BUKTI BARU

# Dr. Hendri: Keamanan Siber Harus Menjadi Prioritas Pembangunan

**Updates. - BUKTIBARU.COM**
Aug 18, 2026 - 06:02

*Dr. Ir. Hendri, ST., MT Wartawan Utama Ketua Umum Jurnalis Nasional Indonesia (JNI)*

OPINI - Rumah sakit menyimpan rekam medis secara digital. Bank memindahkan uang melalui jaringan elektronik. Pemerintah menerbitkan dokumen kependudukan, perizinan, paspor, bantuan sosial, dan pelayanan pajak melalui sistem daring. Pembangkit listrik, jaringan telekomunikasi, transportasi, pergudangan, dan industri semakin bergantung pada perangkat yang terhubung.

Digitalisasi membuat pelayanan lebih cepat, tetapi sekaligus menciptakan ketergantungan baru. Ketika sistem terganggu, dampaknya tidak berhenti di layar komputer. Pasien dapat kehilangan akses terhadap informasi medis, perjalanan masyarakat tertunda, transaksi keuangan terhambat, produksi berhenti, data pribadi tersebar, dan pelayanan negara lumpuh.

Karena itu, keamanan siber tidak boleh lagi dianggap sebagai pekerjaan teknisi setelah aplikasi selesai dibangun. Keamanan siber harus menjadi bagian dari perencanaan pembangunan sejak awal.

Jalan dibangun dengan perhitungan keselamatan. Gedung dilengkapi sistem pencegahan kebakaran. Pembangkit memiliki cadangan dan prosedur keadaan darurat. Sistem digital juga harus dibangun dengan perlindungan, pencadangan, pemulihan, dan pertanggungjawaban yang setara.

Digitalisasi tanpa keamanan ibarat membangun kota modern tanpa pintu, pagar, pemadam kebakaran, dan jalur evakuasi.

## Ancaman Tidak Lagi Bersifat Hipotetis

Ancaman siber bukan kemungkinan yang mungkin terjadi pada masa depan. Ia telah berlangsung setiap hari dengan bentuk yang terus berubah: pencurian akun, penipuan, kebocoran data, perusakan situs, ransomware, serangan terhadap jaringan, pencurian rahasia perusahaan, manipulasi informasi, dan penyusupan melalui perangkat yang tidak diperbarui.

Data BSSN yang disampaikan dalam forum keamanan siber nasional menunjukkan lebih dari 6,8 miliar anomali trafik siber terdeteksi sepanjang Januari 2020 hingga Juni 2025. Sekitar 83 persen di antaranya berkaitan dengan perangkat lunak berbahaya.

Masalahnya bukan hanya besarnya ancaman. Dari 8.769 notifikasi indikasi insiden yang dikirimkan kepada pemilik sistem elektronik selama periode tersebut, hanya sekitar 27,9 persen yang ditindaklanjuti.

Angka itu memperlihatkan kesenjangan serius antara kemampuan mendeteksi dan kemauan atau kemampuan merespons. Sistem dapat mengetahui adanya ancaman, tetapi organisasi yang menerima peringatan belum tentu bertindak cepat.

Ada kemungkinan instansi tidak memiliki tenaga ahli. Ada yang belum menyediakan anggaran. Ada yang kesulitan menutup layanan untuk melakukan perbaikan. Ada pula yang mungkin belum memiliki tata kelola yang menetapkan siapa harus mengambil keputusan ketika ancaman ditemukan.

Dalam keamanan siber, penundaan merupakan risiko. Celah yang dibiarkan terbuka dapat menjadi pintu masuk. Akun yang telah diketahui bocor dapat digunakan untuk memperluas serangan. Perangkat yang tidak diperbarui dapat mengancam seluruh jaringan.

Serangan siber tidak selalu terjadi karena pelaku memiliki teknologi luar biasa.

Banyak serangan berhasil karena kata sandi lemah, akun lama tidak ditutup, hak akses terlalu luas, sistem tidak diperbarui, cadangan data tidak tersedia, atau peringatan keamanan diabaikan.

## Pelajaran Mahal dari Serangan Pusat Data

Serangan ransomware terhadap Pusat Data Nasional Sementara pada Juni 2024 harus menjadi pelajaran penting bagi pembangunan digital. Pemerintah mengakui bahwa serangan tersebut mengganggu sejumlah pelayanan publik, termasuk layanan keimigrasian.

Gangguan itu memperlihatkan bahwa satu kegagalan pada infrastruktur digital dapat memengaruhi banyak lembaga dan jutaan masyarakat. Risiko meningkat ketika sistem pemerintahan semakin terpusat, tetapi arsitektur pencadangan, pemisahan jaringan, dan pemulihannya belum cukup kuat.

Dalam rapat bersama pemerintah, Komisi I DPR RI mengungkap bahwa hanya sekitar dua persen data pada sistem tersebut yang memiliki cadangan di lokasi lain. Pemerintah kemudian melakukan perbaikan tata kelola dan pemulihan sistem.

Pelajaran terbesarnya bukan hanya bahwa suatu pusat data dapat diserang. Tidak ada sistem yang dapat dijamin seratus persen bebas dari serangan. Pertanyaan yang menentukan adalah apakah organisasi mampu mendeteksi serangan dengan cepat, membatasi penyebarannya, mempertahankan layanan penting, memulihkan data, dan menjelaskan kejadian secara terbuka.

Cadangan data tidak cukup hanya dibuat. Cadangan harus dipisahkan dari sistem utama agar tidak ikut terenkripsi, diperiksa integritasnya, dan diuji melalui simulasi pemulihan. Cadangan yang tidak pernah diuji belum dapat dianggap sebagai cadangan yang dapat diandalkan.

Keamanan siber bukan sekadar kemampuan mencegah pelaku masuk. Keamanan siber juga merupakan kemampuan tetap berfungsi ketika serangan berhasil menembus pertahanan.

## Keamanan Siber adalah Investasi Ekonomi

Ada anggapan bahwa keamanan siber hanya menambah biaya proyek digital. Pandangan tersebut keliru karena tidak memperhitungkan biaya gangguan, kehilangan data, pemulihan sistem, tuntutan hukum, kerusakan reputasi, dan hilangnya kepercayaan.

Bank Dunia menegaskan bahwa keamanan siber dapat mendorong pertumbuhan ekonomi melalui peningkatan kepercayaan, daya saing, dan inovasi digital. Negara berkembang yang mampu mengurangi insiden siber diperkirakan berpotensi meningkatkan produk domestik bruto per kapita sekitar 1,5 persen dalam satu dekade.

Keamanan menciptakan kepercayaan. Masyarakat akan menggunakan layanan keuangan digital apabila yakin uang dan identitasnya terlindungi. Perusahaan

akan mengadopsi teknologi awan apabila datanya aman. Investor akan menempatkan pusat data dan kegiatan penelitian di negara yang memiliki kepastian hukum serta sistem keamanan yang kuat.

Sebaliknya, kerentanan menimbulkan biaya sistemik. Dana Moneter Internasional mencatat potensi kerugian ekstrem dari insiden siber meningkat lebih dari empat kali lipat sejak 2017 hingga mencapai sekitar 2,5 miliar dolar AS. Kerugian tidak langsung, seperti hilangnya pelanggan, penurunan reputasi, dan biaya peningkatan keamanan, dapat jauh lebih besar.

Dalam sektor keuangan, serangan terhadap satu lembaga dapat menular melalui hubungan pembayaran, penyedia teknologi, layanan awan, dan kepercayaan masyarakat. Di sektor industri, gangguan pada satu pemasok perangkat lunak dapat menghentikan banyak perusahaan yang menggunakan produk yang sama.

Oleh sebab itu, keamanan siber merupakan kebijakan ekonomi, investasi, perdagangan, industri, dan ketahanan nasional sekaligus.

## Melindungi Infrastruktur Informasi Vital

Serangan terhadap media sosial pribadi tentu merugikan, tetapi serangan terhadap rumah sakit, pembangkit listrik, jaringan telekomunikasi, perbankan, pelabuhan, transportasi, atau sistem pemerintahan dapat mengganggu kepentingan umum.

Peraturan Presiden Nomor 82 Tahun 2022 telah mengatur pelindungan Infrastruktur Informasi Vital, yakni sistem elektronik yang menopang sektor strategis dan dapat menimbulkan dampak serius terhadap pelayanan publik, pertahanan, keamanan, atau perekonomian apabila mengalami gangguan.

Keberadaan peraturan merupakan fondasi penting, tetapi perlindungan harus terlihat dalam praktik. Setiap sektor strategis perlu memiliki daftar aset kritis, pemetaan ketergantungan, standar minimum, audit berkala, pusat operasi keamanan, tim tanggap insiden, dan rencana pemulihan.

Pemetaan ketergantungan sangat penting. Sebuah rumah sakit mungkin memiliki sistem yang baik, tetapi tetap dapat terganggu apabila penyedia listrik, jaringan telekomunikasi, layanan awan, atau perangkat lunak pihak ketiga mengalami serangan.

Satu perusahaan teknologi dapat melayani ratusan lembaga. Apabila perangkat lunaknya disusupi, serangan dapat menyebar melalui pembaruan resmi. Karena itu, pengadaan teknologi harus menilai keamanan rantai pasok, kepemilikan kode, lokasi penyimpanan data, masa dukungan pembaruan, serta kemampuan vendor menangani kerentanan.

Vendor tidak boleh hanya menjanjikan fitur. Mereka harus bertanggung jawab terhadap keamanan sepanjang umur sistem.

Kontrak pemerintah perlu memuat kewajiban pengujian, pelaporan celah, pembaruan keamanan, pemulihan, penghapusan data, dan pengalihan layanan apabila kerja sama berakhir. Ketergantungan pada vendor tanpa akses terhadap

dokumentasi dan kemampuan teknis internal dapat menjadi risiko kedaulatan.

## Data Pribadi Bukan Barang Sisa Digital

Setiap layanan digital mengumpulkan data. Nama, alamat, nomor telepon, identitas kependudukan, rekam kesehatan, lokasi, transaksi, foto wajah, sidik jari, dan pola perilaku memiliki nilai ekonomi sekaligus risiko.

Data pribadi bukan milik bebas perusahaan atau instansi hanya karena masyarakat menyerahkannya ketika menggunakan layanan. Pengumpulan data menciptakan tanggung jawab untuk membatasi penggunaan, menjaga keamanan, dan menghapusnya ketika tidak lagi diperlukan.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur hak subjek data, kewajiban pengendali dan prosesor data, pemrosesan, transfer, sanksi administratif, kelembagaan, serta ketentuan pidana. Setelah masa transisinya berakhir, undang-undang tersebut berlaku penuh mulai 17 Oktober 2024.

Pelaksanaan undang-undang tidak boleh berhenti pada penambahan halaman persetujuan yang panjang. Organisasi harus mengetahui data apa yang dikumpulkan, untuk tujuan apa, siapa yang dapat mengakses, berapa lama disimpan, ke negara mana dipindahkan, dan bagaimana data dihapus.

Prinsip pertama seharusnya sederhana: jangan mengumpulkan data yang tidak diperlukan.

Semakin banyak data disimpan, semakin besar dampak apabila terjadi kebocoran. Data yang sama juga tidak seharusnya disalin ke banyak aplikasi tanpa pengawasan. Setiap salinan memperluas permukaan serangan.

Apabila kebocoran terjadi, masyarakat berhak memperoleh pemberitahuan yang jelas. Informasi tidak boleh disembunyikan dengan alasan menjaga reputasi. Penjelasan harus mencakup jenis data yang terdampak, waktu kejadian, risiko bagi pemilik data, langkah perlindungan yang harus dilakukan, dan tindakan pemulihan organisasi.

Transparansi setelah insiden bukan kelemahan. Transparansi merupakan bagian dari pertanggungjawaban.

## Kecerdasan Buatan Mempercepat Serangan

Kecerdasan buatan memberikan kemampuan besar untuk mendeteksi pola serangan, menganalisis aktivitas jaringan, memeriksa kode, serta mempercepat respons. Namun, teknologi yang sama dapat digunakan pelaku untuk membuat pesan penipuan lebih meyakinkan, meniru suara, memanipulasi video, menemukan kerentanan, dan melakukan serangan secara otomatis.

Global Cybersecurity Outlook 2026 menunjukkan bahwa 94 persen pemimpin yang disurvei memperkirakan kecerdasan buatan menjadi kekuatan paling menentukan dalam perubahan keamanan siber pada 2026. Kerentanan terkait

AI, penipuan digital, phishing, ransomware, dan gangguan rantai pasok menjadi perhatian utama.

Penipuan yang dahulu memerlukan waktu dan kemampuan bahasa kini dapat dibuat dalam jumlah besar. Pelaku dapat meniru gaya komunikasi pimpinan perusahaan, membuat suara palsu seorang pejabat, atau mengirim dokumen yang tampak resmi.

Karena itu, verifikasi tidak boleh lagi hanya bergantung pada apa yang dilihat atau didengar. Transaksi penting harus menggunakan persetujuan berlapis, saluran konfirmasi terpisah, tanda tangan digital, dan pembatasan kewenangan.

Sistem AI yang digunakan pemerintah dan perusahaan juga harus diamankan. Data pelatihan dapat dirusak, perintah pengguna dapat dimanipulasi, informasi rahasia dapat bocor melalui aplikasi, dan keputusan otomatis dapat dipengaruhi masukan berbahaya.

Setiap penggunaan AI perlu disertai penilaian risiko, pengendalian akses, pencatatan aktivitas, pengujian keamanan, serta pengawasan manusia.

## Faktor Manusia Tetap Menentukan

Perangkat keamanan yang mahal dapat gagal hanya karena seorang pegawai membuka lampiran palsu, menggunakan kata sandi yang sama, atau memberikan kode verifikasi kepada penipu.

Namun, menyalahkan pegawai juga bukan penyelesaian. Organisasi harus merancang sistem yang tidak menjadikan satu kesalahan manusia sebagai penyebab runtuhnya seluruh pertahanan.

Autentikasi multifaktor harus digunakan untuk akun penting. Hak akses diberikan berdasarkan kebutuhan. Akun pegawai yang keluar segera ditutup. Aktivitas administrator dicatat. Jaringan dipisahkan agar serangan tidak bergerak bebas. Sistem diperbarui secara teratur, sedangkan surat elektronik mencurigakan diperiksa melalui perlindungan otomatis.

Pelatihan keamanan juga harus berbentuk praktik, bukan sekadar ceramah tahunan. Pegawai perlu mengikuti simulasi phishing, latihan penanganan insiden, dan pembelajaran berdasarkan kasus nyata.

Pimpinan merupakan bagian dari faktor manusia. Banyak kegagalan bukan disebabkan teknisi, melainkan keputusan manajemen yang menunda pembaruan, menolak anggaran cadangan, membeli sistem tanpa audit, atau tidak menetapkan penanggung jawab risiko.

Keamanan siber harus menjadi tanggung jawab pimpinan tertinggi. Menteri, kepala daerah, direktur utama, rektor, kepala rumah sakit, dan pimpinan lembaga harus memahami risiko sistem yang berada di bawah kewenangannya.

Masalah keamanan siber tidak boleh selalu dilimpahkan kepada unit teknologi informasi setelah kejadian.

# Kesenjangan Keamanan Antarorganisasi

Bank besar mungkin mampu membangun pusat operasi keamanan dengan tenaga ahli yang bekerja sepanjang waktu. Namun, pemerintah daerah kecil, sekolah, rumah sakit daerah, koperasi, media lokal, dan UMKM sering tidak memiliki sumber daya yang sama.

Kesenjangan ini berbahaya karena ekosistem digital saling terhubung. Penyerang dapat masuk melalui organisasi yang paling lemah, kemudian bergerak menuju mitra yang lebih besar.

Pemerintah perlu menyediakan layanan keamanan bersama bagi lembaga yang tidak mampu membangun kemampuan sendiri. Layanan tersebut dapat mencakup pemantauan, peringatan ancaman, pemeriksaan kerentanan, respons insiden, pencadangan, dan bantuan pemulihan.

Standar minimum harus mudah diterapkan, tetapi tetap tegas. Organisasi kecil setidaknya wajib memiliki inventaris perangkat, autentikasi multifaktor, pembaruan sistem, cadangan terpisah, perlindungan perangkat, pelatihan pegawai, serta kontak tanggap insiden.

Dukungan pembiayaan perlu diberikan kepada pemerintah daerah, fasilitas kesehatan, lembaga pendidikan, dan UMKM yang mengelola data penting. Digitalisasi mereka tidak boleh dipercepat tanpa perlindungan.

Kesenjangan keamanan siber pada akhirnya menjadi kesenjangan pembangunan. Masyarakat di daerah tidak boleh menerima pelayanan digital yang lebih rentan hanya karena kemampuan fiskal pemerintah daerah terbatas.

# Membangun Industri dan Talenta Siber Nasional

Ketahanan siber tidak mungkin sepenuhnya bergantung pada produk, tenaga ahli, pusat data, dan layanan dari luar negeri. Kerja sama global tetap diperlukan, tetapi negara harus menguasai kemampuan inti.

Industri nasional perlu didorong mengembangkan solusi identitas digital, enkripsi, pusat operasi keamanan, pemantauan jaringan, perlindungan perangkat, pengujian aplikasi, pencadangan, forensik digital, dan keamanan teknologi operasional.

Keberpihakan kepada produk nasional harus disertai standar mutu. Keamanan tidak boleh dikorbankan demi label dalam negeri. Sebaliknya, perusahaan nasional perlu memperoleh akses terhadap pengadaan, laboratorium pengujian, sertifikasi, pembiayaan, dan pasar agar mampu meningkatkan kualitas.

Perguruan tinggi harus menghasilkan lebih banyak ahli keamanan jaringan, kriptografi, forensik, perangkat lunak aman, keamanan AI, serta keamanan sistem industri. Sekolah menengah kejuruan dapat mengembangkan kompetensi administrator jaringan dan teknisi keamanan dasar.

Program beasiswa, pelatihan ulang, kompetisi, laboratorium siber, dan kerja sama industri perlu diperluas. Pemerintah juga harus menyediakan jalur karier yang mampu mempertahankan tenaga ahli di sektor publik.

Talenta keamanan siber tidak hanya berasal dari pendidikan formal. Komunitas peretas etis dan peneliti keamanan dapat membantu menemukan kerentanan sebelum dimanfaatkan penjahat. Pemerintah dan perusahaan perlu menyediakan mekanisme pelaporan celah serta program penghargaan yang memiliki perlindungan hukum.

Peneliti yang melaporkan kelemahan dengan itikad baik tidak boleh langsung diperlakukan sebagai penjahat. Sebaliknya, pengujian tanpa izin dan penyalahgunaan data tetap harus ditindak secara hukum. Batasnya perlu diatur secara jelas.

## Keamanan Tidak Boleh Menjadi Alasan Membatasi Kritik

Penguatan keamanan siber harus melindungi warga negara, bukan menjadi alasan memperluas pengawasan tanpa batas. Perlindungan sistem tidak sama dengan pembatasan kritik, kebebasan pers, kebebasan akademik, atau hak menyampaikan pendapat.

Negara memang berkewajiban menangani kejahatan siber, spionase, peretasan, penipuan, dan serangan terhadap infrastruktur. Namun, setiap tindakan harus memiliki dasar hukum, tujuan yang sah, batas kewenangan, pengawasan, dan mekanisme keberatan.

Sistem keamanan yang kuat harus menjaga kerahasiaan komunikasi masyarakat, membatasi akses aparat terhadap data, serta mencatat setiap penggunaan kewenangan. Pengumpulan data secara berlebihan justru menciptakan risiko baru apabila sistem tersebut disalahgunakan atau diretas.

Keamanan dan kebebasan bukan dua pilihan yang saling meniadakan. Demokrasi membutuhkan ruang digital yang aman sekaligus menghormati hak warga negara.

Keamanan siber yang kehilangan perlindungan hak asasi dapat berubah menjadi alat kontrol. Sebaliknya, kebebasan digital tanpa keamanan dapat dikuasai penipu, peretas, dan pelaku manipulasi.

## Agenda Keamanan Siber dalam Pembangunan

Pertama, setiap proyek digital pemerintah harus memasukkan anggaran keamanan sejak tahap perencanaan. Biaya keamanan, pembaruan, audit, pencadangan, dan pemulihan dihitung sepanjang umur sistem, bukan ditambahkan setelah insiden.

Kedua, pemerintah perlu menyusun daftar nasional aset digital kritis dan ketergantungannya. Negara harus mengetahui sistem mana yang tidak boleh

berhenti, siapa pengelolanya, serta layanan apa yang ikut terdampak apabila sistem tersebut gagal.

Ketiga, standar keamanan minimum harus diwajibkan pada seluruh instansi. Standar mencakup autentikasi multifaktor, enkripsi, pembatasan akses, pembaruan sistem, pemisahan jaringan, pencatatan aktivitas, dan perlindungan perangkat.

Keempat, seluruh layanan penting harus memiliki cadangan data terpisah dan tidak dapat diubah oleh penyerang. Kemampuan memulihkan data harus diuji secara berkala melalui latihan nyata.

Kelima, setiap instansi perlu memiliki tim tanggap insiden atau akses kepada layanan tanggap insiden bersama. Peraturan BSSN Nomor 1 Tahun 2024 telah memberikan kerangka mengenai tim, pelaporan, penanganan, dan kesiapan menghadapi insiden.

Keenam, pelaporan insiden harus diwajibkan dalam batas waktu yang jelas. Menyembunyikan insiden tidak boleh dianggap sebagai cara melindungi reputasi. Pemerintah juga perlu menerbitkan laporan pascainsiden yang menjelaskan penyebab, dampak, pemulihan, dan perbaikan.

Ketujuh, audit keamanan independen harus dilakukan terhadap pusat data, sistem pelayanan publik, infrastruktur vital, serta vendor teknologi. Hasil pentingnya perlu dilaporkan kepada lembaga pengawas dan diringkas untuk masyarakat.

Kedelapan, pemerintah harus melaksanakan simulasi krisis siber lintas sektor. Serangan terhadap listrik, telekomunikasi, perbankan, transportasi, dan pemerintahan tidak dapat ditangani oleh satu lembaga.

Kesembilan, pelaksanaan Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber serta Rencana Aksi Nasional 2024–2028 harus diukur melalui indikator hasil, bukan hanya jumlah rapat, pelatihan, atau dokumen.

Kesepuluh, pengadaan digital wajib menilai keamanan rantai pasok. Vendor harus menyediakan pembaruan, dokumentasi, pelaporan kerentanan, masa dukungan, dan rencana pemindahan data apabila kontrak berakhir.

Kesebelas, pemerintah perlu memperkuat pendidikan dan industri keamanan siber nasional. Belanja negara harus digunakan untuk membangun talenta, penelitian, laboratorium, produk, dan perusahaan dalam negeri yang mampu bersaing.

Kedua belas, literasi masyarakat harus diperluas. Warga perlu memahami kata sandi yang aman, autentikasi berlapis, phishing, penipuan digital, aplikasi palsu, perlindungan data pribadi, dan cara melaporkan kejahatan.

## Keamanan Digital Menentukan Kepercayaan

Indonesia telah memiliki fondasi kebijakan melalui Undang-Undang Pelindungan Data Pribadi, peraturan mengenai Infrastruktur Informasi Vital, Strategi

Keamanan Siber Nasional, Manajemen Krisis Siber, dan pengelolaan insiden.

Tantangannya adalah mengubah aturan menjadi kemampuan nyata.

Keamanan tidak dapat diukur hanya dari banyaknya perangkat yang dibeli. Ukurannya adalah seberapa cepat kerentanan ditutup, seberapa banyak peringatan ditindaklanjuti, seberapa cepat layanan dipulihkan, seberapa kecil data yang terdampak, dan seberapa terbuka pertanggungjawaban diberikan.

Tidak ada teknologi yang membuat serangan hilang sepenuhnya. Namun, tata kelola yang baik dapat mencegah satu kesalahan berkembang menjadi bencana nasional.

Keamanan siber juga bukan tanggung jawab BSSN seorang diri. Kementerian, pemerintah daerah, BUMN, perusahaan swasta, perguruan tinggi, media, fasilitas kesehatan, lembaga keuangan, vendor teknologi, dan masyarakat memegang bagian masing-masing.

Pembangunan digital yang cepat memang penting. Namun, kecepatan tanpa keamanan hanya memperbesar risiko. Negara tidak boleh membangun ribuan aplikasi sambil mengabaikan pembaruan, cadangan, integrasi, dan perlindungan data.

Masyarakat memberikan data dan kepercayaannya kepada negara serta perusahaan. Kepercayaan tersebut harus dibalas dengan perlindungan yang sungguh-sungguh.

Keamanan siber harus menjadi prioritas pembangunan karena ekonomi, pelayanan publik, pertahanan, dan kehidupan sehari-hari telah berpindah ke ruang digital. Ketika ruang itu tidak aman, pembangunan yang terlihat maju dapat berhenti hanya karena satu akun dicuri, satu celah dibiarkan, atau satu cadangan tidak tersedia.

Negara yang kuat pada abad digital bukan hanya negara yang memiliki banyak aplikasi dan pusat data. Negara yang kuat adalah negara yang mampu menjaga sistemnya tetap bekerja, melindungi data rakyatnya, memulihkan layanan ketika diserang, dan meminta pertanggungjawaban ketika terjadi kelalaian.

Jakarta, 18 Agustus 2026

Dr. Ir. Hendri, ST., MT
Wartawan Utama
Ketua Umum Jurnalis Nasional Indonesia (JNI)