LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

MEMBANGUN SISTEM KEAMANAN SIBER DI IBU KOTA NUSANTARA (IKN) DALAM RANGKA MENUNJANG PEMBANGUNAN NASIONAL YANG BERKELANJUTAN

OLEH:

YAYAT POPON RUHIAT, S.I.K.

BRIGADIR JENDERAL POLISI

KERTAS KARYA ILMIAH PERORANGAN (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 puji syukur kehadirat Allah Subhanahu Wata'ala serta atas segala rahmat dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Singkat Angkatan (PPSA) XXIV telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Ilmiah Perseorangan (Taskap) dengan judul: "**MEMBANGUN SISTEM KEAMANAN SIBER DI IBU KOTA NUSANTARA (IKN) DALAM RANGKA MENUNJANG PEMBANGUNAN NASIONAL YANG BERKELANJUTAN**".

Penentuan Tutor dan judul Taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor 118 Tahun 2023 tanggal 13 Juni 2023 tentang Penetapan Judul Taskap Peserta PPSA XXIV tahun 2023 Lemhannas Republik Indonesia, dengan perintah kepada para peserta PPSA XXIV untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah Penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPSA XXIV di Lemhannas RI tahun 2022. Ucapan yang sama juga disampaikan kepada Pembimbing atau Tutor Taskap Mayjen TNI Rido Hermawan, M.Sc dan Tim Penguji Taskap serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari bahwa kualitas Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon adanya masukan guna penyempurnaan naskah ini.

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

Semoga Allah Subhanahu Wata'ala senantiasa memberikan berkah dan bimbingan kepada kita semua dalam melaksanakan tugas dan pengabdian kepada Negara dan bangsa Indonesia yang kita cintai dan kita banggakan.

Sekian dan terima kasih. Wassalamualaikum Warahmatullahi Wabarakatuh.

Jakarta, 29 September 2023

Brigjen. Pol. Yayat Popon Ruhiat, S.I.K.

No. Peserta: 077

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini :

   Nama : Brigjen. Pol. Yayat Popon Ruhiat, S.I.K.

   Pangkat : Brigadir Jenderal Polisi

   Jabatan : Dir Rendalgiatops pada Deputi Bidang Intelijen Siber BIN

   Instansi : Badan Intelijen Negara

   Alamat : Jl. Seno Raya, Pejaten Timur, Pasar Minggu, Jakarta Selatan.

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

   a. Kertas Karya Ilmiah Perseorangan (Taskap) yang saya tulis adalah asli.

   b. Apabila ternyata sebagian atau seluruhnya tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia dinyatakan tidak lulus pendidikan.

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

Jakarta, 29 September 2023

Penulis Taskap

(Materai tempel 10.000)

Brigjen. Pol. Yayat Popon Ruhiat, S.I.K.

No. Peserta: 077

DHARMMA
TANHANA
MANGRVA

DAFTAR ISI

Halaman

KATA PENGANTAR i
PERNYATAAN KEASLIAN iii
DAFTAR ISI iv
TABEL vi
DAFTAR GAMBAR vii

BAB I. PENDAHULUAN

1. Latar Belakang 1
2. Rumusan Masalah 8
3 Maksud dan Tujuan 9
4. Ruang Lingkup dan Sistematika 9
5. Metode dan Pendekatan 10
6. Pengertian 11

BAB II. LANDASAN PEMIKIRAN

7. Umum 15
8. Peraturan Perundang-undangan 15
9. Data dan Fakta 18
10. Kerangka Teoritis 28
11. Lingkungan Strategis 37

BAB III. PEMBAHASAN

12. Umum 48
13. Analisa SWOT Pembangunan Sistem Keamanan Siber di Ibu Kota Nusantara (IKN) 49
14. Membangun Tata Kelola Regulasi Yang Dapat Mendukung Sistem Keamanan Siber di IKN..... 60
15. Strategi Membangun Sinergitas Antar Lembaga dan Kementerian dalam Menghadapi Kedatangan Investasi 67
16. Menyiapkan Infrastruktur Sistem Keamanan Siber di IKN..... 73
17. Menyiapkan Sumber Daya Manusia untuk Mendukung Sistem Keamanan Siber di IKN..... 82
18. Memantapkan Skenario Dukungan Anggaran untuk Sistem Keamanan Siber di IKN 90

BAB IV. PENUTUP

19. Simpulan 93
20. Rekomendasi 96

DAFTAR PUSTAKA:

DAFTAR LAMPIRAN:

1. Alur Pikir
2. Daftar Riwayat Hidup

TABEL

TABEL 1 MATRIKS ANALISIS SWOT PEMBANGUNAN SISTEM KEAMANAN SIBER DI IBU KOTA NUSANTARA (IKN)

TABEL 2 MATRIKS STRATEGI SWOT

DAFTAR GAMBAR

GAMBAR I ELEMEN SMART CITIES

BAB I
PENDAHULUAN

1. Latar Belakang

Pada tahun 2019, pemerintah Indonesia telah mengumumkan rencana untuk memindahkan ibu kota negara dari Jakarta ke suatu lokasi baru. Keputusan ini diambil karena Jakarta menghadapi berbagai masalah seperti kepadatan penduduk yang tinggi, banjir yang sering terjadi, penurunan tanah, dan kemacetan lalu lintas yang parah. Pemerintah berharap dengan memindahkan ibu kota, masalah-masalah tersebut dapat diatasi dan memperluas pembangunan ke wilayah lain di Indonesia[1].

Rancangan Undang-Undang (RUU) Ibu kota Negara (IKN) disahkan menjadi UU IKN pada 18 Januari 2022. Berdasarkan Pasal 360 Undang-Undang No. 23 Tahun 2014 tentang Pemerintahan Daerah, yang mengatur bahwa Pemerintah Pusat dapat membentuk Kawasan Khusus, yang dalam konteks Naskah Akademik Ibu Kota Negara, maka Kawasan Khusus calon Ibu Kota Negara akan berlokasi di antara Kabupaten Penajam Paser Utara (PPU) dan Kabupaten Kutai Kartanegara, Kalimantan Timur.

IKN Nusantara kemudian ditetapkan melalui Undang-Undang No. 3 Tahun 2022 Tentang Ibu Kota Negara. Pembangunan IKN merupakan langkah strategis untuk mengatasi masalah yang terkait dengan keterbatasan ruang dan infrastruktur di Ibu Kota Jakarta serta untuk mendistribusikan pembangunan secara lebih merata di seluruh wilayah Indonesia. IKN Nusantara direncanakan akan menjadi pusat pemerintahan yang modern, berkelanjutan, dan terintegrasi dengan infrastruktur yang memadai.[2] Pembangunan IKN Nusantara juga diharapkan akan memberikan dampak positif dalam hal peningkatan kualitas hidup masyarakat, pembangunan ekonomi, dan pengembangan sosial di wilayah tersebut.

Pembangunan Ibu Kota Negara (IKN) Nusantara tidak hanya ditujukan untuk menjawab tantangan nasional, tetapi juga global. Melihat pembangunan IKN berdasarkan dari kapasitas sebelumnya, pemindahan

[1] Suryadi Jaya. 2022. Analisis Kebijakan Publik Pemindahan ibu Kota Negara. Jurnal Ekonomi & Kebijakan Publik, Vol 13, No. 2.
[2] https://ikn.go.id/tentang-ikn

IKN ke tengah wilayah Indonesia merepresentasikan arti keadilan yang merupakan perwujudan dari sistem demokrasi[3]. Pemerintah Indonesia telah menetapkan IKN juga sebagai proyek strategis nasional yang melibatkan berbagai pihak, termasuk ahli, lembaga terkait, dan masyarakat dalam proses perencanaan dan pengambilan keputusan terkait IKN Nusantara, dimana hal ini akan menjadi tonggak penting dalam mengembangkan potensi Indonesia secara keseluruhan. Keputusan untuk membangun IKN Nusantara juga merupakan langkah penting dalam upaya Indonesia untuk mengembangkan potensi negara dan menciptakan tata kelola pemerintahan yang lebih efektif dengan menggunakan kemajuan teknologi informasi dan kesinambungan bagi bangsa Indonesia. IKN memiliki visi sebagai "kota dunia untuk semua" yang dibangun dan dikelola dengan tujuan untuk menjadi kota berkelanjutan, sebagai penggerak ekonomi indonesia di masa depan dan menjadi simbol identitas nasional yang merepresentasikan keberagaman bangsa indonesia berdasarkan Pancasila dan UUD NRI Tahun 1945.[4]

Salah satu prinsip dalam pembangunan IKN yaitu membangun kota cerdas (*smart-city*), yang merupakan sebuah konsep kota yang sarat akan penggunaan Teknologi Informasi dan Komunikasi (TIK) untuk meningkatkan kualitas hidup warga, efisiensi dalam pelayanan publik dan pengelolaan sumber daya yang lebih baik. *Smart city* IKN diproyeksikan sebagai cerminan kemajuan peradaban Indonesia, menciptakan kota yang lebih berkelanjutan, ramah lingkungan dan inovatif. Beberapa contoh teknologi yang rencananya akan digunakan dalam kota cerdas (*smart-city*) IKN adalah; Sensor Pintar, System Transportasi Cerdas, Aplikasi Mobile Akses untuk Informasi dan Layanan Publik yang hampir seluruh kegiatannya menggunakan jaringan internet (*Internet of Thing/Iot*).[5]

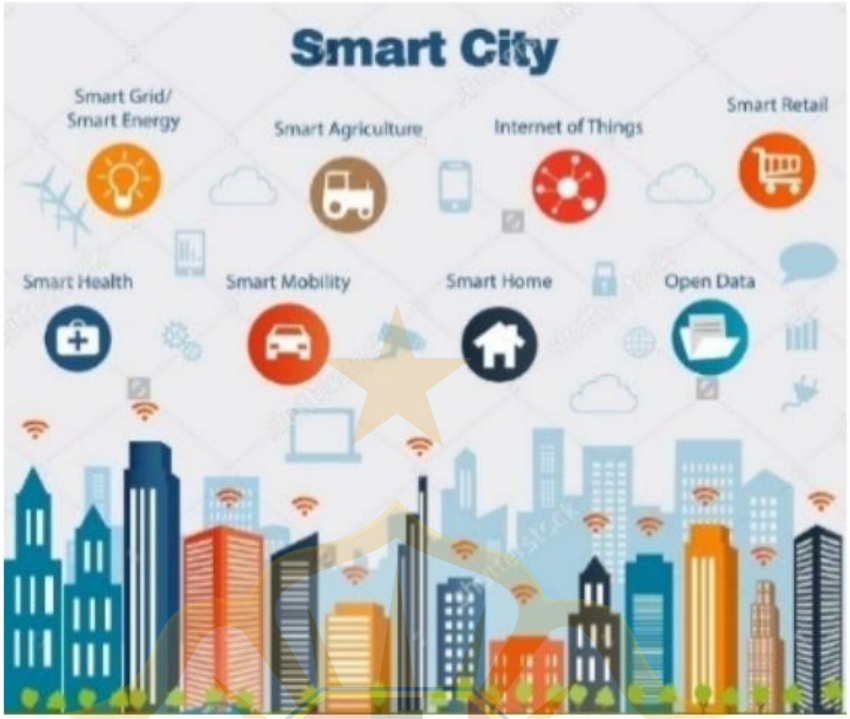
Smart ciity secara khusus merupakan fenomena baru, namun dalam perkembangannya telah meningkat secara pesat dalam beberapa waktu tahun terakhir. Saat ini, *smart city* telah tersebar luas di seluruh dunia dan

[3] Andi Wijayanto. 2022. Ketahanan Nasional di Era Geo V, Materi Slide Paparan
[4] Suharso Monoarfa. 2022. Visi dan Misi IKN sebagai Kota Dunia https://www.mkri.id//
[5] Eddy Cahyono Sugiarto. 2022. IKN Nusantara Magnet Pertumbuhan Ekonomi Baru dan SmartCity. https://www.setneg.go.id/baca/index/ikn_nusantara_magnet_pertumbuhan_ekonomi_baru_dan_smart_city

benua, dengan tujuan untuk menata ruang kota yang lebih pintar dengan menggunakan teknologi tinggi untuk menghadapi masalah krusial di tata perkotaan seperti permasalahan lalu lintas, polusi, kepadatan kota hingga kemisikinan[6].

Penerapan *smart city* sendiri di Indonesia diawali pada tahun 2017 yang dikenal dengan gerakan menuju 100 *smart-city* dengan tujuan agar pemerintah dapat memaksimalkan pengunaan dan pemanfaat teknologi di era digitalisasi dan pelayanan publik yang modern dan terintegrasi. Adapun implementasinya *smart city* di Indonesia, pada tahun 2022 Indonesia sudah memiliki 191 dari 514 wilayah perkotaan Indonesia, namun pada tahun 2022 akan lebih banyak lagi dengan menambah target 50 daerah atau kota yang ditetapkan[7]. Untuk menerapkan sistem *smart city*, harus memperhatikan beberapa enam elemen komponen serta kesiapan infrastruktur kabupaten atau kota untuk dapat menerapkan sistem *smart city*, sehingga semua operasional dapat berjalan normal, sistem keamanan dan privasi tidak menjadi masalah, serta mampu menciptakan kepercayaan masyarakat melalui penerapan *smart city* di suatu wilayah atau kota[8]. Enam elemen tersebut diantaranya adalah *Smart Grid; Smart Agriculture; Smart Health; Smart Mobility; Smart Home; Smart Retail; Internet Of Things; dan Open Data. (*Gambar I*)*

[6] Kourtit K., Nijkamp P. & Arribas D., “Smart cities in perspective – a comparative European study by means of selforganizing maps”, Innovation: The European Journal of Social Science Research, 25:2, 229-246, 2012.
[7] Dyah Ayu Suci. 2022. Data Privasi dan Keamanan Siber pada *Smart city*: Tinjauan Literatur. Jurnal SNATI (ISSN 2807-5935). Volume 2. Nomor 1
[8] M. Alamer & M. A. Almaiah. 2021. "*Cybersecurity in Smart city: A Systematic Mapping Study," International Conference on Information Technology* - ICIT



Gambar I. Elemen Smart Cities

Alamer (2021) menyatakan bahwa Konsep pembangunan *smart city* pada dasarnya bertujuan untuk meningkatkan kualitas hidup penduduk, penggunaan layanan perkotaan, pembangunan berkelanjutan hingga meminimalisir kerusakan lingkungan. Untuk dapat mewujudkan tujuan daripada *smart city*, diperlukan konsep yang mengacu pada kompetensi dan optimalisasi strategi, inovasi teknologi terbaru, dan historis mengenai data-data kehidupan[9].

Namun, konsep pembangunan *smart city* justru menjadi target yang menarik bagi penjahat dan pelaku ancaman dunia maya untuk mengeksploitasi kerentanan pada sistem untuk mencuri data infrastruktur penting dan informasi mengenai hak milik, melakukan *ransomware* operasi, atau meluncurkan serangan siber yang merusak. Serangan siber yang sukses terhadap kota-*smart city* dapat menyebabkan gangguan layanan infrastruktur, kerugian keuangan yang signifikan, paparan data pribadi warga, erosi kepercayaan warga pada sistem pintar itu sendiri, dan fisik dampak terhadap infrastruktur yang dapat menyebabkan kerusakan fisik atau korban

[9] M. Alamer & M. A. Almaiah. 2021. "*Cybersecurity in Smart city: A Systematic Mapping Study," International Conference on Information Technology* - ICIT

jiwa. Komunitas menerapkan teknologi *smart city* harus memperhitungkan risiko terkait ini sebagai bagian dari pendekatan manajemen risiko mereka secara keseluruhan[10].

Tantangan utama yang dihadapi dalam mengimplementasikan konsep *smart city* adalah permasalahan *cyber security* (keamanan siber). *Cyber Security* yang dimaksud berkaitan dengan perlindungan data, penggunaan perangkat lunak, infrastruktur untuk melakukan pengiriman, memproses hingga kualitas penyimpanan data. Hal ini dipahami sebagai salah satu proses dari mencegah, mendeteksi, dan merespon terhadap insiden serangan siber[11].

Peran keamanan siber atau *cyber security* sangat penting dalam pembangunan *smart city*. Seiring dengan kemajuan teknologi dan keterhubungan yang semakin luas, *smart city* mengandalkan infrastruktur digital dan sistem yang terhubung untuk mengelola dan menyediakan berbagai layanan perkotaan yang efisien. Namun, keberadaan infrastruktur digital ini juga membawa risiko keamanan yang signifikan.

Namun tentu dibalik setiap pembangunan dan pemanfaatan infrastruktur Teknologi Informasi dan Komunikasi selalu mengandung di dalamnya kerentanan atau kerawanan.[12] Termasuk dalam pembangunan *smart city* di IKN telah diperkirakan akan berhadapan dengan ancaman siber (*cyber threat*), hal tersebut dikarenakan ketika sebuah konsep *smart city* diimplementasikan secara otomatis akan menjadikan Internet sebagai sumber segala hal (*Internet of Thing/IoT*).

Beberapa potensi ancaman yang telah diprediksi antara lain berupa serangan terhadap infrastruktur siber, contohnya *malware*, *hacking*, pencurian data, pengambilalihan kendali sistem, dll. Selain itu adanya kemungkinan serangan yang bersifat *Artificial Intelligence*, contohnya *deep fake*, Hoax, dsb[13]. Kemudian, metode tren serangan siber ke depan akan

---

[10] United States Cybersecurity and Infrastructure Security Agency dkk. 2023. Cybersecurity Best Practices for Smart Cities. Materi Paparan.

[11] Sengan, S., V., S., Nair, S. K., V., I., J., M., & Ravi, L. (2020). *Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future Generation Computer Systems*

[12] Indri, Sulistyowati. 2021. Pengantar Keamanan Sistem Informasi. https://pustaka.ut.ac.id/ISBN 9786234802177 | E-ISBN : 9786234802184; Tangerang Selatan

[13] https://www.helios.id/blog/detail/mengenal-14-jenis-serangan-siber-dan-cara-mencegahnya

diprediksikan berdasarkan tiga hal, yakni serangan kelompok APT (Advance Persisten Threat), *ransomware*, dan *supply chain attack*[14]. Selanjutnya, Badan Siber dan Sandi Negara (BSSN) telah memprediksi ancaman *cybercrime* terhadap *smart city* IKN Nusantara. BSSN bahkan terus mengembangkan fasilitas pelatihan keamanan sibernya, *Smart City Simulator,* namun tentu selain itu perlu untuk meningkatkan kesadaran akan pentingnya keamanan siber.[15]

Bagaimana ranah siber mengandung kerawanan, terbukti dengan angka kasus kejahatan siber di Indonesia yang secara umum menunjukkan tren yang meningkat sepanjang tahun 2020 dan 2021. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta[16]. Berdasarkan data dari Badan Pusat Statistik (BPS), sepanjang tahun 2021, terdapat lebih dari 1,6 miliar anomali trafik atau serangan siber yang terjadi di seluruh wilayah Indonesia[17].

Adapun jenis serangan siber yang paling banyak terjadi di Indonesia adalah *malware*, yaitu perangkat lunak berbahaya yang dapat merusak atau mencuri data dari perangkat korban. Jenis *malware* yang paling sering ditemukan adalah *ransomware*, yaitu *malware* yang mengenkripsi data korban dan meminta tebusan untuk mengembalikannya[18]. Selain *malware*, serangan siber lain yang juga marak di Indonesia adalah *phishing*, yaitu penipuan online yang bertujuan untuk mendapatkan informasi pribadi atau keuangan korban dengan cara meniru situs web atau email resmi[19].

---

[14] https://www.liputan6.com/tekno/read/5207217/ibm-ungkap-tren-serangan-siber-2023-phishing-dan-ransomware-masih-merajalela

[15] https://bssn.go.id/bssn-ajak-insan-pers-kunjungi-fasilitas-pelatihan-simulasi-keamanan-siber-smart-city-ikn-nusantara/

[16] Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi - Kompas.com. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi.

[17] Indonesia Hadapi 1,6 Miliar Serangan Siber dalam Setahun, Ini Malware .... https://tekno.kompas.com/read/2022/04/08/06020007/indonesia-hadapi-1-6-miliar-serangan-siber-dalam-setahun-ini-malware-terbanyak.

[18] Indonesia Diberondong 1,3 Miliar Serangan Siber Sepanjang 2021. https://www.liputan6.com/bisnis/read/4706493/indonesia-diberondong-13-miliar-serangan-siber-sepanjang-2021.

[19] Badan Pusat Statistik.

Dari data jumlah kasus siber, sepanjang tahun 2017 hingga 2020, tercatat ada 16.845 laporan tindak pidana penipuan siber yang masuk ke Direktorat Tindak Pidana Siber (Ditipidsiber) Polri. Selanjutnya sepanjang Januari hingga September 2020, Ditipidsiber Polri menerima 2.259 laporan kasus kejahatan siber yang mengakibatkan kerugian ekonomi mencapai Rp15,17 miliar Sepanjang Januari hingga Desember 2022, [20] Polri menindak 8.831 kasus kejahatan siber di seluruh Indonesia. Polda Metro Jaya menjadi satuan kerja dengan jumlah penindakan paling banyak terhadap kasus kejahatan siber yaitu 3.709 perkara[21].

Gangguan keamanan siber dapat memiliki dampak yang signifikan bagi masyarakat, khususnya di IKN, antara lain: Serangan keamanan siber yang berhasil dapat menyebabkan kerugian finansial bagi individu maupun organisasi. Hal ini dapat mencakup kehilangan dana dari akun bank yang diretas, kerugian bisnis akibat dari penyalahgunaan data pelanggan, atau biaya pemulihan dan perbaikan sistem yang terkena dampak serangan. Serangan keamanan siber yang berhasil dapat menyebabkan gangguan layanan penting seperti gangguan pada sistem perbankan, infrastruktur kritis, atau layanan publik lainnya. Hal ini dapat mengganggu kehidupan sehari-hari masyarakat dan menyebabkan ketidaknyamanan, kerugian ekonomi, atau bahkan ancaman terhadap keselamatan. Serangan keamanan siber dapat digunakan untuk menyebarkan informasi palsu atau hoaks yang dapat mempengaruhi persepsi dan keputusan masyarakat. Hal ini dapat berdampak negatif terhadap kepercayaan publik, stabilitas sosial, dan proses demokrasi. Serangan keamanan siber yang berhasil dapat mengakibatkan kehilangan data yang berharga, baik itu data pribadi, data bisnis, atau data penelitian. Kehilangan data ini dapat memiliki konsekuensi jangka panjang,

(https://www.bps.go.id/publication/2021/12/15/8d1bc84d2055e99feed39986/statistik-kriminal-2021.html.)

[20] Kejahatan Siber di Indonesia Naik Berkali-kali Lipat - Polri. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat.

[21] Data Penanganan Kasus Kejahatan Siber di Patrolisiber.id https://www.cyberthreat.id/read/10925/Data-Penanganan-Kasus-Kejahatan-Siber-di-Patrolisiberid-kok-Mandek-di-Mei-2020.

seperti hilangnya informasi yang penting, kerugian keuangan, atau kerusakan reputasi.[22]

Penting untuk meningkatkan kesadaran tentang ancaman keamanan siber dan mengambil langkah-langkah pencegahan yang tepat untuk melindungi diri dan organisasi dari serangan. Kolaborasi antara pemerintah, industri, dan individu sangat penting dalam mengatasi masalah keamanan siber untuk melindungi masyarakat secara keseluruhan. Dengan adanya berbagai ancaman pada ranah siber tersebut maka pemilihan sistem, teknologi dan infrastruktur harus didasarkan pada evaluasi risiko dan tingkat keamanannya yang harus diuji sebelum digunakan. Termasuk penyediaan kesiapan sumber daya manusia yang terlatih dan terampil dalam keamanan siber sangat penting. Untuk itu diperlukan kerjasama dan kolaborasi keamanan siber antara pemerintah dengan seluruh pemangku kepentingan termasuk swasta dan masyarakat untuk meningkatkan keamanan siber di IKN.

Dalam pembangunan *smart city*, aspek keamanan siber harus diintegrasikan secara holistik ke dalam perencanaan dan pelaksanaan proyek. Hal ini akan memastikan bahwa *smart city* dapat berfungsi dengan lancar, melindungi data dan infrastruktur, serta memberikan manfaat yang lebih besar bagi warga kota secara keseluruhan.

Dengan adanya sistem keamanan siber yang efektif dan komprehensif di IKN, maka pembangunan nasional yang berkelanjutan dapat terwujud karena data dan informasi penting akan terlindungi dari serangan siber, serta dapat membangun kepercayaan masyarakat dan investor terhadap keamanan siber di IKN. Berdasarkan latar belakang tersebut maka penulis menyajian Kertas Karya Ilmiah Perorangan (Taskap) dengan judul **Membangun Sistem Keamanan Siber Di Ibu Kota Nusantara (IKN) Dalam Rangka Menunjang Pembangunan Nasional Yang Berkelanjutan.**

2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas maka yang menjadi rumusan permasalahan dalam penulisan Taskap ini adalah **“Bagaimana**

[22] Pfleeger, C. P., & Pfleeger, S. L. (2018). Security in Computing. Pearson.

Membangun Sistem Keamanan Siber Di Ibu Kota Nusantara (IKN) Dalam Rangka Menunjang Pembangunan Nasional Yang Berkelanjutan?" Selanjutnya, untuk memudahkan analisa dan pembahasan, rumusan permasalahan di atas dijabarkan ke beberapa pokok-pokok pertanyaan kajian, yaitu:

a. Bagaimana tatakelola regulasi yang dapat mendukung sistem keamanan siber?
b. Bagaimana tata kelola kelembagaan yang tepat untuk mengimplementasikan sistem keamanan siber yang tangguh?
c. Bagaimana menyiapkan infrastruktur sistem keamanan siber?
d. Bagaimana menyiapkan sumber daya manusia untuk mendukung sistem keamanan siber?
e. Bagaimana skenario dukungan anggaran untuk sistem keamanan siber?

3. Maksud dan Tujuan

a. **Maksud:** Pembahasan dalam Kertas Karya Ilmiah Perseorangan (TASKAP) ini, bermaksud memberikan gambaran cara membangun sistem keamanan siber di Ibu Kota Nusantara (IKN) dalam rangka menunjang pembangunan nasional yang berkelanjutan.
b. **Tujuan**; Adapun tujuan penulisan TASKAP ini, adalah untuk menyampaikan gagasan dan konsep mengenai membangun sistem keamanan siber di Ibu Kota Nusantara (IKN) dalam rangka menunjang pembangunan nasional yang berkelanjutan.

4. Ruang Lingkup dan Sistematika

a. **Ruang Lingkup**

Tulisan ini adalah menggambarkan sistem keamanan siber di Ibu Kota Nusantara (IKN) yang sangat penting untuk menunjang pembangunan nasional yang berkelanjutan. Pembahasan terfokus dengan perkembangan teknologi dan ketergantungan kita pada sistem digital, ancaman keamanan siber semakin meningkat dan semakin kompleks serta langkah-langkah yang tepat untuk menjaga keamanan

siber di IKN agar dapat mengatasi berbagai ancaman keamanan siber yang muncul.

b. **Sistematika**

Uraian pembahasan dan analisa terhadap permasalahan di dalam penulisan Kertas Karya Ilmiah Perseorangan ini, disusun melalui sistematika atau tata urut sesuai dengan Juknis Penulisan Taskap dari Lemhannas RI, sebagai berikut:

1) **BAB I: PENDAHULUAN.** Bab ini berisi uraian mengenai latar belakang permasalahan, perumusan masalah, maksud dan tujuan penulisan, ruang lingkup pembahasan, sistematika penulisan, metode dan pendekatan yang digunakan, serta beberapa terkait pengertian pada tulisan ini untuk penyamaan persepsi guna memahami pembahasan.
2) **BAB II: LANDASAN PEMIKIRAN.** Dalam bab ini dibahas mengenai peraturan perundang-undangan, kerangka teoretis yang akan digunakan sebagai landasan dalam merumuskan pemecahan persoalan, data dan fakta seputar permasalahan, serta lingkungan strategis yang menghasilkan pengaruh positif dan negatif, serta untuk mencari strategi dan upaya dalam memecahkan masalah.
3) **BAB III: PEMBAHASAN.** Dalam bab ini idiuraikan imengenai ianalisa sejumlah persoalan Pembahasan didasarkan pada data dan fakta yang diperoleh serta landasan teori yang relevan, guna menemukan faktor penyebab masalah dan merumuskan solusinya.
4) **BAB IV: PENUTUP.** Berisikan simpulan dan rekomendasi. Simpulan berisikan jawaban terhadap pokok-pokok pembahasan yang ditemukan dan dibahas dalam bab-bab sebelumnya. Sedangkan rekomendasi berisikan masukan-masukan dalam rangka membangun sistem keamanan siber di Ibu Kota Nusantara (IKN) dalam rangka menunjang pembangunan nasional yang berkelanjutan.

5. Metode dan Pendekatan

a. **Metode;** Metode yang digunakan dalam penulisan TASKAP ini adalah menggunakan metode penelitian kualitatif, di mana dalam analisisnya tidak menggunakan teknik penghitungan atau statistik.[23] Penelitian kualitatif dalam proses pencarian, pengumpulan dan analisis masalah, memakai teknik studi kepustakaan, melalui cara pengumpulan dan analisa dengan referensi berbagai tulisan akademis berupa dokumen, artikel ilmiah, melalui data tertulis atau internet terkait fakta empiris, teori, peraturan perundang-undangan dan lain sebagainya yang berhubungan dengan permasalahan. Metode lain yang digunakan dalam penulisan ini adalah Analisis SWOT yang merupakan salah satu analisis yang banyak digunakan oleh organisasi, perusahaan maupun lembaga pemerintahan. Analisis ini banyak digunakan karena merupakan analisis yang cukup mendasar dalam menentukan solusi terbaik dalam mengatasi persoalan yang dihadapi organisasi. Metode ini diperkenalkan oleh Albert Humphrey ketika melakukan penelitian di Stamford University pada sekitar tahun 1960-1970.[24]

b. **Pendekatan;** Dalam penyusunan dan pembahasan Kertas Karya Ilmiah Perseorangan ini penulis menggunakan pendekatan deskriptif analisis yang dilakukan secara komprehensif. Tulisan kualitatif deskriptif penyajian hasil penelitiannya berupa narasi dan uraian hingga interpretasi atas suatu fenomena yang menjadi objek penelitian. Jenis penelitian deskripsi tetap memegang unsur-unsur penelitian yang sistematis, aktual dan akurat (Kriyantono, 2007).[25]

6. Pengertian:

a. **Sistem Keamanan Siber**: Sistem Keamanan Siber, juga dikenal sebagai keamanan informasi atau keamanan jaringan, merujuk pada serangkaian tindakan, praktik, dan teknologi yang dirancang untuk melindungi sistem komputer, jaringan, dan data dari ancaman yang berasal dari dunia siber. Secara umum, sistem keamanan siber

[23]Lexy.J. Moleong. 1993. Metodologi Penelitian Kualitatif. Remaja Rosdakarya, Bandung,hlm. 2
[24] Nur'Aini, Fajar. 2016. Teknik Analisis SWOT: Pedoman Menyusun Strategi yang Efektif dan Efisien Serta Cara Mengelola Kekuatan dan Ancaman. Bantul: Anak hebat Indonesia
[25]Kriyantono. Rachmat. 2007. Teknik Praktis Riset Komunikasi. Jakarta: Kencana Prenada Media Group. Hal 58-69

bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan data dan sistem komputer. Ini melibatkan perlindungan terhadap serangan siber yang dapat mengakibatkan kebocoran data, pencurian informasi sensitif, gangguan operasional, atau kerusakan sistem. Sistem keamanan siber juga berperan dalam mendeteksi serangan yang sedang terjadi, merespons secara cepat, dan memulihkan sistem setelah serangan.[26]

b. **Ibu Kota Nusantara (IKN)**; Ibu Kota Nusantara (IKN) adalah ibu kota negara masa depan Indonesia yang rencananya akan diresmikan pada 17 Agustus 2024 bersamaan dengan perayaan Hari Kemerdekaan[27]. Kota ini berlokasi di sebagian Kabupaten Penajam Paser Utara dan di sebagian Kabupaten Kutai Kartanegara, Provinsi Kalimantan Timur[28]. IKN Nusantara juga akan menjadi pusat pemerintahan, bisnis, budaya, dan pendidikan nasional dan menjadi kawasan strategis nasional dengan visi menjadi kota cerdas, hijau, dan berkelanjutan.[29]

c. **Pembangunan Nasional**; Pembangunan nasional adalah suatu usaha menyeluruh dengan memadukan faktor karsa, sarana, dan upaya (Ends-Means-Ways) merupakan metodologi untuk mengubah setiap potensi menjadi kemampuan, agar memperoleh keberhasilan (outcome) sesuai yang diharapkan. Dalam lingkup tata kehidupan bermasyarakat, berbangsa, dan bernegara, secara konseptual mengubah Trigatra (potensi) menjadi Pancagatra (kemampuan). Pembangunan Nasional sebagai suatu sistem adalah upaya seluruh bangsa Indonesia dalam mengejar cita-cita nasional dan tujuan nasional. Masyarakat pada dasarnya adalah pelaku utama pembangunan dan Pemerintah berkewajiban mengarahkan, membimbing, serta menciptakan suasana yang menunjang. Pembangunan adalah mengubah suatu keadaan menjadi keadaan yang lebih baik dengan memanfaatkan berbagai

[26] Whitman, M., & Mattord, H. (2019). Principles of Information Security. Cengage Learning

[27] https://www.kompas.com/tren/read/2022/02/08/190000665/ikn-adalah-singkatan-dari-ibu-kota-negara-baru-apa-itu-ikn-nusantara-.

[28] IKN - Ibu Kota Negara. https://ikn.go.id/.

[29] IKN - Ibu Kota Negara. https://ikn.go.id/.

potensi sumber daya yang tersedia secara optimal, efisien, efektif, dan akuntabel.[30]

d. **Pembangunan Berkelanjutan;** Pembangunan berkelanjutan adalah pembangunan yang memenuhi kebutuhan hidup masa sekarang dengan mempertimbangkan pemenuhan kebutuhan hidup generasi mendatang. Prinsip utama pembangunan berkelanjutan ialah mempertahankan kualitas hidup bagi seluruh manusia pada masa sekarang dan pada masa depan secara berkelanjutan. Pembangunan berkelanjutan dilaksanakan dengan prinsip kesejahteraan ekonomi, keadilan sosial, dan pelestarian lingkungan. Pembangunan berkelanjutan juga menghargai keragaman budaya sebagai alat untuk mencapai kepuasan intelektual, emosional, moral, dan spiritual[31]. Pembangunan berkelanjutan tidak hanya berkaitan dengan pembangunan ekonomi, tetapi juga meliputi pembangunan sosial dan perlindungan lingkungan. Ketiga aspek tersebut saling berkaitan dan merupakan pilar pendorong bagi pembangunan berkelanjutan[32]. Pembangunan berkelanjutan berbeda dari pembangunan hijau, yang lebih mengutamakan keberlanjutan lingkungan di atas pertimbangan ekonomi dan budaya.

e. ***E-government,*** atau pemerintahan elektronik, mengacu pada penggunaan teknologi informasi dan komunikasi (TIK) oleh pemerintah untuk menyediakan layanan publik, berinteraksi dengan warga, dan mengelola urusan pemerintahan secara efektif. Tujuan utama dari e-government adalah meningkatkan efisiensi, transparansi, partisipasi, dan kualitas layanan publik. *E-government* melibatkan penggunaan berbagai teknologi seperti internet, komputer, perangkat mobile, dan sistem informasi untuk memfasilitasi berbagai kegiatan pemerintah. Ini termasuk penyediaan layanan online, pengumpulan dan pengolahan data elektronik, komunikasi elektronik antara pemerintah dan warga,

---

[30] Lemhannas RI.2023. Hanjar Bidang Studi Sistem Manajemen Nasional. Jakarta Lemhannas RI

[31] Pembangunan Berkelanjutan : Tujuan, Manfaat, Ciri dan Dampak. https://www.gurupendidikan.co.id/pembangunan-berkelanjutan/.

[32] Pembangunan Berkelanjutan: Pengertian, Tujuan, dan Contohnya. https://www.linovhr.com/pembangunan-berkelanjutan/.

serta pengelolaan sumber daya dan proses administrasi pemerintah dengan cara yang lebih efisien.[33]

f. ***Smart city:*** *Smart city* adalah kawasan perkotaan yang menggunakan teknologi informasi dan komunikasi (TIK) untuk meningkatkan efisiensi operasional, berbagi informasi dengan publik, dan meningkatkan kualitas layanan pemerintah dan kesejahteraan warga. Tujuan *Smart city* adalah untuk mengoptimalkan fungsi kota dan mendorong pertumbuhan ekonomi sambil meningkatkan kualitas hidup warganya menggunakan teknologi pintar dan analisis data. Nilai *smart city* terletak pada apa yang mereka pilih untuk dilakukan dengan teknologinya, bukan hanya seberapa banyak teknologi yang mereka miliki.[34]

g. ***Internet of Things (IoT)*****:** *Internet of Things* (IoT) dapat didefinisikan sebagai kemampuan dari berbagai peralatan (*devices*) yang saling terintegrasi melalui sebuah jaringan internet. IoT merupakan sebuah teknologi untuk melakukan pengendalian sistem komunikasi, optimalisasi penggunaan *hardware* (perangkat keras), dan proses pertukaran data melalui jaringan internet[35].

[33] UNDP. (2005). E-Government for Development: Implementation Handbook. Tersedia di: https://www.undp.org/publications/e-government-development-implementation-handbook

[34] https://www.techtarget.com/iotagenda/definition/smart-city

[35] Hardyanto, R. H. 2017. Konsep Internet of Things Pada Pembelajaran Berbasis Web. Jurnal Dinamika Informatika Vol. 6 No.1

,

BAB II
LANDASAN PEMIKIRAN

7. Umum

Dalam era digital yang semakin maju, tantangan terbesar bagi sebuah negara bukan hanya berada pada ranah fisik, namun juga dalam dunia siber. Keamanan siber bahkan kini menjadi prioritas utama dalam membangun suatu sistem di sebuah negara, termasuk di Indonesia yang tengah mempersiapkan pembangunan Ibu Kota Nusantara (IKN). Bukan hanya sebagai pusat pemerintahan, IKN juga dirancang sebagai kota pintar (*smart city*) yang mengadopsi teknologi terkini. Oleh karena itu, persiapan dalam aspek keamanan siber menjadi hal yang krusial.

Sebagai kota pintar yang baru dan berbasis teknologi, IKN menjadi target potensial bagi berbagai ancaman siber, membuat perlunya pembangunan sistem keamanan siber yang kuat dan handal sebagai bagian integral dalam proses pembangunan IKN. Pemahaman tentang ancaman dan cara kerja serangan siber menjadi fondasi dalam merumuskan dan menerapkan sistem keamanan siber yang efektif.

Sebelum menganalisa dan membahas hal-hal yang mempengaruhi pembangunan keamanan siber di IKN dalam rangka menunjang pembangunan nasional yang berkelanjutan, terlebih dahulu perlu dipaparkan sejumlah regulasi dan produk hukum yang bisa menjadi landasan hukum, sejumlah data dan fakta berkaitan dengan tema yang diangkat, sejumlah teori yang bisa menjadi landasan berpikir dan melihat sejumlah faktor yang berpengaruh terhadap perumusan pemecahan masalah.

8. Peraturan dan Perundang-undangan

a. **Undang-Undang RI nomor 17 Tahun 2011 tentang Intelijen Negara**

Pasal 4 menjelaskan mengenai peran intelijen negara yaitu melakukan upaya, kegiatan, pekerjaan dan tindakan dalam rangka deteksi dini dan peringatan dini guna mencegah, menangkal dan menanggulangi setiap hakikat ancaman yang bisa muncul dan mengancam kepentingan dan keamanan nasional.

Dalam konteks pembangunan keamanan siber di IKN, jenis ancaman tersebut juga mencangkup ancaman terhada berbagai kejahatan dan serangan siber.

b. **Undang-Undang RI nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik**

Padal Pasal 40 ayat (2) dijelaskan bahwa pemerintah bertanggung jawab untuk menjaga kepentingan publik dari gangguan yang timbul akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang dapat mengganggu ketertiban umum. Hal ini dilakukan sesuai dengan peraturan perundang-undangan yang berlaku.

Dalam konteks pembangunan keamanan siber di IKN, penerapan pasal tersebut dapat menjadi landasan hukum yang relevan untuk melindungi infrastruktur dan sistem keamanan siber di IKN dari gangguan dan serangan siber yang dapat mengganggu ketertiban umum. Dengan membangun sistem keamanan siber yang kuat dan efektif di IKN, pemerintah dapat melindungi kepentingan umum, termasuk melindungi data sensitif, infrastruktur kritis, dan layanan publik dari ancaman siber.

c. **Undang-Undang RI Nomor 3 Tahun 2022 tentang Ibu Kota Negara**

Dalam Pasal 20 dijelaskan bahwa Penyelenggaraan pertahanan dan keamanan di Ibu Kota Nusantara dilaksanakan dengan mengacu pada sistem dan strategi pertahanan dan keamanan yang terintegrasi dengan Rencana Induk Ibu Kota Nusantara dan Rencana Tata Ruang Kawasan Strategis Nasional (KSN) Ibu Kota Nusantara.

Pernyataan dalam pasal UU IKN tersebut menegaskan pentingnya penyelenggaraan pertahanan dan keamanan di Ibu Kota Nusantara berdasarkan sistem dan strategi yang terintegrasi dengan Rencana Induk Ibu Kota Nusantara dan Rencana Tata Ruang KSN Ibu Kota Nusantara. Hal ini menunjukkan bahwa pembangunan keamanan siber di Ibu Kota Nusantara harus menjadi bagian yang integral dari upaya penyelenggaraan pertahanan dan keamanan secara menyeluruh.

d. **Undang-undang RI Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi**

Pasal 58 menyatakan bahwa pemerintah memiliki peran dalam melaksanakan tugas penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Hal tersebut menunjukan bahwa keamanan data pribadi merupakan salah satu aspek penting dalam sistem keamanan siber. Dalam upaya membangun sistem keamanan siber di IKN, pemerintah memiliki kewajiban memperhatikan dan melaksanakan langkah-langkah untuk melindungi data pribadi yang ada di dalam infrastruktur digital IKN.

Dengan adanya undang-undang yang mengatur tentang pelindungan data pribadi, pemerintah dapat menetapkan kebijakan dan aturan yang mengatur pengumpulan, penggunaan, dan pengamanan data pribadi di IKN. Hal ini bertujuan untuk mencegah penyalahgunaan data pribadi oleh pihak yang tidak berwenang dan menjaga privasi serta integritas informasi yang ada di dalam sistem keamanan siber IKN.

e. **Peraturan Presiden RI Nomor 63 Tahun 2022 Tentang Perincian Rencana Induk Ibu Kota Nusantara**

Dalam Lampiran III terkait Rencana Induk IKN dinyatakan bahwa pembangunan keamanan siber di IKN merupakan bagian yang tidak terpisahkan dari rencana pengembangan Nusantara sebagai kota cerdas (*smart city*). Keamanan siber dalam pelaksanaan kota cerdas, terutama dalam menjaga data dan informasi yang ada dalam pemerintahan. BSSN (Badan Siber dan Sandi Negara) menjadi institusi yang ditugaskan menjadi leading sector dalam mewujudkan keamanan siber yang sejalan dengan konsep kota cerdas di Ibu Kota Nusantara.

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

Pada Pasal 1 diterangkan bahwa strategi Keamanan Siber Nasional merupakan panduan kebijakan nasional yang memanfaatkan semua potensi sumber daya siber dengan tujuan untuk menciptakan

Keamanan Siber demi melindungi dan mengembangkan kepentingan bangsa. Sementara yang dimaksud dengan Manajemen Krisis Siber merujuk pada tata cara pengelolaan sumber daya dan metode penanganannya yang dijalankan sebelum, selama, dan setelah munculnya Krisis Siber.

g. **Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024**

Regulasi ini menjelaskan bahwa salah satu sasaran strategis BSSN dalam kurun waktu 2020 hingga 2024 adalah meningkatkan maturitas keamanan siber di Indonesia. Artinya, setiap entitas di berbagai sektor di Indonesia diharapkan memiliki kemampuan untuk mengidentifikasi risiko keamanan siber dan melindungi semua aset yang dimiliki dari ancaman dan insiden siber. Hal ini bertujuan untuk mencapai kematangan entitas dalam penanganan insiden siber secara sistematis dan terstruktur. Dengan menerapkan pendekatan maturitas, akan terbentuk sebuah ekosistem siber yang terpadu, efektif, dan kokoh di Indonesia.

9. Data dan Fakta

a. **Kondisi Tatakelola Regulasi yang Dapat Mendukung Sistem Keamanan Siber Saat Ini.**

Gubernur Lembaga Ketahanan Nasional Republik Indonesia (Lemhannas), Andi Widjajanto menyatakan Indonesia belum memiliki Undang-Undang (UU) Keamanan Siber, yang membuatnya menjadi satu-satunya negara di ASEAN tanpa kebijakan keamanan siber nasional. Ketidakhadiran UU tersebut dapat mengurangi minat investor untuk berinvestasi di Indonesia karena dapat melemahkan kepercayaan mereka terhadap komitmen pemerintah dalam menangani masalah keamanan siber[36].

[36] https://kliklegal.com/lemhannas-cuma-ri-yang-tak-punya-uu-keamanan-siber-di-asean/ diakses pada tanggal 15 Juli 2023 pukul 20.55 WIB

Dalam konteks pembangunan Ibu Kota Negara (IKN) Nusantara yang berbasis teknologi tinggi dan konsep *smart city*, keberadaan UU Keamanan Siber menjadi penting. Keterbatasan indeks keamanan siber Indonesia dan kurangnya komitmen pemerintah dalam memenuhi anggaran untuk peningkatan investasi keamanan siber dapat menghambat investasi, termasuk dalam bidang teknologi dan digital seperti pengembangan *smart city*.

Pemerintah perlu menutup celah regulasi dan meningkatkan kepercayaan investor dalam hal keamanan siber. Penerapan konsep maturitas penanganan insiden siber secara mandiri oleh semua sektor, termasuk pemerintah, IKN, dan ekonomi digital, dapat membentuk ekosistem siber yang terintegrasi, efektif, dan solid di Indonesia. Diperlukan upaya dalam aspek SDM, proses, dan teknologi untuk membangun keamanan siber yang kuat dan responsif.

Meskipun telah disahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pengesahan tersebut tidak dianggap memiliki dampak signifikan terhadap tindakan peretasan. Keamanan siber tetap menjadi tanggung jawab Badan Siber dan Sandi Negara (BSSN), dengan fokus pada penerapan enkripsi yang kuat dalam lalu lintas data.

Indonesia memiliki beberapa undang-undang dan regulasi yang membantu dalam mengatur keamanan siber, termasuk UU ITE dan UU PDP yang baru saja disahkan. Namun tantangan di bidang regulasi siber adalah bagaimana menyesuaikan hukum dan kebijakan dengan perkembangan teknologi yang cepat dan ancaman siber yang terus berubah.

Pengesahan UU Keamanan Siber diarahkan untuk mengatur perlindungan hak asasi manusia, inovasi ilmu pengetahuan dan teknologi, serta kemajuan perekonomian nasional dalam konteks keamanan siber. Adanya UU Keamanan Siber di Indonesia untuk menjaga keamanan siber, menarik investasi, dan membangun ekosistem siber yang solid. Dalam menghadapi tantangan keamanan siber, regulasi yang jelas dan komprehensif serta komitmen pemerintah

diperlukan untuk melindungi kepentingan masyarakat dan negara Indonesia.

b. **Kondisi Tata Kelola Kelembagaan dalam Mengimplementasikan Sistem Keamanan Siber Saat Ini.**

Tata kelola kelembagaan dalam mengimplementasikan sistem keamanan siber di Indonesia melibatkan berbagai instansi pemerintah dan organisasi swasta. Badan Siber dan Sandi Negara (BSSN) merupakan lembaga pemerintah utama yang bertanggung jawab dalam mengkoordinasikan dan melaksanakan kebijakan di bidang keamanan siber di Indonesia. Tugas BSSN mencakup deteksi dan pencegahan ancaman siber, serta pengembangan dan penegakan standar keamanan siber.

Meski BSSN memiliki peran utama, banyak lembaga pemerintah lainnya juga memiliki tanggung jawab dalam keamanan siber, termasuk Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Pertahanan, Kepolisian dan Badan Intelijen Negara (BIN). Oleh karena itu, koordinasi antar lembaga ini sangat penting untuk menciptakan respon yang efektif terhadap ancaman siber.

Selain pemerintah, sektor swasta dan masyarakat sipil juga memiliki peran penting dalam menjaga keamanan siber. Perusahaan teknologi dan penyedia layanan internet harus bekerja sama dengan pemerintah dalam mendeteksi ancaman dan melindungi infrastruktur dan data mereka. Organisasi masyarakat sipil juga dapat membantu dalam upaya pendidikan dan peningkatan kesadaran tentang ancaman siber.

Secara keseluruhan, tata kelola kelembagaan dalam mengimplementasikan sistem keamanan siber di Indonesia membutuhkan koordinasi yang lebih baik antara berbagai lembaga pemerintah, sektor swasta, dan masyarakat sipil. Peran BSSN sebagai lembaga yang seharusnya paling mengerti dan bertanggung jawab terhadap keamanan siber di Indonesia, hingga kini belum sepenuhnya terwujud.

Hal ini bisa dilihat ketika masyarakat dihebohkan dengan ulah hacker Bjorka yang beberapa kali melakukan peretasan dan pencurian data, termasuk pada institusi Badan Intelijen Negara dan lembaga kepresidenan, yang terjadi tahun 2022 lalu. BSSN terkesan kurang sigap dalam mengatasi persoalan, hingga memberikan keterangan yang menyejukan kepada masyarakat. Sebaliknya, yang terlihat adanya kesan saling lempar tanggung jawab antara BSSN dan Kemenkominfo[37].

c. **Kondisi Infrastruktur Sistem Keamanan Siber Saat Ini**

Infrastruktur sistem keamanan siber di Indonesia sedang berada dalam fase transisi. Sejumlah perusahaan di negeri ini semakin menyadari pentingnya keamanan siber, yang tercermin dalam peningkatan anggaran untuk keamanan siber pada tahun 2020. Menurut studi oleh Palo Alto Networks, sebanyak 84% perusahaan Indonesia meningkatkan anggaran keamanan sibernya dibandingkan 2019. Ini menunjukkan bahwa kesadaran akan pentingnya keamanan siber dalam dunia bisnis semakin meningkat[38].

Namun, meskipun arah pembangunan keamanan siber dinilai sudah berada di jalur yang tepat, ada beberapa tantangan yang harus dihadapi. Satu masalah besar adalah bahwa teknologi yang digunakan oleh banyak perusahaan Indonesia masih tertinggal. Misalnya, mayoritas perusahaan Indonesia masih menggunakan sistem keamanan yang tertinggal (*legacy*), seperti penggunaan perangkat lunak antivirus atau antimalware. Hal ini kontras dengan adopsi teknologi keamanan siber yang lebih canggih di negara-negara lain, seperti Singapura, yang telah menerapkan solusi berbasis komputasi awan, seperti SD-WAN (*software-defined wide-area network*), dengan tingkat yang lebih tinggi. Selain itu, 44% responden dalam studi tersebut menyatakan tidak percaya diri dengan keamanan siber yang dimiliki perusahaannya. Ini menunjukkan adanya kebutuhan untuk

[37] https://www.cnbcindonesia.com/news/20220910125507-4-370980/bjorka-berulah-2-instansi-ini-saling-lempar-tanggung-jawab diakses pada tanggal 17 Juli 2023 pukul 21.25 WIB.
[38] https://www.kompas.id/baca/gaya-hidup/2020/07/15/palo-alto-keamanan-siber-indonesia-ke-arah-yang-tepat diakses pada tanggal 17 Juli 2023 pukul 21.25 WIB.

peningkatan kualitas dan efektivitas sistem keamanan siber yang digunakan oleh perusahaan Indonesia[39].

Solusi untuk tantangan ini melibatkan peningkatan investasi dalam teknologi dan praktek keamanan siber yang lebih baik. Misalnya, peningkatan penggunaan otentikasi dua faktor dan pemahaman lebih baik tentang ancaman kejahatan siber seperti serangan phishing dan ransomware. Selain itu, ada kebutuhan untuk melanjutkan peningkatan anggaran dan investasi dalam keamanan siber, serta melanjutkan upaya untuk memperbarui dan meningkatkan teknologi dan infrastruktur yang digunakan.

d. **Kondisi Sumber Daya Manusia untuk Mendukung Sistem Keamanan Siber Saat Ini**

Indonesia saat ini menghadapi krisis kekurangan talenta di sektor digital. Meskipun negara ini memiliki populasi yang besar dan potensi pertumbuhan digital yang signifikan, kemampuan untuk menghasilkan dan mempersiapkan talenta digital masih jauh di bawah kebutuhan. Hasil kajian dari Kementerian Komunikasi dan Informatika (Kemenkominfo), Indonesia setidaknya membutuhkan 600 ribu talenta digital setiap tahunnya, namun dalam praktiknya, perguruan tinggi Indonesia hanya berhasil memenuhi sekitar 150.000 hingga 200.000 talenta digital setiap tahunnya. Kondisi ini menunjukkan adanya kesenjangan besar antara kebutuhan dan ketersediaan sumber daya manusia (SDM) digital yang ada40. Menurut data Kemenkominfo, lebih dari setengah tenaga kerja Indonesia hanya memiliki kemampuan digital dasar hingga menengah. Sementara itu, individu dengan keahlian digital tingkat lanjutan hanya mencakup kurang dari 1% dari total angkatan kerja yang ada41.

Apa yang diungkap oleh Kemenkominfo selaras dengan hasil riset McKinsey dan Bank Dunia yang menyebutkan bahwa Indonesia dalam

---

[39] Ibid

[40] https://www.kominfo.go.id/content/detail/16892/indonesia-butuh-9-juta-digital-talent/0/sorotan_media diakses pada tanggal 6 Agustus 2023 pukul 19.50 WIB.

[41] https://www.cnbcindonesia.com/tech/20220518135208-37-339847/krisis-talenta-digital-butuh-tambahan-47-juta-orang-di-2030 diakses pada tanggal 26 September 2023 pukul 20.30 WIB.

periode 2015 hingga 2030 akan membutuhkan sekitar sembilan juta talenta digital, atau jika dirata-rata dibutuhkan 600 ribu tenaga ahli di bidang siber per tahun. Sementara menurut informasi dari Ekrut, sebuah platform pencarian pekerjaan, terjadi peningkatan permintaan tenaga kerja di sektor teknologi informasi sejak tahun sebelumnya. Detailnya, permintaan untuk data analyst dan scientists meningkat sebesar 76,59%, pemasaran merek sebesar 66%, perencana strategi 62,78%, full stack engineer 50,85%, serta keamanan siber naik 23,91%42.

Akibatnya, menurut Gubernur Lemhannas, Andi Widjajanto, Indonesia memerlukan waktu sekitar 90 tahun untuk mengejar dan memenuhi permintaan talenta digital. Selain itu, kekurangan SDM talenta digital juga pada akhirnya membuat Indonesia masih banyak menjadi pengguna dan banyak bergantung pada teknologi yang ada di dunia saja. Hal ini menjadi masalah terberat untuk Indonesia saat ini43.

Di Indonesia, minat mahasiswa untuk mendalami bidang keamanan siber masih belum mencapai ekspektasi yang diharapkan. Meskipun keamanan siber telah menjadi isu penting di era digital saat ini, banyak mahasiswa masih belum menyadari betapa krusialnya peran ini dalam menjaga integritas dan keamanan data. Hal ini dibuktikan dari hasil survei yang dilakukan oleh BDO Indonesia (firma akuntan publik, pajak, dan penasihat) terhadap talenta teknologi informatika di Indonesia yang mengungkapkan bahwa 9 dari 10 lulusan teknologi memilih untuk menjadi developer perangkat lunak dan hanya satu dari 10 yang berminat mendalami keamanan siber. Kurangnya kesadaran, kombinasi dengan kurangnya informasi dan eksposur terhadap potensi karier di bidang ini, mungkin menjadi beberapa alasan mengapa bidang keamanan siber belum menjadi pilihan utama bagi sebagian besar mahasiswa di tanah air.

[42] https://katadata.co.id/desysetyowati/digital/62451ee00178f/indonesia-kekurangan-500-ribu-talenta-digital-per-tahun diakses pada tanggal 26 September 2023 pukul 20.30 WIB.
[43] https://www.cnbcindonesia.com/tech/20230811145653-37-462260/ri-krisis-butuh-90-tahun-kejar-ketinggalan-talenta-digital diakses pada tanggal 26 September 2023 pukul 20.30 WIB.

Sementara menurut InfraDigital Foundation, tren pekerjaan yang berkaitan dengan keamanan siber menunjukkan peningkatan signifikan. Pada 2022, diperkirakan ada kebutuhan sebanyak 1.232.666 profesional di sektor teknologi informasi. Proyeksi tersebut menunjukkan lonjakan menjadi sekitar 1.979.418 individu pada 2025, sejalan dengan frekuensi serangan siber yang kian intens di Indonesia.

Menurut data dari BSSN pada tahun 2020, ada 650 lembaga pemerintah dan 1.000 entitas yang menyediakan layanan publik yang menawarkan kesempatan kerja di bidang tersebut. Dengan demikian, diperkirakan setiap entitas memerlukan setidaknya lima tenaga kerja dengan keterampilan di bidang keamanan siber. Dengan estimasi tersebut, total kebutuhan SDM di bidang keamanan siber mencapai 18.054 orang44.

Kekurangan talenta digital membuat tidak semua institusi, lembaga, kementerian dan pemerintah daerah di Indonesia memiliki Computer Security Incident Response Team (CSIRT), yang merupakan tim atau entitas yang menyediakan dukungan dan layanan untuk mencegah, mengelola dan menanggapi insiden keamanan siber. Kondisi inilah yang membuat berbagai institusi pemerintah rentan mengalami peretasan dan berbagai insiden keamanan siber.

Guna mengatasi kesenjangan talenta digital tersebut, Kemenkominfo menyelenggarakan Digital Talent Scholarship yang pada tahun 2022 memberikan pelatihan digital teknis bagi 200 ribu peserta dengan tema terkait keamanan siber, kecerdasan buatan, mahadata, komputasi awan dan programing. Program pelatihan terbagi menjadi tujuh akademi, yaitu Vocational School Graduate Academy, Government Transformation Academy, Digital Entrepreneurship Academy, Professional Academy, Tematic Academy, Fresh Graduate Academy, dan Talent Scouting Academy. nisiatif pengembangan talenta digital di tingkat nasional adalah sebuah inisiatif besar yang memerlukan kerja sama antar berbagai lembaga.

[44] https://m.cyberthreat.id/read/8535/Berapa-Kebutuhan-SDM-Keamanan-Siber-di-Indonesia-Ini-Penjelasan-BSSN diakses pada tanggal 26 September 2023 pukul 20.30 WIB.

Penyiapan talenta digital juga dilakukan di luar kampus. Permintaan talenta digital yang tinggi mendorong hadirnya tawaran kursus intensif online atau bootcamp untuk mempelajari ragam kompetensi digital. Selain itu, sejumlah perusahaan teknologi turut andil dalam memperkuat kecakapan teknologi digital melalui pembelajaran di luar kampus yang bisa diikuti secara terbuka. Google Indonesia misalnya, memiliki program Bangkit yang turut menyiapkan talenta digital Indonesia melalui program magang dan studi independen bersertifikat atau MSIB yang memberikan kesempatan kepada mahasiswa belajar di industri teknologi secara nyata.

Program Bangkit sejak tahun 2020 dibuka untuk menjembatani talenta muda Indonesia meraih mimpi menjadi profesional andal di bidang teknologi informasi. Sejak pertama kali program diluncurkan pada hingga saat ini, Google telah melatih lebih dari 6.000 mahasiswa dan memberikan lebih dari 2.900 sertifikasi di bidang machine learning, mobile development, dan cloud computing45.

Dalam upaya meningkatkan kesiapan sumber daya manusia (SDM) untuk mendukung sistem keamanan siber, Badan Siber dan Sandi Negara (BSSN) juga telah menyiapkan sejumlah langkah strategis. BSSN telah menyiapkan berbagai program pelatihan di Pusat Pengembangan SDM BSSN guna mempersiapkan kebutuhan talenta digital khususnya di bidang keamanan siber yang dibutuhkan IKN. Program ini mencakup simulasi keamanan siber smart city dan simulasi bertahan dan menyerang. Simulasi ini bertujuan untuk mempersiapkan peserta dalam menangani potensi kerawanan dan ancaman siber yang semakin tinggi seiring dengan peningkatan pemanfaatan teknologi digital.

Dalam simulasi keamanan siber smart city, peserta diajarkan bagaimana membangun dan menjaga sistem keamanan infrastruktur siber dalam konteks smart city. Sedangkan dalam simulasi bertahan dan menyerang, peserta melatih respons mereka dalam menghadapi

[45] https://www.kompas.id/baca/humaniora/2023/02/20/permintaan-tinggi-penyiapan-talenta-digital-juga-dilakukan-di-luar-kampus diakses pada tanggal 26 September 2023 pukul 20.30 WIB.

insiden siber melalui 250 skenario yang telah disiapkan BSSN dengan menggunakan Cybersecurity Online Simulation Platform (CSOSP).

Dalam rangka peningkatan kapabilitas SDM ini, BSSN telah menghasilkan 1.120 lulusan pada 2021 dan 402 lulusan hingga pertengahan 2022, dengan total 1.522 lulusan. Untuk tahun 2022 ini, BSSN menargetkan 1.120 lulusan lagi dari program pelatihan ini46.

Selain itu, BSSN juga telah mempersiapkan pusat pengembangan SDM yang dilengkapi dengan simulator kota pintar, keamanan siber, dan finansial. Aparatur sipil negara (ASN) dari seluruh kementerian dan lembaga yang akan ditugaskan di IKN Nusantara di bidang keamanan siber akan dilatih di pusat pengembangan ini.

Dengan upaya-upaya ini, BSSN berharap bisa menyiapkan SDM yang kompeten dan siap mengawal sistem elektronik digital di IKN, sehingga semua proses bisa berjalan lancar dan aman. Namun, BSSN juga menyadari bahwa peningkatan SDM ini harus dilakukan secara berkelanjutan mengingat kerawanan dan ancaman siber terus berkembang.

Sebelumnya, sejak tahun 2021 BSSN terlibat dalam pengembangan SDM keamanan siber melalui pembentukan Computer Security Incident Response Team (CSIRT) di berbagai instansi lembaga/kementerian dan pemerintah daerah. CSIRT menjadi tim yang bertugas untuk merespon dan mengelola insiden keamanan siber. Mereka memiliki peran penting dalam mendeteksi, menganalisis, memulihkan dari insiden, serta melakukan upaya proaktif untuk mencegah terjadinya insiden. Pada tahun 2020 hingga 2022, telah terbentuk 57 CSIRT dan pada tahun 2023 ini akan dibentuk 31 CSIRT lagi. Hal ini menunjukkan bahwa peningkatan jumlah dan kompetensi SDM dalam bidang keamanan siber menjadi fokus penting pemerintah47.

---

[46] https://www.cnnindonesia.com/teknologi/20220701162217-192-816124/ribuan-anggota-pasukan-siber-disiapkan-kawal-ikn diakses pada tanggal 17 Juli 2023 pukul 22.50 WIB.

[47] https://bssn.go.id/bertekad-wujudkan-keamanan-siber-sektor-pemerintah-sebagai-bagian-holistik-keamanan-siber-nasional-bssn-kembali-bentuk-31-csirt-organisasi-sektor-pemerintah-pusat-di-tahun-2023/ diakses pada tanggal 17 Juli 2023 pukul 22.50 WIB

Untuk mendukung operasional CSIRT, SDM perlu dilatih dan dibekali dengan pengetahuan dan keterampilan yang relevan, seperti pengetahuan tentang strategi keamanan siber nasional, tata kelola keamanan siber, dan manajemen risiko keamanan siber. Selain itu, SDM juga perlu memahami dan mampu mengimplementasikan Sistem Pemerintah Berbasis Elektronik (SPBE), yang mencakup penjaminan keutuhan dan ketersediaan data dan informasi. SDM juga perlu mampu mendukung tujuan penjaminan kerahasiaan, ketersediaan, keutuhan, dan keaslian data dan layanan SPBE.

Menyikapi hal ini, BSSN telah melakukan langkah-langkah seperti menyelenggarakan kegiatan persiapan pembentukan CSIRT, diskusi panel tentang strategi keamanan siber, dan asistensi pembentukan CSIRT. Namun, upaya ini harus terus ditingkatkan dan diperluas untuk memastikan bahwa SDM keamanan siber di Indonesia dapat menghadapi tantangan yang semakin kompleks di era digital ini.

e. **Kondisi Skenario Dukungan Anggaran untuk Sistem Keamanan Siber Saat Ini.**

Politik anggaran untuk dukungan sistem keamanan siber di Indonesia hingga kini masih lemah. Pada tahun 2023 misalnya, Badan Siber dan Sandi Negara (BSSN) hanya mendapatkan anggaran sekitar 30% dari anggaran yang dibutuhkan, atau sekitar Rp 1 triliun dari total anggaran Rp 3-4 triliun yang seharusnya. Ini menunjukkan adanya *gap* pendanaan yang signifikan dalam mewujudkan sistem keamanan siber yang mumpuni. Tidak mengherankan jika indeks keamanan siber Indonesia dinilai rendah.

Melihat kondisi ini, penting bagi pemerintah Indonesia untuk mencari alternatif pembiayaan guna menutup defisit anggaran tersebut. Beberapa opsi yang mungkin di pertimbangkan adalah kemitraan publik-swasta, hibah dari negara mitra atau lembaga internasional, atau bahkan mendorong investasi swasta dalam industri keamanan siber.

Peningkatan investasi di bidang keamanan siber ini tidak hanya penting untuk melindungi infrastruktur nasional dan data pribadi warga, tetapi juga memiliki implikasi yang luas bagi ekonomi digital Indonesia.

Menurut pernyataan yang dilontarkan, jika Indonesia tidak dapat menutup 'lubang' keamanan ini, investasi di bidang digital dan teknologi mungkin akan berkurang atau bahkan berhenti.

Untuk mendukung industri start-up dan teknologi digital yang berkembang pesat, pemerintah harus menunjukkan komitmen kuat untuk meningkatkan indeks pertahanan siber. Diharapkan, dalam empat tahun ke depan, indeks pertahanan siber Indonesia bisa meningkat melebihi rata-rata global. Hal ini akan memberikan kepercayaan kepada investor bahwa Indonesia mengambil keamanan siber dengan serius, dan oleh karena itu, merupakan tempat yang aman untuk investasi di bidang digital dan teknologi.

Oleh karena itu, meski tantangannya besar, upaya ini penting bagi pertumbuhan dan keberlanjutan ekonomi digital Indonesia. Peran aktif pemerintah dalam mendukung sistem keamanan siber merupakan investasi yang berharga, yang hasilnya akan lebih dari sekedar perlindungan terhadap infrastruktur dan data, tetapi juga peningkatan kepercayaan investor dan perkembangan ekonomi digital nasional.

10. Kerangka Teoritis

a. Konsep *Smart City*

Smart city adalah konsep kota cerdas yang menggunakan teknologi informasi dan komunikasi (TIK) untuk meningkatkan kualitas hidup penduduknya dan efisiensi kota itu sendiri. Konsep *smart city* mencakup berbagai aspek kehidupan di kota, termasuk transportasi, infrastruktur, energi, lingkungan, dan pelayanan publik. Tujuannya adalah untuk menciptakan kota yang lebih berkelanjutan, ramah lingkungan, dan efisien. Penggunaan teknologi: *Smart city* menggunakan teknologi informasi dan komunikasi (TIK) untuk menghubungkan infrastruktur dan pelayanan publik. Contoh teknologi yang sering digunakan adalah jaringan sensor, sistem informasi geografis (GIS), dan platform data terbuka, *Artificial Intelegent, Command Centre*, dll. Konsep *smart city* diharapkan dapat membantu

kota-kota di seluruh dunia untuk menjadi lebih efisien, berkelanjutan, dan ramah lingkungan[48].

Konsep kota pintar pertama kali diperkenalkan pada tahun 1990 untuk menggabungkan perangkat keras dan perangkat lunak berbasis teknologi informasi dan komunikasi (TIK) canggih dalam perencanaan kota (Bibri & Krogstie, 2017)[49].

Sebagai kota yang dirancang menjadi *smart city*, Ibu Kota Nusantara diarahkan untuk menjadi lebih efektif, efisien, "hijau", dan lebih aman dibandingkan kota-kota lain di Indonesia dan di dunia pada umumnya. Teknologi canggih akan menjadi basis utama dalam mencapai target kenyamanan, keselamatan, dan keamanan kota dengan tujuan memberikan pelayanan publik yang terkoordinasi, termasuk didalamnya upaya untuk mencapai target sebagai Kota Layak Huni (*livable city*).

Smart City di seluruh dunia umumnya merupakan respon dari tantangan utama yang saat ini dihadapi dunia seperti perubahan iklim, sumber daya yang terbatas, Urbanisasi, dan pertumbuhan populasi yang tinggi. Selain itu, *smart city* bertujuan untuk mengamankan daya saing ekonomi di ruang perkotaan dan membiarkan warga kota merasakan gaya hidup yang lebih berkelas.

Kota pintar tidak hanya tentang menyebarkan platform pintar untuk melakukan layanan terkait kota secara efisien, tetapi ini sangat besar konsep yang terdiri dari beberapa objek fisik dan elektronik yang berinteraksi dan berkomunikasi melalui jaringan kabel dan nirkabel. Pada sisi lain kota pintar adalah tentang beberapa ilmu yang berhubungan dengan komputer yang digunakan sepanjang proses kecerdasan buatan seperti kecerdasan buatan, komputasi awan, komputasi tertanam dan biometrik. Selain teknologi modern yang disewa yang dianggap sebagai inti dari seluruh peraturan kota pintar seperti RFID (Sistem Identifikasi Frekuensi Radio) dan perangkat

---

[48] Nam, T., & Pardo, T. A. (2011). Conceptualizing *smart city* with dimensions of technology, people, and institutions. In Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times (pp. 282-291).
Hillson, D., & Murray-Webster, R. (2017). Understanding and Managing Risk Attitude. Routledge.

[49] Bibri, S. E., & Krogstie, J. (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. Sustainable Cities and Society, 31, 183–212. https://doi.org/10.1016/j.scs.2017.02.016

genggam pintar (ponsel, laptop, tablet, dll.). Jelas, kota pintar adalah sistem besar yang kompleks dan saling bergantung dan ini mengarah pada beberapa masalah dan tantangan politik, sosial, ekonomi, dan teknis. Biaya dan pendanaan, kebutuhan populasi yang terus berubah, kolaborasi antar pemangku kepentingan, antarmuka yang ramah pengguna, interoperabilitas, keamanan dan privasi adalah contoh masalah yang dihadapi kota pintar.[50]

Oleh sebab itu, masalah terkait keamanan di kota pintar adalah nyata dan aktual serta perlu dipertimbangkan dan dianalisis secara instan. Dengan demikian, keamanan, privasi, dan masalah terkait menjadi topik hangat terutama karena teknologi dan sistem kota pintar menjadi sangat penting untuk mengoptimalkan kota dan meningkatkan kualitas hidup.

b. **Teori Hukum Siber**

Lawrence Lessig (1999) [51], seorang profesor hukum, mengemukakan bahwa regulasi di dunia maya dipengaruhi oleh empat faktor: Hukum, Norma, Pasar, dan Arsitektur. Oleh karena itu, tata kelola IKN sebaiknya tidak hanya berfokus pada regulasi formal, tetapi juga melibatkan norma sosial, insentif pasar, dan infrastruktur teknologi. Ini dikenal sebagai 'model regulasi empat faktor' Lessig dan bisa digunakan untuk memahami dan merancang regulasi adaptif untuk keamanan siber, termasuk di IKN. Hukum adalah peraturan formal yang dibuat oleh pemerintah atau badan regulator.

Dalam konteks IKN, teori ini memiliki implikasi mendalam. Pertama, regulasi hukum formal merupakan instrumen penting untuk mendefinisikan batasan, hak, dan kewajiban dalam dunia maya. Oleh karena itu, pembentukan regulasi keamanan siber di IKN harus didasarkan pada hukum yang jelas, komprehensif, dan adaptif dengan perkembangan teknologi. Kedua, norma sosial berperan penting dalam menentukan bagaimana individu dan organisasi berperilaku dalam dunia maya. Sebagai contoh, jika masyarakat IKN memandang

[50] AlDairi, Anwaaar dan Tawalbeh, Lo'ai. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Jurnal ScienceDirect Procedia Computer Science 109C (2017), 1086-1091.
[51] Larry Lessig, (1999). Code: And Other Laws of Cyberspace. New York: Basic Books.

pentingnya keamanan siber dan menjadikannya sebagai norma, maka peluang terjadinya pelanggaran akan berkurang.

Dengan demikian, membangun tata kelola regulasi yang mendukung sistem keamanan siber di IKN bukan hanya tentang merumuskan hukum, tetapi juga tentang memahami dan mengintegrasikan norma sosial, insentif pasar, dan arsitektur teknologi. Semua faktor ini harus diperhitungkan agar regulasi keamanan siber di IKN benar-benar efektif dan adaptif dengan tantangan masa depan.

c. **Teori Kepastian Hukum**

Menurut Jan Michiel Otto seperti dalam Soeroso (2011), kepastian hukum dapat didefinisikan sebagai serangkaian situasi antara lain:[52]

1) Ketersediaan aturan yang jelas, terstruktur, dan dapat diakses, yang dikeluarkan oleh negara dengan otoritasnya.
2) Lembaga-lembaga berwenang, seperti pemerintah, konsisten dalam menerapkan aturan tersebut dan juga mematuhi aturan tersebut.
3) Masyarakat pada umumnya mematuhi dan mengadaptasi perilaku mereka sesuai dengan aturan-aturan tersebut.
4) Hakim yang independen secara konsisten menerapkan aturan hukum saat menangani kasus hukum.
5) Keputusan yang dikeluarkan oleh pengadilan diimplementasikan dengan tepat.

Dengan kata lain, kepastian hukum membutuhkan adanya aturan hukum yang dirancang oleh otoritas yang kompeten dan dihormati. Oleh karena itu, aturan-aturan ini memiliki kekuatan hukum yang memastikan bahwa hukum berlaku sebagai pedoman yang wajib ditaati oleh semua pihak.[53]

d. **Teori Peran**

Menurut Ralph Linton (1956)[54], "role" atau peranan adalah elemen dinamis dari "status" atau kedudukan. Ketika seseorang menjalankan hak dan tanggung jawabnya sesuai dengan statusnya, berarti ia sedang

[52] Soeroso. 2011. Pengantar Ilmu Hukum. Jakarta: PT. Sinar Grafika
[53] Asikin zainal. 2012, Pengantar Tata Hukum Indonesia, Rajawali Press, Jakarta
[54] Linton, Ralph (1956). The Study of Man, an Introduction. New York: Aplleton Century Crofts. H.114.

menjalankan perannya. Oleh karena itu, konsep peranan dan kedudukan sangat terkait dan bergantung satu sama lain. Kedudukan tanpa peranan, atau sebaliknya, peranan tanpa kedudukan, tidak mungkin ada. Setiap orang memiliki beragam peranan yang mereka ambil dari berbagai aspek dalam kehidupan sosialnya. Ini menandakan bahwa peranan tersebut menentukan bagaimana seseorang berkontribusi kepada masyarakat dan sekaligus menentukan apa yang masyarakat harapkan darinya.

Sementara Paul B. Horton dan Robert L. Horton (1982)[55] mendefinisikan "peran" sebagai perilaku yang diharapkan dari seseorang dalam status tertentu. Lebih lanjut, mereka mendefinisikan "status" sebagai posisi atau kedudukan seseorang dalam suatu organisasi, kelompok atau struktur sosial. Status lebih merujuk pada posisi yang dipegang seseorang, bukan pada individu itu sendiri. Posisi tersebut bisa dalam konteks organisasi pemerintahan, jabatan perusahaan, keluarga, kelompok sosial, atau posisi lain yang diakui oleh masyarakat secara umum.

Dalam konteks tata kelola kelembagaan dalam membangun sistem keamanan siber di IKN, setiap lembaga yang terlibat dalam sistem keamanan siber di IKN harus memiliki kedudukan atau status yang jelas. Dalam hal ini, "status" merujuk pada peran dan tanggung jawab resmi dari lembaga tersebut dalam kerangka keamanan siber.

Seperti yang ditekankan oleh Linton dan Horton, konsep peran sangat berkaitan dengan ekspektasi. Dalam konteks IKN, masyarakat mempunyai ekspektasi bahwa lembaga-lembaga yang bertanggung jawab atas keamanan siber akan menjalankan peranannya dengan baik. Ekspektasi ini mencakup aspek-aspek seperti responsivitas, efisiensi, dan transparansi. Mengingat keamanan siber adalah isu yang kompleks, maka setiap lembaga mungkin mempunyai beragam peranan yang harus dijalankan.

Oleh karena setiap lembaga memiliki peranannya masing-masing, koordinasi dan kolaborasi antar-lembaga menjadi sangat penting.

[55] Horton, Paul B. dan Horton, Robert L. (1982). Introductory Sociology. USA: Dow Jones-Irwin. H.19.

Konsep "peran" menekankan pentingnya masing-masing lembaga untuk mengenali dan menghormati peran serta status dari lembaga lainnya, untuk memastikan kerja sama yang harmonis dan efektif.

e. **Teori Sinergitas**

Berdasarkan pendapat Deardoff dan Williams yang dikutip oleh Usman (2011) [56], sinergitas diartikan sebagai proses di mana kombinasi antara dua entitas atau lebih menghasilkan dampak yang lebih signifikan daripada jika entitas tersebut menjalankannya secara individu.

Slamet Mulyana (2008)[57] menjelaskan bahwa sinergitas dapat direalisasikan melalui mekanisme koordinasi dan komunikasi. Dalam koordinasi, penting untuk mendefinisikan relasi antara para pihak yang terlibat. Sementara itu, komunikasi adalah proses pertukaran data antar individu, termasuk pertukaran informasi antara satu entitas dengan entitas lainnya.

Dalam konteks membangun tata kelola kelembagaan yang tepat untuk mengimplementasikan sistem keamanan siber yang tangguh di IKN, hubungan antara teori sinergitas dengan pendekatan tersebut adalah sebagai berikut:

1) Integrasi Lembaga: Untuk memastikan keamanan siber yang tangguh, berbagai lembaga di IKN harus bekerja bersama-sama, menggabungkan keahlian dan sumber daya mereka. Ini menciptakan sinergitas yang ditekankan oleh Deardoff dan Williams, di mana kombinasi usaha dari berbagai lembaga menghasilkan dampak yang lebih besar daripada jika mereka bekerja secara terpisah.
2) Koordinasi yang Kuat: Seperti yang disebutkan oleh Slamet Mulyana, sinergitas dapat direalisasikan melalui mekanisme koordinasi yang kuat. Dalam konteks keamanan siber di IKN,

[56] Husaini, Usman (2011). Manajemen teori, praktik dan riset pendidikan. Jakarta: Bumi aksara
[57] Firmansyah, MI. 2016. Studi Deskriptif Tentang Sinergitas Kewenangan Antara BPJS Kesehatan dengan Organisasi Profesi dalam Penyediaan Layanan Kesehatan di Kota Surabaya. Jurnal Kebijakan dan Manajemen Publik Universitas Airlangga Surabaya, Volume 4, Nomor 2, Edisi Mei-Agustus 2016, Halaman 146-156

koordinasi antara lembaga pemerintah, sektor swasta, dan komunitas harus ditingkatkan untuk memastikan bahwa semua pihak memiliki pemahaman yang sama tentang ancaman, kebutuhan, dan strategi.

3) Komunikasi Terpadu: Komunikasi efektif antara semua pemangku kepentingan adalah kunci untuk menciptakan sinergitas. Pertukaran informasi mengenai potensi ancaman, respons insiden, serta pembaruan kebijakan dan teknologi adalah esensial untuk memastikan semua pihak tetap *up-to-date* dan bergerak dalam arah yang sama.

4) Peningkatan Resiliensi dan Keefektifan: Ketika lembaga-lembaga bekerja bersama dalam sinergi, keseluruhan sistem menjadi lebih kuat. Dengan kolaborasi, lembaga dapat membagikan tanggung jawab dan mendukung satu sama lain dalam menghadapi ancaman, sehingga keseluruhan sistem keamanan siber di IKN menjadi lebih tangguh.

f. **Teori Manajemen SDM**

Menurut Suparyadi (2015) [58], manajemen sumber daya manusia (SDM) adalah suatu pendekatan yang dirancang untuk mempengaruhi sikap, tindakan, dan prestasi karyawan agar mereka dapat memberikan kontribusi sebaik mungkin terhadap pencapaian tujuan organisasi. Tujuan utama dari manajemen SDM adalah mengoptimalisasi dampak karyawan terhadap kinerja organisasi. Hal ini melibatkan berbagai aspek, mulai dari analisis pekerjaan, perencanaan kebutuhan SDM, rekrutmen, seleksi, hingga pelatihan, penilaian kinerja, dan pembinaan hubungan kerja yang harmonis.

Manajemen SDM kini semakin dilihat sebagai elemen strategis dalam bisnis karena kontribusinya yang signifikan dalam mendorong inovasi, kepuasan karyawan dan pelanggan, serta produktivitas keseluruhan. Dengan meningkatnya globalisasi, manajemen SDM menghadapi tantangan tambahan, seperti mempersiapkan karyawan untuk tugas

[58] Suparyadi. 2015. Manajemen Sumber Daya Manusia: Menciptakan keunggulan Bersaing Berbasis Kompetensi SDM. Yogyakarta: penerbit Andi.

internasional dan menyesuaikan dengan tuntutan pasar global. Lebih lanjut, dalam era digital saat ini, manajemen SDM harus memastikan bahwa karyawan tetap relevan dan adaptif dengan kemajuan teknologi, bukan menjadi usang atau tergantikan oleh inovasi teknologi.

Manajemen sumber daya manusia (SDM) memiliki peran yang sangat signifikan dalam mempersiapkan sumber daya manusia untuk mendukung sistem keamanan siber di IKN. Hubungan antara teori manajemen SDM dengan upaya tersebut dapat diuraikan sebagai berikut:

1) Analisis Pekerjaan dan Perencanaan Kebutuhan: Sebelum melakukan rekrutmen tenaga ahli keamanan siber, penting bagi IKN untuk melakukan analisis pekerjaan mendalam. Ini akan menentukan jenis keahlian, pengetahuan, dan keterampilan yang diperlukan. Selanjutnya, perencanaan kebutuhan SDM akan memastikan bahwa IKN memiliki jumlah tenaga ahli yang cukup untuk mengatasi ancaman keamanan siber yang berkembang.
2) Rekrutmen dan Seleksi: Mengingat pentingnya keamanan siber, proses rekrutmen dan seleksi harus dilakukan dengan sangat hati-hati. Kandidat yang dipilih harus memiliki kompetensi teknis dan etika kerja yang kuat. Menggunakan prinsip-prinsip manajemen SDM yang diuraikan oleh Suparyadi, proses ini akan memastikan bahwa hanya individu yang paling berkualitas yang dipekerjakan.
3) Pelatihan dan Pengembangan: Dalam dunia keamanan siber yang terus berubah, pelatihan dan pengembangan menjadi krusial. Ini bukan hanya tentang memberikan karyawan keterampilan awal, tetapi juga tentang memastikan bahwa mereka tetap update dengan perkembangan terbaru. Ini sesuai dengan pendapat Suparyadi bahwa manajemen SDM harus memastikan karyawan tetap relevan dan adaptif terhadap kemajuan teknologi.
4) Penilaian Kinerja dan Pengembangan Karir: Penilaian kinerja yang objektif dapat membantu IKN dalam mengidentifikasi area-area yang memerlukan perhatian lebih serta mengidentifikasi individu yang mungkin memerlukan pelatihan tambahan atau

pendampingan. Selanjutnya, dengan menyediakan jalur pengembangan karir yang jelas, IKN dapat memotivasi dan mempertahankan talenta-talenta terbaik di bidang keamanan siber.

5) Membangun Budaya Keamanan: Salah satu aspek kunci manajemen SDM adalah pembinaan hubungan kerja yang harmonis dan mempengaruhi sikap serta tindakan karyawan. Ini berarti bahwa selain keterampilan teknis, manajemen SDM juga harus memfokuskan pada pembentukan budaya organisasi yang menekankan pentingnya keamanan siber.

g. **Teori Anggaran**

Hilton (2000)[59] menyatakan bahwa anggaran adalah rencana yang rinci yang diungkapkan dalam bentuk kuantitatif yang menunjukkan bagaimana sumber daya akan diperoleh dan digunakan dalam periode waktu tertentu. Sementara, Hansen dan Mowen (2004)[60] menekankan bahwa anggaran adalah rencana keuangan untuk masa depan yang menentukan tujuan dan langkah-langkah yang diperlukan untuk mencapainya. Horngren, Datar & Foster (2006)[61] mendefinisikan anggaran sebagai ekspresi kuantitatif dari rencana aksi yang diajukan oleh manajemen untuk periode waktu tertentu dan merupakan alat untuk koordinasi tindakan yang diperlukan untuk menerapkan rencana tersebut.

Dari ketiga definisi tersebut, dapat disimpulkan bahwa anggaran adalah alat perencanaan yang rinci dan kuantitatif mengenai bagaimana sumber daya diperoleh dan digunakan dalam jangka waktu tertentu, dengan menetapkan tujuan dan tindakan yang diperlukan untuk mencapainya.

Adapun karakteristik dari suatu anggaran mencakup:[62]

---

[59] Welsch, Glenn A, Hilton, Ronald W, Gordon, Paul N.(2000). Anggaran:Perencanaan Dan Pengendalian Laba. Jakarta: Salemba Empat

[60] Hansen & Mowen. (2004). Manajemen Biaya, Edisi Bahasa Indonesia. Buku Kedua. Jakarta: Salemba Empat

[61] Horngren, Charles, T., Srikant, Datar, M., dan George, Foster, (2006), Akuntansi Biaya Penekanan Manajerial, Buku 1, alih bahasa P. A. Lestari, Jakarta: Erlangga

[62] Mulyadi (2010). Akuntansi Biaya. Edisi 5. Yogyakarta: UUP-STIM YKPN.

1) Dinyatakan dalam bentuk moneter tetapi juga dapat didukung dengan satuan non-moneter seperti jumlah produksi atau jumlah penjualan.
2) Berlaku untuk periode waktu tertentu, seringkali selama satu tahun.
3) Menyediakan perkiraan keuntungan yang mungkin diperoleh oleh sebuah unit bisnis.
4) Mewakili komitmen dari manajemen, yang berarti manajemen bertanggung jawab untuk mencapai tujuan yang telah dianggarkan.
5) Proposal anggaran ditinjau dan disetujui oleh pihak yang berwenang.
6) Setelah anggaran disetujui, perubahan hanya dapat dilakukan dalam kondisi tertentu.
7) Melakukan evaluasi berkala dengan membandingkan antara perkiraan anggaran dengan realisasi aktualnya.

11. Lingkungan Strategis

a. **Faktor Global**

Dalam dunia yang semakin global dan terinterkoneksi, upaya pembangunan sistem keamanan siber di Ibu Kota Negara (IKN) tak lepas dari berbagai pengaruh dinamika global. Perkembangan teknologi global misalnya, sangat mempengaruhi cara sistem keamanan siber dibangun dan diterapkan. Sebagai contoh, kemajuan dalam teknologi seperti *Artificial Intelligence* (AI), *Blockchain*, dan *Internet of Things* (IoT) menawarkan berbagai kemungkinan baru dalam mengamankan infrastruktur siber, tetapi juga membawa ancaman dan tantangan keamanan baru yang harus diatasi.

Tren ancaman keamanan siber global juga mempengaruhi bagaimana keamanan siber IKN semestinya dibangun. Berdasarkan informasi yang diberikan oleh Palo Alto Networks, terdapat lima tren utama dalam ancaman keamanan siber global pada tahun 2023. Pertama, terdapat serangan yang semakin meningkat dalam adopsi teknologi 5G seiring

dengan meningkatnya penggunaan teknologi ini. Kedua, serangan terhadap perangkat medis yang terkoneksi juga menjadi ancaman keamanan siber yang signifikan. Dalam konteks ini, digitalisasi dalam industri kesehatan telah membuka peluang bagi serangan siber, dengan data sensitif dan sistem lama yang sering kali menjadi target utama. Ketiga, serangan terhadap rantai pasokan *cloud* juga diperkirakan akan meningkat. Keempat, perdebatan tentang penguasaan data. Seiring dengan meningkatnya ketergantungan pada data dan informasi digital, isu-isu terkait perlindungan data dan penguasaan data akan menjadi semakin penting dalam konteks keamanan siber. Kelima, Metaverse diprediksi akan menjadi "wahana bermain baru" bagi penjahat siber. Dengan perkiraan belanja tahunan untuk produk virtual mencapai 54 miliar dolar AS, Metaverse dapat menjadi target utama bagi serangan siber.[63] Dalam konteks IKN, perlu ada upaya untuk memahami dan beradaptasi dengan ancaman siber global, serta membangun kapabilitas untuk melindungi infrastruktur siber dari serangan internasional.

Faktor global lain yang berpengaruh adalah standar internasional dalam keamanan siber. Organisasi internasional seperti *International Standards Organization* (ISO) dan *Internet Engineering Task Force* (IETF) telah merumuskan sejumlah standar keamanan siber. Mengadopsi standar ini dalam sistem keamanan siber IKN dapat membantu memastikan bahwa upaya keamanan siber di IKN berada pada tingkat yang sama dengan standar global, dan sekaligus memfasilitasi kerjasama internasional dalam hal keamanan siber.

Terakhir, perkembangan hukum dan peraturan internasional terkait keamanan siber juga menjadi pengaruh penting. Kompleksitas dan variasi dalam metode dan teknik kejahatan siber hingga kini belum mampu diimbangi dengan adanya peraturan hukum yang cukup, terutama dalam konteks hukum internasional. Faktanya, hukum internasional belum sepenuhnya siap untuk membentuk instrumen

[63] https://swa.co.id/swa/trends/prediksi-5-tren-keamanan-siber-di-asia-pasifik-tahun-2023 diakses pada tanggal 17 Juli 2023 pukul 19.55 WIB

hukum yang dapat menjadi landasan hukum bagi berbagai negara. Ada beberapa ketentuan mengenai cybercrime, seperti Konvensi *Cybercrime* yang berlaku di Eropa, namun ini masih bersifat regional dan undang-undang tentang *cybercrime* yang ada di setiap negara, yang tentu hanya berlaku di negara bersangkutan[64]. Oleh karena itu, kebutuhan akan kerangka hukum dalam menghadapi kejahatan siber menjadi tantangan baru dalam dunia hukum. Dengan mempertimbangkan dan menanggapi dinamika global ini, pembangunan sistem keamanan siber di IKN dapat menjadi lebih efektif dan relevan dalam konteks global, sekaligus memberikan kontribusi terhadap pembangunan nasional yang berkelanjutan.

b. **Faktor Regional**

Dinamika regional memiliki pengaruh terhadap upaya membangun sistem keamanan siber di Ibu Kota Nusantara (IKN). Wilayah ASEAN, yang mencakup sepuluh negara anggota dengan tingkat pembangunan dan kapabilitas teknologi yang berbeda-beda, memiliki tantangan tersendiri dalam membangun dan menjaga keamanan siber.

Berdasarkan data National Cyber Security Index (NCSI) pada tahun 2022, posisi Indonesia dalam hal keamanan siber memiliki skor 38.96 dan menempati urutan keenam di kawasan Asia Tenggara. Sementara secara internasional, Indonesia menempati posisi ke-83 dari total 160 negara. Penilaian yang dilakukan oleh NCSI menggunakan berbagai indikator, antara lain: regulasi hukum nasional seputar keamanan siber, keberadaan badan pemerintah yang berfokus pada keamanan siber, kerjasama antar pemerintah dalam bidang keamanan siber, dan bukti-bukti publik seperti *website* resmi pemerintah atau program lainnya yang terkait.

Dalam hal keamanan siber terbaik di Asia Tenggara, Malaysia menduduki peringkat pertama dengan skor 79,22, yang juga membawanya ke peringkat ke-18 secara global. Disusul Singapura menempati posisi kedua di Asia Tenggara dengan skor keamanan siber

[64] Maskun, Manuputty, Nooor dan Sumardi, (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. Jurnal MMH, Jilid 42, Nomor 4, Oktober 2013. Hal.512

sebesar 71,43, yang diikuti oleh Thailand, Filipina, dan Brunei Darussalam yang masing-masing memiliki skor 64,9, 42,86, dan 41,56. Sementara itu, beberapa negara di Asia Tenggara memiliki peringkat keamanan siber yang lebih rendah daripada Indonesia, seperti Vietnam dengan skor 36,36, Laos 18,18, Kamboja 15,58, dan Myanmar 10,39[65]. Kondisi keamanan siber yang dimiliki sejumlah negara tetangga akan menjadi cambuk bagi pemerintah Indonesia dalam memperkuat keamanan siber nasional.

Hal lain yang berdampak adalah kolaborasi dan integrasi antar negara anggota dalam bidang keamanan siber. Dalam dekade terakhir, ASEAN telah berusaha memperkuat kerjasama regional dalam bidang ini, termasuk melalui berbagai inisiatif seperti kerjasama penegakan hukum siber dan pertukaran informasi ancaman siber. Peningkatan kolaborasi ini membantu IKN dalam membangun sistem keamanan siber yang kuat karena memungkinkan akses ke pengetahuan, keahlian, dan sumber daya yang dibagikan di seluruh wilayah. Selain itu, inisiatif seperti ini juga mendukung upaya IKN dalam merespons dan memulihkan dari serangan siber dengan lebih cepat dan efektif.

Selain itu, pertumbuhan ekonomi digital di wilayah ASEAN juga mempengaruhi upaya pembangunan sistem keamanan siber di IKN. Dengan meningkatnya penetrasi internet dan digitalisasi ekonomi, ancaman siber juga meningkat. Oleh karena itu, IKN harus mempersiapkan sistem keamanan siber yang mampu menghadapi tantangan ini untuk mendukung pertumbuhan dan pembangunan ekonomi berkelanjutan. Dinamika ini mendorong peningkatan investasi dalam infrastruktur keamanan siber dan pengembangan keahlian keamanan siber di IKN.

c. **Faktor Nasional**

1) **Geografi**

Kondisi geografi Ibu Kota Nusantara (IKN) di Kalimantan mempengaruhi bagaimana mengembangkan sistem keamanan

[65] https://databoks.katadata.co.id/datapublish/2022/03/07/keamanan-siber-indonesia-peringkat-ke-6-di-asia-tenggara diakses pada tanggal 17 Juli 2023 pukul 20.05 WIB.

siber untuk mendukung pembangunan nasional yang berkelanjutan. Salah satu elemen penting dalam pembangunan sistem keamanan siber di IKN adalah ketersediaan infrastruktur internet yang kuat dan handal perlu lebih dahulu diwujudkan. Hal ini masih menjadi pekerjaan rumah Kementerian Komunikasi dan Informasi untuk menyiapkan dan menyediakan infrastruktur dan akses internet yang handal. Seperti diketahui bahwa di Indonesia masih terjadi kesenjangan infrastruktur digital, di mana kualitas akses internet di luar pulau Jawa akan cenderung memiliki kualitas yang lebih rendah dibandingkan di Jawa.

Dalam konteks IKN yang akan dikembangkan sebagai kota pintar, maka yang dibutuhkan bukan hanya sekedar koneksi internet yang lancar dan stabil, IKN membutuhkan gateway untuk lalu lintas data internasional tersendiri. Jika lalu lintas data internet harus lebih dahulu diarahkan ke Jakarta atau ke Manado dan baru terkoneksi dengan jaringan internet internasional tentu hal tersebut akan mengurangi kecepatan akses internet di IKN. Oleh sebab itu Kemenkominfo perlu menginisiasi *gateway* internasional baru di IKN.

Jadi, secara keseluruhan, kondisi geografi IKN mempengaruhi bagaimana infrastruktur internet dan sistem keamanan siber harus dirancang dan diimplementasikan untuk mendukung pembangunan nasional yang berkelanjutan. Hal ini juga mempengaruhi jumlah anggaran yang dibutuhkan untuk menyiapkan dan membangun infrastruktur yang dibutuhkan.

2) **Demografi**

Kondisi demografi di Ibu Kota Nusantara (IKN) mempengaruhi upaya pembangunan sistem keamanan siber dalam berbagai cara penting. Demografi mempengaruhi perencanaan dan pelaksanaan infrastruktur digital dan strategi keamanan siber, serta pemahaman dan adaptasi masyarakat terhadap teknologi dan praktik keamanan siber.

Pertama, kepadatan penduduk dan distribusinya di IKN akan berdampak pada perencanaan dan penyebaran infrastruktur telekomunikasi dan siber. Area dengan kepadatan populasi tinggi mungkin memerlukan lebih banyak sumber daya dan perhatian dalam hal menjamin keandalan dan keamanan jaringan. Selain itu, tingkat urbanisasi di IKN akan mempengaruhi permintaan dan penyerapan teknologi digital dan layanan berbasis internet, yang pada gilirannya akan mempengaruhi kebutuhan keamanan siber.

Kedua, struktur umur populasi IKN juga berpengaruh. Populasi yang lebih muda cenderung lebih akrab dengan teknologi digital dan lebih mungkin untuk mengadopsi praktik baru, termasuk dalam hal keamanan siber. Namun, mereka juga mungkin lebih rentan terhadap risiko tertentu, seperti penipuan online atau cyberbullying. Oleh karena itu, pendidikan dan peningkatan kesadaran tentang keamanan siber akan sangat penting untuk demografi ini.

Ketiga, tingkat pendidikan dan kemampuan masyarakat IKN dalam menggunakan teknologi digital dan memahami isu-isu keamanan siber juga akan berdampak pada strategi dan taktik yang digunakan untuk membangun sistem keamanan siber. Ini mungkin melibatkan pengembangan program pendidikan dan pelatihan, serta kampanye kesadaran masyarakat.

Keempat, faktor demografi lainnya seperti tingkat penggunaan internet, akses ke layanan broadband, dan kepemilikan perangkat digital juga akan berdampak pada perencanaan dan implementasi sistem keamanan siber. Jumlah pengguna internet dan perangkat yang digunakan untuk mengakses internet akan mempengaruhi jumlah potensi ancaman dan kerentanan yang perlu dijaga dalam sistem keamanan siber.

Singkatnya, dalam membangun keamanan siber di IKN, kondisi demografi berupa estimasi perkiraan jumlah penduduk hingga gambaran kemampuan literasi digital penduduknya akan menjadi bahan pertimbangan dalam perencanaan dan implementasi

sistem keamanan siber guna mewujudkan tujuan pembangunan nasional yang berkelanjutan.

3) **Politik**

Dinamika politik di Indonesia memiliki peran penting dalam mempengaruhi upaya pembangunan sistem keamanan siber di Ibu Kota Nusantara (IKN). Politik, dalam hal ini, dapat berfungsi sebagai katalis, pendukung, atau hambatan terhadap upaya tersebut, tergantung pada berbagai faktor.

a) Pembentukan Kebijakan: Politik dapat mempengaruhi upaya pembangunan sistem keamanan siber melalui kebijakan dan regulasi yang dibuat dan diberlakukan oleh pemerintah. Misalnya, pemerintah dapat menetapkan undang-undang dan regulasi yang mendorong atau memerlukan adopsi standar keamanan siber tertentu, atau dapat memberikan insentif bagi sektor swasta untuk berinvestasi dalam teknologi dan infrastruktur keamanan siber. Di sisi lain, politik juga dapat menjadi hambatan jika ada ketidaksepakatan atau konflik politik mengenai isu-isu tertentu yang terkait dengan keamanan siber.

b) Alokasi Sumber Daya: Politik juga berperan dalam alokasi sumber daya untuk keamanan siber. Anggaran untuk penelitian, pengembangan, dan implementasi teknologi dan infrastruktur keamanan siber sering kali ditentukan melalui proses politik. Dalam konteks ini, dinamika politik yang mendukung pembangunan nasional yang berkelanjutan dapat mendorong alokasi sumber daya yang lebih besar untuk keamanan siber.

c) Koordinasi Antar Lembaga: Upaya membangun sistem keamanan siber sering kali melibatkan koordinasi antara berbagai lembaga pemerintah dan pihak swasta. Dinamika politik dapat mempengaruhi efektivitas koordinasi ini, tergantung pada hubungan antara lembaga-lembaga

tersebut dan sejauh mana mereka berbagi visi yang sama tentang pentingnya keamanan siber.

d) Pemahaman dan Kesadaran Publik: Politik juga dapat mempengaruhi sejauh mana masyarakat memahami dan peduli tentang keamanan siber. Pemimpin politik dan partai politik dapat berperan dalam membentuk opini publik tentang isu-isu keamanan siber, dan mereka dapat menggunakan pengaruh mereka untuk mempromosikan kesadaran dan pendidikan tentang keamanan siber.

Saat ini dukungan politik terhadap pembangunan IKN sebagai *smart city,* termasuk adanya kebutuhan untuk membangun sistem keamanan siber di IKN yang handal sangat kuat. Kondisi ini berpengaruh positif terhadap pembentukan kebijakan, alokasi sumber daya, koordinasi antar lembaga, dan pemahaman dan kesadaran publik terhadap pentingnya membangun keamanan siber yang kuat.

4) **Ekonomi**

Kondisi ekonomi berperan penting dalam menentukan jalannya pembangunan sistem keamanan siber di Ibu Kota Nusantara (IKN). Dalam hal ini, kondisi ekonomi, baik pada skala nasional maupun lokal, dapat mempengaruhi berbagai aspek dari upaya ini, termasuk ketersediaan sumber daya, keterlibatan sektor swasta, dan keberlanjutan investasi. Berikut adalah pengaruh ekonomi terhadap upaya tersebut.

a) Ketersediaan Sumber Daya: Pembangunan sistem keamanan siber memerlukan investasi yang cukup dalam teknologi dan infrastruktur, serta dalam penelitian dan pengembangan. Kondisi ekonomi yang baik, ditandai dengan pertumbuhan ekonomi yang stabil dan tinggi, dapat meningkatkan ketersediaan sumber daya finansial dan manusia untuk investasi ini. Sebaliknya, kondisi ekonomi yang lemah atau tidak stabil dapat membatasi ketersediaan sumber daya ini.

b) Keterlibatan Sektor Swasta: Sektor swasta memainkan peran penting dalam pengembangan dan penerapan teknologi keamanan siber. Kondisi ekonomi yang baik, yang ditandai dengan tingkat investasi dan aktivitas bisnis yang tinggi, dapat mendorong keterlibatan sektor swasta dalam upaya ini. Di sisi lain, kondisi ekonomi yang buruk dapat menurunkan tingkat keterlibatan sektor swasta.

c) Keberlanjutan Investasi: Keberlanjutan investasi dalam keamanan siber adalah kunci untuk pembangunan sistem keamanan siber yang efektif dan tahan lama. Kondisi ekonomi yang baik, dengan pertumbuhan ekonomi yang stabil dan berkelanjutan, dapat mendukung keberlanjutan investasi ini. Sebaliknya, kondisi ekonomi yang tidak stabil atau resesi dapat mengancam keberlanjutan investasi.

d) Perubahan Ekonomi Struktural: Dalam konteks IKN, perubahan ekonomi struktural, seperti urbanisasi dan digitalisasi, dapat meningkatkan permintaan akan keamanan siber dan mempengaruhi jenis dan tingkat investasi yang dibutuhkan. Misalnya, digitalisasi ekonomi dan masyarakat dapat meningkatkan ancaman siber dan meningkatkan kebutuhan investasi dalam keamanan siber.

Jadi, ekonomi dapat mempengaruhi upaya membangun sistem keamanan siber di IKN dalam berbagai cara. Untuk mencapai tujuan ini, penting bagi pemerintah dan pihak lain yang terlibat untuk mempertimbangkan faktor-faktor ekonomi ini dan merumuskan strategi yang memadai.

5) **Sosial Budaya**

Masyarakat Indonesia umumnya masih belum memiliki literasi digital yang cukup sehingga lebih rentan terhadap serangan siber, seperti *phishing*, *scam*, atau *malware*. Mereka mungkin tidak menyadari risiko yang ada atau bagaimana melindungi diri dari serangan tersebut. Ini berarti bahwa dalam masyarakat dengan tingkat literasi digital yang rendah, sistem keamanan siber

mungkin lebih sering diuji dan berpotensi lebih rentan terhadap pelanggaran.

Literasi digital juga mempengaruhi kemampuan seseorang untuk mengimplementasikan praktik keamanan siber yang baik. Misalnya, seseorang yang memiliki pemahaman yang baik tentang teknologi dan keamanan siber akan lebih mungkin untuk membuat password yang kuat, memperbarui *software* dan sistem operasi mereka secara teratur, dan berhati-hati dengan *link* atau *file* yang mencurigakan. Masyarakat yang memiliki tingkat literasi digital yang tinggi lebih mungkin untuk berpartisipasi secara aktif dalam upaya keamanan siber, baik itu melalui melaporkan ancaman potensial atau mendukung kebijakan dan program keamanan siber.

Norma dan nilai budaya suatu masyarakat juga dapat mempengaruhi sikap mereka terhadap keamanan siber. Misalnya, dalam budaya yang menghargai privasi dan otonomi individu, mungkin akan ada dukungan yang lebih besar untuk upaya keamanan siber yang melindungi data pribadi. Sebaliknya, dalam budaya yang menekankan kepentingan komunitas atau negara di atas individu, mungkin ada lebih banyak toleransi terhadap pengawasan atau kontrol siber oleh pihak berwenang.

Pembangunan sistem keamanan siber di IKN yang efektif akan membutuhkan keterlibatan dan partisipasi aktif dari komunitas lokal. Ini bisa melibatkan pelibatan komunitas dalam pelaksanaan dan pengawasan kebijakan keamanan siber, serta dalam pengembangan solusi dan teknologi keamanan siber yang lokal.

Kemampuan dan kesediaan masyarakat untuk mengadopsi dan menggunakan teknologi baru juga akan mempengaruhi keberhasilan pembangunan sistem keamanan siber. Ini mencakup pelatihan dan pendidikan untuk membantu masyarakat memahami dan menggunakan teknologi baru secara aman dan efektif.

Oleh sebab itu, respons masyarakat terhadap inisiatif keamanan siber dapat bervariasi, tergantung pada bagaimana mereka

memandang manfaat dan biaya dari inisiatif tersebut. Dukungan masyarakat dapat membantu memfasilitasi pelaksanaan dan efektivitas dari inisiatif keamanan siber, sementara resistensi atau oposisi masyarakat dapat menjadi hambatan.

Dengan demikian, memahami dan mempertimbangkan faktor sosial budaya adalah penting dalam perencanaan dan pelaksanaan strategi keamanan siber di IKN. Upaya untuk membangun sistem keamanan siber yang kuat harus mencakup upaya untuk membangun kesadaran dan pemahaman masyarakat tentang isu-isu keamanan siber, serta menghormati dan mempertimbangkan norma dan nilai budaya mereka.

6) **Pertahanan dan Keamanan**

Indonesia telah mengambil beberapa langkah penting untuk meningkatkan keamanan siber dan pertahanan nasional. Ini termasuk pembentukan Badan Siber dan Sandi Negara (BSSN) pada tahun 2017, yang bertanggung jawab untuk melindungi informasi pemerintah dan masyarakat dari ancaman siber.

Selain itu, pemerintah Indonesia juga telah mencanangkan pembentukan pusat data nasional untuk mengelola dan melindungi data pemerintah dan masyarakat, serta bekerja sama dengan sektor swasta dan mitra internasional dalam upaya ini. Langkah-langkah ini menunjukkan komitmen pemerintah terhadap peningkatan keamanan siber.

Namun, pertahanan dan keamanan siber adalah bidang yang terus berkembang dan membutuhkan investasi berkelanjutan dalam teknologi, infrastruktur, dan pendidikan untuk menghadapi ancaman yang semakin canggih. Oleh karena itu, meskipun ada kemajuan, perlu ada upaya berkelanjutan untuk memastikan bahwa sistem keamanan siber di IKN dan seluruh Indonesia semakin kuat dan efektif.

BAB III
PEMBAHASAN

12. Umum

Badan Siber dan Sandi Negara (BSSN) Indonesia sedang mempersiapkan diri untuk membangun sistem keamanan siber yang kuat dan andal di Ibu Kota Nusantara (IKN). Sebagai langkah pertama dalam upaya ini, BSSN sudah mulai bergerak memberikan pelatihan keamanan siber kepada aparatur sipil negara (ASN) yang akan ditugaskan di IKN. Tujuannya adalah untuk membekali ASN dengan kemampuan dan pengetahuan yang diperlukan untuk menangani tantangan keamanan di era digital. Pelatihan ini akan mencakup penggunaan simulator kota pintar dan akan dilakukan secara bertahap, menyesuaikan dengan kesiapan dan kebutuhan ASN. Selain itu, BSSN juga merencanakan pengembangan infrastruktur keamanan siber, termasuk membangun pusat pengamanan data negara dan data recovery center (DRC) nasional di IKN. Tujuannya adalah untuk memastikan bahwa data dan informasi negara tetap aman dan terlindungi dari ancaman siber[66].

Bagi Indonesia, tantangan keamanan siber tidak ringan. Sepanjang tahun 2021, Indonesia mengalami 1,6 miliar serangan siber. Malware, trojan, dan upaya pengumpulan informasi ilegal untuk mencari celah keamanan adalah beberapa bentuk serangan yang paling sering terjadi. Bahkan BSSN sendiri pernah menjadi korban peretasan. Untuk mengatasi ancaman tersebut, BSSN telah mengambil langkah-langkah untuk memperkuat sistem keamanan siber nasional. Beberapa langkah tersebut antara lain memasang sensor honeynet, melakukan analisis malware, membentuk tim respons insiden keamanan siber (CSIRT), dan menerapkan kriptografi.

Keamananan siber harus menjadi tanggung jawab yang terintegrasi antar kementerian atau lembaga lainnya. Oleh karena itu, dalam membangun sistem keamanan siber di IKN, penting bagi semua pihak untuk patuh dengan sistem dan standar keamanan siber yang telah dibuat oleh

[66] https://www.kompas.id/baca/polhuk/2022/03/07/siapkan-sistem-keamanan-siber-di-ikn diakses pada tanggal 1 Agustus 2023 pukul 20.34 WIB

BSSN. Pemetaan infrastruktur teknologi perlu dilakukan bahkan sebelum melatih ASN. Pemetaan ini esensial untuk mengetahui dan memahami semua jenis dan karakter infrastruktur teknologi yang akan digunakan di IKN, yang nantinya akan membantu dalam mencegah serangan siber. Pencegahan serangan menjadi hal utama, mengingat serangan siber bisa terjadi kapan saja dan seringkali berlangsung secara bertahap.

Secara umum, usaha untuk mempersiapkan IKN sebagai kota pintar harus disertai dengan pengamanan siber yang komprehensif dan antisipatif. Setiap lembaga, baik pemerintah maupun swasta, harus memastikan bahwa mereka mematuhi standar keamanan siber dan siap untuk merespons dan menangani serangan siber yang mungkin terjadi.

Dalam perencanaan keamanan siber di antaranya adalah faktor regulasi, kelembagaan, infrastruktur, keterbatasan SDM dan minimnya dukungan anggaran sering menjadi hambatan dan kendala dalam mewujudkan sistem keamanan siber yang handal. Faktor-faktor inilah yang akan menjadi pokok pembahasan dan analisa dalam Bab ini yang sebelumnya akan didahului oleh analisa SWOT guna memberikan gambaran terkait pembangunan sistem keamanan siber di IKN.

13. Analisa SWOT Pembangunan Sistem Keamanan Siber di Ibu Kota Nusantara (IKN)

Analisis SWOT adalah teknik yang dirancang untuk membantu organisasi dan bisnis memahami dan mengevaluasi faktor-faktor internal dan eksternal yang berpotensi mempengaruhi keberhasilan mereka. Ini adalah metode strategis yang melibatkan penilaian kekuatan dan kelemahan internal perusahaan, serta peluang dan ancaman yang datang dari lingkungan eksternal. Teknik ini memiliki tujuan untuk memperkuat posisi perusahaan di pasar dengan menentukan tindakan yang perlu diambil.

Menurut Rangkuty (2013), analisis SWOT didasarkan pada logika yang memungkinkan suatu organisasi untuk memaksimalkan kekuatan dan peluang mereka, sementara juga berusaha untuk meminimalkan kelemahan dan ancaman. Dengan kata lain, analisis SWOT membantu perusahaan untuk memanfaatkan kekuatan dan peluang mereka sebaik mungkin, sambil

berusaha untuk memitigasi kelemahan dan ancaman yang mungkin menghambat kesuksesan mereka[67].

Kata SWOT sendiri sebenarnya adalah akronim yang merujuk ke kekuatan (***Strengths***), kelemahan (***Weaknesses***), peluang (***Opportunities***), dan ancaman (***Threats***) yang dihadapi suatu organisasi/perusahaan. Pearce & Robinson (2014) menyatakan bahwa strategi yang efektif biasanya muncul dari keselarasan antara sumber daya dan kapabilitas internal perusahaan dengan situasi eksternal atau lingkungan di mana mereka beroperasi[68]. Teori ini digunakan untuk menganalisis seberapa siap pemerintah dalam membangun sistem keamanan siber di IKN, dengan melihat kekuatan dan peluang yang ada serta sejumlah upaya untuk mengantisipasi dan sebisa mungkin menghilangkan hambatan dan ancaman yang ada.

a. ***Strength*** (Kekuatan)

Kekuatan dari membangun sistem keamanan siber di Ibu Kota Nusantara (IKN) antara lain: 1) Perencanaan lebih mudah. Dikarenakan pembangunan IKN dimulai dari nol, ini memungkinkan pemerintah dan pembuat kebijakan untuk merencanakan dan membangun infrastruktur keamanan siber yang kuat dan terintegrasi sejak awal. Tidak seperti kota-kota yang telah ada sebelumnya, di mana keamanan siber seringkali harus ditambahkan sebagai lapisan tambahan, IKN memiliki keuntungan unik dengan kemampuan untuk merancang dan membangun sistem keamanan siber yang canggih dan komprehensif sejak awal; 2) Tambahan landasan hukum. Pemerintah baru-baru ini telah meresmikan Perpres nomor 47 Tahun 2023 yang berkaitan dengan Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Dokumen ini dapat menjadi landasan hukum dan pedoman bagi IKN dalam membangun sistem keamanan sibernya; 3) Lembaga khusus keamanan siber nasional: Dengan adanya BSSN sebagai lembaga yang memimpin sektor keamanan siber nasional, IKN memiliki mitra strategis dalam menyusun dan merencanakan sistem keamanan sibernya; 4) Kapabilitas SDM IKN. BSSN telah menunjukkan

[67] Rangkuti, Freddy. (2013). Teknik Membedah Kasus Bisnis Analisis SWOT Cara Perhitungan Bobot, Rating, dan OCAI. Jakarta: Penerbit PT. Gramedia Pustaka Utama.
[68] A.Pearce, John II, Richard B.Robinson, Jr. (2014). Manajemen strategi. Jakarta: Salemba Empat.

komitmennya dengan menyiapkan pelatihan keamanan siber khusus bagi Aparatur Sipil Negara (ASN) yang akan bertugas di IKN. Ini menandakan bahwa tenaga kerja yang akan ditempatkan di IKN akan memiliki pemahaman dan kesiapan dalam menangani isu-isu keamanan siber; 5) Dukungan penuh pemerintah. Dengan dukungan penuh pemerintah, IKN berada dalam posisi yang kuat untuk menjadi model *smart city* modern, aman, nyaman, dan inklusif. Dukungan ini tidak hanya dalam bentuk kebijakan dan regulasi, tetapi juga dalam investasi dan kerjasama strategis. Dengan dukungan ini, IKN dapat menjadi pelopor dalam keamanan siber, menetapkan standar untuk kota-kota lainnya di Indonesia dan di seluruh dunia.

Secara keseluruhan, pembangunan sistem keamanan siber di IKN memang mempunyai sejumlah kekuatan yang memungkinkan kota ini untuk menghadapi tantangan keamanan siber dengan cara yang inovatif dan efektif. Dengan memanfaatkan kekuatan ini, IKN dapat menjadi contoh bagi kota-kota lain dalam hal penerapan dan integrasi keamanan siber dalam pembangunan kota.

b. ***Weakness*** (Kelemahan)

Sejumlah kelemahan yang ditemukan dalam membangun sistem keamanan siber di Ibu Kota Nusantara (IKN), diantaranya: 1) Konsep *smart city* pada IKN belum mendetail. Sejauh ini, implementasi konsep *smart city* dalam pembangunan IKN belum dijabarkan secara mendetail dan sepertinya masih akan bergantung pada siapa yang akan menjadi investor IKN dalam sejumlah sektor pembangunannya. Hal ini dapat menyebabkan kesulitan dalam perencanaan dan implementasinya; 2) Membutuhkan dukungan anggaran yang besar. Keamanan siber adalah investasi yang mahal. Membutuhkan dukungan anggaran yang besar untuk membeli perangkat keras dan perangkat lunak yang diperlukan, serta untuk melatih dan mempekerjakan staf yang kompeten; 3) Infrastruktur digital yang tersedia di IKN masih minim. Keberadaan infrastruktur digital yang masih minim dapat menghambat pelaksanaan kebijakan keamanan siber yang efektif.kuat. Jika belum tersedia atau minim, ini bisa menjadi kelemahan besar; 4) Koordinasi lintas lembaga

lemah. Selama ini, koordinasi dan sinergitas lintas lembaga dalam mewujudkan keamanan siber nasional masih lemah. Bahkan beberapa kali terjadi saling lempar tanggung jawab ketika terjadi insiden keamanan siber; 5) Belum ada strategi keamanan siber yang komprehensif: Selama ini Indonesia masih belum memiliki strategi keamanan siber yang terarah dan berkelanjutan. Tanpa strategi keamanan siber yang komprehensif, Indonesia berisiko tidak memiliki visi dan arah yang jelas dalam menghadapi ancaman siber; 6) Kurangnya dukungan regulasi. Ketidakhadiran Undang-Undang Keamanan Siber membuat pelaksanaan dan penegakan kebijakan keamanan siber menjadi kurang maksimal dan bisa menimbulkan zona abu-abu dalam implementasinya; 7) Indonesia kekurangan talenta digital. Ini adalah tantangan di banyak negara, tidak hanya di Indonesia. Menarik dan mempertahankan talenta digital yang terampil bisa menjadi tantangan, terutama mengingat persaingan global untuk talenta ini; 8) Keterbelakangan teknologi keamanan siber. Teknologi keamanan siber di Indonesia yang masih relatif tertinggal dibandingkan dengan negara-negara maju sehingga bisa menjadi titik lemah dalam menghadapi ancaman siber yang semakin canggih.

Mengenali dan mengatasi kelemahan ini adalah bagian penting dari membangun sistem keamanan siber yang kuat dan efektif. Dengan pemahaman yang jelas tentang tantangan ini, pembuat kebijakan dan perencana dapat mencari solusi dan strategi yang dapat mengatasi atau memitigasi kelemahan ini.

c. ***Opportunity*** (Peluang)

Selain keunggulan dan kelemahan, secara eksternal membangun sistem keamanan siber di Ibu Kota Nusantara (IKN) juga memiliki sejumlah peluang, antara lain: 1). IKN bisa menjadi kota dunia dan simbol kemajuan Indonesia. Dengan perencanaan dan implementasi yang tepat, pembangunan sistem keamanan siber yang kuat di IKN dapat menjadikan kota ini sebagai salah satu kota pintar terkemuka di dunia. Ini bukan hanya akan meningkatkan reputasi internasional IKN dan Indonesia, tetapi juga menunjukkan komitmen Indonesia terhadap

keamanan siber dan pembangunan berkelanjutan; 2) Sistem keamanan siber IKN bisa menjadi *role model* untuk diimplementasikan secara nasional. Jika berhasil, sistem keamanan siber di IKN bisa menjadi contoh bagi kota-kota lain di Indonesia. Dengan membagikan pengetahuan dan pengalaman yang diperoleh, IKN dapat memainkan peran penting dalam meningkatkan keamanan siber secara nasional; 3) Perkembangan teknologi keamanan siber semakin maju. Teknologi keamanan siber yang terus berkembang memberikan peluang bagi IKN untuk mengimplementasikan teknologi keamanan siber terbaru yang lebih handal memberikan pengamanan terhadap berbagai ancaman siber yang ada; 4) Menyediakan peluang untuk bekerja sama dengan lembaga penelitian dan industri dalam pengembangan teknologi dan solusi keamanan siber. Dengan statusnya sebagai ibu kota baru, IKN dapat menarik kerjasama dari berbagai pihak, termasuk universitas, lembaga penelitian, dan perusahaan teknologi. Kerjasama seperti ini dapat membantu IKN untuk mengembangkan dan menerapkan teknologi dan solusi keamanan siber yang paling efektif; 5) Sejumlah institusi telah menyiapkan strategi keamanan siber bagi IKN: Dengan adanya perencanaan dan strategi keamanan siber IKN yang disusun oleh sejumlah institusi seperti Bappenas, Polri, BSSN, dan Kemenhan, maka nantinya pemerintah bisa mengkolaborasikan konsep dan perencanaan dari sejumlah institusi tersebut bisa saling melengkapi guna mewujudkan sistem keamanan siber terbaik bagi IKN; 6) Adopsi hasil riset global. Banyaknya riset dan penelitian global terkait sistem keamanan siber pada *smart city* memberikan peluang bagi IKN untuk belajar dan mengadopsi praktik terbaik dari seluruh dunia. Hal ini memungkinkan IKN untuk menghindari kesalahan dan mempercepat pembangunan sistem keamanan yang efektif dan efisien; 7) Sumber daya terabaikan. Keberadaan *ethical hacker* di Indonesia yang memiliki kompetensi tinggi dalam bidang keamanan siber menjadi aset berharga. Mereka dapat berperan aktif dalam proses pengujian dan pemastian keamanan sistem IKN, serta menjadi sumber daya dalam melawan potensi ancaman dari pihak yang tidak bertanggung jawab.

Memanfaatkan peluang-peluang ini dapat membantu IKN untuk membangun sistem keamanan siber yang kuat dan efektif, yang tidak hanya melindungi kota dan penduduknya, tetapi juga membantu meningkatkan keamanan siber di seluruh Indonesia.

d. ***Threat*** (Tantangan)

Sejumlah tantangan yang dihadapi dalam membangun sistem keamanan siber di Ibu Kota Nusantara (IKN) antara lain: 1) *Smart city* membutuhkan pengamanan yang kompleks dan kuat. Sebagai sebuah konsep kota pintar atau *smart city*, IKN diharapkan akan memanfaatkan berbagai teknologi digital dalam operasional sehari-harinya. Semua aspek pengaturan kota, dari manajemen lalu lintas hingga pelayanan publik akan terhubung dan terintegrasi melalui jaringan digital. Hal ini bukan hanya akan meningkatkan efisiensi dan kenyamanan, tetapi juga bisa menambah kompleksitas dan menimbulkan ancaman keamanan yang baru dan lebih kompleks; 2) Ancaman siber di Indonesia sangat tinggi. Dalam beberapa tahun terakhir, Indonesia telah menjadi sasaran berbagai jenis serangan siber, dari peretasan hingga serangan ransomware. Dengan meningkatnya digitalisasi dan integrasi teknologi di IKN, tingkat ancaman juga dapat meningkat; 3) Insiden peretasan dan pencurian data masih sering terjadi di Indonesia: Meskipun upaya peningkatan keamanan telah dilakukan, insiden peretasan dan pencurian data masih sering terjadi. Ini menunjukkan bahwa masih ada celah keamanan yang perlu ditangani; 4) Literasi digital masyarakat masih belum merata. Salah satu tantangan terbesar adalah literasi digital masyarakat yang belum merata. Banyak individu yang tidak menyadari risiko yang ada di dunia digital atau tidak tahu bagaimana melindungi diri mereka sendiri. Hal ini memudahkan para pelaku kejahatan siber untuk mengeksploitasi masyarakat, mulai dari penipuan online hingga pembobolan data pribadi.

Mengenali ancaman-ancaman ini adalah langkah penting dalam membangun sistem keamanan siber yang kuat dan efektif. Menghadapi ancaman ini membutuhkan kerjasama antara pemerintah, sektor

swasta, dan masyarakat, serta pendekatan yang holistik dan fleksibel yang bisa beradaptasi dengan perubahan ancaman dan teknologi.

INTERNAL	EKSTERNAL
STRENGTH (KEKUATAN)	**OPPORTUNITY (PELUANG)**
1) Perencanaan lebih mudah karena semua didesain dari awal 2) Pemerintah baru saja mengesahkan Perpres nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber 3) Indonesia sudah memiliki lembaga BSSN yang menjadi *leading sector* dalam keamanan siber nasional 4) BSSN sudah menyiapkan pelatihan keamanan siber bagi ASN yang akan ditempatkan di IKN 5) Dukungan penuh pemerintah untuk mewujudkan IKN sebagai *smart city* yang modern, aman, nyaman dan inklusif	1) Sistem keamanan siber IKN bisa menjadi role mode untuk diimplementasikan secara nasional 2) Teknologi keamanan siber terus berkembang 3) Menyediakan peluang untuk bekerja sama dengan lembaga penelitian dan industri dalam pengembangan teknologi dan solusi keamanan siber, yang bisa memperkuat jaringan keamanan siber IKN. 4) Sejumlah institusi seperti Bappenas, Polri, BSSN, Kemenhan telah memiliki dan menyusun strategi keamanan siber IKN 5) Banyak riset dan penelitian global terkait pengamanan siber pada smart city yang bisa diadopsi. 6) Indonesia memiliki ethical hacker yang memiliki kompetensi mumpuni dalam keamanan siber
WEAKNESS (KELEMAHAN)	**THREATH (ANCAMAN)**
1) Konsep *smart city* yang akan diusung oleh IKN belum mendetail 2) Membutuhkan dukungan anggaran yang besar 3) Dukungan infrastruktur digital yang tersedia masih minim 4) Koordinasi dan sinergitas lintas lembaga dalam mengelola	1) *Smart city* membutuhkan pengamanan yang kompleks dan kuat, karena semua pengaturan kota telah terintegrasi. 2) Ancaman siber di Indonesia sangat tinggi. 3) Insiden peretasan dan pencurian data masih sering terjadi di Indonesia

Tkeamanan siber masih lemah 5) a Indonesia belum memiliki strategi b keamanan siber yang komprehensif 6) e Indonesia belum memiliki UU l Keamanan Siber 7) Indonesia kekurangan talenta 1 digital 8) · Teknologi keamanan siber di Indonesia masih relatif tertinggal	4) Literasi digital masyarakat belum merata sehingga masyarakat masih rentan menjadi korban kejahatan siber karena ketidaktahuannya.

M

atriks Analisis SWOT Pembangunan Sistem Keamanan Siber di Ibu Kota Nusantara (IKN)

Rangkuti (2006: 13) menjelaskan dalam mencari dan merumuskan strategi yang tepat digunakan matriks SWOT yang di dalamnya merupakan kombinasi strategi dari:

a. Strategi SO (*Strength and Opportunity*). Strategi ini merupakan salah satu upaya memaksimalkan kekuatan yang dimiliki agar bisa memanfaatkan peluang sebesar-besarnya.
b. Strategi ST (*Strength and Threat*). Strategi yang dibuat dengan mengoptimalkan kekuatan yang dimiliki guna mengantisipasi dan mengatasi ancaman yang ada.
c. Strategi WO (*Weakness and Opportunity*). Strategi ini merupakan upaya untuk diterapkan dengan mencoba memanfaatkan semua peluang dengan cara meminimalkan kelemahan yang ada.
d. Strategi WT (*Weakness and Threath*). Strategi ini bersifat *defensive*, yang dilakukan dengan cara meminimalkan kelemahan yang ada serta menghindari ancaman.

STRATEGI SO	STRATEGI WO

1. Perencanaan sistem keamanan siber *smart city* IKN perlu mengadopsi teknologi terkini 2. Memanfaatkan pendekatan keamanan siber yang holistik dan dukungan penuh pemerintah, IKN dapat menjadikan sistem keamanannya sebagai role model yang nantinya bisa diimplementasikan secara nasional. 3. Memanfaatkan perkembangan riset dan teknologi keamanan *smart city* dunia, IKN bisa berkolaborasi dengan universitas, lembaga penelitian, dan industri untuk mengembangkan solusi keamanan siber yang terdepan dan inovatif. 4. Dengan dukungan pemerintah dan kemampuan integrasi teknologi, IKN memiliki peluang untuk menjalin kerjasama dengan lembaga penelitian dan industri global dalam pengembangan teknologi dan solusi keamanan siber, sehingga memperkuat jaringan keamanan siber IKN dan menempatkannya pada standar global. 5. Adanya Perpres Nomor 47 tahun 2023 memungkinkan pemerintah segera menyusun rencana aksi nasional keamanan siber yang bisa memasukan rencana embangunan sistem keamanan siber IKN 6. Pemerintah bisa merangkul *ethical hacker* Indonesia untuk membantu menguji dan mencari kelemahan dari sistem keamanan siber IKN 7. Pembangunan sistem keamanan siber yang handal dengan adopsi teknologi dan inovasi keamanan terkini akan mendukung	1. Mengingat kekurangan talenta digital dan literasi digital masyarakat yang belum merata, IKN dapat memanfaatkan peluangnya sebagai kota simbol kemajuan dengan menarik institusi pendidikan dan lembaga pelatihan keamanan siber untuk berlokasi di sana, sekaligus menjalin kerja sama dengan mereka. 2. IKN bisa memanfaatkan perkembangan riset dan teknologi keamanan *smart city* dengan mendirikan pusat riset yang berfokus pada pengembangan dan adaptasi teknologi keamanan siber terbaru. 3. BSSN memberikan pembekalan kemampuan pengamanan siber *smart city* 4. Perguruan tinggi di Indonesia menyiapkan talenta digital untuk memenuhi kebutuhan SDM unggul IKN. 5. Pemerintah dan DPR segera membahas kembali dan menyelesaikan RUU Keamanan dan Pertahanan Siber untuk memperkuat regulasi terkait sistem keamanan siber nasional. 6. Untuk mengatasi kurangnya literasi digital masyarakat, IKN bisa menjadikannya sebagai salah satu program unggulan kota dengan berkolaborasi dengan institusi pendidikan, komunitas, dan industri dalam penyelenggaraan program-program literasi digital.

Tabe pembangunan nasional berkelanjutan sesuai dengan visi pemindahan ibu kota negara.	
STRATEGI ST	**STRATEGI WT**
1. Perencanaan sistem keamanan siber harus memastikan aman dari ancaman siber yang sering terjadi di Indonesia maupun bentuk ancaman siber terbaru 2. Memanfaatkan dukungan penuh pemerintah dalam mewujudkan IKN sebagai *smart city* yang modern untuk memperkuat kebijakan dan regulasi yang melindungi dari serangan siber 3. Menggunakan pendekatan yang mengintegrasikan keamanan siber ke dalam semua aspek perencanaan dan pembangunan kota untuk mendeteksi dan mencegah insiden peretasan dan pencurian data yang sering terjadi. 4. Memanfaatkan fleksibilitas dan kemampuan integrasi dengan infrastruktur teknologi lainnya untuk mengembangkan sistem keamanan siber yang dapat beradaptasi dengan cepat terhadap ancaman siber yang meningkat di Indonesia.	1. Menghadapi literasi digital masyarakat yang belum merata, luncurkan program edukasi yang intensif dan menyeluruh untuk meningkatkan kesadaran dan pengetahuan masyarakat tentang keamanan siber, sehingga dapat mengurangi insiden peretasan. 2. Untuk mengatasi dukungan regulasi siber yang belum optimal dan risiko ethical hacker yang rentan dipidanakan, pemerintah sebaiknya memperbaharui atau membuat regulasi baru yang mendukung perkembangan keamanan siber dan memberikan perlindungan kepada mereka yang melaporkan celah keamanan. 3. Agar tidak tergantung pada satu vendor atau penyedia teknologi tertentu, pemerintah bisa mempertimbangkan untuk diversifikasi penyedia teknologi, sehingga mengurangi potensi titik kelemahan dalam sistem keamanan siber. 4. Mengingat konsep *smart city* yang belum mendetail, perencanaan sistem keamanan siber IKN harus memiliki fleksibilitas tinggi sehingga mudah dilakukan penyesuaian mengikuti proses pengembangan IKN ke depan.
Matriks Strategi SWOT	

Dalam menunjang pembangunan nasional yang berkelanjutan, pembangunan sistem keamanan siber di Ibu Kota Nusantara (IKN) memegang peranan krusial. Terlepas dari kekuatan, kelemahan, peluang, dan ancaman yang ada, ada satu elemen fundamental yang dapat menjadi tonggak utama dalam memastikan keamanan siber di IKN, yaitu penguatan regulasi, khususnya dengan segera disahkannya RUU Keamanan Siber.

RUU Keamanan Siber bukan sekadar peraturan tertulis. Regulasi ini menjadi panduan aksi, pemantap kebijakan, serta fondasi hukum yang memastikan bahwa semua elemen keamanan siber bergerak seirama dan efektif. Regulasi yang jelas dan kuat akan memastikan bahwa: 1) Ada kerangka kerja jelas bagi semua lembaga yang terlibat dalam pengamanan siber, termasuk BSSN dan lembaga lainnya, sehingga meningkatkan koordinasi dan efisiensi; 2) Menyediakan garis panduan bagi pembangunan infrastruktur keamanan siber yang resilien dan responsif terhadap ancaman terbaru; 3) Memandu pelatihan, pengembangan, dan perekrutan talenta digital dan keamanan siber agar sesuai dengan standar keamanan nasional dan global; dan 4) Menyediakan justifikasi hukum untuk alokasi dana yang memadai bagi inisiatif keamanan siber.

Dengan adanya RUU Keamanan Siber, IKN akan memiliki kerangka hukum yang memastikan penerapan teknologi yang tepat, kolaborasi antarlembaga, serta edukasi masyarakat tentang pentingnya literasi digital. Ini bukan hanya mempengaruhi bagaimana IKN membangun dan mengoperasikan infrastrukturnya, tetapi juga bagaimana masyarakat, bisnis, dan lembaga pemerintah berinteraksi dalam lingkungan digital yang aman. Selain itu, kehadiran regulasi yang kuat akan memfasilitasi kerjasama lebih erat dengan pihak ketiga, seperti universitas, lembaga penelitian, dan industri global. Melalui kerjasama ini, IKN dapat memanfaatkan inovasi terbaru dan praktek terbaik dalam keamanan siber.

Singkatnya, RUU Keamanan Siber bukan hanya menjadi pintu gerbang untuk keamanan digital IKN tetapi juga menjadi simbol komitmen nasional dalam menciptakan lingkungan digital yang aman, terpercaya, dan inklusif untuk semua warga Indonesia. Memastikan keberlanjutan RUU ini dan

pelaksanaannya dengan benar akan menjadi kunci keberhasilan IKN sebagai contoh kota masa depan yang aman dan maju di era digital.

14. Membangun Tata Kelola Regulasi Yang Dapat Mendukung Sistem Keamanan Siber di IKN.

Kondisi keamanan siber sebuah negara menjadi indikator vital dalam era digitalisasi global saat ini. Sayangnya, menurut sejumlah indeks global, Indonesia masih berada di posisi yang kurang memuaskan dalam hal keamanan siber. Konfirmasi mengenai kondisi ini datang dari Gubernur Lemhamnas, Andi Widjajanto. Berdasarkan indeks yang dikeluarkan oleh Massachusetts Institute of Technology (MIT), Indonesia hanya mampu menempati posisi paling bontot di antara negara-negara anggota G20[69].

Salah satu hal yang cukup mencemaskan dari hasil indeks tersebut adalah bahwa Indonesia berada di bawah rata-rata global dalam empat variabel kunci. Variabel-variabel tersebut meliputi infrastruktur kritis, sumber daya yang dialokasikan, kapasitas organisasional, serta komitmen kebijakan pemerintah. Diantara keempat variabel tersebut, dua yang menjadi kelemahan utama Indonesia adalah kapasitas organisasional dan komitmen kebijakan pemerintah. Ironisnya, di tengah-tengah gempuran era digital, Indonesia masih belum memiliki regulasi khusus yang mengatur keamanan siber.

Meski banyak negara di Asia Tenggara telah mempersiapkan diri dengan aturan keamanan siber, Indonesia ternyata menjadi satu-satunya negara yang belum memiliki aturan semacam itu. Tidak mengherankan jika infrastruktur digital di Indonesia memperlihatkan masih ada banyak "lubang" yang perlu segera ditambal. Adanya celah keamanan ini tentu berisiko, terutama karena Presiden Joko Widodo terus mendorong percepatan transformasi digital di Indonesia. Transformasi digital yang tidak didukung oleh fondasi keamanan siber yang kuat dapat menimbulkan potensi risiko yang besar.

[69] https://www.cnbcindonesia.com/tech/20230530121921-37-441764/keamanan-siber-ri-banyak-bolongnya-gampang-dibobol-hacker diakses pada tanggal 6 Agustus 2023 pukul 21.20 WIB

Meskipun saat ini Indonesia telah memiliki UU ITE dan UU PDP, namun regulasi tersebut tampaknya belum mampu memberikan perlindungan maksimal bagi siber tanah air. Andi Widjajanto menegaskan bahwa salah satu pekerjaan rumah besar bagi Indonesia adalah menyiapkan dua regulasi penting di bidang keamanan siber. Keberadaan UU keamanan siber dan kebijakan nasional tentang keamanan siber menjadi sangat krusial untuk memastikan keamanan dan ketahanan digital nasional[70].

Dalam transformasi digital, beberapa sektor menonjol sebagai area yang paling rentan terhadap ancaman siber. Tiga sektor tersebut adalah kesehatan, finansial, dan pemerintah. Menariknya, sektor keuangan di Indonesia dianggap sebagai sektor yang paling rentan. Ini tentu menjadi peringatan bagi stakeholder terkait untuk meningkatkan perlindungan pada sektor tersebut.

Walau dengan berbagai kelemahan tersebut, ada satu hal yang bisa dianggap sebagai berita baik. Indonesia, hingga saat ini, belum menjadi target utama serangan siber, terutama jika dibandingkan dengan Amerika Serikat atau negara-negara di Eropa Barat. Namun, kondisi ini seharusnya tidak membuat kita lengah. Sebaliknya, ini adalah momentum yang tepat bagi Indonesia untuk memperkuat arsitektur keamanan sibernya. Saat ini adalah waktu yang tepat bagi Indonesia untuk mengakselerasi penguatan keamanan sibernya demi masa depan yang lebih aman dan terlindungi di era digital.

Pada 20 Juli 2023, pemerintah telah mengeluarkan regulasi baru berupa Peraturan Presiden RI Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Strategi Keamanan Siber Nasional menjadi arah kebijakan nasional dalam memanfaatkan seluruh sumber daya siber nasional untuk mewujudkan Keamanan Siber dalam mempertahankan dan memajukan kepentingan nasional. Keberadaan regulasi ini memberikan landasan hukum dalam membangun keamanan siber di Indonesia, baik dari sisi tata kelola, manajemen resiko, kesiapsiagaan dan ketahanan, pentingnya penguatan keamanan dan perlindungan infrastruktur informasi yang vital, kemandirian dalam kriptografi

[70] Ibid

nasional, penguatan kapabilitas, kapasitas dan kualitas, hingga pentingnya membangun kerja sama internasional. Selain itu, regulasi ini juga mengatur rencana aksi nasional Keamanan Siber yang akan menjadi pedoman para pihak dalam membangun, mengembangkan dan terus memperkuat keamanan siber nasional.

Namun demikian, ketika berbicara tentang pembangunan sistem keamanan siber di Ibu Kota Nusantara (IKN), sangatlah penting untuk memiliki fondasi hukum yang kuat. Meskipun saat ini sudah ada Peraturan Presiden RI Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, RUU Keamanan Siber memiliki peranan yang tak bisa diabaikan dalam menciptakan Tata Kelola Regulasi Yang Mendukung Sistem Keamanan Siber di IKN.

RUU Keamanan Siber, jika disahkan, akan menjadi landasan hukum tertinggi dalam ranah keamanan siber di Indonesia, termasuk di IKN. Sementara Perpres merupakan instrumen hukum yang memberikan petunjuk pelaksanaan, RUU ini akan memberikan kepastian hukum yang jauh lebih kuat dan menentukan standar, ketentuan, serta sanksi yang jelas dan tegas dalam keamanan siber. Hal ini sangat penting untuk menciptakan lingkungan digital yang aman dan terpercaya bagi seluruh warga, pemerintah, serta pelaku usaha di IKN.

RUU ini akan membantu memperjelas tanggung jawab dan kewenangan berbagai lembaga pemerintah dalam pengelolaan keamanan siber. Dengan begitu, akan ada pembagian tugas yang lebih jelas antara lembaga-lembaga tersebut, seperti BSSN, Kemenhan, dan Polri. Hal ini akan mengoptimalkan penggunaan sumber daya dan mencegah adanya tumpang tindih dalam tata kelola keamanan siber.

RUU Keamanan Siber akan memfasilitasi kerjasama yang lebih erat antara pemerintah dengan sektor swasta, akademisi, serta komunitas. Ini penting, mengingat keamanan siber bukan hanya tanggung jawab pemerintah semata, tetapi melibatkan berbagai pihak yang memiliki keahlian dan sumber daya untuk mendukung pencapaian tujuan keamanan siber yang optimal. RUU ini juga dapat membantu dalam memastikan bahwa Indonesia, khususnya IKN, tetap kompetitif dan relevan di panggung global, dengan

menunjukkan komitmen kuat negara dalam menjaga keamanan siber dan melindungi data serta privasi warganya. Dengan demikian, IKN tidak hanya menjadi simbol kemajuan teknologi dan infrastruktur bagi Indonesia tetapi juga refleksi dari komitmen serius negara dalam menjaga keamanan dan kedaulatan di dunia digital.

Berkaca pada kondisi regulasi terkait dengan keamanan siber di atas, ketersediaan regulasi memiliki dampak mendalam terhadap upaya pembangunan sistem keamanan siber di Ibu Kota Nusantara (IKN). Indonesia, meski memiliki potensi besar dalam ekonomi digital dan transformasi teknologi, ternyata masih berada di bawah rata-rata global dalam indeks keamanan siber. Posisi ini menyoroti kebutuhan mendesak untuk peningkatan regulasi dan infrastruktur keamanan siber di negara kita, khususnya di IKN sebagai representasi modernitas dan inovasi Indonesia.

IKN idealnya harus menjadi simbol kemajuan, inovasi, dan keandalan teknologi Indonesia. Namun, tanpa dukungan regulasi keamanan siber yang kuat, reputasi IKN di kancah internasional dapat tercoreng. Investor, perusahaan multinasional, dan partner internasional mungkin akan ragu untuk berinvestasi atau berkolaborasi dalam membangun IKN sebagai sebuah kota pintar modern jika belum tersedia regulasi yang memadai berkaitan dengan keamanan siber.

Selanjutnya, belum adanya regulasi khusus keamanan siber di Indonesia, sementara negara tetangga di Asia Tenggara sudah memilikinya, menunjukkan bahwa Indonesia, khususnya IKN, memiliki jarak yang perlu ditempuh. Dalam jangka pendek, ini mungkin memerlukan konsultasi dan kolaborasi dengan negara-negara yang telah memiliki kerangka kerja keamanan siber yang mapan untuk mempelajari *best practices* mereka.

Tidak bisa dipungkiri, tantangan yang dihadapi dalam meningkatkan keamanan siber di IKN adalah besar. Namun, dengan pendekatan yang tepat dan komitmen penuh dari semua pemangku kepentingan, IKN memiliki potensi untuk tidak hanya memenuhi standar keamanan siber global tetapi juga menjadi pemimpin di kawasan ini. Pada akhirnya, ketidakhadiran regulasi keamanan siber yang kuat saat ini adalah sebuah rintangan bagi IKN. Namun, dengan kesadaran yang meningkat dan urgensi yang sudah

diakui oleh pemimpin negara, IKN memiliki momentum untuk merancang dan mengimplementasikan sistem keamanan siber yang handal, menjadikannya sebagai benteng digital di era modern.

Lawrence Lessig (1999), seorang profesor hukum, mengemukakan bahwa regulasi di dunia maya dipengaruhi oleh empat faktor: Hukum, Norma, Pasar, dan Arsitektur. Oleh karena itu, tata kelola IKN sebaiknya tidak hanya berfokus pada regulasi formal, tetapi juga melibatkan norma sosial, insentif pasar, dan infrastruktur teknologi[71]. Ini dikenal sebagai 'model regulasi empat faktor' Lessig dan bisa digunakan untuk memahami dan merancang regulasi adaptif untuk keamanan siber, termasuk di IKN. Hukum adalah peraturan formal yang dibuat oleh pemerintah atau badan regulator. Dalam konteks IKN, ini mencakup UU ITE, UU PDP, dan UU lain yang berlaku. Regulasi hukum harus jelas, efektif, dan ditegakkan dengan baik. Namun, hukum sendiri tidak cukup. Itulah sebabnya mengapa kita perlu melihat tiga faktor lainnya. Kedua adalah norma. Norma adalah aturan tak tertulis yang masyarakat setujui dan patuhi. Dalam konteks keamanan siber, ini bisa berupa etika dan norma perilaku online yang baik. Sebagai contoh, norma masyarakat dapat mencakup penolakan terhadap perilaku seperti phishing atau pembajakan. Membangun dan mempromosikan norma ini dapat membantu mendukung upaya regulasi hukum.

Ketiga, pasar mengatur perilaku melalui mekanisme ekonomi, seperti insentif dan hambatan. Misalnya, jika perusahaan dapat meningkatkan reputasinya atau mendapatkan lebih banyak pelanggan dengan memiliki standar keamanan siber yang baik, mereka akan memiliki insentif pasar untuk melakukannya. Oleh karena itu, pemerintah dan regulator dapat menciptakan kondisi di mana pasar mendorong keamanan siber yang lebih baik. Keempat, arsitektur (teknologi): Arsitektur atau teknologi juga bisa mengatur perilaku. Misalnya, jika sistem teknologi dirancang dengan fitur keamanan yang kuat, pengguna akan lebih sulit untuk melakukan tindakan yang merugikan keamanan. Dalam hal ini, desain dan penggunaan teknologi dapat dan harus menjadi bagian dari strategi regulasi.

[71] Larry Lessig, (1999). Code: And Other Laws of Cyberspace. New York: Basic Books.

Jika merujuk pada kondisi regulasi dan perundang-undangan yang ada saat ini, guna mendukung pembangunan sistem keamanan siber di IKN, setidaknya dibutuhkan dua regulasi. Pertama, segera dilakukan pembahasan dan pengesahan terhadap Rancangan Undang-Undang Keamanan dan Ketahanan Siber, dan yang kedua adanya undang-undang khusus, terkait dengan sistem keamanan siber kota pintar. Selain itu, pemerintah perlu merevisi dan pemyempurnakan UU ITE agar UU lebih bertaji dalam menghadapi kejahatan siber yang terus berkembang. Pada sisi lain, perlu ada perbaikan redaksional hukum terhadap pasal-pasal karet yang multitafsir yang membuka peluang terjadinya kriminalisasi. Hal lain yang perlu ditambahkan adalah perlindungan hukum terhadap *ethical hacker* dan praktisi keamanan siber yang membantu melakukan pengecekan kelemahan pada satu sistem digital semestinya dilindungi dan tidak dikriminalisasi. Saat mereka menemukan adanya lubang keamanan pada sistem, dan memberikan informasinya kepada pemilik sistem, hal tersebut semestinya bukan dianggap peretasan dan upaya melakukan akses ilegal. Sebaliknya, hal tersebut merupakan bentuk kontribusi agar pemilik sistem atau penyedia layanan digital dapat memperbaiki kelemahan keamanan yang ditemukan. Fenomena tersebut sebenarnya merupakan suatu norma umum yang berlaku global. Sejumlah perusahaan besar seperti Microsoft atau Google bahkan seringkali mengganjar para *ethical hacker* yang mampu menemukan kelemahan keamanan yang dimilikinya dengan hadiah besar.

Hal ini karena tata kelola regulasi yang mendukung sistem keamanan siber di IKN idealnya harus mencerminkan praktik terbaik di tingkat internasional, namun tetap relevan dengan konteks nasional Indonesia. Memastikan keamanan siber di Ibu Kota Nusantara (IKN) adalah langkah krusial dalam mempersiapkan perkembangan teknologi dan integrasi digital yang pesat. Sebuah tata kelola regulasi yang baik haruslah responsif terhadap tantangan keamanan siber yang dinamis, seraya mendukung inovasi dan pertumbuhan. Berikut upaya membangun tata kelola regulasi yang diharapkan dapat mendukung sistem keamanan siber di IKN:

a. Pemahaman Konteks:

Sebelum menetapkan regulasi, pemerintah harus memahami benar kondisi keamanan siber saat ini di Indonesia dan bagaimana perkembangannya di masa depan, terutama dengan adanya IKN. Pemahaman konteks ini melibatkan analisis SWOT, pemetaan aktor kunci, dan pemahaman terhadap tren teknologi yang muncul.

b. Kolaborasi Multi-Stakeholder:

Pembuatan regulasi tidak bisa dilakukan oleh pemerintah saja. Diperlukan kerjasama antara pemerintah, industri, komunitas teknologi, akademisi, dan masyarakat untuk menghasilkan regulasi yang inklusif dan efektif. Dialog dan diskusi harus rutin dilakukan untuk memahami perspektif dan kebutuhan dari masing-masing pihak.

c. Mengadopsi Standar Internasional:

Dengan melihat ke berbagai negara yang telah maju dalam keamanan siber, Indonesia bisa belajar dan mengadopsi standar internasional yang telah terbukti efektif. Ini akan membantu IKN dalam berkolaborasi dan berkomunikasi dengan entitas internasional.

d. Penyusunan Regulasi yang Fleksibel:

Dengan perkembangan teknologi yang begitu cepat, regulasi harus dirancang dengan fleksibilitas, memungkinkan penyesuaian ketika ada teknologi atau ancaman baru.

e. Penyusunan Dokumen Strategis:

Buat dokumen strategis seperti "Blueprint Keamanan Siber IKN" yang mencakup visi, misi, tujuan, serta strategi untuk mencapainya. Dokumen ini akan menjadi panduan bagi semua stakeholder.

f. Mekanisme Respons Cepat:

Buatlah mekanisme respons cepat untuk insiden kea manan, yang melibatkan koordinasi antar-instansi, serta integrasi dengan sektor swasta dan komunitas.

g. Adaptasi dan Inovasi:

Pertahankan sikap yang adaptif dan terbuka terhadap inovasi. Saat ada perkembangan baru dalam dunia siber, tata kelola harus siap beradaptasi dan inovatif dalam mencari solusi.

Dengan tata kelola regulasi yang komprehensif dan terstruktur seperti ini, diharapkan sistem keamanan siber di IKN dapat terbangun dengan kuat, tangguh menghadapi ancaman, serta mendukung perkembangan teknologi dan inovasi di ibu kota baru Indonesia.

15. Membangun Tata Kelola Kelembagaan Yang Tepat Untuk Mengimplementasikan Sistem Keamanan Siber Yang Tangguh di IKN.

Indonesia saat ini sudah memiliki Badan Siber dan Sandi Negara (BSSN) yang menjadi *leading sector* terkait dengan keamanan siber nasional. BSSN adalah lembaga pemerintah Indonesia yang memiliki peran penting dalam keamanan informasi dan keamanan siber nasional. Lembaga ini didirikan pada 19 Mei 2017 berdasarkan Peraturan Presiden Nomor 53 Tahun 2017. BSSN merupakan penggabungan dan penguatan dari beberapa badan sebelumnya, termasuk Lembaga Sandi Negara dan Direktorat Keamanan Informasi, yang berada di bawah Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika.

Alasan utama dibentuknya BSSN adalah meningkatnya tantangan dan ancaman keamanan siber seiring dengan kemajuan teknologi komunikasi dan informasi. BSSN bertanggung jawab untuk membangun dan menjaga keamanan informasi dan siber nasional. Lembaga ini juga berperan dalam peningkatan pertumbuhan ekonomi nasional, khususnya terkait dengan e-commerce. Pada 29 Oktober 2019, BSSN dan PT Huawei Tech Investment, sebuah perusahaan teknologi China, resmi menjalin kerja sama di bidang keamanan siber.

Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, yang ditetapkan oleh Presiden Joko Widodo pada 13 April 2021, adalah dasar hukum terkini dari BSSN. Lembaga ini berada di bawah dan bertanggung jawab langsung kepada Presiden. BSSN memiliki visi untuk menjadi institusi yang tepercaya dalam menjaga keamanan siber dan sandi nasional. Dalam menjalankan misinya, BSSN menerapkan tata kelola keamanan siber dan sandi yang komprehensif, membangun kemandirian teknologi keamanan siber dan sandi, serta berupaya mendorong tumbuhnya industri dalam negeri di bidang tersebut.

Organisasi BSSN terdiri dari sekretariat utama, inspektorat, empat bidang deputi, dan empat pusat penelitian dan pendidikan. BSSN bertanggung jawab melaksanakan berbagai fungsi di bidang keamanan siber, termasuk perumusan dan penetapan kebijakan teknis, pelaksanaan kebijakan, penyusunan norma, standar, prosedur, dan kriteria, serta pengawasan atas pelaksanaan tugas di lingkungan BSSN.

Selama ini BSSN juga berkoordinasi dengan berbagai lembaga lain, termasuk Kementerian Luar Negeri, Kementerian Pertahanan, Tentara Nasional Indonesia, Kepolisian Republik Indonesia, dan Kementerian Komunikasi dan Informatika, untuk mendukung pelaksanaan tugas-tugas yang terkait dengan keamanan siber.

Keberadaan BSSN sebagai lembaga yang bertanggung jawab terhadap keamanan siber di Indonesia, sedikit banyak telah mendorong adanya kesadaran pentingnya keamanan siber. Berdasarkan *The Global Cybersecurity Index (GCI),* skor keamanan siber Indonesia pada tahun 2022 mencapai 94,88 dan menempatkan Indonesia pada peringkat 24 dari 194 negara di dunia. Pencapaian tersebut mencederung meningkat jika dibandingkan pada tahun 2018, Indonesia masih berada di peringkat 41[72]. Sekalipun jika merujuk pada indikator lain, yaitu *National Cyber Security Index (NCSI)*, skor indeks keamanan siber Indonesia masih memiliki nilai 38,96 poin dari 100 pada tahun 2022. Angka tersebut menempatkan Indonesia pada peringkat 83 dari 160 negara di dunia, dan menjadi Indonesia berada di peringkat 3 terendah di antara negara-negara G20 lainnya[73].

Situasi ini memperlihatkan bahwa keberadaan BSSN dalam mengelola dan membangun keamanan siber di Indonesia masih perlu ditingkatkan. Terlebih pada tahun 2021 dan 2022, situs resmi BSSN sempat mengalami peretasan. Hal ini jelas mencoreng integritas BSSN sebagai lembaga yang dibentuk untuk mencegah potensi serangan siber di Indonesia. Eksistensi BSSN juga kembali dipertanyakan ketika lembaga ini diberitakan oleh

[72] https://inet.detik.com/security/d-6227093/indeks-keamanan-siber-ri-ke-24-di-tingkat-global-ke-3-di-asean diakses pada tanggal 6 Agustus 2023 pukul 20.18 WIB.
[73] https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20 diakses pada tanggal 6 Agustus 2023 pukul 20.18 WIB.

sejumlah media terlibat saling lempar tanggung jawab dengan Kementerian Komunikasi dan Informasi dalam menanggapi serentetan pencurian data yang dilakukan oleh hacker berjuluk Bjorka pada tahun 2022 lalu.

Pada tahun lalu, Indonesia mengalami serangan hacker Bjorka yang mengakibatkan bocornya surat rahasia untuk Presiden Jokowi, termasuk dari Badan Intelijen Negara (BIN). Data ini dijual oleh Bjorka dengan harga yang cukup murah di forum breached.to. Isu ini memunculkan "pertikaian" antara berbagai institusi di Indonesia, yang saling lempar tanggung jawab. Menteri Komunikasi dan Informatika, Johnny G Plate, menunjuk Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertanggung jawab menangani serangan hacker.

Sementara BSSN merespons, bahwa keamanan siber adalah tanggung jawab bersama, bukan hanya BSSN. BSSN juga menjelaskan bahwa mereka berwenang untuk merumuskan dan menetapkan kebijakan teknis di bidang keamanan siber, sesuai dengan pedoman dan peraturan yang mereka buat. Hal ini sesuai dengan amanat PP No. 71 Tahun 2019, penyelenggara sistem elektronik harus menyediakan sistem yang aman dan dapat dipertanggungjawabkan. Kominfo berpendapat bahwa instansinya telah bekerja dalam lingkup hukum dan aturan yang tersedia, dan tidak dapat melampaui atau menabrak tugas dan fungsi lembaga atau institusi lain. Sebab menurut PP 71 tahun 2019, serangan siber menjadi domain teknis BSSN[74].

Pertikaian antar lembaga terkait insiden keamanan siber menunjukan tata kelola kelembagaan terkait keamanan siber di negeri ini masih memerlukan pembenahan. BSSN sebagai leading sector semestinya bisa berlaku seperti Badan Nasional Penanggulangan Terorisme (BNPT) yang cenderung lebih mampu mengorkestrasi upaya penanggulangan tindak pidana terorisme di Indonesia hingga negeri ini kini relatif lebih aman dari aksi teror. Dalam arti, BSSN semestinya bisa selalu ada di depan dan mampu memberikan penjelasan yang lengkap saat terjadi adanya insiden terkait keamanan siber yang terjadi di Indonesia. Tidak hanya harus tahu dan

[74] https://www.cnbcindonesia.com/news/20220910125507-4-370980/bjorka-berulah-2-instansi-ini-saling-lempar-tanggung-jawab diakases pada tanggal 6 Agustus 2023 pukul 20.20 WIB.

mampu menjelaskan apa yang terjadi, lembaga ini semestinya juga bisa segera menginformasikan kepada publik sejumlah langkah yang akan diambil agar insiden keamanan siber yang terjadi tidak berulang.

Carut marut tata kelola kelembagaan terkait keamanan siber terjadi karena sebelumnya, Indonesia belum memiliki strategi keamanan siber nasional serta manajemen krisis siber, sehingga belum ada pembagian peran dan kewenangan yang jelas dalam memitigasi dan menangani krisis siber. Bahkan hingga kini tim respon insiden keamanan siber (CSIRT) belum dimiliki oleh seluruh instansi pemerintah.

Hal tersebut merupakan satu tantangan dalam tata kelola kelembagaan yang semestinya memi

Oleh sebab itu, keluarnya Perpres 47 tahun 2023 semestinya menjadi momentum untuk mengatur tata kelola kelembagaan dalam sistem keamanan siber nasional. Para pihak terkait harus memiliki peran dan kewenangan yang jelas dalam membangun sistem keamanan siber. Seperti telah dijelaskan oleh Ralph Linton, "role" atau peranan adalah elemen dinamis dari "status" atau kedudukan. Ketika seseorang menjalankan hak dan tanggung jawabnya sesuai dengan statusnya, berarti ia sedang menjalankan perannya. Oleh karena itu, konsep peranan dan kedudukan sangat terkait dan bergantung satu sama lain. Kedudukan tanpa peranan, atau sebaliknya, peranan tanpa kedudukan, tidak mungkin ada. Ini menandakan bahwa peranan tersebut menentukan bagaimana seseorang berkontribusi kepada masyarakat dan sekaligus menentukan apa yang masyarakat harapkan darinya.

Penguatan tata kelola sistem keamanan siber sangat krusial bagi IKN. Hal ini karena sejak awal, IKN sudah direncanakan akan dibangun dengan konsep *smart city*. Selaras dengan Teori Sinergitas Deardoff dan Williams, yang mengartikan sinergitas sebagai proses dimana kombinasi antara dua entitas atau lebih menghasilkan dampak yang lebih signifikan daripada jika entitas tersebut menjalankannya secara sendiri-sendiri. Pembangunan IKN sebagai *smart city*, harus menjadi momentum bagi BSSN untuk bersinergi dengan Otorita IKN, Bappenas dan berbagai *stakeholder* terkait dan membuktikan bahwa Indonesia mampu mewujudkan sistem keamanan siber

yang handal dan mampu memberikan proteksi terhadap pengelolaan IKN sebagai kota pintar di mana berbagai infrastruktur dan pelayanan publik akan terintegrasi dalam sistem berbasis internet.

Tata kelola keamanan siber di IKN akan menjadi komponen yang super penting dalam menjaga integritas, keandalan, dan keamanan informasi dan infrastruktur kritis. Oleh sebab itu, berikut beberapa pertimbangan mengenai tata kelola, *leading sector*, dan kementerian yang mungkin perlu dilibatkan:

Tata Kelola kelembagaan yang akan bertanggung jawab terhadap sistem keamanan siber di IKN mensyaratkan perlunya pembentukan badan terpusat. Pemerintah dapat membentuk sebuah badan atau otoritas khusus yang bertanggung jawab atas keamanan siber di IKN. Badan ini akan mengoordinasikan antara berbagai *stakeholder*, guna menetapkan standar keamanan IKN, dan memastikan pelaksanaannya. Sejumlah tugas dan kewenangan dari badan keamanan siber IKN ini nantinya akan bertanggung jawab terhadap:

a. Pembentukan Kerangka Kerja Keamanan Siber: Pada tahap awal, pemerintah harus menetapkan kerangka kerja keamanan siber nasional yang mencakup kebijakan, peraturan, dan prosedur. Kerangka kerja ini akan membantu menentukan standar dan praktik terbaik dalam bidang keamanan siber.
b. Penyusunan Strategi dan Kebijakan Keamanan Siber: Setelah kerangka kerja diatur, pemerintah harus merumuskan strategi dan kebijakan keamanan siber yang menetapkan tujuan, sasaran, dan inisiatif kunci. Strategi ini harus melibatkan semua pemangku kepentingan utama, termasuk pemerintah, sektor swasta, organisasi non-pemerintah, dan masyarakat umum.
c. Membangun Infrastruktur Keamanan Siber: Langkah selanjutnya adalah membangun infrastruktur yang kuat untuk mendukung implementasi kebijakan dan strategi tersebut. Ini mencakup pembentukan pusat respon insiden keamanan siber (CSIRT), pengadaan teknologi dan perangkat keras keamanan canggih, dan pelatihan sumber daya manusia.

d. Peningkatan Kapasitas dan Pelatihan: Tata kelola yang efektif juga membutuhkan peningkatan kapasitas dan pelatihan yang berkelanjutan. Pemerintah harus berinvestasi dalam pengembangan keterampilan keamanan siber di seluruh sektor dan tingkat, dan juga menyediakan pelatihan untuk para pemangku kepentingan utama.
e. Kerjasama dan Koordinasi Antar Lembaga: Untuk mewujudkan tata kelola yang kuat dan efektif, kerjasama dan koordinasi antar lembaga sangat penting. Ini mencakup koordinasi antara badan pemerintah, sektor swasta, dan organisasi internasional.
f. Evaluasi dan Penilaian Kinerja: Akhirnya, pemerintah harus memantau dan mengevaluasi kinerja sistem keamanan siber secara rutin. Ini melibatkan penilaian risiko, audit keamanan, dan peninjauan kinerja lembaga keamanan siber.

Dalam hal ini, Badan Siber dan Sandi Negara (BSSN) tetap menjadi *leading sector* yang akan mengkoordinir keamanan siber IKN. BSSN tidak akan bertindak sendirian, namun akan ada sejumlah lembaga dan kementerian yang perlu dilibatkan, diantaranya:

a. Kementerian Komunikasi dan Informatika: Untuk regulasi teknologi dan komunikasi.
b. Kementerian Pertahanan: Dalam aspek pertahanan nasional siber.
c. Kementerian Keuangan: Mengelola aspek keamanan dalam transaksi keuangan dan anggaran negara.
d. Kementerian Dalam Negeri: Koordinasi dengan pemerintah daerah dan lembaga pemerintahan lainnya.
e. Kementerian Luar Negeri: Dalam hal kerjasama internasional dan perjanjian terkait keamanan siber.
f. TNI dan Polri: Dalam penegakan hukum dan respons terhadap insiden keamanan siber.
g. Badan Intelijen Negara: Untuk pengumpulan intelijen dan analisis ancaman.
h. Lembaga Regulator dan Pengawas: Seperti Otoritas Jasa Keuangan (OJK) untuk sektor keuangan.
i. Otorita IKN: Sebagai pengelola pemerintahan IKN.

Pembentukan tata kelola yang efektif akan memerlukan kolaborasi yang erat antara berbagai sektor pemerintah, swasta, dan non-pemerintah. Ini akan memastikan bahwa keamanan siber diterapkan secara konsisten di seluruh sektor dan dapat menanggapi dinamika ancaman yang cepat berubah. Dengan pendekatan terintegrasi dan partisipasi dari semua stakeholder relevan, IKN dapat membangun keamanan siber yang kuat dan resilien yang mendukung visi menjadi kota dunia yang inklusif dan berkelanjutan

16. Menyiapkan Infrastruktur Sistem Keamanan Siber di IKN

Indonesia terdiri dari lebih dari 17.000 pulau, yang membuat pembangunan infrastruktur fisik maupun digital menjadi sangat menantang. Biaya investasi yang diperlukan untuk menghubungkan setiap pulau dengan jaringan kualitas tinggi menjadi salah satu hambatan utama. Konsentrasi Pembangunan di Pulau Jawa, menyebabkan sebagian besar infrastruktur digital berkualitas tinggi terkonsentrasi di Pulau Jawa, khususnya di kota-kota besar seperti Jakarta, Bandung, Surabaya, dan Yogyakarta. Hal ini membuat wilayah lain seperti Sumatera, Kalimantan, Sulawesi, dan Papua mengalami ketertinggalan.

Meskipun banyak wilayah yang telah mendapatkan akses internet, kualitasnya seringkali tidak stabil dan berkecepatan rendah. Ini mempengaruhi kualitas pengalaman pengguna dan membatasi pemanfaatan teknologi informasi untuk kegiatan produktif. Beberapa wilayah terpencil, biaya akses internet cenderung lebih tinggi dibandingkan dengan wilayah perkotaan. Hal ini disebabkan oleh kurangnya kompetisi dan biaya infrastruktur yang lebih tinggi. Pemerintah Indonesia telah menyadari kesenjangan ini dan berupaya meningkatkan infrastruktur digital dengan program seperti Palapa Ring. Namun, implementasinya membutuhkan waktu dan sumber daya yang signifikan.

Demikian halnya dengan IKN, meskipun wilayah IKN sedang dalam tahap pembangunan intensif, infrastruktur digital di Kalimantan secara umum masih memerlukan perhatian. Kementerian Komunikasi dan Informatika (Kemenkominfo) telah melakukan pemetaan terhadap kebutuhan kapasitas jaringan *backbone* (jaringan utama) dan jaringan akses (*lastmile*) di Ibu Kota

Negara (IKN) Baru. Pemetaan ini mencakup infrastruktur yang mendukung perangkat aktif dan pasif untuk layanan *broadband* tetap (*fixed broadband*) dan layanan *broadband* seluler (*mobile broadband*).

Kemenkominfo juga telah menyelesaikan desain infrastruktur jaringan telekomunikasi di IKN. Desain ini didasarkan pada masterplan atau peta jalan dari Badan Perencanaan Pembangunan Nasional (Bappenas). Koordinasi telah dilakukan antara Kemenkominfo dan pihak-pihak terkait untuk mempersiapkan layanan telekomunikasi dengan teknologi seluler terbaru, yaitu 5G, di IKN. Tujuannya adalah mendukung layanan publik dan implementasi konsep *smart city*. Teknologi 5G diharapkan dapat mengatasi masalah *latency* (keterlambatan) yang mungkin terjadi saat menggunakan teknologi 4G, sehingga sistem *smart city* di IKN Baru dapat berfungsi dengan optimal[75].

Kemenkominfo, melalui BLU Badan Aksesibilitas Telekomunikasi dan Informasi (Bakti), berencana membangun jaringan Palapa Ring Integrasi antara tahun 2022-2024. Jaringan ini akan mendukung konektivitas internet di berbagai wilayah Indonesia, termasuk IKN, dengan menghubungkan jaringan yang sudah ada dari Palapa Ring Tengah ke IKN melalui kota Balikpapan. Kemenkominfo berkomitmen untuk mengambil langkah-langkah strategis dalam pembangunan infrastruktur telekomunikasi dan adopsi teknologi digital di IKN Baru. Semua upaya ini dilakukan untuk mendukung visi Indonesia 2045 dan konsep "Kota Dunia Untuk Semua".

IKN akan dibangun dengan konsep kota pintar (*smart city*). Konsep kota pintar pertama kali diperkenalkan pada tahun 1990 untuk menggabungkan perangkat keras dan perangkat lunak berbasis teknologi informasi dan komunikasi (TIK) canggih dalam perencanaan kota (Bibri & Krogstie, 2017)[76].

Smart city memanfaatkan TIK untuk meningkatkan kualitas hidup warganya, mendorong ekonomi, memfasilitasi proses untuk menyelesaikan masalah transportasi dan lalu lintas melalui manajemen yang tepat,

[75] https://investor.id/it-and-telecommunication/279206/kemenkominfo-siap-bangun-infrastruktur-telko-di-ikn-baru diakses pada tanggal 7 Agustus 2023 pukul 20.30 WIB.
[76] Bibri, S. E., & Krogstie, J. (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. Sustainable Cities and Society, 31, 183–212. https://doi.org/10.1016/j.scs.2017.02.016

mendorong lingkungan yang bersih dan berkelanjutan, dan menyediakan interaksi yang dapat diakses dengan otoritas pemerintah yang relevan (Ismagilova , Hughes, Dwivedi & Raman, 2019)[77].

Sebagai kota yang dirancang menjadi *smart city*, Ibu Kota Nusantara diarahkan untuk menjadi lebih efektif, efisien, "hijau", dan lebih aman dibandingkan kota-kota lain di Indonesia dan di dunia pada umumnya. Teknologi canggih akan menjadi basis utama dalam mencapai target kenyamanan, keselamatan, dan keamanan kota dengan tujuan memberikan pelayanan publik yang terkoordinasi, termasuk didalamnya upaya untuk mencapai target sebagai kota layak huni (*livable city*).

Sebagai sebuah *smart city,* Ibu Kota Nusantara akan dilengkapi dengan teknologi informasi dan komunikasi terkini. Ibu Kota Nusantara sebagai *smart city* merupakan sebuah kota dengan optimalisasi pemanfaatan teknologi dan inovasi dalam upaya mencapai optimalisasi pelayanan publik bagi seluruh masyarakatnya. Tidak hanya itu, teknologi yang digunakan dalam Ibu Kota Nusantara juga diarahkan untuk dapat merespon kebutuhan masyarakat modern, khususnya dalam peningkatan efisiensi, keamanan, serta kualitas hidup dengan pemanfaatan teknologi terkini[78].

Perencanaan kota berdasarkan konsep kota pintar diharapkan dapat mengatasi tantangan perkotaan seperti transportasi yang padat, jaringan energi karbon tinggi, pemeliharaan dan perbaikan infrastruktur, serta keamanan dan kebijakan perkotaan serta menggunakan teknologi dan sistem canggih. Karena kompleksitas sistem yang dibutuhkan untuk pengembangan kota pintar, fungsionalitas sistem kota pintar menjadi rentan. Kerentanan tersebut dapat disebabkan oleh risiko operasional, risiko strategi, dan risiko eksternal (Mikes, 2012)[79].

Penggunaan teknologi, sistem integrasi, dan tata kelola dapat mengundang risiko teknis dan non-teknis. Risiko seperti itu mungkin tidak dipahami dengan baik oleh para perencana, dan dapat menyebabkan

[77] Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019). Smart cities: Advances in research—An information systems perspective. International Journal of Information Management, 47, 88–100. https://doi.org/10.1016/j.ijinfomgt.2019.01.004.

[78] Buku Saku Pemindahan Ibu Kota Negara. 2021. Kementerian Perencanaan Pembangunan Nasional/ Badan Perencanaan Pembangunan Nasional Republik Indonesia.

[79] Mikes, A. (2012). Managing Risks: A New Framework. June.

kesalahan persepsi tentang aplikasi dan keuntungan kota pintar. Kemampuan merancang ekosistem *smart city* dan kemampuan mengintegrasikannya dengan proses manajemen risiko yang lebih baik dapat mendukung tujuan *smart city*[80].

Keamanan siber *Smart city* adalah masalah yang sangat penting yang melibatkan pertimbangan beberapa masalah keamanan tentang teknologi, aplikasi, infrastruktur, dan informasi/data. Terutama keamanan dunia maya dipengaruhi oleh integrasi teknologi yang muncul dan menghasilkan komunikasi intensif, kompleksitas tinggi, dan saling ketergantungan tinggi, yang mengarah pada permukaan serangan tanpa batas dan masalah terkait kriptografi. Keamanan siber kota pintar merupakan isu penting yang membutuhkan kolaborasi internasional, termasuk pakar dari seluruh dunia.

Konsep kota cerdas pada dasarnya menyediakan sebuah layanan yang dapat mengelola dan membantu menyelesaikan isu–isu sosial-ekonomi yang berhubungan dengan permasalahan masyarakat. Terdapat beberapa kelompok pada isu sosialekonomi tersebut diantaranya kesehatan, komunikasi, transportasi, privasi masyarakat, dan *entrepreneurship*[81].

a. Kesehatan dan Risiko Keamanan Siber:

   Kesehatan, salah satu aspek paling vital dalam kehidupan kita, saat ini mengalami transformasi digital. Dengan semakin banyaknya data kesehatan yang disimpan secara digital, informasi tersebut menjadi harta berharga yang, sayangnya, juga menarik bagi para peretas. Di Indonesia sendiri, kita telah melihat betapa nyatanya ancaman ini dengan insiden di Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais[82]. Mereka menjadi sasaran serangan, sebuah peringatan keras bagi kita semua bahwa keamanan siber adalah prioritas. Tidak cukup bagi kita untuk bermigrasi ke cloud atau teknologi canggih

[80] Sharif, R.A. dan Pokharel, Shaligram. (2022). *Smart city* Dimensions and Associated Risks: Review of literature. Journal Sustainable Cities and Society 77 (2022)103542. https://www.sciencedirect.com/journal/sustainable-cities-and-society

[81] Bapppenas RI, (2022). Rencana Aksi Strategis Pembangunan Ibu Kota Negara Bidang Pertahanan dan Keamanan. Jakarta: Bappenas RI.

[82] https://www.suara.com/tekno/2017/05/14/050900/rs-harapan-kita-dan-dharmais-diserang-hacker-ini-kata-kominfo diakses pada tanggal 7 Agustus 2023 pukul 20.20 WIB.

lainnya tanpa memastikan bahwa keamanannya juga meningkat seiring dengan perkembangan tersebut.

b. Komunikasi dan Kerentanannya:

Saat kita berbicara tentang komunikasi di era digital, kita membahas lebih dari sekedar panggilan telepon atau pesan teks. Infrastruktur telekomunikasi adalah jantung dari kota cerdas. Namun, jantung ini rentan terhadap serangan siber, terutama dengan adopsi teknologi M2M yang memperluas jaringan komunikasi kita. M2M, sementara memfasilitasi efisiensi, juga menciptakan lebih banyak pintu masuk bagi para peretas.

c. Transportasi dalam Kota Cerdas:

Transportasi, sebagai tulang punggung perkotaan, telah mengalami perubahan revolusioner berkat konsep kota cerdas. Layanan yang terintegrasi seperti pengaturan lalu lintas, sistem navigasi, dan pengelolaan parkir mengubah cara kita berinteraksi dengan lingkungan kota. Namun, dengan integrasi ini datang risiko keamanan tambahan. Sebagai contoh, penggunaan GPS memang memfasilitasi navigasi yang lebih baik, tetapi pada saat yang sama, memperkenalkan masalah privasi, karena lokasi kita dapat dengan mudah dilacak dan dimonitor.

d. Privasi Masyarakat dan Tantangan Keamanan:

Dalam kota cerdas, konsep privasi menjadi lebih kompleks. Di satu sisi, layanan berbasis teknologi informasi memberikan kemudahan dan efisiensi, tetapi di sisi lain, mereka mengumpulkan data pribadi kita, menciptakan tantangan besar dalam menjaga informasi tersebut tetap aman dan pribadi. Serangan terhadap data pribadi bukan hanya masalah teoritis; itu adalah realitas yang dapat mengakibatkan kerugian finansial dan kerusakan reputasi.

e. Entrepreneurship dan Ekonomi Digital:

Kota cerdas adalah katalis untuk inovasi dan pertumbuhan ekonomi. Namun, di balik potensi pertumbuhan ekonomi yang luar biasa ini, ada ancaman yang bersembunyi, terutama dalam sektor perbankan dan bisnis. Di era digital, transaksi keuangan telah menjadi lebih cepat dan mudah, tetapi juga menjadi target bagi peretas. Serangan pada sektor

ini bisa memiliki dampak yang jauh lebih besar, mengancam seluruh ekosistem ekonomi kota.

Dengan demikian, saat kita merangkul konsep kota cerdas, kita harus selalu waspada terhadap potensi risiko. Meski menjanjikan banyak keuntungan, kota cerdas juga memerlukan perhatian khusus pada aspek keamanan dan privasi. Sebagai masyarakat, kita harus bekerja sama untuk memastikan bahwa teknologi bekerja untuk kebaikan kita, tanpa mengorbankan keamanan dan privasi kita.

Selain itu, dalam perkembangan kota cerdas, faktor pemerintahan sering kali menjadi tonggak utama yang mempengaruhi banyak aspek, termasuk keamanan siber. Dengan mengakui bahwa permasalahan kota cerdas tidak hanya berlandaskan pada isu socio-ekonomi, kita mesti melihat lebih dalam pada bagaimana faktor pemerintahan mempengaruhi keamanan siber. Pemerintahan, dengan segala kebijakannya, dapat mempengaruhi banyak sektor, mulai dari infrastruktur hingga energi. Namun, ada titik krusial dalam pelaksanaan ini: bagaimana pemerintahan memastikan bahwa keamanan siber tetap terjaga.

a. Kebutuhan terhadap Pengujian Keamanan

Salah satu permasalahan yang sering muncul adalah banyak entitas pemerintah yang menjadi klien perusahaan teknologi cenderung melupakan pengujian keamanan. Fokus utamanya biasanya hanya pada fungsionalitas sistem yang mereka peroleh, sedangkan aspek keamanan seringkali menjadi sekunder. Hal ini tentu menjadi sebuah ironi, mengingat keamanan siber adalah salah satu pilar utama dalam pembangunan kota cerdas. Dengan mengabaikan pengujian keamanan, seluruh infrastruktur yang telah dibangun bisa saja rentan terhadap serangan. Oleh karena itu, penting bagi pemerintah untuk memberi perhatian lebih pada pengujian keamanan sistem yang mereka gunakan.

b. Ancaman pada Infrastruktur Kritis

Infrastruktur kritis menjadi bagian yang sangat penting dalam pemerintahan. Setiap gangguan, baik itu keterlambatan atau hilangnya layanan, bisa berdampak besar pada kelancaran proses pemerintahan.

Bidang kesehatan, industri, dan telekomunikasi merupakan beberapa dari infrastruktur kritis yang harus terus-menerus diawasi keamanannya. Mengingat sebagian besar infrastruktur kritis kini menggunakan teknologi seperti Internet-of-Things (IoT) dan smart grids, maka tantangan keamanan siber menjadi semakin kompleks. Tak hanya itu, data yang dihasilkan dari infrastruktur ini—biasanya dalam skala besar atau big data—perlu mendapatkan perlindungan ekstra. Data tersebut harus disimpan, dikelola, dan dilindungi dengan baik agar tidak mengalami gangguan atau serangan yang bisa mengakibatkan kerugian besar.

c. Optimisasi Energi dan Utilitas

Saat berbicara tentang energi dan utilitas, kita tidak bisa lepas dari konsep smart grids. Teknologi ini mengubah cara kita mengelola dan mendistribusikan energi, memberikan efisiensi yang lebih baik. Namun, ada harga yang harus dibayar: keamanan dan privasi data. Dengan mengandalkan teknologi cloud computing untuk mendukung fitur-fitur smart grids, kita juga harus siap menghadapi tantangan keamanan yang datang bersamanya. Baik pemerintah maupun pengguna harus selalu waspada dan memastikan bahwa data mereka tetap aman.

Sebagai kesimpulan, membangun kota cerdas memang menawarkan banyak keuntungan. Namun, kita harus selalu ingat bahwa keamanan siber adalah aspek yang sama pentingnya. Tanpa pengujian, perlindungan, dan optimasi yang tepat, visi kota cerdas bisa saja sirna seketika. Oleh karena itu, kerjasama antara pemerintah, perusahaan teknologi, dan masyarakat sangat diperlukan untuk menciptakan lingkungan kota cerdas yang aman dan berkelanjutan.

Merujuk pada informasi dari Rencana Aksi Strategis Pembangunan Ibu Kota Negara Bidang Pertahanan dan Keamanan yang dimiliki oleh Bappenas RI, konsep sistem keamanan siber IKN dibangun secara komprehensif guna menciptakan sebuah sistem yang kokoh untuk menjaga keamanan informasi digital.

Pada fondasi keamanan siber, terdapat infrastruktur yang menjadi penunjang utama dalam menjaga keamanan informasi. Terdapat tiga pilar utama dalam infrastruktur ini:

a. *Network/Communication Security:* Memastikan bahwa semua komunikasi yang terjadi dalam jaringan terlindungi dari intersepsi atau gangguan pihak ketiga yang tidak berwenang.
b. *Application Security*: Fokus pada keamanan aplikasi untuk mencegah adanya celah yang bisa dieksploitasi oleh pihak yang berpotensi merugikan.
c. *Data Security:* Melindungi data dari akses yang tidak sah, serta memastikan integritas dan ketersediaan data kapan pun dibutuhkan.

Tiga hal tersebut diimplementasikan pada beberapa kegiatan seperti pembangunan *Cyber Security Operation Center* (CSOC), pembangunan Pusat Data Keamanan Siber IKN, pembangunan Jaringan Keamanan Siber IKN, pemasangan sensor anomali siber pada titik-titik yang akan dipantau, pembuatan infrastruktur untuk penerapan framework keamanan siber, hingga pembangunan infrastruktur forensik digital.

a. *Cybersecurity Operations Centre* (CSOC) IKN: Sebagai tulang punggung dari tim Keamanan Siber IKN, CSOC memainkan peran penting dalam memantau dan mendeteksi ancaman yang bisa mengganggu keamanan siber. CSOC mengandalkan ribuan peranti yang dipasang di seluruh jaringan IKN. Setiap peranti ini berfungsi memberikan peringatan atau alert ketika mendeteksi ancaman, dan tim CSOC bertanggung jawab untuk menganalisa dan memberikan respons terhadap ancaman tersebut.
b. Pusat Data Keamanan Siber IKN: Merupakan pusat pengendalian utama bagi Keamanan Siber IKN. Dilengkapi dengan fasilitas jaringan yang canggih, komputer dengan kapasitas komputasi tinggi, serta penyimpanan data masif, pusat data ini menjaga data strategis dan rahasia IKN dari ancaman siber serta memastikan ketersediaan layanan data.

c. Sensor Anomali Siber: Sebagai salah satu benteng pertahanan, sensor ini dipasang pada berbagai perangkat keras di IKN, terutama pada perangkat pendukung kota cerdas. Sensor ini memonitor aktivitas jaringan, mendeteksi ancaman, dan memberikan respons cepat untuk menangkal potensi serangan.
d. Infrastruktur Forensik Digital: Fokus pada identifikasi dan penyelidikan ancaman digital. Ini termasuk investigasi kejahatan yang berhubungan dengan perangkat digital dan jaringan komputer.

Selain infrastruktur yang telah dijelaskan di atas, implementasi infostruktur Keamanan Siber IKN juga memiliki peran sentral. Infostruktur, yang mengacu pada aspek perangkat lunak dan manajemen data, menjadi jantung dari sistem keamanan siber. Ada beberapa komponen utama dalam infostruktur ini:

a. Pembuatan Perangkat Lunak Keamanan Siber: Ini melibatkan pengembangan atau adopsi perangkat lunak yang dirancang khusus untuk melindungi informasi dan sistem dari serangan siber.
b. Perangkat Lunak Pemantau Trafik: Perangkat lunak jenis ini fokus pada pemantauan aktivitas jaringan untuk mendeteksi perilaku mencurigakan atau ancaman potensial.
c. Aplikasi Manajemen Keamanan Siber IKN: Aplikasi ini menjadi pusat kontrol untuk mengelola berbagai aspek keamanan, termasuk manajemen risiko, respons insiden, dan pelaporan.
d. Perlindungan Data Strategis dan Rahasia: Menggunakan teknik-teknik canggih untuk memastikan bahwa data yang paling kritis aman dari akses yang tidak sah atau kehilangan.
e. Teknik Kriptografi: Mengacu pada penggunaan algoritma dan metode enkripsi untuk mengamankan data dan komunikasi, memastikan kerahasiaan, integritas, dan otentikasi.

Sementara infrastruktur dan infostruktur menangani aspek teknis, suprastruktur memastikan bahwa ada organisasi dan tata kelola yang tepat untuk mendukung keamanan siber. Dalam hal ini, beberapa elemen penting meliputi:

a. Pembentukan Unit Organisasi: Ini bisa berbentuk Kantor Keamanan Siber IKN atau Badan Keamanan Siber IKN, yang memiliki tanggung jawab utama untuk mengawasi dan mengelola semua inisiatif keamanan siber di IKN Nusantara.
b. Tata Kelola dan SOP: Penyusunan tata kelola yang jelas, standar operasional prosedur (SOP), serta peraturan yang mengatur bagaimana keamanan siber harus dikelola dan diterapkan.
c. Kepatuhan Standar: Ini termasuk kepatuhan terhadap standar internasional seperti ISO 27001, yang memberikan kerangka kerja untuk manajemen keamanan informasi.
d. Anggaran: Memastikan alokasi dana yang cukup untuk mendukung semua inisiatif keamanan siber, termasuk pembelian peralatan, pelatihan personil, dan operasi sehari-hari.
e. Personil: Merekrut, melatih, dan mempertahankan tim keamanan siber yang berkualitas untuk menghadapi tantangan yang terus berkembang di dunia siber.

Dengan kombinasi infrastruktur, infostruktur, dan suprastruktur yang kokoh, IKN Nusantara berkomitmen untuk memastikan keamanan dan integritas informasinya dalam menghadapi ancaman siber yang konstan dan berkembang. Konsep keamanan siber yang diadopsi oleh IKN Nusantara mencerminkan keseriusan dan komitmen untuk memastikan bahwa setiap data dan informasi yang dikelola berada dalam perlindungan yang maksimal.

Namun demikian, berdasarkan paparan di atas, strategi menyiapkan infrastruktur sistem keamanan siber di IKN tidak bisa dilakukan secara sembrono dan terpisah dari kerangka pembangunan IKN. Bahkan sebaliknya sebagian rencana pembangunan infrastruktur sistem keamanan siber harus menunggu saat perencanaan tata kota IKN sudah final dan memiliki perencanaan yang mendetil. Hal ini karena infrastruktur sistem keamanan siber IKN harus mampu melindungi berbagai infrastruktur dan kegiatan yang berlangsung di IKN. Oleh sebab itulah hingga kini belum ada satu perencanaan mendetil mengenai seperti apa sistem keamanan siber IKN akan dibangun kelak. Meski demikian, baik Bappenas, BSSN, BIN hingga TNI dan Polri masing-masing memiliki satu konsepsi sistem keamanan siber

yang kelak bisa dikolaborasikan guna mewujudkan satu sistem keamanan siber yang handal bagi IKN.

17. Menyiapkan Sumber Daya Manusia untuk Mendukung Sistem Keamanan Siber di IKN

Pada era digitalisasi yang sedang berkembang pesat, persiapan sumber daya manusia (SDM) yang berkualitas di bidang keamanan siber menjadi salah satu kunci utama untuk menjaga integritas, keamanan, dan kelancaran aktivitas di IKN. Salah satu kunci utama dalam membangun sistem keamanan siber yang kuat adalah dengan memiliki sumber daya manusia (SDM) yang kompeten dan handal. Namun, saat ini terdapat dua tantangan utama yang perlu dicarikan solusinya untuk memaksimalkan pemanfaatan teknologi digital, sekaligus mendukung sistem keamanan siber di IKN.

Pertama, Indonesia masih kekurangan talenta digital mumpuni. Talenta digital adalah orang yang cakap dan mampu menggunakan teknologi digital. Biasanya pengaplikasiannya untuk berbagai hal positif dan produktif. Padahal, total jumlah pemilik telepon seluler di Indonesia terdata 370,1 juta orang dan pengguna internet 210,3 juta orang. Selain itu, pengguna aktif media sosial mencapai 196,7 juta orang. Apalagi, potensi ekonomi digital Indonesia juga besar. Hingga tahun 2025, nilainya diperkirakan mencapai Rp 1.700 triliun[83].

Indonesia membutuhkan banyak talenta digital yang berkualitas demi bisa melakukan transformasi digital. Talenta itu dibutuhkan bukan sekadar untuk bisa mengoptimalkan peluang ekonomi digital Indonesia yang besar, melainkan juga menciptakan ruang digital yang bersih, sehat, dan bermanfaat dalam meningkatkan kesejahteraan masyarakat. Dari proyeksi pemerintah dalam 15 tahun mendatang, kebutuhan talenta digital Indonesia mencapai sembilan juta orang. Ini berarti rata-rata dibutuhkan sekitar 600.000 talenta digital setiap tahunnya. Akan tetapi, dalam praktiknya, perguruan tinggi Indonesia hanya berhasil memenuhi sekitar 150.000 hingga

[83] https://www.kompas.id/baca/nusantara/2023/07/29/indonesia-masih-kekurangan-talenta-digital diakses pada tanggal 6 Agustus 2023 pukul 20.00 WIB.

200.000 talenta digital setiap tahunnya. Kondisi ini menunjukkan adanya kesenjangan besar antara kebutuhan dan ketersediaan sumber daya manusia (SDM) digital yang ada[84].

Kedua, selaras dengan kesadaran tentang pentingnya talenta digital, literasi digital juga menjadi komponen krusial. Indonesia memang memiliki jumlah pengguna internet yang besar, namun belum tentu semua masyarakat memiliki pemahaman yang benar tentang internet, terutama dalam hal keamanan siber. Hal ini berisiko menyebabkan masyarakat menjadi korban hoaks, misinformasi, dan kejahatan siber lainnya. Sebab, serangan siber dapat berasal dari mana saja, dan target utamanya sering kali adalah masyarakat biasa. Melalui teknik seperti *phishing* atau *scam*, pelaku serangan siber mencoba mengeksploitasi ketidaktahuan pengguna. Dengan literasi digital yang baik, masyarakat Indonesia, khususnya yang akan tinggal di IKN akan lebih waspada terhadap taktik-taktik tersebut dan menjadi garis pertahanan pertama dalam melawan ancaman siber.

Dalam membangun sumber daya manusia yang mumpuni dalam bidang teknologi informasi dan keamanan siber membutuhkan upaya kolaboratif dan terpadu. Peningkatan kapasitas SDM, baik melalui pendidikan formal maupun pelatihan, serta pengembangan literasi digital merupakan langkah krusial dalam memastikan keberhasilan implementasi sistem keamanan siber di IKN. Dengan dukungan dan komitmen dari semua pihak, Indonesia dapat memanfaatkan potensi digitalnya secara maksimal dan memastikan keamanan siber yang tangguh.

Selama ini minat anak muda menekuni dunia digital cukup tinggi mengingat mereka umumnya merupakan *digital native* atau terlahir sudah mengenal teknologi. Namun, kemampuan mereka perlu terus ditingkatkan agar bisa mengimbangi perkembangan teknologi digital yang cepat. Oleh sebab itu, perguruan tinggi perlu adaptif dengan tren perkembangan teknologi digital saat ini dan ke depan, agar SDM yang dihasilkan sesuai dengan kebutuhan dunia kerja. Hal tersebut menunjukkan bahwa digital skill

[84] https://www.kominfo.go.id/content/detail/16892/indonesia-butuh-9-juta-digital-talent/0/sorotan_media diakses pada tanggal 6 Agustus 2023 pukul 19.50 WIB.

menjadi salah satu keterampilan yang harus dimiliki agar bisa terserap oleh industri. Terlebih, kebutuhan terhadap SDM talenta digital cukup tinggi.

Untuk mengatasi kesenjangan talenta digital, pemerintah telah menyiapkan kebijakan melalui dua pendekatan. Pertama, pendekatan jangka panjang. Upaya ini dilakukan melalui revitalisasi pendidikan, seperti perubahan kurikulum. Kedua, pendekatan jangka pendek. Hal ini secara paralel dilakukan pemerintah melalui berbagai program pendidikan dan pelatihan yang bekerja sama dengan institusi pendidikan dan platform *e-commerce.*

Talenta digital Indonesia sendiri punya potensi untuk berkembang hingga tingkat global karena dalam sejumlah pelatihan dan pendidikan hasil kerja sama pemerintah dengan perusahaan teknologi informasi berskala global seperti Google, persentase kelulusan peserta di atas 80 persen. Angka ini jauh lebih tinggi dibandingkan tingkat kelulusan program pelatihan Google di negara lain yang rata-rata mencapai 50-60 persen[85]. Meskipun persentase kelulusan cukup tinggi, tapi jumlah lulusannya belum mampu memenuhi kebutuhan talenta keamanan siber di Indonesia.

Sementara itu, IKN dirancang sebagai kota pintar (*smart city*) akan membutuhkan banyak SDM di bidang keamanan siber. Oleh karena itu, BSSN menyiapkan pusat pengembangan SDM yang dilengkapi dengan simulator kota pintar, keamanan siber, dan finansial. Nantinya, aparatur sipil negara (ASN) dari seluruh kementerian dan lembaga, yang akan ditugaskan di IKN Nusantara di bidang keamanan siber, akan dilatih di pusat pengembangan tersebut.

Selaras dengan teori Manajemen SDM dari Suparyadi (2015) yang menyatakan bahwa tujuan utama dari manajemen SDM adalah mengoptimalisasi dampak karyawan terhadap kinerja organisasi. Hal ini melibatkan berbagai aspek, mulai dari analisis pekerjaan, perencanaan kebutuhan SDM, rekrutmen, seleksi, hingga pelatihan, penilaian kinerja, dan pembinaan hubungan kerja yang harmonis. Badan Siber dan Sandi Nasional (BSSN) mengadakan pelatihan keamanan siber untuk mempersiapkan

[85] https://www.kompas.id/baca/humaniora/2022/09/05/dukungan-untuk-pengembangan-talenta-digital-meningkat diakses ada tanggal 6 Agustus 2023 pukul 20.00 WIB.

pegawai mereka menjadi pelatih bagi ASN dari kementerian dan lembaga lain yang akan bertugas di IKN Nusantara, Kalimantan Timur. Salah satu alat pelatihan yang dibuat oleh BSSN adalah simulator kota pintar. Tujuannya adalah untuk mendukung pembangunan *smart city* di IKN. Dengan adanya teknologi *smart city*, beberapa ancaman dari peretas seperti penyerangan sensor gas dan pengambilalihan turbin listrik menjadi perhatian. Oleh karena itu, peserta diajarkan teknik peretasan untuk memahami logika peretas dan mengantisipasi serangan yang mungkin terjadi[86].

Selain itu, ada juga kelas simulasi keamanan siber menggunakan platform daring, yaitu *Cyber Security Online Simulation Platform* (CSOSP). Di sini, peserta akan belajar meretas dan mempertahankan keamanan siber sistem elektronik. Peserta diajarkan tentang kerawanan keamanan yang sering terjadi pada aplikasi website, seperti SQL *injection, broken access control, cryptographic failures*, dan lainnya. SQL *injection* adalah salah satu serangan yang paling banyak terjadi di dunia, dan peserta diajarkan cara memanfaatkannya dan bagaimana cara mengatasinya. Keseluruhan skenario kerawanan tersebut dipelajari dalam waktu tiga hari. Namun, peserta diberikan akses ke lab simulasi untuk periode tertentu setelah pelatihan agar mereka dapat memperdalam pengetahuannya.

Pakar digital forensik, Ruby Alamsyah, mengapresiasi pelatihan yang diselenggarakan BSSN. Namun, ia juga mengingatkan bahwa pelatihan singkat tidak cukup untuk menjadikan seseorang ahli di bidang tersebut. Mereka perlu belajar di tempat-tempat yang lain untuk mendapatkan pengetahuan dan keterampilan yang lebih beragam. Pemerintah perlu memastikan bahwa mereka yang telah dilatih tidak dimutasi atau dipindahkan ke bidang lain yang tidak relevan, yang pada akhirnya dapat membuka celah keamanan kembali[87].

Sementara terkait belum meratanya literasi digital di tengah masyarakat. Kemenkominfo bekerja sama dengan sejumlah penggiat literasi digital terus berupaya meningkatkan dan memperluas jangkauan literasi digital masyarakat. Kemenkominfo melalui program Literasi Digital nasional

[86] https://www.kompas.id/baca/polhuk/2022/03/19/penjaga-keamanan-siber-pemerintah-belajar-meretas-sebelum-diretas diakses pada tanggal 7 Agustus 2023 pukul 20.20 WIB
[87] Ibid

menargetkan 50 juta masyarakat Indonesia terliterasi secara digital hingga tahun 2024[88].

Dari paparan di atas dapat disimpulkan bahwa sejauh ini pemerintah telah berhasil mengidentifikasi kendala dan tantangan terkait kesiapan SDM Indonesia dalam menghadapi transformasi digital dan kebutuhan SDM unggul terkait dengan IKN. Sejumlah langkah dan upaya yang dilakukan untuk mengatasi tantangan tersebut juga sudah berada pada jalur yang benar.

Kesiapan Sumber Daya Manusia (SDM) unggul menjadi salah satu faktor krusial dalam membangun sistem keamanan siber di Ibu Kota Negara (IKN). Hal ini karena sebagai kota pintar IKN akan menghadapi kompleksitas ancaman siber. Mulai dari serangan DDoS, ransomware, hingga serangan yang menyasar infrastruktur kritis, semua membutuhkan keahlian khusus untuk mendeteksinya dan mencegahnya. SDM yang unggul dan memiliki keahlian khusus di bidang keamanan siber diperlukan untuk mengidentifikasi, menganalisis, dan merespons ancaman-ancaman tersebut dengan cepat dan efektif.

Selain itu, sebagai Ibu Kota Negara, IKN tentunya akan dilengkapi dengan berbagai infrastruktur digital canggih. Namun, setiap teknologi memiliki kerentanannya. SDM unggul dengan pengetahuan mendalam tentang sistem dan arsitektur keamanan siber diperlukan untuk memastikan bahwa seluruh infrastruktur digital tersebut dilindungi dari potensi ancaman. Bagaimanapun, perkembangan teknologi terus berkembang dengan pesat, juga akan senantiasa diikuti oleh perkembangan metode serangan siber. SDM unggul di IKN dituntut mampu selalu *update* dengan perkembangan teknologi dan taktik serangan terbaru. Mereka harus mampu memahami teknologi terbaru, mengadopsinya ke dalam sistem keamanan, dan menyesuaikan strategi pertahanan sesuai dengan perkembangan tersebut.

Keberadaan SDM unggul di IKN tidak hanya berperan dalam aspek teknis saja, tetapi juga dalam membentuk kultur keamanan siber di IKN. Mereka bisa menjadi pelopor dan pendidik bagi masyarakat luas,

[88] https://www.kominfo.go.id/content/detail/49602/siaran-pers-no99hmkominfo062023-tentang-kolaborasi-kominfo-dan-tni-perkuat-literasi-digital-sektor-pemerintahan/0/siaran_pers diakses pada tanggal 7 Agustus 2023 pukul 20.20 WIB.

memastikan bahwa setiap individu memahami pentingnya keamanan siber dan bagaimana cara melindungi diri serta data-data mereka di dunia digital. Oleh sebab itu, guna memastikan keberlanjutan sistem keamanan siber di IKN, diperlukan investasi pada pembangunan kapasitas SDM jangka panjang untuk mempersiapkan generasi muda sebagai tenaga ahli keamanan siber di masa depan. Dengan demikian, penyiapan SDM unggul dalam keamanan siber bukan hanya sekadar memiliki tim yang mampu mengatasi ancaman saat ini, tetapi juga mempersiapkan IKN untuk menghadapi tantangan keamanan siber di masa mendatang. Beberapa upaya untuk menyiapkan SDM unggul yang berkelanjutan, dapat dilakukan melalui serangkai upaya berikut ini:

a. Pendidikan dan Pelatihan yang Berkesinambungan:

   Salah satu cara paling efektif untuk menyiapkan sumber daya manusia (SDM) dalam mendukung keamanan siber adalah melalui pendidikan dan pelatihan yang berkesinambungan. Pendidikan dasar mengenai keamanan siber harus dimulai sejak dini di lembaga pendidikan. Ini meliputi pemahaman dasar tentang bahaya dunia maya, bagaimana cara kerja serangan siber, serta teknik dasar pertahanan dan pencegahan.

b. Kerja Sama dengan Institusi dan Industri Terkait:

   Kerjasama dengan perguruan tinggi, lembaga riset, dan industri teknologi informasi sangat krusial. Dengan kolaborasi ini, pelatihan-pelatihan spesialisasi keamanan siber dapat diadakan untuk mempersiapkan SDM yang memiliki keahlian khusus dalam mengatasi ancaman-ancaman siber terbaru.

c. Rekrutmen dan Penempatan yang Tepat:

   Pemerintah perlu aktif merekrut individu yang memiliki kemampuan di bidang keamanan siber. Proses rekrutmen harus dilakukan secara ketat dengan memastikan bahwa mereka yang direkrut memang memiliki kualifikasi yang dibutuhkan. Selain itu, penempatan SDM di unit-unit keamanan siber di berbagai institusi pemerintah di IKN harus dilakukan dengan cermat.

d. Budaya Keamanan Siber:

Selain pendidikan formal, budaya keamanan siber harus ditanamkan di setiap lini pemerintahan. Semua pegawai harus sadar bahwa mereka adalah bagian dari rantai keamanan dan setiap tindakan yang mereka lakukan dapat mempengaruhi keamanan keseluruhan sistem.

e. Update Teknologi dan Infrastruktur:

Mempersiapkan SDM tidak hanya tentang memberikan pelatihan, tetapi juga memastikan bahwa mereka memiliki alat dan infrastruktur yang memadai untuk bekerja. Seiring dengan perkembangan ancaman siber, teknologi keamanan juga harus terus diperbarui.

f. Simulasi dan Latihan Rutin:

Untuk memastikan kesiapan SDM dalam menghadapi ancaman siber, simulasi serangan siber dapat dilakukan secara berkala. Dengan ini, tim keamanan siber dapat mempraktekkan pengetahuan dan keterampilan mereka dalam situasi nyata dan menemukan area-area yang perlu ditingkatkan.

g. Sertifikasi Profesional:

Pentingnya memiliki SDM yang memiliki kualifikasi dan kemampuan yang telah diakui secara internasional. Oleh karena itu, penyediaan akses ke sertifikasi profesional di bidang keamanan siber, seperti Certified Information Systems Security Professional (CISSP) atau Certified Ethical Hacker (CEH), dapat meningkatkan kualitas SDM.

h. Kerjasama Internasional:

Membangun hubungan dengan negara-negara lain untuk berbagi pengetahuan, riset, dan best practices dalam bidang keamanan siber. Dengan kolaborasi internasional, Indonesia bisa mendapatkan wawasan mengenai ancaman global dan solusi terbaru.

i. Penelitian dan Pengembangan:

Mengalokasikan dana untuk riset dan pengembangan dalam bidang keamanan siber. Inovasi dan solusi baru sering kali muncul dari penelitian, dan mendukung inisiatif ini bisa membantu Indonesia tetap berada di garis depan keamanan siber.

j. Kampanye Kesadaran Publik:

Mengadakan kampanye kesadaran publik mengenai pentingnya keamanan siber. Semakin banyak masyarakat yang sadar tentang pentingnya keamanan siber, semakin tinggi kemungkinan mereka untuk menjalankan praktik yang aman dan mendukung inisiatif keamanan.

k. Wacana Matra Siber:

Tingginya kebutuhan talenta keamanan siber di Indonesia dan melihat akan semakin kompleksnya ancaman siber pasca pembangunan IKN sebagai smart city, wacana Gubernur Lembaga Ketahanan Nasional (Lemhannas), Andi Widjajanto mengusulkan pembentukan Angkatan Siber untuk melengkapi 3 matra TNI yakni Angkatan Darat, Laut dan Udara memiliki momentum yang tepat.

Dengan langkah-langkah tersebut, diharapkan IKN dapat memiliki SDM yang tangguh dan siap menghadapi ancaman siber di era digital ini. Keamanan siber bukan hanya tanggung jawab tim khusus, tetapi menjadi tanggung jawab seluruh komponen pemerintahan dan masyarakat di IKN.

18. Memantapkan Skenario Dukungan Anggaran untuk Sistem Keamanan Siber di IKN.

Sekalipun pemerintahan Presiden Joko Widodo terus menggelorakan percepatan transformasi digital, namun perlu diakui bahwa persoalan terkait dengan keamanan siber di Indonesia, belum menjadi salah satu prioritasnya. Hal ini dapat dilihat dari rendahnya anggaran yang diberikan kepada BSSN selama ini.

Pada tahun 2022 lalu alokasi anggaran untuk BSSN hanya sekitar Rp 500 miliar dan itu sudah habis untuk belanja barang dan pegawai. Hal ini membuat nyaris tidak ada anggaran untuk penguatan keamanan siber. Alokasi anggaran BSSN terhadap peningkatan keamanan siber Indonesia hanya di bawah 10 persen[89]. Tidak mengherankan jika kemudian keamanan ekosistem siber di Indonesia kurang optimal dalam mencegah serangan kejahatan siber. Selama ini BSSN masih lemah dalam peralatan dan sumber

[89] https://www.kompas.id/baca/polhuk/2021/11/05/derasnya-kritik-pada-bssn-dari-peretasan-aplikasi-satria-hingga-kolam-renang diakses pada tanggal 6 Agustus 2023 pukul 20.00 WIB.

daya manusia. Namun, untuk memperkuat BSSN, perlu anggaran besar. Realitanya, untuk 2022, dari kebutuhan anggaran sebesar Rp 3,5 triliun, hanya sekitar Rp 500 miliar yang disetujui[90].

Hal inilah yang melatarbelakangi pentingnya dilakukan pemantapan skenario dukungan anggaran untuk sistem keamanan siber di Ibu Kota Nusantara (IKN). Sebab, anggaran sistem keamanan siber bukanlah sekedar isu teknis atau finansial semata, melainkan menjadi hal yang krusial dalam menjamin keamanan dan kesejahteraan warga negara di era digital saat ini. Menjadi satu ironi, jika percepatan transformasi digital yang digaungkan oleh pemerintahan Presiden Joko Widodo, dilakukan dengan mengabaikan pembangunan keamanan siber. Sementara terbukti bahwa keamanan siber di negeri ini masih terbilang rentan. Kecilnya alokasi anggaran bagi BSSN, sebagai lembaga yang seharusnya menjadi benteng pertahanan digital negara menjadi buktinya. Angka ini tentu jauh dari memadai, terutama ketika melihat bahwa sebagian besar anggaran tersebut telah habis hanya untuk belanja barang dan pegawai, meninggalkan sedikit ruang bagi peningkatan keamanan siber itu sendiri.

Dalam konteks pembangunan Ibu Kota Nusantara, IKN memiliki peran sentral dalam dinamika kehidupan berbangsa dan bernegara. Dengan potensi digital yang besar, IKN menjadi magnet bagi berbagai aktivitas yang berbasis teknologi. Namun, di balik potensi tersebut, ancaman kejahatan siber selalu mengintai. Keamanan siber yang lemah dapat mengundang serangan yang tidak hanya merugikan finansial, tetapi juga integritas data negara dan kepercayaan publik. Oleh karena itu, untuk memastikan bahwa IKN dan Indonesia pada umumnya siap menghadapi era digital dengan seluruh risikonya, pemerintah harus segera mempertimbangkan kembali prioritas anggarannya. Investasi pada keamanan siber bukanlah beban, melainkan langkah preventif yang akan menghemat banyak biaya di masa mendatang.

Horngren, Datar & Foster (2006) 221 mendefinisikan anggaran sebagai ekspresi kuantitatif dari rencana aksi yang diajukan oleh manajemen untuk

[90] https://www.kompas.id/baca/polhuk/2021/10/26/peretasan-bssn-menggerus-kepercayaan-publik diakses pada tanggal 6 Agustus 2023 pukul 20.00 WIB.

periode waktu tertentu dan merupakan alat untuk koordinasi tindakan yang diperlukan untuk menerapkan rencana tersebut. Tanpa adanya dukungan anggaran yang memadai, berbagai perencanaan untuk membangun sistem keamanan siber di IKN tidak akan pernah bisa dijalankan.

Dalam rangka memantapkan skenario dukungan anggaran untuk sistem keamanan siber di Ibu Kota Negara (IKN) diperlukan perencanaan yang matang dan kolaborasi antara berbagai pemangku kepentingan. Berikut adalah beberapa langkah yang dapat diambil untuk mencapai tujuan ini:

a. Pemahaman Kebutuhan Keamanan Siber: Pertama dan terpenting, penting untuk memahami kebutuhan keamanan siber secara menyeluruh untuk IKN. Ini melibatkan evaluasi risiko, identifikasi celah keamanan, dan penentuan prioritas tindakan. Pengertian ini akan membantu memastikan bahwa dana yang dialokasikan digunakan dengan efektif dan efisien.
b. Penyusunan Anggaran yang Realistis: Langkah selanjutnya adalah penyusunan anggaran yang realistis berdasarkan kebutuhan ini. Anggaran ini harus mempertimbangkan semua biaya yang terkait dengan peningkatan keamanan siber, termasuk investasi dalam infrastruktur dan teknologi, pengembangan kapasitas dan pelatihan, dan pemeliharaan dan pembaruan berkelanjutan.
c. Lobby dan Advokasi Anggaran: Setelah anggaran disusun, langkah berikutnya adalah mendapatkan dukungan politik untuk anggaran tersebut. Ini mungkin melibatkan lobi dan advokasi di berbagai tingkat pemerintah, termasuk Komisi I DPR dan pihak berwenang anggaran lainnya. Argumentasi untuk mendukung anggaran keamanan siber harus menekankan pentingnya keamanan siber bagi stabilitas dan pertumbuhan ekonomi IKN.
d. Pengalokasian Dana dari Sumber Lain: Selain dana anggaran pemerintah, mungkin juga perlu mencari sumber dana lain, seperti donasi internasional, investasi swasta, atau pinjaman dari bank pembangunan. Pendanaan yang beragam ini dapat membantu memastikan bahwa kegiatan keamanan siber memiliki sumber daya yang cukup bahkan dalam situasi anggaran yang sulit.

e. Pemanfaatan Dana Secara Efektif: Setelah dana disetujui dan dialokasikan, penting untuk memastikan bahwa dana tersebut digunakan dengan cara yang paling efektif. Ini berarti memantau penggunaan dana, melakukan audit keuangan secara teratur, dan mengevaluasi kinerja program keamanan siber untuk memastikan bahwa mereka memberikan hasil yang diharapkan.

f. Pendayagunaan dan Pembaruan Anggaran: Proses anggaran adalah siklus yang berkelanjutan. Setelah setiap periode anggaran, perlu dilakukan peninjauan dan pembaruan anggaran berdasarkan hasil evaluasi dan perubahan dalam lingkungan keamanan siber.

g. Pengawasan dan Transparansi Anggaran: Dalam pemanfaatan anggaran, penting untuk melaksanakan pengawasan dan transparansi anggaran. Hal ini untuk memastikan bahwa dana tersebut benar-benar digunakan untuk tujuan yang telah ditentukan.

Melalui pendekatan ini, dapat dibuat skenario dukungan anggaran yang kuat untuk sistem keamanan siber di IKN. Proses ini membutuhkan kerjasama, koordinasi, dan komitmen dari berbagai pihak, tetapi hasilnya akan berdampak signifikan pada peningkatan keamanan siber di IKN.

BAB IV
PENUTUP

19. Simpulan

Hasil kajian ini menegaskan bahwa tatakelola regulasi yang kokoh, kelembagaan yang efektif, infrastruktur yang andal, sumber daya manusia yang kompeten, serta dukungan anggaran yang memadai menjadi pilar-pilar utama dalam memastikan keamanan siber. Melalui integrasi elemen-elemen tersebut, IKN tidak hanya dapat melindungi aset digital dan informasi strategisnya dari ancaman eksternal, tetapi juga memastikan bahwa pembangunan nasional berjalan secara optimal tanpa gangguan dalam lingkungan digital yang semakin kompleks dan dinamis.

Tatakelola regulasi merupakan salah satu pilar utama dalam memastikan keberhasilan implementasi sistem keamanan siber. Seiring dengan perkembangan teknologi yang pesat, pentingnya regulasi yang

kohesif, komprehensif, dan adaptif menjadi kunci dalam menjamin integritas dan ketahanan infrastruktur digital, khususnya di Ibu Kota Nusantara (IKN). Regulasi harus dirancang dengan mempertimbangkan tantangan keamanan saat ini serta potensi ancaman di masa depan, memungkinkan pemerintah dan entitas terkait untuk bergerak cepat dalam merespons ancaman serta menerapkan solusi keamanan yang tepat.

Selain itu, tatakelola regulasi juga harus mendukung kolaborasi antara sektor publik dan swasta, memastikan bahwa para pihak memiliki pemahaman yang sama mengenai standar keamanan yang harus diterapkan. Dengan adanya regulasi yang jelas dan terperinci, organisasi dapat membangun dan memelihara sistem mereka sesuai dengan standar tertinggi, mencegah potensi kerentanan dan meningkatkan ketahanan terhadap serangan siber. Dengan demikian, tatakelola regulasi yang efektif akan menjadi fondasi kuat dalam mendukung pembangunan sistem keamanan siber yang tangguh dan berkelanjutan.

Selain regulasi, tata kelola kelembagaan berperan menciptakan fondasi yang kuat untuk mengimplementasikan sistem keamanan siber. Kelembagaan yang tepat haruslah memadukan struktur organisasi yang jelas dengan pembagian peran dan tanggung jawab yang terdefinisi dengan baik. Ini memastikan bahwa setiap elemen dari kelembagaan memiliki visi, misi, dan tujuan yang jelas dalam upaya bersama melindungi aset digital dan infrastruktur kritis. Setiap *stakeholder* harus memiliki kompetensi dan kapasitas yang diperlukan untuk menghadapi ancaman keamanan siber yang semakin kompleks. Selanjutnya, mekanisme koordinasi dan kolaborasi antar lembaga harus ditingkatkan untuk menjamin efisiensi dan efektivitas dalam penanganan isu keamanan siber. Hal ini memerlukan kerangka kerja komunikasi yang solid dan platform bersama bagi lembaga-lembaga terkait untuk berbagi informasi, riset, dan praktik terbaik. Dengan adanya tata kelola kelembagaan yang solid, IKN akan lebih tangguh dan responsif dalam menghadapi berbagai ancaman siber, sehingga mampu melindungi aset dan kepentingan nasional dalam era digital saat ini.

Infrastruktur keamanan siber menjadi salah satu pilar penting dalam memastikan keberlangsungan dan keamanan sumber daya digital IKN.

Untuk mempersiapkannya, ada keharusan untuk mengintegrasikan teknologi dan solusi terkini yang menawarkan perlindungan maksimal terhadap ancaman yang ada dan potensial. Ini termasuk membangun infrastruktur dasar seperti *Cybersecurity Operations Centre (CSOC),* yang bertindak sebagai pusat komando dalam mendeteksi, menganalisis, dan merespons insiden keamanan. Selain itu, ada juga kebutuhan untuk implementasi teknologi seperti sensor anomali siber dan infrastruktur forensik digital yang dapat membantu dalam deteksi dini dan investigasi kejadian yang berkaitan dengan pelanggaran keamanan.

Selain *hardware* dan *software*, persiapan infrastruktur keamanan siber juga harus mempertimbangkan aspek jaringan yang aman, termasuk komunikasi dan transmisi data yang terenkripsi, serta layanan *cloud* yang aman. Penerapan teknologi seperti kriptografi, *network security*, dan *application security* harus menjadi prioritas. Penting juga untuk memastikan bahwa seluruh komponen infrastruktur diperbarui secara berkala untuk menangani ancaman terbaru dan memiliki kapabilitas pemulihan bencana yang memadai. Dengan infrastruktur yang kuat dan terintegrasi, sistem keamanan siber akan lebih tangguh dalam menghadapi ancaman yang konstan dan berubah-ubah.

Sumber daya manusia adalah aset kritikal dalam memastikan keberhasilan implementasi dan operasional sistem keamanan siber. Untuk menyiapkan sumber daya manusia yang kompeten, pendidikan dan pelatihan khusus di bidang keamanan siber harus menjadi prioritas utama. Sertifikasi di bidang keamanan siber dapat membantu dalam memvalidasi keterampilan dan pengetahuan individu, memastikan bahwa mereka memiliki keahlian yang diperlukan untuk menghadapi ancaman siber yang semakin kompleks.

Selain pendidikan dan pelatihan, pengembangan budaya keamanan di seluruh organisasi juga esensial. Semua karyawan, tidak hanya tim IT, harus memahami pentingnya keamanan siber dan peran mereka dalam menjaga integritas dan kerahasiaan data. Inisiatif seperti *war game* keamanan, simulasi serangan, dan program kesadaran keamanan dapat membantu memperkuat kesiapan sumber daya manusia dan mempromosikan

pemahaman yang lebih dalam tentang isu-isu keamanan siber. Dengan pendekatan holistik ini, sumber daya manusia akan menjadi lapisan pertahanan yang kuat dalam strategi keamanan siber suatu organisasi.

Pada akhirnya, dalam membangun dan memelihara sebuah sistem keamanan siber yang tangguh dibutuhkan dukungan anggaran. Pengalokasian dana yang tepat, konsisten, dan berkelanjutan menunjukkan komitmen serius dari pemerintah dalam melindungi aset digitalnya dari potensi ancaman. Mengingat ancaman siber yang semakin berkembang, anggaran harus fleksibel dan mampu beradaptasi dengan perubahan teknologi dan kebutuhan keamanan yang baru. Ini berarti diperlukannya revisi periodik untuk memastikan bahwa alokasi dana mencerminkan kebutuhan keamanan siber terkini dan mampu mendanai teknologi, alat, dan layanan terbaru yang dapat meningkatkan postur keamanan.

Selain itu, skenario dukungan anggaran harus mencakup dana untuk pendidikan dan pelatihan sumber daya manusia, serta penelitian dan pengembangan di bidang keamanan siber. Investasi dalam sumber daya manusia, melalui pelatihan dan program sertifikasi, memastikan bahwa tim keamanan memiliki pengetahuan dan keterampilan yang diperlukan untuk menghadapi ancaman saat ini dan mendatang. Sedangkan alokasi dana untuk penelitian dan pengembangan memungkinkan inovasi dan adaptasi terhadap ancaman baru, memastikan bahwa sistem keamanan siber tetap efektif dan *up-to-date* dengan perkembangan teknologi dan metode serangan. Diharapkan dengan adanya dukungan sistem keamanan siber yang mumpuni pada IKN,

20. Rekomendasi

Berkaitan dengan paparan di atas, sejumlah rekomendasi yang dapat disampaikan kepada lembaga/kementerian/institusi terkait adalah sebagai berikut:

a. Pengembangan Regulasi dan Kebijakan: Kemenkominfo segera menyelesaikan pembahasan UU Keamanan Siber dan revisi UU ITE dengan DPR guna mendukung upaya pengauatan sistem keamanan

siber, termasuk sanksi bagi pelanggar dan insentif bagi mereka yang menerapkan praktik keamanan siber terbaik.

b. Pembentukan Badan Otoritas Keamanan Siber IKN: BSSN dan Otorita IKN membentuk sebuah lembaga yang memiliki wewenang untuk mengatur, mengawasi, dan bertanggung jawab untuk mengkoordinasikan upaya memitigasi dan menanggulangi insiden keamanan siber.
c. Membangun Infrastruktur Keamanan Siber: Otorita IKN mengalokasikan anggaran khusus untuk pembangunan dan pemeliharaan infrastruktur keamanan siber seperti CSOC *(Cybersecurity Operations Center)*. Ini mencakup juga investasi dalam teknologi terbaru untuk mendeteksi, mencegah, dan merespons ancaman siber.
d. Inisiasi Pembentukan Matra Siber: Lemhannas, BSSN dan Kemenhan dapat mulai menginisiasi rencana pembentukan Matra Siber di Indonesia secara lebih mendetil dan komprehensif guna dikonsultasikan kepada DPR dan masyarakat. Keberadaan Matra Siber meningkatkan ketersediaan dan kesiapan SDM Indonesia terhadap pertahanan dan keamanan siber di Indonesia.
e. Pendidikan dan Pelatihan Keamanan Siber: BSSN dan Kemendikbudristek membuat program pelatihan standar untuk profesional keamanan siber serta pendidikan dasar tentang kesadaran keamanan siber. Kerjasama dengan institusi pendidikan tinggi untuk memperkuat kurikulum keamanan siber dan menambah jumlah tenaga ahli di bidang ini.
f. Penelitian dan Pengembangan: BSSN dan BRIN mendirikan pusat-pusat riset yang fokus pada inovasi dan penelitian di bidang keamanan siber. Kerjasama dengan industri dan akademia untuk mengembangkan solusi yang sesuai dengan tantangan keamanan siber yang terus berkembang.
g. Alokasi Anggaran yang Memadai: Kemenkeu dan Otorita IKN menjamin kesiapan alokasi anggaran yang cukup untuk inisiatif keamanan siber, dengan mekanisme peninjauan periodik untuk memastikan bahwa dana tersebut digunakan secara efektif dan efisien.
h. Kerjasama Internasional: BSSN, Kemenkominfo dan seluruh instansi pengampu *Security Operation Center* (BIN, Polri, Kejaksaan dan

TNI/Kemenhan) mengembangkan kerjasama bilateral dan multilateral dengan negara-negara lain untuk berbagi informasi intelijen, *best practices*, dan sumber daya dalam bidang keamanan siber.