INTERNATIONAL JOURNAL OF SOCIAL AND MANAGEMENT STUDIES (IJOSMAS)

Vol.6 No. 5 https://www.ijosmas.org e-ISSN: 2775-0809

KEMANDIRIAN SIBER INDONESIA: TANTANGAN DAN PELUANG MENUJU KEDAULATAN DIGITAL

Saepudin Hidayat[1] Aris Setyo Radyawanto[2]

Universitas Brawijaya[1] Universitas Mercubuana[2]

saepudinh44@gmail.com[1] aris.radyawanto2@gmail.com[2]

Abstrak. Indonesia menghadapi lonjakan signifikan ancaman keamanan siber yang mengancam kedaulatan dan keamanan nasional. Data Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan serangan siber dari 12,8 juta pada 2018 menjadi 74,2 juta pada 2020, dan mencapai lebih dari 3,6 miliar serangan sepanjang tahun 2025. Ancaman yang dominan meliputi *malware*, *social engineering*, serangan DDoS, serta kebocoran data yang menjadi isu krusial. Pemerintah telah merumuskan Strategi Keamanan Siber Nasional (SKSN) yang selaras dengan nilai kedaulatan, kemandirian, keamanan, kebersamaan, dan adaptif, termasuk penguatan infrastruktur siber, peningkatan kapasitas sumber daya manusia, dan penegakan hukum siber. Regulasi seperti Rancangan Undang-Undang Keamanan dan Ketahanan Siber menjadi prioritas untuk mendukung kedaulatan digital. Industri keamanan siber lokal berkembang pesat, dengan peningkatan talenta muda melalui kompetisi dan pelatihan. Meskipun menghadapi tantangan investasi, koordinasi antar-lembaga, dan pengembangan teknologi lokal, kemandirian siber Indonesia merupakan fondasi utama dalam mewujudkan kedaulatan digital nasional. Diperlukan kolaborasi lintas sektor untuk membangun ekosistem keamanan siber yang kuat dan adaptif menghadapi ancaman siber yang semakin kompleks di era digital.

Kata kunci: Kemandirian Siber, Keamanan Siber Nasional, Ancaman Siber Indonesia.

PENDAHULUAN

Indonesia menghadapi peningkatan ancaman keamanan siber yang signifikan dalam beberapa tahun terakhir. Data Badan Siber dan Sandi Negara (BSSN) menunjukkan lonjakan serangan siber dari 12,8 juta pada tahun 2018 menjadi 74,2 juta pada tahun 2020. Jenis ancaman yang umum terjadi meliputi malware, *social engineering*, injeksi SQL, serangan DDoS, dan pembajakan domain. Kebocoran data menjadi salah satu isu yang paling meresahkan. Dalam debat Pilgub DKI Jakarta 2024, calon gubernur nomor urut 2, Dharma Pongrekun, menyoroti pentingnya kemandirian internet sebagai solusi utama untuk mencegah kebocoran data di Indonesia. Menurutnya, selama Indonesia belum mandiri dalam akses internet, ancaman kebocoran data akan terus menghantui, terlepas dari berbagai upaya untuk melindungi privasi. Kemandirian siber juga menjadi kunci dalam mendukung visi "Astacita" Presiden Prabowo Subianto dan Wakil Presiden Gibran Rakabuming Raka, yang bertujuan memperkuat sistem pertahanan dan keamanan negara serta mendorong kemandirian nasional di berbagai sektor strategis.

Pengembangan industri keamanan siber lokal dan peningkatan kapasitas sumber daya manusia menjadi fokus utama sebagai upaya mengurangi ketergantungan pada teknologi asing sekaligus memperkuat ekosistem keamanan siber nasional. Namun, tantangan besar seperti infrastruktur, investasi, koordinasi antar-lembaga, dan regulasi komprehensif masih harus diatasi untuk mewujudkan kemandirian siber yang berkelanjutan. Oleh karena itu, artikel ini akan membahas urgensi kemandirian siber bagi Indonesia, strategi nasional yang diterapkan, serta tantangan dan peluang yang dihadapi dalam membangun sistem keamanan siber yang tangguh dan mandiri.

METODE

Metode yang digunakan dalam artikel ini adalah metode *literature review*, yaitu suatu pendekatan penelitian yang mengumpulkan, menganalisis, dan menyintesis hasil-hasil penelitian terdahulu yang relevan dengan topik kemandirian dan keamanan siber di Indonesia. Proses literature review dilakukan dengan mengidentifikasi sumber data sekunder seperti jurnal ilmiah, artikel, laporan resmi, dan dokumen kebijakan yang berkaitan dengan keamanan siber, ancaman siber, strategi nasional, dan pengembangan industri siber.

HASIL DAN PEMBAHASAN

Urgensi Kemandirian Siber bagi Indonesia

Indonesia menghadapi peningkatan ancaman keamanan siber yang signifikan dalam beberapa tahun terakhir. Data Badan Siber dan Sandi Negara (BSSN) menunjukkan lonjakan serangan siber dari 12,8 juta pada tahun 2018 menjadi 74,2 juta pada tahun 2020. Jenis ancaman yang umum terjadi meliputi malware, social engineering, injeksi SQL, serangan DDoS, dan pembajakan domain. Kebocoran data menjadi salah satu isu yang paling meresahkan. Dalam debat Pilgub DKI Jakarta 2024, calon gubernur nomor urut 2, Dharma Pongrekun, menyoroti pentingnya kemandirian internet sebagai solusi utama untuk mencegah kebocoran data di Indonesia. Menurutnya, selama Indonesia belum mandiri dalam akses internet, ancaman kebocoran data akan terus menghantui, terlepas dari berbagai upaya untuk melindungi privasi. Kemandirian siber juga menjadi kunci dalam mendukung visi "Astacita" Presiden Prabowo Subianto dan Wakil Presiden Gibran Rakabuming Raka, yang bertujuan memperkuat sistem pertahanan dan keamanan negara serta mendorong kemandirian nasional di berbagai sektor strategis.

Strategi Keamanan Siber Nasional Indonesia

Pemerintah Indonesia telah mengambil langkah-langkah konkret untuk memperkuat pertahanan siber nasional. Melalui Peraturan Presiden No. 53 Tahun 2017 dan perubahannya No. 133 Tahun 2017, pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) untuk mengimplementasikan keamanan siber secara efektif dan efisien.

BSSN telah mengembangkan Strategi Keamanan Siber Nasional sebagai referensi bersama bagi semua pemangku kepentingan keamanan siber dalam merumuskan dan mengembangkan kebijakan keamanan siber di instansi masing-masing. Strategi ini didasarkan pada prinsip-prinsip:

1. Kedaulatan
2. Kemandirian
3. Keamanan
4. Kebersamaan
5. Adaptif

Visi Strategi Keamanan Siber Nasional adalah "Membangun dan memelihara keamanan siber nasional dengan mensinergikan berbagai pemangku kepentingan untuk berpartisipasi dalam mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional." Tujuan strategisnya adalah mencapai:

1. Ketahanan Siber
2. Keamanan Layanan Publik
3. Penegakan Hukum Siber
4. Budaya Keamanan Siber
5. Keamanan Siber dalam Ekonomi Digital

Perkembangan Regulasi dan Kebijakan

BSSN saat ini sedang mendorong Rancangan Undang-Undang Keamanan dan Ketahanan Siber untuk dimasukkan dalam program legislasi nasional (Prolegnas) sebagai prioritas. RUU ini dipandang sebagai langkah krusial untuk mendukung visi "Astacita" pemerintahan saat ini.

Untuk mencapai hal tersebut, BSSN telah menguraikan beberapa inisiatif utama:

1. Memperkuat keamanan siber untuk infrastruktur kritis: BSSN akan melakukan sertifikasi peralatan keamanan siber yang akan digunakan dalam infrastruktur vital. Lembaga ini juga akan meningkatkan intensitas fungsi kontrol informasi untuk diteruskan ke kementerian dan lembaga terkait untuk penyaringan konten, penegakan hukum, dan netralisasi informasi.

2. Mendukung sektor pertanian digital: BSSN akan memperkuat keamanan siber di kementerian dan lembaga yang mengawasi pertanian digital, termasuk Kementerian Pertanian, Kementerian Komunikasi dan Informatika, Kementerian Pendidikan Tinggi, Sains dan Teknologi, dan Badan Riset dan Inovasi Nasional (BRIN).

3. Terlibat dalam forum internasional: BSSN berencana untuk berperan aktif dalam menciptakan perdamaian global melalui forum bilateral dan multilateral tentang keamanan siber dan kriptografi, menunjukkan komitmen Indonesia untuk menjaga keamanan siber di tingkat internasional.

Pengembangan Industri Keamanan Siber Lokal

Industri keamanan siber lokal di Indonesia menunjukkan perkembangan yang menjanjikan. PT ITSEC Asia Tbk merupakan salah satu perusahaan keamanan siber lokal terbesar di Indonesia. Didirikan sejak 2010, ITSEC Asia kini telah mengembangkan layanan bisnisnya ke berbagai negara di Asia Pasifik, termasuk Indonesia, Singapura, Australia, dan Dubai.

Sebagai perusahaan keamanan siber terbesar di Asia Pasifik, ITSEC Asia memiliki visi untuk menjadi perusahaan keamanan siber terbesar dan terpercaya di kawasan tersebut. Pada tahun 2024, ITSEC Asia berencana untuk melakukan pengembangan solusi dan adopsi teknologi terkini, sejalan dengan pilar bisnisnya di bidang konsultasi, solusi teknologi, dan managed security services.

Selain itu, Cyber Breaker Competition (CBC) Season 2 yang digelar pada September 2025 juga menunjukkan antusiasme generasi muda Indonesia untuk menekuni bidang keamanan digital. Kompetisi ini mencatat 619 peserta dari berbagai daerah, meningkat dibandingkan musim sebelumnya. Hal ini mencerminkan besarnya potensi pengembangan talenta nasional di sektor keamanan siber.

Deputi Bidang Kreativitas Digital dan Teknologi Kementerian Ekonomi Kreatif, Muhammad Neil El Himam, menegaskan bahwa keamanan siber harus dipandang sebagai peluang bisnis, bukan sekadar beban biaya. Harapannya, para pegiat keamanan siber dapat berkembang dari individu menjadi perusahaan, bahkan industri tersendiri.

Tantangan Menuju Kemandirian Siber

Meskipun berbagai upaya telah dilakukan, Indonesia masih menghadapi beberapa tantangan dalam mewujudkan kemandirian siber:

1. Infrastruktur dan Investasi: Membangun infrastruktur internet yang sepenuhnya mandiri membutuhkan investasi besar dalam pembangunan pusat data, jaringan kabel serat optik, satelit, dan

teknologi lainnya. Sebagian besar teknologi internet saat ini dikembangkan oleh perusahaan asing, sehingga mengurangi ketergantungan ini memerlukan pengembangan teknologi dalam negeri yang kompetitif.

2. Sumber Daya Manusia: Indonesia masih kekurangan tenaga ahli di bidang keamanan siber. Diperlukan program pendidikan dan pelatihan yang komprehensif untuk menghasilkan talenta lokal yang mampu mengembangkan dan mengoperasikan sistem keamanan siber nasional.

3. Koordinasi Antar-Lembaga: Perlunya peningkatan koordinasi dan kolaborasi antara berbagai pemangku kepentingan terkait keamanan siber masih menjadi tantangan. Sinergi antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil sangat diperlukan untuk membangun ekosistem keamanan siber yang kuat.

4. Regulasi yang Komprehensif: Meskipun RUU Keamanan dan Ketahanan Siber sedang didorong, Indonesia masih memerlukan kerangka regulasi yang lebih komprehensif untuk mengatur berbagai aspek keamanan siber, termasuk perlindungan data pribadi, keamanan infrastruktur kritis, dan penanganan insiden siber.

Strategi Menuju Kemandirian Siber

Untuk mewujudkan kemandirian siber, Indonesia perlu menerapkan strategi komprehensif yang mencakup:

1. Pengembangan Teknologi Lokal: Mendorong inovasi dan pengembangan teknologi keamanan siber dalam negeri melalui insentif fiskal, pendanaan riset, dan kolaborasi antara industri dan akademisi.

2. Penguatan Kapasitas SDM: Meningkatkan kuantitas dan kualitas tenaga ahli keamanan siber melalui program pendidikan formal, pelatihan profesional, dan sertifikasi internasional.

3. Kerjasama Internasional Strategis: Menjalin kerjasama dengan negara-negara maju di bidang keamanan siber, seperti yang telah dilakukan dengan Inggris, untuk transfer teknologi dan pengetahuan.

4. Pembangunan Infrastruktur Digital Nasional: Mengembangkan infrastruktur digital yang mandiri dan aman, termasuk pusat data nasional, jaringan komunikasi, dan sistem keamanan yang terintegrasi.

5. Penguatan Regulasi dan Tata Kelola: Mempercepat pengesahan RUU Keamanan dan Ketahanan Siber serta mengembangkan kerangka regulasi yang komprehensif untuk mengatur berbagai aspek keamanan siber

KESIMPULAN

Kemandirian siber merupakan aspek krusial bagi kedaulatan nasional Indonesia di era digital. Meskipun masih menghadapi berbagai tantangan, Indonesia telah menunjukkan komitmen yang kuat untuk mewujudkan kemandirian siber melalui pengembangan strategi nasional, penguatan regulasi, dan pembangunan kapasitas. Industri keamanan siber lokal yang berkembang dan antusiasme generasi muda untuk terlibat dalam sektor ini memberikan harapan bagi masa depan kemandirian siber Indonesia. Dengan strategi yang tepat dan kolaborasi yang efektif antara berbagai pemangku kepentingan, Indonesia dapat memperkuat posisinya dalam lanskap

keamanan siber global dan melindungi kepentingan nasionalnya di dunia digital. Kemandirian siber bukanlah tujuan akhir, melainkan proses berkelanjutan yang memerlukan adaptasi terhadap perkembangan teknologi dan ancaman yang terus berubah. Oleh karena itu, Indonesia perlu terus mengembangkan kapasitas, infrastruktur, dan kerangka regulasi untuk menghadapi tantangan keamanan siber di masa depan.

DAFTAR PUSTAKA

Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, & Fried Sinlae. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. *Journal Zetroem*, *6*(1), 114–119. https://doi.org/10.36526/ztr.v6i1.3376

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Arianto, Adi Rio & Anggraini, G. (2019). *Melalui Indonesia Security Incident Response Team on*. *09 Nomo 1*, 13–30.

Dinata, A. C., & Syafaat, A. (2025). *Peran BSSN dalam Menangani Ancaman Siber di Indonesia Abstrak Pendahuluan Kajian Teori Keamanan Siber*. *01*(01).

Galang Ramadhan. (2025). Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi Ancaman Siber. *Konstitusi : Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi*, *2*(2 SE-Articles), 257–266. https://doi.org/10.62383/konstitusi.v2i2.722

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime melalui Badan Siber dan Sandi Negara. Jurnal Dinamika Global, 7(2), 295-315. DOI: 10.36859/jdg.v7i02.1187

Gunawan Idat, Dhani. 2020. "Memanfaatkan Era Ekonomi Digital Untuk Memperkuat Ketahanan Nasional". *Jurnal Lemhannas RI* 7 (2), 5-11. https://doi.org/10.55960/jlri.v7i2.67.

Iqbal Afriyadi, & Jhon Veri. (2025). SLR: Peran Keamanan Siber Dalam Pengembangan Wirausaha Di Era Teknologi . *Journal of Innovation Research and Knowledge*, *4*(8 SE-Articles), 5705–5720. https://bajangjournal.com/index.php/JIRK/article/view/9392

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698

Sudarmadi, Damar Apri and Runturambi, Arthur Josias Simon (2019) "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*: Vol. 2: No. 2, Article 7. DOI: 10.7454/jkskn.v2i2.10028