga reputasi dan integritas data negara.Hambatan terkait Keamanan Siber untuk perdagangan dan investasi mencakup setidaknya tiga kategori kekhawatiran: spionase politik, spionase ekonomi, privasi dan keamanan informasi warga Negara[25]

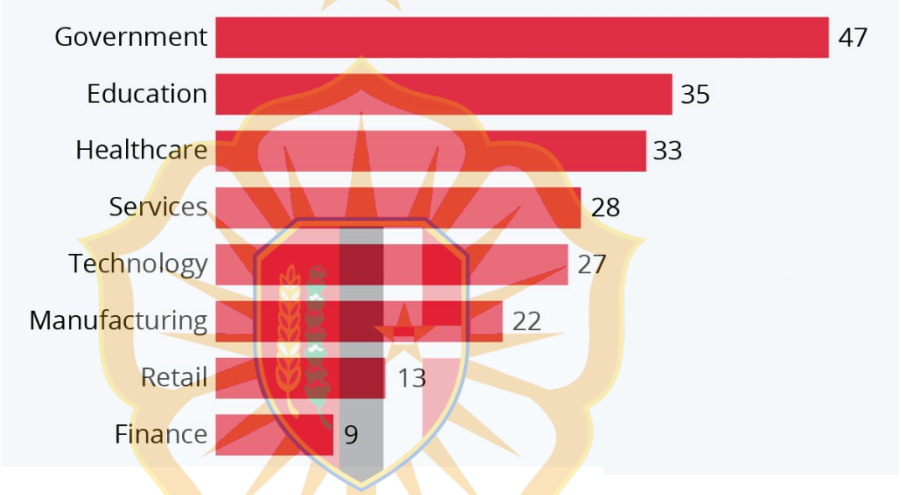
Dengan infrastruktur teknologi yang canggih, IKN Nusantara otomatis menjadi target potensial bagi aktor siber yang memiliki kepentingan tertentu. Serangan siber seperti DDoS, *ransomware*, atau infiltrasi sistem bisa menghambat operasional pemerintah, merusak sistem vital, bahkan menciptakan keresahan di masyarakat. Jika dilihat dari gambar 3.2 dibawah ini dapat dilihat jika serangan *malware*/*ransomware* menduduki peringkat teratas dalam jumlah serangan.



[25] Nir Kshetri - The Quest to Cyber Superiority_ Cybersecurity Regulations, Frameworks, and Strategies of Major Economies-Springer International Publishing (2016), h. 80

Gambar 3.2. Grafik jenis serangan siber Q1 2020 diseluruh dunia

Sedangkan jika dilihat dari gambar 3.3 dibawah ini, sektor pemerintahan menduduki peringkat pertama dalam serangan *ransomware* yang terjadi di seluruh dunia menurut hasil riset dari BlakFog pada bulan november 2021



Gambar 3.3. Grafik target serangan *ransomware* Nov 2021 di seluruh dunia

Teori Keamanan-Siber menekankan pentingnya meningkatkan kapabilitas pertahanan siber melalui pengembangan teknologi, pendidikan keamanan siber bagi pegawai pemerintah dan masyarakat, serta kerjasama internasional. Teori ini menggarisbawahi bahwa ancaman siber global bisa merusak sistem informasi, integritas data, dan infrastruktur digital suatu negara, berpotensi mengganggu pemerintahan, infrastruktur kritis, dan struktur sosial masyarakat. Oleh karena itu, dalam upaya pengembangan IKN, prioritas utama harus diberikan pada keamanan siber untuk mencegah potensi gangguan terhadap visi modern dan maju yang diimpikan.Contohnya di Amerika, sudah menjadi pertimbangan sejak lama bahwa serangan kepada system yang menjalankan Amerika, paling utama adalah saluran listrik,

sebuah Amerika yang lumpuh akan menjadi hadiah yang diinginkan oleh teroris Al-Qaeda.[26]

Indonesia, yang tengah giat membangun Ibu Kota Nusantara (IKN) dengan visi modern dan teknologi, perlu menyadari bahwa setiap kemajuan teknologi membawa risiko potensial. Ancaman seperti serangan DDoS, *ransomware*, dan infiltrasi pada sistem pemerintahan bisa mengganggu operasional negara dan menciptakan kekhawatiran. Lebih serius lagi, jika data sensitif pemerintah atau rahasia negara dicuri oleh aktor asing, hal ini bisa mengancam kedaulatan. Aktor tersebut dapat memanipulasi informasi, merusak reputasi negara, atau bahkan menggunakan data tersebut sebagai alat tekanan diplomasi. Kesadaran akan risiko ini sangat penting dalam upaya membangun IKN yang aman dan berkelanjutan.Salah satu kesulitan utama dalam menentukan arah serangan dunia maya adalah menemukan bukti pelaku sebenarnya dan lokasi dari mana serangan itu diluncurkan[27]

Namun, Teori Keamanan-Siber tidak hanya memfokuskan pada risiko, tetapi juga solusi. Perlindungan adalah sebuah proses, bukan produk. Sistem perlindungan, dan infrastruktur secara keseluruhan, harus berfungsi dan berkembang dari waktu ke waktu, dan dalam hal sistem perlindungan, ia harus mampu bereaksi dalam waktu yang sangat singkat serta beradaptasi dalam waktu yang jauh lebih lama. kerangka waktu.[28] Pendidikan dan kesadaran mengenai keamanan siber, pengembangan teknologi keamanan yang canggih, dan kerjasama internasional dalam pertahanan siber merupakan langkah strategis yang sangat dianjurkan.

13. Potensi ancaman siber global yang dapat mengancam keamanan dan kedaulatan Indonesia dalam pengembangan Ibu Kota Nusantara (IKN).

a. Potensi Ancaman Siber Global Yang Dapat Mengancam Keamanan Dan Kedaulatan Indonesia.

---

[26] (Wiley Corporate F&A) MacDonnell Ulsch - Cyber Threat!_ How to Manage the Growing Risk of Cyber Attacks-Wiley (2014), h. 59

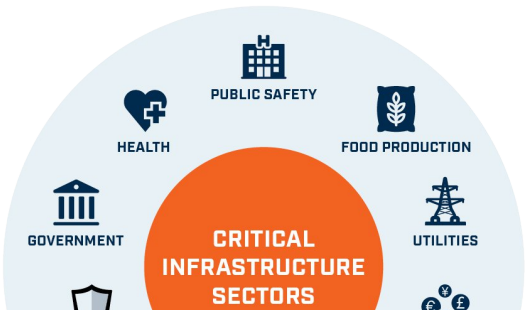
[27] CRC Press. Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber WarfareJohnson, Thomas A (2015), h, 232.

[28] CRC PRess. Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber WarfareJohnson, Thomas A (2015), h, 139.

Potensi ancaman siber global memang kian meningkat seiring perkembangan teknologi dan digitalisasi. Dalam skala nasional, terutama dengan pengembangan Ibu Kota Nusantara (IKN), Indonesia berada pada posisi yang rentan. IKN yang direncanakan sebagai simbol modernisasi dan transformasi digital Indonesia, tanpa diragukan lagi, akan menjadi titik krusial bagi serangan siber. Teori Keamanan-Siber (*CyberSecurity*) menjelaskan bahwa ancaman siber global tidak hanya pencurian namun serangan siber dapat menggangu stabilitas, merusak infrastruktur kritis, dan pada akhirnya mengancam kedaulatan nasional. Selain itu serangan siber juga dapat mengakibatkan kerusakan fisik, trauma psikologi serta kerugian ekonomi seperti yang nampak pada gambar manifsetasi serangan siber dibawah ini. Contoh konkret adalah serangan terhadap fasilitas pemerintah, gangguan layanan publik, atau pencurian data rahasia negara yang bisa disalahgunakan oleh pihak-pihak asing.

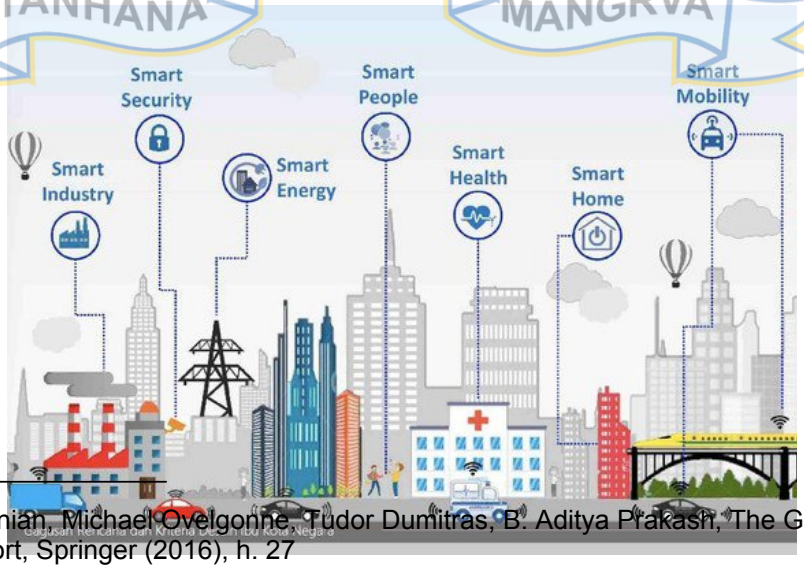
Gambar 3.4. Manifestasi serangan siber

Dalam konteks IKN, keamanan siber bukanlah sekadar isu teknis, tetapi menjadi soal strategis. Jika infrastruktur digital IKN berhasil ditembus, hal ini bisa berdampak pada sistem pemerintahan, keuangan, sektor kesehatan serta sektor sektor lain yang merupakan sektor infrastuktur kritis seperti yang nampak pada gambar dibawah ini.



Gambar 3.5. Sektor Infrastruktus Kritis

Tidak hanya kerugian materiil, tetapi juga kerugian reputasi dan kepercayaan publik yang bisa terjadi. Jika data nasional jatuh ke tangan asing, kedaulatan Indonesia terancam. Data tersebut bisa dimanfaatkan untuk mempengaruhi kebijakan, menekan negosiasi internasional, atau merusak hubungan bilateral. Namun, Teori Keamanan-Siber menawarkan solusi dengan penerapan teknologi keamanan, pendidikan siber, dan kerjasama internasional sebagai kunci menanggulangi ancaman.Hal ini menunjukkan bahwa negara-negara harus sangat waspada dalam melacak apa yang sedang terjadi di jaringan di dalam negara mereka, dan bahwa mereka tetap waspada terhadap laporan kerentanan dunia maya baru.[29]



[29] V.S. Subrahmanian, Michael Ovelgonne, Tudor Dumitras, B. Aditya Prakash, The Global Cyber-Vulnerability Report, Springer (2016), h. 27

Gambar 3.6. Gambaran pengembangan IKN

Indonesia, dengan rencana pengembangan IKN yang canggih dan modern seperti pada gambar 3.7. diatas, harus menyadari potensi ancaman yang sama. Faktor geografis dan geopolitik, serta kepentingan ekonomi dan strategis IKN, dapat menjadikannya target empuk bagi aktor siber asing yang ingin menggoyang stabilitas dan kedaulatan Indonesia. Bila informasi penting negara bocor atau infrastruktur digital IKN berhasil ditembus, ini bukan hanya soal kerugian finansial, tetapi juga integritas dan kepercayaan publik Ancaman terhadap infrastruktur kritis negara kita melalui serangan dunia maya adalah akibat langsung dari rangkaian perangkat lunak digital yang canggih, keterbukaan sebagian besar jaringan, keterkaitan Internet, dan terbatasnya jangkauan program keamanan dunia maya yang lemah. [30]

Berdasarkan Teori Keamanan-Siber, ada beberapa langkah penting yang harus dilakukan. Pertama, penguatan infrastruktur siber melalui teknologi keamanan terdepan. Kedua, pelatihan dan edukasi bagi stakeholder terkait, dari level pemerintah hingga masyarakat umum. Ketiga, kerjasama internasional dalam bidang keamanan siber, baik untuk pertukaran informasi maupun untuk pengembangan teknologi. Kita juga harus memahami Empat Pilar Perlindungan Infrastruktur Informasi Kritis yaitu pencegahan dan peringatan dini, deteksi, reaksi, manajemen krisis.[31]

Dalam konteks Indonesia dan pengembangan IKN, ada beberapa pelajaran yang dapat diambil. Pertama, perlunya investasi dalam teknologi keamanan siber yang canggih dan up-to-date. Investasi ini harus mencakup perangkat keras, perangkat lunak, dan sumber daya manusia. Kedua, pendidikan dan pelatihan keamanan siber bagi semua pegawai dan pihak yang terlibat dalam pengembangan dan

[30] CRC Press. Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber WarfareJohnson, Thomas A (2015), h, 54.
[31] Peter Trim, Yang-Im Lee - Strategic Cyber Security Management-Routledge (2022), h. 68

pengoperasian IKN adalah esensial karena orang sering dianggap sebagai mata rantai terlemah dalam hal keamanan dunia maya namun mereka juga memiliki potensi terbesar untuk membantu organisasi mendeteksi dan mengidentifikasi insiden keamanan dunia maya.[32] Terakhir, kerjasama internasional dalam bidang keamanan siber dapat memperkuat pertahanan dan respons terhadap serangan.

b. Model Analisis Ancaman Siber Global dalam Konteks Pengembangan IKN.

Dalam memahami bagaimana ancaman siber global dapat berdampak pada pengembangan Ibu Kota Negara Nusantara, kita memerlukan suatu model analisis. Model ini akan memungkinkan para pemangku kepentingan untuk mengidentifikasi, mengevaluasi, dan merespons potensi risiko dalam konteks yang spesifik. Berikut adalah model analisis yang disarankan:

1) Identifikasi Ancaman Potensial

a) Aktor Ancaman: Identifikasi siapa yang mungkin menjadi pelaku serangan. Apakah mereka aktor negara, kelompok kriminal, *hacktivist*, atau *insider*?

b) Motif: Apa tujuan dari aktor tersebut? Motif dapat berkisar dari keuntungan finansial, politik, hingga tujuan ideologis.

c) Vektor Serangan: Melalui metode apa ancaman dapat masuk? Apakah melalui *email phishing*, perangkat IoT yang tidak aman, atau celah *software*?

2) Analisis Kerentanan

a) Infrastruktur Teknologi: Periksa sistem IT yang digunakan dalam pengembangan IKN. Apakah mereka memiliki

[32] Centre For Cyber Security Belgium, Cyber Security Incident Management Guide-Centre For Cyber Security Belgium (2015), h. 20

keamanan yang memadai? Apakah ada celah yang dapat dimanfaatkan oleh pelaku?

b) **Sumber Daya Manusia:** Manusia sering kali menjadi titik lemah dalam sistem keamanan. Seberapa baik karyawan dan kontraktor dilatih dalam keamanan siber?

c) **Ketidaktahuan:** Apakah ada sistem atau proses yang tidak diketahui seberapa amannya?

3) **Evaluasi Dampak Potensial**

a) **Dampak Fisik:** Apakah serangan siber dapat mengakibatkan kerusakan fisik pada infrastruktur IKN?

b) **Dampak Data:** Bisakah data penting dicuri, diubah, atau dihapus?

c) **Dampak Reputasi:** Bagaimana dampak potensial suatu insiden keamanan terhadap citra publik IKN dan pemerintah?

d) **Dampak Ekonomi:** Apa biaya finansial dari potensi serangan tersebut?

4) **Mitigasi Risiko**

a) **Penguatan Keamanan:** Implementasi solusi keamanan teknis seperti firewall, sistem deteksi intrusi, dan enkripsi.

b) **Pelatihan dan Kesadaran:** Edukasi para pemangku kepentingan tentang keamanan siber dan praktik terbaik.

c) **Rencana Tanggap Darurat:** Siapkan rencana aksi untuk merespons insiden keamanan yang terjadi.

5) **Evaluasi Berkala dan Pembaruan**

a) **Pemantauan:** Gunakan alat pemantauan untuk mendeteksi aktivitas mencurigakan.

b) **Pengujian:** Lakukan pengujian penetrasi secara berkala untuk mengevaluasi kekuatan sistem keamanan.

c) **Pembaruan:** Pastikan semua sistem tetap diperbarui dan patch keamanan teraplikasi.

c. Identifikasi Potensi Ancaman Siber dan Infrastruktur Teknologi yang Paling Berdampak pada Pengembangan IKN di Indonesia.

Pengembangan Ibu Kota Nusantara (IKN) Nusantara adalah proyek ambisius yang melibatkan teknologi mutakhir untuk menciptakan kota masa depan Indonesia. Namun, seiring pertumbuhan teknologi, potensi ancaman siber dan risiko terhadap infrastruktur juga meningkat, berdampak pada keamanan, keandalan, dan integritas proyek ini. Serangan siber telah menjadi ancaman dominan dalam era digital saat ini, berdampak besar pada negara dan organisasi besar. Ancaman siber terhadap IKN meliputi: serangan DDoS, *ransomware*, spionase siber serta sabotase. Tantangan lain yang dihadapi IKN meliputi: ketergantungan pada teknologi asing, keterbatasan infrastruktur teknologi, kesalahan manusia serta bencana alam.

Analisis ancaman ini penting untuk keberlanjutan IKN. Strategi mitigasi termasuk pembentukan tim tanggap darurat siber, audit keamanan rutin, pelatihan kesadaran keamanan, serta perancangan infrastruktur yang tahan bencana dan redundan.Dalam mengembangkan rencana respons terintegrasi yang efektif yang mengarah pada manajemen krisis yang sukses, pemerintah harus mengikuti tiga prinsip utama yaitu membuat rencana darurat dan mendokumentasikannya dalam buku pegangan melakukan simulasi untuk meningkatkan rencana dan melatih staf, menunjuk petugas tindakan krisis untuk membuat dan melaksanakan rencana.[33]

Pemerintah harus berkolaborasi dengan sektor swasta, komunitas keamanan siber, serta negara-negara lain untuk berbagi intelijen ancaman, best practices, dan solusi. Kesuksesan pengembangan IKN tidak hanya diukur dari keindahannya atau teknologi canggih yang diterapkan, namun juga dari seberapa aman dan tahan lama kota tersebut dari ancaman siber dan kelemahan infrastruktur teknologi di masa mendatang.

d. Potensi Ancaman Siber Global terhadap Pengembangan Ibu Kota Nusantara (IKN) di Indonesia.

---

[33] Domenic Antonucci - The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities-Springer (2017), h. 283

Dalam era globalisasi dan revolusi digital, pengembangan Ibu Kota Nusantara (IKN) Indonesia berpotensi terkena ancaman siber global. Rencana membangun kota berbasis teknologi tinggi membuatnya jadi target bagi aktor siber dengan motif politik, ekonomi, atau ideologi. Ancaman utama termasuk serangan siber yang merusak, ubah, atau curi data infrastruktur penting. Contoh nyata adalah *ransomware* yang mengenkripsi data dan memaksa pemerintah membayar tebusan. Ini tak hanya rugikan finansial, juga hambat operasional IKN dan reputasi sebagai kota masa depan.Serangan ini juga cukup sulit untuk ditangkal karena perancang *virus* dan *malware* menjadi lebih canggih dalam produk yang mereka buat, industri selalu berada dalam posisi bereaksi dan berusaha mengejar ketinggalan dengan desain *malware*[34]

Pengembangan Ibu Kota Nusantara (IKN) Indonesia mengandung banyak data dan informasi strategis yang bila jatuh ke tangan yang salah, dapat merugikan keamanan, ekonomi, dan kedaulatan negara. Dalam pengembangan Ibu Kota Nusantara (IKN) di Indonesia, teknologi untuk layanan publik membawa efisiensi tetapi juga risiko ancaman siber tersendiri. Dalam pembangunan Ibu Kota Nusantara (IKN) di Indonesia, keamanan dan pertahanan sangat penting untuk menjaga kedaulatan negara. Ancaman siber global dapat mengganggu sistem-sistem ini.

Ancaman terhadap infrastruktur teknologi, data dan informasi strategis dalam pengembangan Ibu Kota Nusantara (IKN) meliputi:

1) **Serangan Terhadap Infrastruktur Kritis:** Infrastruktur seperti pasokan listrik, air, dan transportasi berbasis teknologi bisa diserang, seperti yang terjadi di Ukraina pada 2015.
2) **Serangan DDoS:** Penyerangan untuk membanjiri sistem sehingga layanan tidak berfungsi, contohnya layanan perbankan di beberapa negara.
3) ***Ransomware*:** *Malware* yang mengenkripsi data dan meminta tebusan, seperti serangan WannaCry yang melanda banyak institusi pada 2017.

[34] CRC PRess. Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber WarfareJohnson, Thomas A (2015), h, 18.

4) **Sabotase dan Espionase:** Pengambilan atau manipulasi data untuk spionase industri atau negara, seperti serangan Stuxnet pada 2010.
5) **Keamanan IoT:** Pertumbuhan IKN membawa banyak perangkat IoT dengan keamanan rendah, seperti serangan DDoS pada 2016 melalui perangkat IoT.
6) **Ancaman Internal:** Ancaman dari dalam sistem, baik disengaja maupun tidak, seperti tindakan karyawan yang mengunduh malware atau menjual data.
7) **Pencurian Data (*Data Breach*):** Aktor siber meretas jaringan untuk mencuri data penting. Contohnya, Equifax mengalami kebocoran data pada 2017 yang mengungkapkan informasi pribadi 147 juta orang.
8) **Manipulasi Data:** Selain mencuri data, aktor siber bisa merusak atau memanipulasi data, menyebabkan informasi yang salah atau menyesatkan. Stuxnet adalah kasus yang merusak dan memberikan informasi yang salah.
9) ***Phishing* dan Serangan *Man-in-the-Middle*:** Melalui manipulasi atau tipu daya, aktor siber mendapatkan akses ke informasi pribadi atau kredensial. Serangan *phishing* pada John Podesta adalah contohnya.
10) **Serangan *Cloud Computing*:** Layanan *cloud* sering digunakan untuk menyimpan data, tetapi serangan pada penyedia layanan dapat berdampak besar. Capital One mengalami kebocoran data pada 2019 akibat serangan pada konfigurasi *cloud* mereka.
11) **Serangan pada Komunikasi Militer:** Gangguan komunikasi militer seperti yang terjadi di Estonia pada 2007 dapat mengacaukan pengambilan keputusan.
12) **Kompromi Sistem Radar dan Pertahanan Udara:** Gangguan pada radar dan sistem pertahanan udara bisa mengancam deteksi ancaman.

Dalam konteks IKN, infrastruktur teknologi yang canggih dan terkoneksi menjadi dua mata pisau. Di satu sisi, teknologi ini memungkinkan efisiensi, inovasi, dan kualitas hidup yang lebih baik. Namun di sisi lain, mereka membuka peluang bagi ancaman siber yang bisa merusak, baik secara fisik maupun digital. Salah satu bentuk perkembangan teknologi adalah semakin banyaknya perangkat IOT atau *Internet of Things* dimana akan lebih banyak perangkat yang terhubung, dan skenario jenis "*wild west*" potensial di mana peretasan ke satu perangkat dapat mempermudah peretasan ke perangkat lain yang saling terhubung.[35]

Ancaman yang diketahui, seperti *phishing*, DoS, MiTM, *malware*, dan injeksi SQL, dapat ditemui menggunakan solusi keamanan lapisan atas. Namun, tantangan terbesar yang harus diatasi adalah kerentanan *zero-day* dan serangan hibrid karena kami tidak memiliki kemungkinan solusi keamanan untuk hal tersebut, termasuk *Cloud Vulnerability*, AI and *Machine Learning* dan serangan *Social Engineering*.[36]

Perlindungan data dan informasi strategis adalah esensial, mengingat pentingnya data tersebut dalam operasional dan keputusan strategis. Indonesia harus membangun kerangka kerja keamanan siber yang kokoh, termasuk *multi-layered security*, pelatihan kesadaran siber bagi pegawai dan masyarakat, serta kerjasama internasional untuk menghadapi ancaman siber global. Ada banyak standar keamanan dunia maya yang ada saat ini yang telah dikembangkan oleh berbagai badan yang menangani kebutuhan khusus, dan daftarnya terus bertambah, tetapi penting bagi pemerintah untuk mengidentifikasi mana yang memberikan nilai paling besar bagi pemerintah. Lebih penting lagi, menyelaraskan dengan standar yang “benar” membantu memfasilitasi pembagian dan transparansi pada serangan dunia maya terbaru di dalam dan di luar pemerintahan.[37]

---

[35] Domenic Antonucci - The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities-Springer (2017), h. 53

[36] Nitul Dutta, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, Emil Pricop - Cyber Security_ Issues and Current Trends (Studies in Computational Intelligence, 995)-Springer (2021), h. 8

[37] Domenic Antonucci - The Cyber Risk Handbook. Creating and Measuring Effective

Kerjasama dan teknologi keamanan yang canggih sangat penting dalam mengatasi ancaman ini. Bertahun-tahun sejak serangan 2007 di Estonia, telah terjadi peningkatan luar biasa dalam peretasan negara dan spionase terbuka. Insiden dan serangan telah meningkat hingga tingkat yang mengkhawatirkan. Para pemimpin utama serangan siber ini adalah AS, Cina, Rusia, Iran, dan Israel. Motif masing-masing bervariasi, namun tujuan keseluruhannya adalah untuk mendapatkan keunggulan industri, keuangan, dan militer[38]

Ancaman-ancaman tersebut menunjukkan betapa pentingnya mengimplementasikan tindakan keamanan yang kuat dalam setiap aspek layanan publik dan pelayanan masyarakat di IKN. Pemerintah perlu bekerja sama dengan pakar keamanan siber, industri, dan masyarakat sipil untuk memastikan bahwa infrastruktur kritis dan sistem layanan tetap aman dan handal dalam menghadapi potensi ancaman siber global.

14. Dampak Dari Potensi Ancaman Keamanan Siber Dan Infrastruktur Teknologi Terhadap IKN.

a. Analisis tentang dampak dari potensi ancaman keamanan siber terhadap perkembangan dan keberlangsungan IKN sebagai pusat pemerintahan dan ibu kota negara.

Dalam konteks pembangunan Ibu Kota Nusantara (IKN) Nusantara sebagai pusat pemerintahan dan lambang kedaulatan negara, ancaman keamanan siber memainkan peran krusial. Teori Kedaulatan Siber mengilustrasikan cara menjaga kedaulatan digital suatu negara di era siber yang penuh ancaman. Kedaulatan ini meluas ke ranah siber, di mana integritas data dan infrastruktur digital menjadi prioritas utama. Bagi IKN Nusantara, yang mengadopsi teknologi modern, keamanan siber bukan hanya perlindungan data, tetapi juga kelangsungan pemerintahan dan layanan sosial-ekonomi.

Cybersecurity Capabilities-Springer (2017), h. 81

[38] John A. Adams Jr. - Cyber Blackout_ When the Lights Go Out -- Nation at Risk-FriesenPress (2015), h. 43

Dengan memahami Teori Kedaulatan Siber, Indonesia perlu memastikan otonomi dan keamanan siber nasional, termasuk di IKN. Perlindungan infrastruktur kritis, kelangsungan layanan pemerintah, serta integritas data menjadi penting. Kedaulatan siber bukan hanya soal pertahanan, tetapi juga tentang memastikan pemerintahan memiliki kendali penuh atas keputusan terkait ruang siber, menegaskan kemandirian dari intervensi asing.

Dalam pandangan Teori Kedaulatan Siber, ancaman siber dapat menyebabkan dampak negatif yang merata, mengganggu berbagai aspek kehidupan seperti ekonomi, layanan publik, infrastruktur penting, dan stabilitas nasional. Kedaulatan siber menegaskan bahwa setiap negara harus menguasai data dan informasi di wilayah sibernya, dan gangguan terhadap ini dapat langsung mengganggu fungsi negara dan kesejahteraan warga. Dari segi ekonomi, serangan pada sektor finansial bisa berujung pada kerugian besar, termasuk kehilangan kepercayaan investor dan pelanggan, serta hentinya operasi bisnis.

Layanan publik juga terancam oleh ancaman siber. Misalnya, serangan terhadap pelayanan kesehatan bisa menghambat akses pasien atau pada sistem pendidikan yang mengganggu proses belajar. Bahkan, serangan pada pasokan air atau listrik bisa memicu krisis kemanusiaan. Infrastruktur penting seperti transportasi dan komunikasi adalah tiang utama negara modern. Serangan siber pada infrastruktur ini bisa berhenti kan operasi sehari-hari, menyebabkan kerugian ekonomi dan potensi bencana.

Dalam stabilitas nasional, ancaman siber bisa dipakai untuk mempengaruhi opini publik, memicu instabilitas politik, atau bahkan konflik militer. Propaganda di media sosial bisa menciptakan ketegangan sosial atau konflik internal. Teori Kedaulatan Siber menyoroti bahwa keamanan siber bukan hanya urusan teknis, melainkan juga soal kedaulatan. Setiap negara perlu mengendalikan wilayah sibernya, dan pelanggaran terhadap ini adalah ancaman bagi kelangsungan dan stabilitas negara.

b. Dampak Ancaman Keamanan Siber.

Ancaman keamanan siber di Ibu Kota Negara Nusantara (IKN) memiliki potensi konsekuensi serius bagi pemerintahan, ekonomi, dan masyarakat. Ancaman keamanan siber di Ibu Kota Negara Nusantara (IKN) terkait gangguan pada layanan publik dapat memiliki dampak yang merugikan, termasuk gangguan fungsi pemerintahan dan kerugian ekonomi. Era digital saat ini menjadikan data dan informasi sangat penting dalam pengambilan keputusan pemerintahan dan ekonomi. Ibu Kota Negara Nusantara (IKN) sebagai pusat pemerintahan Indonesia memiliki tanggung jawab untuk melindungi data dan informasi yang strategis dan vital. Kepercayaan publik adalah faktor penting dalam fungsi pemerintahan. Dalam era digital yang maju, tuntutan masyarakat terhadap perlindungan dan pengelolaan data juga semakin tinggi. Reputasi adalah aset yang sangat berharga bagi pemerintah dan institusi. Ancaman keamanan siber yang tidak ditangani dengan baik dapat merusak reputasi, terutama jika data sensitif terpapar atau disalahgunakan. Desinformasi dan propaganda di era digital telah menjadi salah satu instrumen yang paling efektif untuk menggoyang stabilitas politik, sosial, dan ekonomi suatu negara. Dalam konteks Ibu Kota Negara Nusantara (IKN), sebagai pusat kegiatan pemerintahan dan administrasi negara, dampak dari desinformasi dan propaganda yang diperkuat oleh ancaman keamanan siber bisa sangat merugikan.

Beberapa dampak yang dapat ditimbulkan oleh serangan siber antara lain :

1) **Energi:** Sistem listrik dan pembangkit listrik menjadi target utama ancaman siber. Contohnya, serangan siber pada Ukraina tahun 2015 yang mengakibatkan pemadaman listrik masif.
2) **Transportasi:** Teknologi tinggi dalam sistem transportasi, seperti lalu lintas udara dan kereta, dapat diserang. Contoh, serangan siber pada sistem kontrol kereta bisa menyebabkan kecelakaan.
3) **Komunikasi:** Jaringan telekomunikasi dan internet krusial. Gangguan bisa mengisolasi IKN dari dunia. Serangan DDoS bisa melumpuhkan jaringan.

4) **Perbankan:** Serangan siber terhadap sistem perbankan bisa menghambat transaksi dan menyebabkan kerugian finansial besar.
5) **Layanan Kesehatan dan Air Bersih:** Sistem kesehatan dan distribusi air rentan terhadap serangan. Kontaminasi air bersih atau gangguan pada rumah sakit bisa mengakibatkan krisis kesehatan.
6) ***E-Government*:** Layanan pemerintah seperti pembayaran pajak bisa lumpuh jika portal e-government diserang, mengakibatkan penundaan transaksi dan kerugian waktu bagi masyarakat.
7) **Sistem Pendidikan:** Serangan terhadap sistem manajemen informasi akademik dapat menghambat belajar mengajar.
8) **Layanan Transportasi Publik:** Sistem tiketing transportasi yang digital bisa terganggu, mengakibatkan masalah bagi penumpang.
9) **Layanan Keuangan Publik:** Serangan yang mengganggu sistem manajemen dana publik bisa merusak kepercayaan masyarakat.
10) **Kerusakan Reputasi:** Kehilangan data sensitif, terutama data pribadi warga, dapat merusak reputasi pemerintah dan mengurangi kepercayaan masyarakat pada inisiatif digital pemerintah.
11) **Kerugian Ekonomi:** Kehilangan data ekonomi dapat menghambat kegiatan ekonomi dan menyebabkan kerugian finansial.
12) **Hambatan Kebijakan:** Kehilangan data penting bisa mengganggu proses pengambilan keputusan pemerintah dan kebijakan yang didasarkan pada data akurat.
13) **Menurunnya Partisipasi Masyarakat:** Jika data pribadi tidak aman, masyarakat ragu untuk ikut program pemerintah digital seperti sensus atau pelaporan online, menghambat partisipasi yang diperlukan.
14) **Keraguan terhadap Teknologi:** Kepercayaan hilang bisa menghambat adopsi teknologi baru di IKN, menghentikan perkembangan dan penerapan teknologi yang potensial.
15) **Kolaborasi Lembaga Terhambat:** Jika data terancam, kolaborasi antar lembaga pemerintah sulit, mengganggu penggunaan data lintas lembaga untuk kebijakan publik.

16) **Kehilangan Kepercayaan Masyarakat:** Keamanan siber yang kurang bisa mengurangi kepercayaan publik pada kompetensi dan tanggung jawab pemerintah atau institusi terkait.
17) **Skepsis terhadap Inisiatif Digital:** Gagal melindungi data bisa membuat masyarakat ragu-ragu terhadap inisiatif digital lainnya, menghambat adopsi dan partisipasi.
18) **Kerugian Kerjasama Internasional:** Reputasi yang tercoreng dapat menghambat kerjasama internasional, terutama dalam hal pertukaran intelijen atau keamanan siber.
19) **Gangguan Bisnis:** Serangan siber ganggu operasional perusahaan di IKN, besar maupun kecil, dengan risiko kerugian data, kerusakan perangkat, atau akses terhenti.
20) **Kerugian Investasi:** Lemahnya keamanan siber IKN meragukan investor, menghambat aliran modal dan proyek infrastruktur.
21) **Biaya Pemulihan:** Setelah serangan, biaya tinggi pemulihan sistem, perangkat, dan data, termasuk konsultasi, pelatihan, dan perangkat canggih.
22) **Kehilangan Pendapatan:** Bisnis online terganggu, menurunkan pendapatan.
23) **Polarisasi Masyarakat:** Desinformasi yang disebarkan secara luas dapat memecah belah masyarakat, menciptakan kesenjangan pandangan antara kelompok-kelompok tertentu dan bahkan memicu konflik.
24) **Kehilangan Kepercayaan Publik:** Propaganda dan desinformasi dapat menyebabkan masyarakat kehilangan kepercayaan terhadap institusi pemerintah, media, dan organisasi lainnya.
25) **Manipulasi Opini Publik:** Dengan teknologi dan metode tertentu, aktor siber dapat memanipulasi persepsi publik mengenai isu-isu tertentu, merusak reputasi individu atau organisasi, atau bahkan mempengaruhi hasil pemilihan umum.
26) **Gangguan Kebijakan Publik:** Informasi yang salah atau disengaja dapat menghambat pembuatan kebijakan yang efektif dan berdampak pada kesejahteraan masyarakat.

c. Dampak Ancaman Infrastruktur Teknologi yang Tidak Baik.

Dalam era digital, teknologi membawa peluang dan tantangan, terutama dalam keamanan siber. Teori Kedaulatan Siber menunjukkan pentingnya negara, termasuk Indonesia, mengelola ruang siber seperti wilayah fisiknya. IKN sebagai simbol teknologi maju Indonesia punya peran penting dalam kedaulatan siber, namun juga hadapi ancaman yang menggoyahkan fondasi ini. Serangan siber bisa ganggu layanan esensial seperti kesehatan dan pendidikan, serta risiko kehilangan data sensitif pemerintah yang mengancam keamanan nasional dan dimanfaatkan pihak asing. Hilangnya kekayaan intelektual dan kerusakan pada sistem informasi adalah biaya yang menimbulkan banyak peringatan baik bagi jajaran korporat perusahaan besar maupun bagi para pemimpin pemerintahan di seluruh dunia.[39] Dalam ekonomi yang bergantung pada teknologi, serangan siber bisa hambat operasi ekonomi, rugikan finansial, dan rusak kepercayaan investor. Bahkan, retas sistem keamanan nasional bisa mengancam keamanan fisik negara. Kepercayaan publik tergerus jika pemerintah tak mampu lindungi data dan infrastruktur kritikal. Melalui Teori Kedaulatan Siber, terlihat perlunya melindungi infrastruktur teknologi IKN. Beberapa dampak ancaman infrastruktur teknologi yang tidak baik antara lain adalah :

1) Hambatan Pembangunan.

Risiko yang timbul dari rentannya infrastruktur teknologi terhadap serangan siber memiliki potensi menimbulkan kerugian finansial yang cukup besar. Selain biaya pemulihan teknis, terdapat pula potensi kerugian dalam transaksi dan operasional bisnis akibat gangguan yang terjadi, dampak ini secara langsung dapat mengganggu anggaran pendapatan dan belanja negara (APBN) serta investasi di IKN.

Tidak mampunya melindungi data strategis menghambat proses pengambilan keputusan pemerintah. Informasi yang dicuri

[39] CRC PRess. Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber WarfareJohnson, Thomas A (2015), h, 293.

atau dirusak bisa dimanfaatkan untuk manipulasi atau propaganda, menghambat inovasi karena para pemangku kepentingan akan menjadi lebih hati-hati dalam mengadopsi teknologi baru. Efisiensi operasional pun terganggu, infrastruktur teknologi yang tidak memadai mengakibatkan kinerja sistem lambat, tak responsif, bahkan sering mengalami downtime, yang berdampak pada pelayanan publik dan kebutuhan akses masyarakat.

Tidak hanya itu, reputasi IKN sebagai ibu kota modern dan maju dapat tercoreng. Kepercayaan investor asing dan domestik mungkin menurun, mengingat mereka mencari lingkungan bisnis yang stabil dan aman dalam hal teknologi. Jika IKN tidak dapat menjamin keamanan siber dan infrastruktur teknologi, investor bisa mengambil keputusan serius terkait investasinya. Jangka panjangnya, ancaman siber berkelanjutan terhadap infrastruktur teknologi yang belum siap bisa menghambat IKN dalam meraih visi dan misi sebagai pusat inovasi dan efisiensi di Indonesia.

2) **Ketergantungan Asing.**

Dalam pembangunan IKN, menjaga kedaulatan teknologi menjadi esensial agar Indonesia dapat beroperasi mandiri dan efisien tanpa bergantung terlalu besar pada pihak eksternal. Ancaman terhadap infrastruktur teknologi, seperti serangan siber, bisa mengganggu sistem dan menghambat perkembangan teknologi dalam negeri. Namun, saat mencari solusi cepat, seperti penggunaan teknologi asing, risiko tertentu perlu dipertimbangkan.

Pertama, ketergantungan pada teknologi luar dapat membuat Indonesia rentan terhadap geopolitik. Pasokan dan dukungan teknis dapat terhambat oleh kebijakan politik, sanksi, atau pertimbangan lain dari negara penyedia teknologi. Kedua, ketergantungan eksternal bisa menghambat inovasi lokal dan perkembangan industri teknologi dalam negeri. Terakhir, dari segi data dan keamanan informasi, bergantung pada teknologi luar bisa menghadirkan risiko keamanan dan privasi. Data penting negara

bisa berada di tangan pihak ketiga dengan regulasi dan standar yang berbeda dalam hal keamanan dan perlindungan data.

3) Kualitas Layanan Publik Berkurang.

Ibu Kota Negara Nusantara (IKN) diharapkan memiliki standar layanan publik yang tinggi untuk meningkatkan kualitas hidup masyarakatnya. Namun, ancaman terhadap infrastruktur teknologi, terutama dalam bentuk serangan siber, dapat menghambat layanan publik. Misalnya, gangguan pada sistem transportasi umum yang bergantung pada teknologi canggih dapat mengganggu jadwal dan rute, bahkan menghentikan layanan secara keseluruhan, berdampak pada ketidakpastian dan kerugian ekonomi bagi masyarakat.

Sistem kesehatan juga dapat terdampak, ketika gangguan pada informasi rumah sakit mengganggu akses pasien dan dokter terhadap data medis, bahkan bisa mengganggu operasi medis. Pendidikan yang semakin mengandalkan teknologi pun bisa terganggu oleh gangguan platform *e-learning*, berpotensi menghambat proses belajar-mengajar. Layanan keuangan dan perbankan juga terancam oleh ketidakstabilan infrastruktur teknologi, mengakibatkan transaksi bermasalah, keterlambatan, hingga kehilangan data keuangan penting.

Semua contoh ini menggarisbawahi pentingnya infrastruktur teknologi yang stabil bagi kualitas layanan publik. Gangguan, baik akibat serangan siber maupun faktor teknis lainnya, berpotensi merugikan masyarakat.

4) Ketidakstabilan Ekonomi.

Investor, baik domestik maupun internasional, sangat mempertimbangkan kualitas infrastruktur teknologi sebelum berinvestasi. Infrastruktur teknologi yang kurang memadai dapat meningkatkan risiko investasi, mengurangi efisiensi operasional, dan mempengaruhi keputusan investor. Industri seperti teknologi informasi, *fintech*, dan *e-commerce* memerlukan konektivitas

internet yang handal. Gangguan berulang dapat merugikan perusahaan dan mencoreng reputasi.

Operasional bisnis, terutama di sektor teknologi, logistik, dan manufaktur, sangat bergantung pada infrastruktur teknologi yang stabil. Gangguan sistem bisa menghentikan produksi, mengganggu rantai pasokan, dan merusak kepercayaan pelanggan. Misalnya, perusahaan manufaktur dengan otomasi membutuhkan jaringan stabil; ketidakstabilan dapat berujung pada kerugian produksi.

Infrastruktur teknologi yang tidak stabil dapat menyebabkan ketidakpastian ekonomi lebih luas, menghambat pertumbuhan GDP, dan menurunkan lapangan pekerjaan. Sektor pariwisata yang bergantung pada teknologi untuk pemesanan dan promosi dapat terdampak jika infrastruktur tidak mendukung.

5) Konektivitas Nasional Terhambat.

Dalam era globalisasi dan digitalisasi, konektivitas menjadi kunci dalam membangun dan menjaga hubungan antar wilayah di suatu negara. Infrastruktur teknologi yang kuat memungkinkan Ibu Kota Negara Nusantara (IKN) tetap terhubung dengan seluruh wilayah Indonesia, memfasilitasi komunikasi, distribusi informasi, inovasi, dan kebijakan secara cepat dan efisien. Namun, jika infrastruktur teknologi di IKN tidak memadai atau rentan terhadap gangguan, dampaknya bisa sangat merugikan.

Pertama, koordinasi antara pemerintah pusat di IKN dan pemerintah daerah di seluruh Indonesia dapat terhambat, terutama dalam situasi darurat atau bencana. Keterbatasan komunikasi dapat menghambat pengambilan keputusan dan distribusi bantuan. Kedua, dari segi ekonomi, IKN memiliki hubungan komersial dengan daerah-daerah lain. Infrastruktur teknologi yang buruk dapat mengganggu proses bisnis, termasuk pemesanan, pelacakan pengiriman, dan transaksi keuangan. Ini berdampak pada kerugian finansial dan pertumbuhan ekonomi regional dan nasional. Ketiga, terhambatnya konektivitas bisa mempengaruhi integrasi sosial dan budaya. Pertukaran informasi dan ide antar

wilayah dapat terbatas, memengaruhi kesadaran masyarakat terhadap isu-isu nasional.

6) Pembangunan Ekonomi Digital Terganggu.

Ibu Kota Negara Nusantara (IKN), yang diharapkan menjadi pusat administrasi dan inovasi, memiliki potensi besar untuk mendorong ekonomi digital Indonesia. Namun, kerentanannya terhadap ancaman teknologi dapat merusak pertumbuhan ekonomi digital di wilayah tersebut. Dalam era digital, infrastruktur teknologi adalah pusat kehidupan ekonomi, dan gangguan dalam infrastruktur ini dapat mempengaruhi berbagai sektor.

Gangguan pada infrastruktur juga memperlambat proses digitalisasi layanan publik yang sedang ditingkatkan. Masyarakat menjadi kurang percaya terhadap upaya pemerintah dalam meningkatkan layanan melalui digitalisasi. Lebih jauh, ketidakstabilan infrastruktur teknologi juga menghambat pendidikan dan pelatihan dalam keahlian digital yang esensial bagi pertumbuhan ekonomi berbasis teknologi di IKN.

d. Dampak Ancaman Siber Serta Lemahnya Infrastruktur Teknologi Terhadap Perkembangan Dan Keberlangsungan Ibu Kota Negara Nusantara.

Pembangunan ibu kota modern tak hanya melibatkan aspek fisik, melainkan juga integrasi teknologi dan informasi dalam segala aspek kehidupan kota. Pada era digital ini, teknologi menjadi motor pembangunan yang mengoptimalkan layanan publik, mobilitas, komunikasi, dan pertumbuhan ekonomi. Ancaman serius terhadap keamanan siber dapat mengakibatkan pencurian, penyalahgunaan, atau kerusakan data pemerintahan, data pribadi warga, informasi infrastruktur krusial, dan informasi strategis lainnya. Selain dampak materiil, ini merusak kepercayaan publik, bahkan mengancam stabilitas dan keamanan nasional.

Kekurangan infrastruktur teknologi berdampak pada ketidakmampuan IKN beradaptasi dengan perubahan zaman,

memperlambat inovasi, merosotkan efisiensi, dan menambah biaya operasional. Contohnya, gangguan sistem transportasi terintegrasi, proyek terhenti akibat data yang tak tersedia atau komunikasi terputus, dan layanan publik terhambat. Jika dibiarkan, ancaman-ancaman ini memperlambat perkembangan IKN, merosotkan daya saingnya, dan merugikan bangsa. Investasi dalam IKN mungkin tak memberikan hasil seperti yang diharapkan. Parahnya lagi, IKN yang seharusnya menjadi simbol kemajuan bisa jadi justru menjadi contoh kegagalan integrasi fisik dan digital.

Beberapa dampak ancaman siber serta lemahnya infrastruktur teknologi terhadap perkembangan dan keberlangsungan Ibu Kota Negara Nusantara dan Indonesia antara lain adalah:

1) **Ketidakstabilan Sosial dan Politik.**

Kehilangan kepercayaan masyarakat pada pemerintah adalah dampak serius lainnya. Bocornya data atau gangguan layanan publik karena ancaman siber bisa mengikis kepercayaan masyarakat, berpotensi memicu protes atau ketidakstabilan politik. Ancaman siber juga dapat dimanfaatkan untuk menyebarkan desinformasi atau merusak reputasi pemerintah, bahkan menggoyang kepercayaan pada proses demokrasi seperti pemilihan umum. Ini dapat merusak iklim politik, mengancam demokrasi, dan memicu polarisasi masyarakat.

2) **Penurunan Daya Saing Internasional.**

Dalam aspek perdagangan, kelemahan infrastruktur teknologi dapat menghambat kemampuan Indonesia untuk berpartisipasi dalam perdagangan digital, yang kini menjadi tren dominan di dunia. Ancaman serangan siber terhadap sektor perdagangan bisa mengganggu alur barang dan jasa, merusak rantai pasokan, dan akhirnya merusak citra Indonesia sebagai mitra dagang yang dapat diandalkan. Di bidang investasi, ketidakpastian dalam hal keamanan siber mungkin membuat investor asing enggan untuk mengalokasikan modal mereka di Indonesia. Investor memerlukan

jaminan bahwa aset dan data mereka akan aman dari risiko serangan siber.

Dalam konteks diplomasi, kegagalan dalam menghadapi ancaman siber dapat mempengaruhi hubungan bilateral dengan negara-negara lain. Negara-negara yang telah membangun ketahanan siber yang kuat mungkin ragu untuk berbagi informasi atau teknologi dengan Indonesia, khawatir akan risiko kebocoran atau penyalahgunaan data.

3) **Ancaman Integritas Nasional.**

Integritas nasional adalah fondasi utama bagi keberlangsungan sebuah negara. Kedaulatan, keutuhan wilayah, dan kesejahteraan rakyat bergantung pada kemampuan negara menjaga integritasnya. Di era digital seperti sekarang, ancaman terhadap integritas nasional tidak lagi terbatas pada bentuk konvensional, melainkan juga melalui serangan siber dan manipulasi teknologi. Sebagai pusat pemerintahan dan lambang kemajuan Indonesia di masa depan, Ibu Kota Negara Nusantara (IKN) memiliki tanggung jawab besar dalam menjaga integritas ini.

15. Konsep pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi serta Upaya Pencegahan dan Mitigasi Ancaman Siber Global

Sesuai dengan metodologi PESTL serta SWOT yang akan dipergunakan pada penelitian ini, ~~maka~~ perumusan konsep sistem keamanan siber dan infrastruktur teknologi Ibu Kota Nusantara yang kokoh dan terintegrasi akan didasarkan~~bertumpu~~ pada upaya merumuskan alternatif kebijakan dalam~~pada~~ berbagai kondisi. PESTL serta SWOT bukanlah~~bukan suatu~~ metode untuk meramalkan masa depan, ~~akan~~ tetapi bertujuan untuk mempersiapkan rencana aksi/mitigasi melalui kerangka analisis multidimensi.

Dari uraian peraturan perundang-undangan, data dan fakta, teori, dan lingkungan strategis, serta kondisi sistem keamanan siber di wilayah Ibu Kota Nusantara, maka dapat diidentifikasi~~diidentifikasikan~~ elemen PESTL serta SWOT sebagai berikut:

a. **Faktor Politik**, Dalam konteks perencanaan PESTL untuk keamaman siber dan infrastruktur teknologi, Faktor Politik memegang peranan yang cukup penting karena banyak sekali factor politik terutama factor dari luar yang akan dapat mempengaruhi proses pengambilan keputusan, seperti aspek geopolitik hubungan negara dan dinamika global mungkin memicu serangan siber akibat ketegangan antarnegara yang dapat menimbulkan dampak risiko serangan siber dari negara lain, risiko persaingan teknologi antar negara serta pisiko peningkatan spionase; ketidakmampuan dalam menjaga kepatuhan terhadap peraturan, perubahan regulasi pemerintah terhadap data digital serta ada tren kerja sama internasional dalam menangani isu keamanan siber juga menjadi factor politik yang perlu diperhatikan.

b. **Faktor Ekonomi.** Dalam perencanaan menggunanan metode PESTL untuk keamanan siber dan infrastruktur teknologi, penting untuk mempertimbangkan Faktor Ekonomi karena faktor-faktor ini merupakan faktor penentu kinerja perekonomian yang berdampak langsung pada pengambilan keputusan dan memiliki dampak jangka panjang. Faktor-faktor ekononi yang menjadi pertimbangan yaitu IKN merupakan kawasan baru yang dirancang untuk menjadi kawasan ekonomi terpadu dan berkelanjutan, Pemindahan IKN juga berpotensi untuk mempercepat pertumbuhan ekonomi di Kawasan Indonesia timur, akan tetapi serangan siber yang terjadi juga rentan mengganggu stabilitas ekonomi.

c. **Faktor Sosial.** Faktor sosial ini meneliti lingkungan sosial pasar, dan mengukur faktor-faktor penentu seperti tren budaya, demografi, analisis populasi, dll. Dalam metode PESTL untuk keamanan siber dan infrastruktur teknologi, beberapa factor sosial yang dapat dijadikan bahan pertimbangan adalah perubahan perilaku pengguna dalam menggunakan fasilitas internet serta peningkatan kesadaran masyarakat tentang keamanan siber, namun juga ada factor social yang menghambat yaitu pemangku kepentingan yang beragam juga menambah kompleksitas, termasuk pemerintah, sektor swasta, lembaga penelitian, dan masyarakat umum, yang memiliki peran dan kepentingan yang berbeda, serta Kekurangan tenaga ahli keamanan siber adalah

risiko yang dapat menghambat pemantauan dan perbaikan keamanan, kegagalan mendeteksi dan merespons serangan siber tepat waktu yang berdampak pada kerugian finansial, reputasi, dan data sensitif.

d. **Faktor Teknologi.** Faktor ini memegang peranan paling penting dalam malakukan Analisa PESTL dalam taskap yang membahas masalah keamanan siber dan infrastruktur teknologi terkait dengan pemindahan IKN. Beberapa factor teknologi yang harus dijadikan perhatian adalah kemajuan teknologi seperti quantum computing dan kecerdasan buatan yang membawa inovasi dan risiko serangan siber baru, transisi ke komputasi awan menghadirkan efisiensi namun juga tantangan keamanan, serangan siber meningkat baik dalam volume maupun kompleksitas karena digitalisasi yang berkembang, teknologi *emergent* seperti IoT, 5G, dan AI yang memperluas bidang keamanan siber, besar dan kompleks nya jaringan infrastruktur teknologi yang harus dilindungi, risiko kegagalan teknologi juga muncul, seperti kerusakan pusat data yang merugikan operasional.

e. **Faktor Lingkungan.** Faktor Lingkungan meliputi segala sesuatu yang mempengaruhi atau ditentukan oleh lingkungan sekitar. Adapun beberapa Faktor Lingkungan yang mempengarui pengambilan keputusan adalah IKN dirancang sebagai kota hijau dengan konsep ramah lingkungan yang memperhatikan aspek keberlanjutan dalam pembangunannya, manfaat lingkungan ini juga diharapkan dapat meningkatkan kualitas hidup masyarakat dan memperkuat ketahanan lingkungan di Indonesia

Dari analisa faktor-faktor dalam PESTL tersebut kemudian kita pilah-pilah kembali faktor-faktor tersebut menggunakan metode SWOT untuk mendapatkan faktor-faktor Kekuatan (*Strength*), Kelemahan (*Weakness*), Peluang (*Opportunity*) serta Ancaman (*Threats*). Adapaun faktor-faktor tersebut adalah :

a. **Kekuatan (*Strength*)**. Factor factor yang dapat dianggap sebagai sebuah kekuatan terkait keamanan siber dan infrastruktur teknologi antara lain Perubahan regulasi pemerintah terhadap data digital, perubahan perilaku pengguna ingternet, Masyarakat yang semakin

sadar akan keamanan siber, adanya Kerjasama internasional, Kawasan IKN sebagai Kawasan ekonomi terpadu serta IKN dirancang sebagai kota hijau.

b. **Kelemahan (*Weakness*).** Sedangkan Faktor yang dianggap sebagai kelemahan dalam rangka pemindahan IKN antara lain aspek geopolitik, ketidakmampuan dalam menjaga kepatuhan serta besar dan kompleksnya jaringan dan infrastruktur di IKN

c. **Peluang (Opportunity).** Beberapa factor yang bisa diangap sebagai peluang adalah pemindahan IKN dapat mempercepat pertumbuhan ekononomi di Indonesia timur, perubahan teknologi yang cepat, transisi ke komputasi awan serta pemindahan IKN yang dapat meningkatnya kualitas hidup dan memperkuat ketahanan lingkungan.

d. **Ancaman (*Threats*).** Faktor perubahan teknologi dan transisi ke komputasi awan selain bisa menjadi peluang namun di satu sisi juga akan menjadi sebuah ancaman siber baru. Selain itu juga ada factor ancaman seperti serangan siber yang terjadi dapat menggangu stabilitas ekonomi, banyaknya pemangku kepentingan yang terlibat, kekurangan tenaga ahli dalam bidang keamanan siber, peningkatan jumlah dan komplesitas serangan siber, timbulnya teknologi emergen yang menambah luas jaringan, kegagalan dalam mendeteksi dan merespon serta potensi kegagalan teknologi yang dipergunakan.

Pembangunan sistem keamanan siber dan infrastruktur teknologi yang tangguh menjadi kebutuhan mendesak di era digitalisasi saat ini. Dalam menghadapi tantangan yang kompleks, mengadopsi Teori Strategi Keamanan Siber Nasional bersama dengan Konsep Kewaspadaan Nasional merupakan pendekatan holistik yang dapat memastikan ketahanan siber Indonesia, termasuk Ibu Kota Negara Nusantara (IKN).

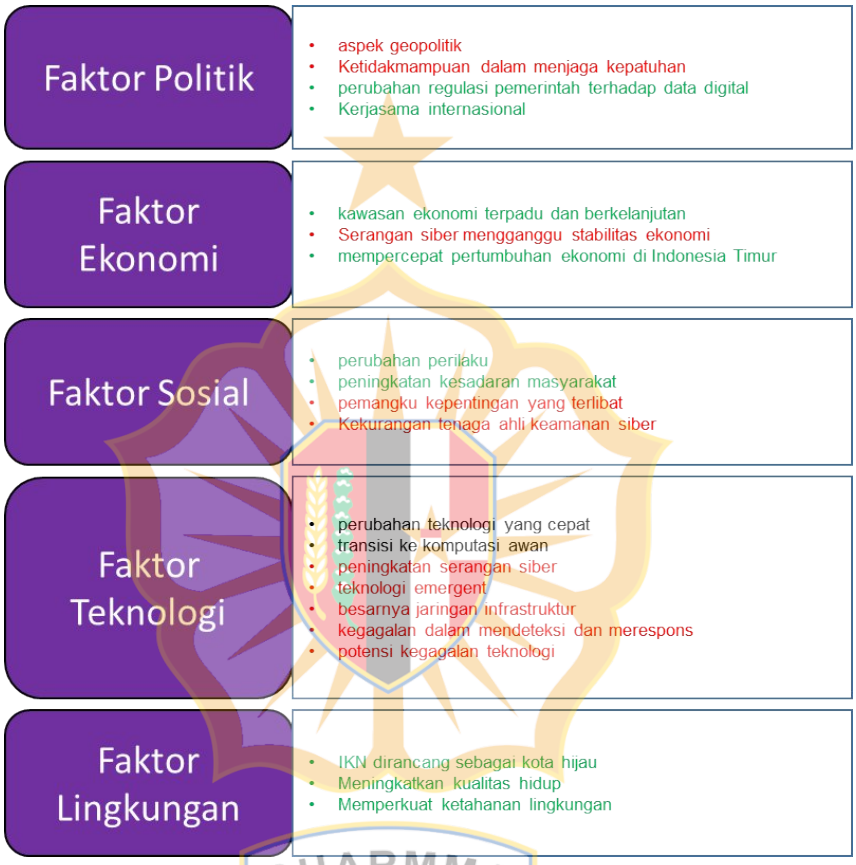
Teori Strategi Keamanan Siber Nasional menekankan pada pembentukan infrastruktur siber yang kokoh, kolaborasi lintas sektor, dan fleksibilitas dalam menghadapi ancaman yang terus berkembang. Untuk IKN, ini bisa berarti memperkuat pusat data nasional, merumuskan regulasi yang mendukung keamanan siber, serta menjalin kerja sama internasional dalam pertukaran informasi mengenai ancaman siber dan praktik terbaik. Peran aktif

sektor swasta dan partisipasi masyarakat penting untuk membentuk ekosistem siber yang aman, di mana setiap entitas memahami tanggung jawabnya dalam menjaga keamanan informasi.

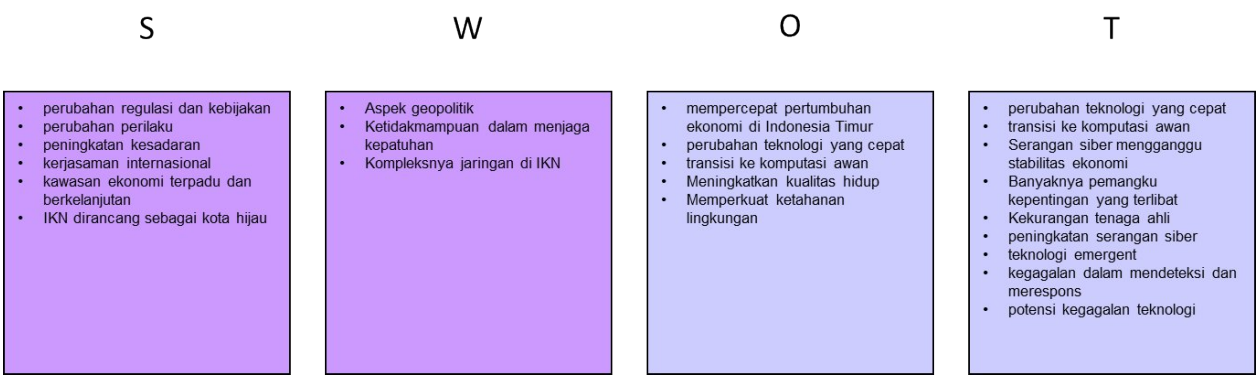
Sementara itu, Konsep Kewaspadaan Nasional menggarisbawahi perlunya kesadaran dan kesiapsiagaan masyarakat serta pemerintah. Pendidikan dan pelatihan keamanan siber perlu menjadi prioritas utama, mencakup semua lapisan masyarakat agar mereka mampu mengenali, mencegah, dan melaporkan potensi ancaman siber. Dengan demikian, langkah-langkah ini dapat memberikan dasar yang kuat dalam membangun sistem keamanan siber yang tahan lama dan adaptif di tengah perubahan dinamika teknologi dan ancaman. Sehingga kita bisa memastikan bahwa setiap anggota organisasi mengetahui risiko keamanan dunia maya dan peran yang dapat mereka mainkan dalam mendeteksinya. Ubah mereka menjadi firewall manusia. Setiap anggota organisasi harus mengetahui cara melaporkan jika mereka melihat sesuatu yang tidak normal di komputer atau perangkat seluler mereka. Pastikan detail kontak untuk melakukannya mudah diakses.[40] Selain itu, harus ada mekanisme deteksi dini yang mampu memberikan peringatan secepat mungkin tentang ancaman potensial, memungkinkan respons yang cepat dan efektif.

Berangkat dari identifikasi lima elemen PESTL yang kemudian ditransisikan menjadi analisa SWOT –serta analisis berdasarkan kerangka teoretis, berikut ini merupakanmaka digambarkan ilustrasi Analisis PESTL& SWOT dalam merumuskan konsep pembangunan sistem keamanan siber dan infrastruktur teknologi Ibu Kota Nusantara yang kokoh dan terintegrasi sebagai berikut:

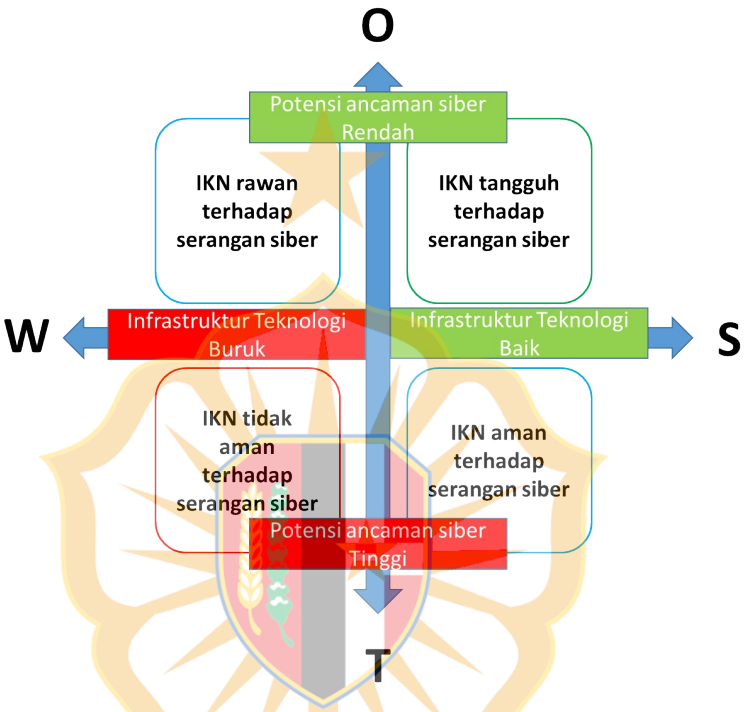
[40] Centre For Cyber Security Belgium - Cyber Security Incident Management Guide-Centre For Cyber Security Belgium (2015), h. 20



Gambar 3.7. Analisis PESTL *(*Politik, Ekonomi, Sosial, Teknologi & Lingkungan*).*



Gambar 3.8. Analisis SWOT *(Strength, Weakness, Opportunity, Threats)*



Gambar 3.9. Kuadran SWOT *(Strength, Weakness, Opportunity, Threats)*

Berdasarkan ilustrasi PESTL dan SWOT di atas~~diatas~~, dengan mengacu pada peraturan perundang-undangan, analisis terhadap data dan fakta, lingkungan strategis, tantangan, dan ancaman~~, serta permasalahan~~ yang dihadapi, maka konsep pembangunan sistem keamanan siber dan infrastruktur teknologi di IKN harus bisa dibangun dengan baik. Agar konsep pembangunan sistem keamanan siber dan infrastruktur teknologi Ibu Kota Nusantara yang terintegrasi tersebut dapat terwujud, maka diperlukan~~perlu~~ memperhatikan langkah-langkah strategis dan komprehensif sebagai berikut.

a. Tinjauan Keamanan Siber dan Infrastruktur Teknologi di IKN.

Evaluasi kondisi keamanan siber dan infrastruktur teknologi di Ibu Kota Negara Nusantara (IKN) adalah langkah kritis untuk memahami

kesiapan kita dalam menghadapi ancaman digital di era modern. Investasi dalam teknologi modern tidak secara otomatis menjamin keamanan yang tinggi, karena perkembangan teknologi juga memicu perkembangan metode serangan.

Analisis kerentanan mengungkap beberapa potensi celah. Pertama, ketergantungan pada *vendor* teknologi asing bisa membawa risiko terhadap kerentanan atau backdoor yang tidak terdeteksi. Kedua, kekurangan sumber daya manusia terlatih di bidang keamanan siber dapat menjadi titik lemah, di mana teknologi canggih bisa dieksploitasi tanpa pengetahuan yang memadai. Ketiga, integrasi antara sistem lama dan baru dapat menciptakan ketidakcocokan dan menjadi pintu masuk bagi penyerang.

Kesiapan IKN dalam menghadapi ancaman siber global bergantung pada kemampuan sistem dalam mendeteksi, mencegah, dan merespons serangan dengan cepat dan adaptif. Pemerintah telah melakukan upaya untuk memperkuat keamanan siber melalui kerjasama internasional, pelatihan intensif, serta penelitian dan pengembangan di bidang keamanan siber, untuk memberikan lapisan perlindungan tambahan.

b. Konsep Pembangunan Sistem Keamanan Siber yang Kokoh dan Terintegrasi.

Pentingnya integrasi ini jelas terlihat dalam mengatasi kebutuhan untuk berbagi informasi dan sumber daya secara cepat ketika menghadapi ancaman. Selain itu, dalam menghadapi perubahan ancaman yang terus berkembang, adaptabilitas menjadi sangat penting. Sistem harus mampu beradaptasi sesuai kebutuhan, tidak hanya untuk mencegah serangan, tetapi juga untuk mengurangi dampaknya dan dengan cepat pulih jika pelanggaran terjadi. Pendekatan berlapis dalam keamanan, dengan berbagai lapisan pertahanan, memastikan bahwa jika satu pertahanan gagal, lapisan lainnya tetap siap untuk bertindak.

Penting juga untuk mengakui bahwa kerjasama antarsektoral, yang melibatkan pemerintah, sektor swasta, institusi akademik, dan masyarakat sipil, sangat krusial dalam memahami ancaman dan

menemukan solusi yang efektif. Pendekatan ini diperkuat oleh regulasi dan kebijakan yang mendukung praktik keamanan siber yang baik dan memberikan dasar hukum untuk bertindak. Dengan demikian, Pendekatan Keamanan Siber yang Kokoh dan Terintegrasi tidak hanya berkaitan dengan teknologi semata, tetapi juga dengan bagaimana semua elemen ini saling berinteraksi untuk menciptakan pertahanan yang kuat dan adaptif seperti :

1) **Penyusunan konsep sistem keamanan siber yang terpadu dan holistik untuk IKN.**

Penyusunan konsep sistem keamanan siber yang terpadu dan holistik untuk Ibu Kota Negara Nusantara (IKN) memerlukan pemahaman yang dalam tentang lanskap ancaman siber saat ini dan kebutuhan serta prioritas nasional dalam konteks keamanan siber. Berikut langkah-langkah dan elemen kunci dalam merancang konsep tersebut:

a) **Pemahaman Lanskap Ancaman:** Memahami ancaman yang ada melibatkan pemantauan terus-menerus terhadap sumber ancaman, baik dari aktor negara maupun non-negara.

b) **Penilaian Risiko:** Identifikasi ancaman dan nilai risiko terhadap infrastruktur kritis, data pemerintah, dan informasi rahasia.

c) **Pendekatan Berlapis:** Konsep keamanan siber yang terpadu memerlukan pendekatan berlapis, di mana setiap lapisan keamanan saling melindungi.

d) **Integrasi Teknologi dan Manusia**: Sementara teknologi penting, faktor manusia tetap kunci.

e) **Pembuatan Kebijakan dan Prosedur:** Kebijakan dan prosedur yang jelas memberikan kerangka kerja untuk tindakan dan tanggapan terhadap insiden, serta membimbing semua aktivitas keamanan siber.

f) **Kerjasama dan Kolaborasi:** Karena ancaman siber lintas batas, kerjasama antara lembaga pemerintah, sektor swasta, dan mitra internasional penting.

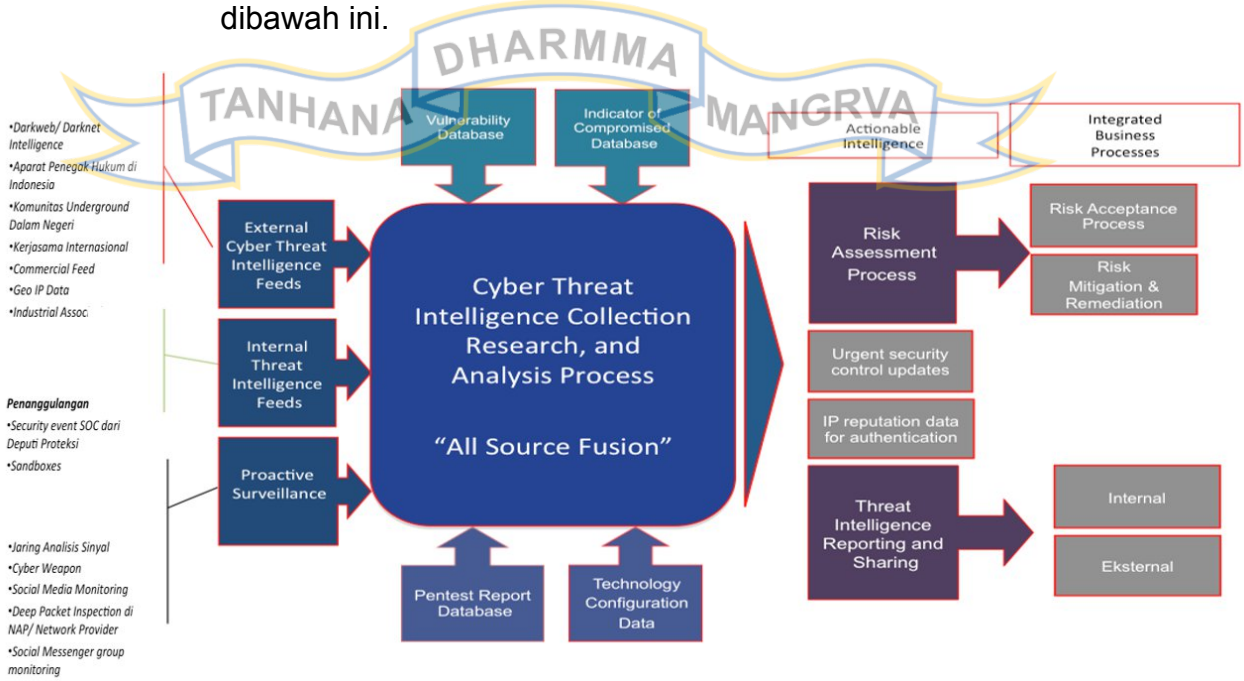
g) **Adaptabilitas dan Inovasi:** Ancaman siber berubah dengan cepat, sehingga sistem keamanan siber harus adaptif dan inovatif.

h) **Penguatan Hukum:** Undang-undang dan regulasi harus mendukung tindakan keamanan siber, memberikan dasar hukum untuk pencegahan, deteksi, dan respons terhadap insiden siber.

i) **Audit dan Review Berkala:** Audit dan peninjauan rutin diperlukan untuk memastikan efektivitas sistem.

2) **Penyusunan Pendekatan proaktif dalam deteksi dan pencegahan serangan siber.**

Pendekatan proaktif dalam deteksi dan pencegahan serangan siber adalah langkah-langkah sebelum serangan terjadi, menitikberatkan antisipasi, pemahaman ancaman, dan persiapan. Ini melibatkan pemantauan *real-time*, identifikasi pola mencurigakan, serta evaluasi risiko untuk cegah penetrasi dari aktor siber jahat. Salah satu caranya adalah menggunakan Teknologi *Threat Intelligence*, memberikan informasi terbaru tentang ancaman dan teknik serangan oleh pelaku, serta memberikan saran tindakan yang dapat dilakukan untuk menyeleisaikan masalah yang dapat timbul, seperti pada gambar dibawah ini.



Gambar 3.10. *Actionable Cyber Threat Intelligence*

Mengetahui metode serangan memungkinkan tim keamanan untuk lebih siap dalam deteksi dan pencegahan. Pengujian keamanan reguler seperti penetration testing penting untuk temukan celah sebelum dimanfaatkan penyerang. Pendidikan dan pelatihan bagi pegawai krusial, mengenali serangan seperti phishing. Pendekatan proaktif termasuk kebijakan jelas untuk patching dan pembaruan sistem. Ini memadukan teknologi canggih, kebijakan, dan SDM terlatih untuk aktif memantau, deteksi, dan cegah ancaman sebelum kerusakan.

3) **Penekanan pada penguatan keamanan perangkat lunak, jaringan, dan data untuk melindungi IKN dari serangan siber.**

Penekanan pada penguatan keamanan perangkat lunak, jaringan, dan data mengacu pada strategi khusus yang diambil untuk meningkatkan proteksi dan ketahanan terhadap potensi serangan siber pada aset-aset teknologi kritis di Ibu Kota Nusantara (IKN). Setiap komponen – perangkat lunak, jaringan, dan data – memiliki peran penting dalam ekosistem teknologi, dan masing-masing memerlukan pendekatan keamanan yang berbeda.

a) **Keamanan Perangkat Lunak:** Langkah-langkah untuk memastikan perangkat lunak bebas dari kerentanan meliputi pembaruan berkala, pengujian keamanan seperti *penetration testing*, dan penerapan prinsip pemrograman aman dalam pengembangan.

b) **Keamanan Jaringan:** Penguatan pertahanan terhadap serangan pada infrastruktur jaringan IKN melibatkan penggunaan *firewall*, sistem deteksi dan pencegahan intrusi (IDS/IPS), serta teknologi lain seperti VPN untuk enkripsi komunikasi.

c) **Keamanan Data:** Langkah-langkah untuk melindungi informasi dari pencurian, manipulasi, atau kehilangan meliputi

enkripsi data saat istirahat maupun transmisi, mengatur hak akses dengan benar, dan menerapkan solusi *backup* serta pemulihan data agar data dapat cepat dipulihkan dalam kasus insiden keamanan.

c. Konsep Pembangunan Infrastruktur Teknologi yang Terjamin Keamanannya.

Konsep Pembangunan Infrastruktur Teknologi yang Terjamin Keamanannya di Ibu Kota Negara Nusantara (IKN) mengedepankan pendekatan holistik dalam membangun dan memelihara aspek teknologi kota tersebut. Keamanan harus ditanamkan ke dalam setiap lapisan infrastruktur, mulai dari desain awal hingga implementasi. Ini mencakup penerapan fitur keamanan pada perangkat keras dan perangkat lunak, serta menjaga keberlanjutan melalui pembaruan dan pemeliharaan rutin. Selain itu, keamanan juga tentang manusia; oleh karena itu, pendidikan dan pelatihan keamanan bagi seluruh personel menjadi krusial. Mengelola akses ke sistem untuk memastikan hanya individu yang berwenang yang dapat mengakses informasi tertentu juga merupakan bagian integral dari konsep ini. Dan, meskipun pencegahan adalah kunci, kesiapan untuk merespons dan pulih dari insiden keamanan potensial juga sama pentingnya. Di tengah era digital saat ini, membangun IKN dengan infrastruktur teknologi yang terjamin keamanannya, Langkah-langkah strategis untuk menjamin kestabilan, keandalan, dan kedaulatan digital negara antara lain :

1) Merancang infrastruktur teknologi dengan lapisan keamanan kokoh dan terintegrasi memerlukan analisis risiko, desain berlapis, pemisahan jaringan, enkripsi, autentikasi kuat, manajemen *patch* dan pembaruan, pendidikan dan pelatihan, pemantauan dan deteksi, rencana respons insiden, serta evaluasi berkala.
2) Membangun *framework* infrastruktur teknologi dengan lapisan keamanan kokoh dan terintegrasi melibatkan identifikasi aset, perlindungan fisik, keamanan perangkat lunak, keamanan jaringan,

manajemen akses dan identitas, monitoring, backup dan pemulihan, respons terhadap insiden, pendidikan dan kesadaran keamanan, serta audit dan pengujian keamanan.

3) Integrasi teknologi canggih seperti kecerdasan buatan dan analisis *big data* dapat mendukung deteksi dini ancaman siber. AI dapat mendeteksi anomali, memberikan respons otomatis, analisis *big data* untuk intelijen ancaman, pelatihan mesin untuk phishing, otomatisasi dan orkestrasi, analisis sentimen dan media sosial, prediksi ancaman dengan *machine learning*, serta peningkatan forensik.

Dalam menerapkan teknologi canggih ini, penting bagi organisasi untuk terus mempertahankan etika dan privasi data. Selain itu, meskipun AI dan *big data* menyediakan alat yang kuat untuk deteksi dini, peran manusia tetap esensial dalam pengambilan keputusan dan interpretasi konteks serangan. Sementara penggunaan analitik *Big Data* membuka kemungkinan besar untuk organisasi (yaitu, peluang), itu juga dapat membuka organisasi terhadap ancaman baru. Peretas menyadari pergeseran ini dan mengembangkan keduanya lebih gigih dan lebih cerdas dalam cara mereka mengakses jaringan secara tidak sah. Ada dua jenis utama ancaman yaitu Peningkatan risiko pelanggaran privasi serta Kepatuhan terhadap peraturan.[41] Dengan menggabungkan kecerdasan buatan dan analisis big data ke dalam strategi keamanan siber, Ibu Kota Negara Nusantara dapat lebih siap dalam mendeteksi, mencegah, dan merespons ancaman siber, memastikan integritas dan keamanan infrastrukturnya.

d. Perlunya Peningkatan Sumber Daya Manusia dan Kesadaran Keamanan.

Peningkatan sumber daya manusia dan kesadaran keamanan menjadi aspek kunci dalam membangun sistem keamanan siber yang kokoh dan terintegrasi. Ancaman siber sering kali memanfaatkan

[41] Domenic Antonucci - The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities-Springer (2017), h. 50

kesalahan manusia, seperti kelalaian dalam menjaga kata sandi atau mengidentifikasi tautan berbahaya. Oleh karena itu, sumber daya manusia yang terampil dan memiliki kesadaran keamanan yang baik dapat menjadi pertahanan pertama dalam menghadapi ancaman siber.

Dalam menghadapi ancaman yang semakin kompleks, dibutuhkan tenaga ahli keamanan siber yang memahami secara mendalam taktik dan teknik yang digunakan oleh penyerang. Namun, upaya peningkatan sumber daya manusia tidak hanya berkaitan dengan spesialis keamanan siber, tetapi juga seluruh anggota organisasi. Kesadaran keamanan siber harus ditanamkan pada semua individu dalam organisasi, sehingga mereka mampu mengenali dan melaporkan aktivitas yang mencurigakan. Kesadaran ini harus dipraktikkan dari puncak organisasi hingga lapisan terbawah melalui pelatihan rutin, simulasi, dan kampanye edukasi.

Pelatihan tidak hanya sebatas pemahaman teknis dasar, tetapi juga meliputi pemahaman mendalam tentang taktik serta strategi yang digunakan oleh penyerang. Selain itu, pemahaman tentang hukum dan etika di dunia siber juga perlu ditekankan, agar para profesional keamanan siber memiliki integritas moral dan patuh terhadap regulasi. Pengembangan sumber daya manusia harus berlangsung secara kontinu. Mengingat perkembangan ancaman siber yang cepat, pelatihan harus dilakukan secara berkala agar tim keamanan siber selalu mendapatkan pembaruan mengenai teknik serangan terbaru dan cara pencegahannya. Simulasi dan latihan rutin juga membantu meningkatkan kesiapan tim terhadap serangan aktual.

Selanjutnya, kolaborasi dengan lembaga pendidikan dan pelatihan juga penting untuk memastikan ketersediaan tenaga ahli yang siap menghadapi tantangan keamanan siber di masa depan. Pendidikan formal dan sertifikasi dalam keamanan siber akan memastikan Indonesia memiliki sumber daya manusia yang berkualifikasi dan siap menghadapi tantangan di era digital.

Untuk mendorong kesadaran dan edukasi tentang keamanan siber di Ibu Kota Nusantara (IKN) dan seluruh Indonesia, beberapa pendekatan dapat diterapkan:

1) **Kampanye Publik:** Menggunakan media masa dan media sosial untuk meluncurkan kampanye keamanan siber yang memvisualisasikan dampak serangan dan pentingnya pencegahan.
2) ***Workshop* dan Pelatihan:** Mengadakan workshop dan pelatihan keamanan siber bagi berbagai kelompok, dengan materi yang disesuaikan untuk tingkat pemahaman mereka.
3) **Kerjasama dengan Sektor Pendidikan:** Kolaborasi dengan institusi pendidikan untuk menyisipkan materi edukasi keamanan siber dalam kurikulum.
4) **Pembentukan Komunitas Keamanan Siber:** Mendorong pembentukan komunitas keamanan siber yang memfasilitasi berbagi informasi dan praktik terbaik.
5) **Simulasi dan Latihan:** Mengadakan simulasi serangan siber di berbagai instansi untuk menguji kesiapan dan respons tim.
6) **Bahan Edukasi Digital:** Membuat *e-brochure*, video edukatif, dan modul pelatihan *online* yang mudah diakses.
7) **Pusat Respons Keamanan Siber:** Membentuk pusat respons yang berfungsi sebagai tim tanggap darurat dan sumber informasi.
8) **Penggunaan Teknologi:** Menggunakan aplikasi *mobile* untuk menyebarkan kuis, informasi ancaman siber, dan tips keamanan.
9) **Insentif:** Memberikan penghargaan bagi individu atau organisasi yang aktif berpartisipasi dalam program keamanan siber dan edukasi.
10) **Regulasi dan Kebijakan:** Mengeluarkan regulasi yang mewajibkan sektor-sektor tertentu memberikan edukasi keamanan siber kepada pelanggan atau pasiennya.

e. Implementasi Konsep Pembangunan Sistem Keamanan Siber Dan Infrastruktur Teknologi Yang Kokoh Dan Terintegrasi Di IKN.

Untuk menerapkan konsep pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi di IKN, berikut adalah langkah-langkah konkret beserta rekomendasinya:

1) ***Blueprint* Keamanan Siber:** Membuat rancang rencana keamanan siber berdasarkan risiko dan prioritas.
2) **Integrasi Teknologi Canggih:** Gunakan AI dan analisis *big data* untuk deteksi dini ancaman.
3) **Pusat Operasi Keamanan Siber (SOC):** Dirikan pusat pemantauan dan respon insiden 24/7.
4) **Pelatihan dan Sertifikasi:** Latih tim keamanan dan fasilitasi sertifikasi.
5) **Kerjasama Multipihak:** Kolaborasi dengan sektor swasta, akademisi, dan lembaga internasional.
6) **Pembentukan *Join Operation Cyber Command* IKN:** Buat badan standar keamanan siber.
7) **Audit dan Evaluasi Rutin:** Lakukan audit berkala dan perbaiki strategi.
8) **Pengembangan Kebijakan Akses:** Tentukan kebijakan akses ketat dengan teknologi IAM.
9) **Pencegahan Insiden Fisik:** Tingkatkan keamanan fisik infrastruktur.
10) **Program Kesadaran Keamanan:** Edukasi pegawai dan masyarakat.

Evaluasi Berkala penting dalam keamanan siber. Ancaman siber berubah cepat dan tak terduga, sehingga strategi harus sesuai dengan ancaman terkini. Evaluasi memberi gambaran efektivitas kebijakan dan praktik keamanan. Tanpa evaluasi, bisa ada celah yang dimanfaatkan penyerang. Langkah-langkah butuh komitmen, dana, dan dukungan pemangku kepentingan di IKN. Dengan dedikasi dan tindakan terkoordinasi, IKN bisa mengembangkan infrastruktur teknologi yang aman dan tahan ancaman siber.

Adapun upaya yang dapat dilakukan oleh pemerintah dalam melakukan pencegahan serta melakukan mitigasi terhadap ancaman siber global antara lain :

1) Kerangka Strategi Keamanan Siber dalam Pengembangan IKN

Strategi ini menekankan identifikasi aset kritis, pengembangan sistem deteksi dan respons terhadap insiden, peningkatan kesadaran keamanan di kalangan masyarakat, kolaborasi lintas sektor, dan pembaruan regulasi keamanan siber. Tujuannya adalah untuk memastikan integritas, keberlanjutan, dan keamanan operasional IKN di tengah era digital yang penuh dengan tantangan. Kerangka ini memiliki beberapa komponen kunci:

a) Visi & Misi Keamanan Siber IKN:

Visi: Membuat IKN sebagai pusat pemerintahan dan inovasi yang memiliki infrastruktur teknologi yang aman dan tangguh terhadap ancaman siber.

Misi: Mengintegrasikan prinsip-prinsip keamanan siber dalam semua aspek pengembangan dan operasi IKN, melindungi data dan aset digital, serta meningkatkan kesadaran keamanan di kalangan masyarakat dan pemangku kebijakan.

b) Penilaian Risiko & Kerentanan:

Melakukan audit berkala keamanan siber untuk mengidentifikasi risiko dan kerentanan serta mengembangkan sistem pelaporan insiden keamanan siber yang tanggap dan efektif.

c) Pengembangan Infrastruktur Teknologi yang Aman:

Menetapkan standar keamanan untuk perangkat keras, perangkat lunak, dan jaringan serta mengintegrasikan solusi keamanan canggih seperti kecerdasan buatan dan enkripsi dalam infrastruktur teknologi IKN.

d) Pendidikan & Pelatihan Keamanan Siber:

Membuat program pelatihan keamanan siber untuk pegawai pemerintah dan pihak terkait serta mengadakan kampanye kesadaran keamanan siber untuk masyarakat IKN.

e) **Kerjasama & Kolaborasi:**

Membangun kerjasama dengan entitas pemerintah, sektor swasta, akademisi, dan lembaga internasional dalam bidang keamanan siber serta membuat platform berbagi informasi tentang ancaman dan solusi keamanan.

f) **Respons & Pemulihan:**

Mendirikan tim respons insiden siber (CSIRT/CERT) dengan kemampuan untuk merespons dan memulihkan sistem dari serangan siber serta menetapkan protokol tindakan saat insiden keamanan siber terjadi.

g) **Pengawasan & Evaluasi:**

Menetapkan indikator kinerja utama (KPI) untuk keamanan siber serta melakukan peninjauan berkala terhadap efektivitas strategi keamanan siber.

h) **Hukum & Kebijakan:**

Mengembangkan dan memperbarui peraturan serta kebijakan yang mendukung penguatan keamanan siber serta endorong sistem peradilan dan penegakan hukum terkait kejahatan siber.

i) **Pendanaan & Investasi:**

Mengalokasikan anggaran yang memadai untuk inisiatif keamanan siber serta mendorong investasi dalam riset dan pengembangan keamanan siber.

j) **Adaptasi & Inovasi:**

Melakukan riset dan pengembangan untuk mengantisipasi tantangan keamanan siber di masa depan serta mengintegrasikan inovasi teknologi terbaru dalam pendekatan keamanan siber IKN.

2) **Rencana Pencegahan dan Mitigasi Ancaman Ibu Kota Nusantara (IKN) dalam Konteks Kewaspadaan Nasional.**

Dalam konteks kewaspadaan nasional, penting bagi Ibu Kota Nusantara (IKN) untuk memiliki rencana pencegahan dan mitigasi yang komprehensif guna mengantisipasi berbagai ancaman. Berikut adalah penjelasan berdasarkan konsep-konsep yang telah disebutkan:

a) ***Early Warning System*** **(Sistem Peringatan Dini):** Suatu mekanisme yang mengidentifikasi indikator atau tanda-tanda awal dari suatu ancaman sehingga dapat diambil tindakan preventif. Implementasi di IKN: Mengembangkan infrastruktur teknologi yang mampu memonitor, menganalisis, dan memberikan peringatan dini terhadap potensi ancaman, seperti serangan siber, bencana alam, atau gangguan keamanan lainnya. Pusat kontrol dan komando bisa diinstal di lokasi strategis untuk memastikan informasi disebarkan dengan cepat dan efektif.

b) ***Early Detection*** **(Deteksi Dini):** Proses mendeteksi aktivitas atau ancaman yang mencurigakan pada tahap awal. Implementasi di IKN: Menggunakan teknologi surveilans, intelijen buatan, dan analisis big data untuk mengidentifikasi aktivitas mencurigakan baik di dunia nyata maupun dunia maya. Kerjasama dengan lembaga intelijen dan kepolisian akan memperkuat proses ini.

c) **Tangkal Dini:** Tindakan proaktif yang diambil untuk mengatasi ancaman pada fase awal. Implementasi di IKN: Peningkatan patroli keamanan, penerapan sistem keamanan siber yang kuat, dan respons cepat terhadap laporan dari masyarakat atau sistem peringatan dini. Semua instansi terkait harus memiliki SOP yang jelas mengenai bagaimana cara bertindak saat menerima peringatan.

d) **Cegah Dini:** Upaya mencegah potensi ancaman sebelum terwujud menjadi suatu insiden. Implementasi di IKN: Kampanye kesadaran keamanan di kalangan masyarakat dan *stakeholder*, regulasi yang mendukung pencegahan ancaman, serta kerjasama erat dengan sektor swasta dan komunitas untuk mengidentifikasi dan mencegah risiko.

e) **Tanggap Dini:** Respon cepat dan efektif setelah ancaman terdeteksi atau terjadi. Implementasi di IKN: Pembentukan unit respons cepat yang dapat bergerak ketika ancaman terjadi, memastikan komunikasi yang efektif antara berbagai entitas pemerintah dan masyarakat, serta mempersiapkan infrastruktur dan sumber daya yang dibutuhkan untuk menangani insiden.

3) **Peran Pemerintah, Swasta, dan Masyarakat dalam Mencegah Ancaman Siber.**

Dalam konteks Strategi Keamanan Siber Nasional, peran masing-masing pemangku kepentingan sangatlah penting untuk memastikan keamanan dan ketahanan infrastruktur siber. Pemerintah berperan sebagai pelindung kedaulatan digital, regulator, dan koordinator utama dalam merumuskan kebijakan serta respons terhadap ancaman siber. Dalam kerangka teori keamanan nasional, negara memiliki tanggung jawab untuk mengidentifikasi potensi ancaman yang mungkin timbul dan mengalokasikan sumber daya yang diperlukan guna membangun pertahanan yang kuat dan responsif. Ini melibatkan pendirian lembaga-lembaga khusus yang berfokus pada keamanan siber, pengembangan regulasi yang mendukung, serta penerapan kebijakan proaktif yang berfokus pada pencegahan dan respons terhadap ancaman digital.

Dalam konteks ini, sektor swasta memegang peran penting sebagai pemilik dan operator utama dari infrastruktur kritis. Swasta bertanggung jawab untuk menjaga keamanan jaringan, sistem, dan data mereka sendiri. Dalam prinsip-prinsip keamanan siber,

perusahaan-perusahaan memiliki tanggung jawab untuk memastikan integritas, kerahasiaan, dan ketersediaan data. Tanggung jawab ini mencakup penerapan protokol keamanan terbaik, pelatihan dan edukasi bagi karyawan, serta kerja sama yang erat dengan pemerintah untuk pertukaran informasi mengenai ancaman siber yang mungkin timbul.

Sementara itu, masyarakat juga memiliki peran penting dalam strategi keamanan siber nasional. Kesadaran individu dalam menjaga keamanan informasi pribadi dan kemampuan untuk mengidentifikasi potensi ancaman seperti serangan *phishing* menjadi sangat penting. Teori keamanan siber nasional menekankan pentingnya pendidikan dan pelatihan bagi masyarakat guna meningkatkan kesadaran dan kesiapsiagaan mereka dalam menghadapi ancaman siber. Selain itu, pihak-pihak lain seperti organisasi non-pemerintah, lembaga penelitian, dan komunitas siber juga memiliki peran dalam melakukan penelitian, pelatihan, dan advokasi. Mereka berkolaborasi dengan pemerintah, sektor swasta, dan masyarakat untuk memastikan bahwa strategi keamanan siber yang diterapkan bersifat komprehensif, selalu diperbarui sesuai perkembangan ancaman, dan mampu mengatasi tantangan yang terus berubah.

BAB IV
PENUTUP

20. Simpulan.

Ancaman siber global, yang mencakup serangan dari aktor negara maupun non-negara, dapat menghancurkan infrastruktur kritis, mengakses informasi sensitif, dan mengganggu stabilitas ekonomi dan politik. Selain itu, penerapan teknologi canggih dalam berbagai sektor pembangunan IKN menambah kompleksitas upaya pengamanan siber. Oleh karena itu, perlunya pendekatan komprehensif yang melibatkan pemerintah, sektor swasta, masyarakat, dan internasional dalam menghadapi potensi ancaman tersebut menjadi sangat penting. Kesimpulannya, memastikan keamanan siber di IKN bukan hanya menjadi tanggung jawab sektor teknologi saja, tetapi merupakan kebutuhan nasional yang memerlukan kolaborasi lintas sektor guna menjaga keamanan dan kedaulatan negara dalam era digital saat ini.

Ancaman siber, jika tidak ditangani dengan benar, dapat merusak fondasi digital IKN, mulai dari penghentian layanan kritis, kehilangan data sensitif, hingga dampak ekonomi yang signifikan akibat gangguan operasional. Selain itu, kerentanan dalam infrastruktur teknologi dapat menjadi pintu masuk bagi aktor jahat untuk menggangu, memanipulasi, atau bahkan menghancurkan sistem yang mendukung kehidupan sehari-hari masyarakat IKN. Dampak dari ancaman-ancaman ini bisa menghambat pertumbuhan ekonomi, menurunkan kepercayaan investor dan masyarakat, serta mengancam kedaulatan dan integritas nasional. Oleh karenanya, perlindungan terhadap aspek keamanan siber dan penguatan infrastruktur teknologi menjadi prioritas utama dalam agenda pembangunan IKN. Pembentukan Joint Operation Cyber Command IKN juga perlu dilakukan yang bertugas mengawasi segala hal terkait dengan keamanan siber di IKN. Kesimpulannya, keberlangsungan dan perkembangan IKN di masa depan sangat bergantung pada sejauh mana kita membentuk suatu badan yang mampu menjaga, melindungi, dan mengembangkan sistem keamanan siber dan infrastruktur teknologi yang tangguh dan adaptif terhadap perubahan ancaman di era digital.

Ancaman siber global yang berpotensi menghancurkan sistem informasi, meretas data sensitif, atau bahkan mengganggu operasional kegiatan vital, dapat menimbulkan dampak devastatif bagi kestabilan, perekonomian, dan kedaulatan Indonesia. IKN dapat diharapkan mampu menghadapi, merespon, dan mengatasi setiap ancaman yang muncul. Kesimpulannya, konsep pembangunan yang kokoh dan terintegrasi ini akan menjadi penopang utama dalam mewujudkan visi IKN sebagai pusat perkembangan bangsa yang aman, modern, dan inovatif, serta menjaga integritas dan kedaulatan Indonesia di era digital global.

21. Rekomendasi.

a. Untuk Pemerintah Otorita Ibu Kota Nusantara (IKN): Pemerintah Otorita Ibu Kota Nusantara (IKN) berada dalam posisi yang strategis untuk memastikan keamanan siber di wilayah ibu kota baru negara. Oleh karena itu, sangat penting bagi otoritas IKN untuk memprioritaskan aspek keamanan dalam setiap layanan publik digitalnya. Selanjutnya, pembentukan Joint Operation Cyber Command IKN menjadi salah satu langkah proaktif yang bisa diambil. Tim ini, yang idealnya bekerja sama dengan entitas keamanan lain seperti BIN, TNI, dan Polri, akan menjadi garda terdepan dalam mendeteksi, merespons, dan memulihkan insiden keamanan siber, memastikan bahwa IKN tetap aman dari ancaman siber dan mampu pulih dengan cepat saat insiden terjadi.

b. Untuk Kementerian Komunikasi dan Informatika: Dalam upaya melindungi infrastruktur kritikal nasional, terutama di Ibu Kota Nusantara (IKN), sangat penting bagi kita untuk meningkatkan standar keamanan siber. Standar yang lebih ketat dan spesifik akan memastikan setiap aspek dari infrastruktur kita terlindungi dengan baik. Selanjutnya, pembentukan Pusat Keamanan Siber Nasional di IKN menjadi langkah strategis yang sangat direkomendasikan.

c. Untuk Badan Siber dan Sandi Negara (BSSN): Badan Siber dan Sandi Negara (BSSN) memiliki tanggung jawab strategis dalam memastikan keamanan siber nasional. Sebagai langkah awal, BSSN perlu mengambil inisiatif dalam mengkoordinasikan seluruh *stakeholder* siber di Tanah Air,

memastikan ada sinkronisasi kebijakan, tindakan, dan respons terhadap ancaman. Selain itu juga perlu melakukan pembentukan *Computer Security Incident Response Team* (CSIRT) di IKN. BSSN perlu memprioritaskan pembinaan melalui program pelatihan dan sertifikasi bagi profesional keamanan siber, terutama mereka yang beroperasi di IKN. Terakhir, BSSN harus mempererat hubungan dengan entitas keamanan siber dari negara-negara lain.

d. Untuk Badan Riset dan Inovasi Nasional: Badan Riset dan Inovasi Nasional (BRIN) berperan krusial dalam mendorong inovasi dan riset di Indonesia. Dalam konteks keamanan siber, sangat penting bagi BRIN untuk mengalokasikan dana riset yang signifikan untuk pengembangan teknologi keamanan siber domestik.
e. Untuk Lembaga Swasta dan Industri Teknologi: Lembaga Swasta dan Industri Teknologi memegang peran penting dalam peta digitalisasi Indonesia. Dalam menghadapi tantangan keamanan siber yang kian kompleks, direkomendasikan bagi mereka untuk proaktif mengadopsi praktik terbaik dalam desain dan operasional sistem mereka. Di samping itu, dalam era globalisasi teknologi informasi, kerjasama antara swasta dan pemerintah menjadi sebuah keharusan, bukan pilihan.
f. Untuk Badan Intelijen Negara (BIN): Dalam era digital yang sedang berkembang pesat, keamanan siber menjadi salah satu aspek vital dalam memastikan keamanan nasional. Direkomendasikan bagi Badan Intelijen Negara (BIN) untuk mengintensifkan integrasi intelijen siber ke dalam operasi rutinnya. Selain itu, kerjasama internasional dalam bidang intelijen siber harus terus ditingkatkan.
g. Untuk Kementerian Pertahanan: Kementerian Pertahanan memegang peran strategis dalam memastikan keamanan dan kedaulatan negara, terutama di era digital saat ini. Oleh karena itu, sangat penting bagi Kementerian Pertahanan untuk mengembangkan Satuan Khusus Keamanan Siber. Selain itu, mengingat perkembangan teknologi yang cepat dan kompleksitas ancaman siber yang terus meningkat, investasi dalam penelitian dan pengembangan teknologi pertahanan siber menjadi hal yang tak bisa ditawar.

h. Untuk Tentara Nasional Indonesia (TNI): Untuk Tentara Nasional Indonesia (TNI), era digital menuntut transformasi dan adaptasi yang sigap terhadap ancaman siber yang semakin meningkat. Pertama, latihan dan sertifikasi dalam bidang keamanan siber harus menjadi prioritas. Selain itu, sertifikasi akan memastikan bahwa personel memiliki standar kompetensi yang diakui secara internasional dalam menjaga keamanan informasi dan infrastruktur kritikal. Kedua, kolaborasi dengan industri teknologi dan keamanan sangat esensial. Terakhir, pertimbangan pembentukan matra baru dalam bentuk Angkatan Siber menjadi langkah progresif. Angkatan ini akan berfokus khusus pada pertahanan dan operasi siber, melengkapi tugas TNI Angkatan Darat, Laut, dan Udara.

i. Untuk Kepolisian Republik Indonesia (Polri): Untuk Kepolisian Republik Indonesia (Polri) di era digital saat ini, penting untuk menghadapi dan menanggulangi tantangan keamanan siber yang semakin kompleks. Pertama-tama, pembentukan Unit Siber menjadi langkah penting. Dengan adanya unit khusus, Polri dapat lebih cepat dan tepat dalam mengidentifikasi serta menanggapi insiden keamanan siber. Selain itu, kerjasama dengan pihak ketiga, khususnya penyedia layanan teknologi dan pakar keamanan siber, akan memberikan akses ke teknologi terbaru dan *best practices* dalam bidang keamanan informasi.

j. Untuk Kementerian Keuangan: Alokasi Anggaran Khusus: Dalam era digitalisasi yang semakin maju, keamanan siber menjadi salah satu pilar penting untuk menjaga integritas dan keandalan informasi, khususnya yang berkaitan dengan data keuangan nasional. Anggaran ini seharusnya mencakup investasi dalam teknologi keamanan mutakhir, pelatihan bagi para profesional IT, serta perekrutan dan pengembangan sumber daya manusia yang kompeten di bidang keamanan siber. Selain itu, penting bagi Kementerian Keuangan untuk melakukan audit keamanan siber secara berkala.

k. Untuk Badan Perencanaan Pembangunan Nasional (Bappenas): Bappenas memiliki peran kunci dalam merencanakan arah pembangunan bangsa, termasuk dalam aspek keamanan siber. Oleh karena itu, sangat penting bagi Bappenas untuk mengintegrasikan keamanan siber ke dalam

setiap elemen perencanaan pembangunan nasional. Setiap proyek infrastruktur dan teknologi yang dibiayai oleh negara harus mempertimbangkan dan memastikan aspek keamanan yang ketat agar mampu melindungi data dan aset nasional. Selain itu, Bappenas sebaiknya mengkoordinasikan kerjasama multisektoral antara berbagai kementerian dan lembaga.

I. Untuk Dewan Perwakilan Rakyat (DPR): PDewan Perwakilan Rakyat (DPR) sebagai wakil rakyat memiliki peran strategis dalam memastikan keamanan informasi nasional. Dalam konteks keamanan siber, DPR seharusnya melakukan pengawasan ketat atas penggunaan anggaran negara yang diperuntukkan bagi keamanan siber. Selain itu, DPR harus proaktif dalam menginisiasi, mendukung, atau merevisi perundang-undangan yang relevan dengan keamanan siber. Terakhir, penting bagi DPR untuk selalu membuka ruang dialog dan konsultasi dengan berbagai pemangku kepentingan, termasuk akademisi, praktisi keamanan siber, dan masyarakat umum.

Dengan rekomendasi di atas, diharapkan dapat memastikan bahwa semua aspek pemerintahan dan keamanan di IKN memiliki persiapan dan respons yang memadai terhadap potensi ancaman siber.

Jakarta, 27 Agustus 2023

Penulis,

Dr. Pratama Dahlian Persadha, S.Sos., M.M.

DAFTAR PUSTAKA

Buku/Jurnal/Artikel/Slide Paparan:

BPS, Kepadatan Penduduk menurut Provinsi (jiwa/km2) 2019-2021, (2023)

Kementerian ESDM, Statistik Ketenagalistrikan Tahun 2021, (2022)

Wisadirana. Darsono. Pembanguna berdimensi kerakyatan. Yayasan Obor. (2004)

BSSN, Lanskap Keamanan Siber 2022, (2023)

Petrosyan, Ani, Annual cost of cybercrime worldwide 2017-2028, (2023)

Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. (2015).

Peter Trim, Yang-Im Lee - Strategic Cyber Security Management-Routledge (2022)

Nir Kshetri - The Quest to Cyber Superiority_ Cybersecurity Regulations, Frameworks, and Strategies of Major Economies-Springer International Publishing (2016)

MacDonnell Ulsch - Cyber Threat!_ How to Manage the Growing Risk of Cyber Attacks- Wiley Corporate F&A (2014)

Johnson, Thomas A - Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare - CRC Press (2015)

V.S. Subrahmanian, Michael Ovelgonne, Tudor Dumitras, B. Aditya Prakash - The Global Cyber-Vulnerability Report-Springer (2016)

Centre For Cyber Security Belgium - Cyber Security Incident Management Guide-Centre For Cyber Security Belgium (2015)

Domenic Antonucci - The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities-Springer (2017)

Nitul Dutta, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, Emil Pricop - Cyber Security_ Issues and Current Trends (Studies in Computational Intelligence, 995)-Springer (2021)

John A. Adams Jr. - Cyber Blackout_ When the Lights Go Out -- Nation at Risk-FriesenPress (2015)

Peraturan Perundang-Undangan:

UU Dasar Negara Republik Indonesia Tahun 1945

UU Nomor 3 Tahun 2022 Tentang Ibu Kota Negara

UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat.

Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik

Panduan Pengamanan Siber bagi Instansi Pemerintah oleh Badan Siber dan Sandi Negara (BSSN).

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

Rencana Pembangunan Jangka Menengah Nasional (RPJMN 2020-2024)

Internet:

CISA. (2021). Cyber-Attack Against Ukrainian Critical Infrastructure. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

The New York Times. (2017). Cyberattack Hits Ukraine Then Spreads Internationally. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

BBC News Indonesia. (2016). AS tuduh Rusia lakukan serangan siber untuk 'menganggu pemilu AS'. https://www.bbc.com/indonesia/dunia/2016/10/161008_dunia_as_pemilu_rusia

BBC News. (2017). How a cyber attack transformed Estonia. https://www.bbc.com/news/39655415

The New York Times. (2012).In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

The One Brief. (2017). The Bangladesh Bank Heist: Lessons In Cyber Vulnerability. https://theonebrief.com/the-bangladesh-bank-heist-lessons-in-cyber-vulnerability/

CIPD. (2023). PESTLE Analysis. https://www.cipd.org/en/knowledge/factsheets/pestle-analysis-factsheet/

CIPD. (2023). SWOT Analysis https://www.cipd.org/uk/knowledge/factsheets/swot-analysis-factsheet

BSSN. (2023). Kepala BSSN Hinsa Siburian Paparkan Sistem Keamanan Siber di IKN pada Seminar Ketahanan Nasional HUT ke-58 Lemhannas https://www.bssn.go.id/kepala-bssn-hinsa-siburian-paparkan-sistem-keamanan-siber-di-ikn-pada-seminar-ketahanan-nasional-hut-ke-58-lemhannas/

UK IT- Governance. (2019) What is Cybersecurity https://www.itgovernance.co.uk/what-is-cybersecurity

ENISA. (2019). National Cybersecurity Strategy, European Union Agency for Network and Information Security, https://www.enisa.europa.eu/topics/national-cyber-security-strategies

ANTARA. (2023). Menkominfo nyatakan Indonesia optimalkan konektivitas digital ASEAN https://www.antaranews.com/berita/3692229/menkominfo-nyatakan-indonesia-optimalkan-konektivitas-digital-asean

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LAMPIRAN 1 : "ALUR PIKIR"

ALUR PIKIR
PEMBANGUNAN SISTEM KEAMANAN SIBER DAN INFRASTRUKTUR TEKNOLOGI IBU KOTA NUSANTARA DALAM RANGKA KEWASPADAAN NASIONAL

ANCAMAN SIBER GLOBAL PADA PEMINDAHAN IBUKOTA BARU IKN NUSANTARA YANG BISA MELUMPUHKAN NEGARA

RUMUSAN MASALAH

Bagaimana membuat dan mendesain **PEMBANGUNAN SISTEM KEAMANAN SIBER DAN INFRASTRUKTUR TEKNOLOGI IBU KOTA NUSANTARA DALAM RANGKA KEWASPADAAN NASIONAL?**

PERTANYAAN KAJIAN

a. Apa saja potensi ancaman siber global yang dapat mengancam keamanan dan kedaulatan Indonesia dalam pengembangan Ibu Kota Nusantara (IKN)?
b. Bagaimana dampak dari ancaman keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi terhadap perkembangan dan keberlangsungan IKN dan Indonesia di masa depan?
c. Bagaimana konsep perencanaan, implementasi, evaluasi pembangunan sistem keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi untuk mewujudkan kewaspadaan nasional dalam melindungi IKN dari ancaman siber global dan menjaga kedaulatan Indonesia?

LANDASAN PEMIKIRAN
(REGULASI, KEBIJAKAN, IMPLEMENTASI)

UUD NRI 1945, UU No 3/2022, UU No 19/2019, PerPres No 39/2019, Permenkominfo No 20/2016, Permenkominfo No 5/2020, Perban BSSN No 4/2021, UU No 27/2022, Buku, Jurnal

ANALISIS KAJIAN

1. Mengidentifikasi dan memetakan potensi ancaman siber global serta dampaknya yang dapat mengancam keamanan dan kedaulatan Indonesia dalam pengembangan IKN Nusantara.
2. Melakukan analisis dampaknya terhadap keamanan nasional dan infrastruktur kritis di Ibu Kota Nusantara. Termasuk kerugian ekonomi yang besar dan merusak citra serta menurunkan daya saing Indonesia di mata dunia internasional.
3. Penerapan rencana strategis keamanan siber dan infrastruktur teknologi yang kokoh dan terintegrasi di IKN untuk mewujudkan kewaspadaan nasional dalam meningkatkan keamanan dan kedaulatan Indonesia.

PERKEMBANGAN LINGKUNGAN STRATEGIS

1. Global
2. Regional
3. Nasional

PEMBANGUNAN SISTEM KEAMANAN SIBER DAN INFRASTRUKTUR TEKNOLOGI IKN YANG KUAT DAN TANGGUH

KEWASPADAAN NASIONAL INDONESIA YANG AMAN DAN TERJAGA