KORLANTAS

Dr. Hendri: Mempertahankan Kedaulatan Indonesia di Era Perang Digital

Updates. - KORLANTAS.ID

Mar 1, 2026 - 07:19

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

OPINI - Dalam perang konvensional, masyarakat dapat melihat pesawat tempur, kapal perang, tentara, dan ledakan. Dalam perang digital, serangan dapat berlangsung tanpa suara. Tanda yang pertama kali terlihat mungkin hanya sebuah layar bertuliskan “layanan tidak tersedia”.

Namun, di balik layar tersebut, pelayanan imigrasi dapat berhenti, transaksi keuangan terganggu, data pasien tidak dapat diakses, sistem transportasi kehilangan kendali, jaringan komunikasi lumpuh, atau informasi rahasia negara dicuri.

Tidak ada peluru yang ditembakkan, tetapi pelayanan publik dapat terhenti. Tidak ada wilayah yang diduduki secara fisik, tetapi data, opini publik, proses ekonomi, dan keputusan politik dapat dipengaruhi dari tempat yang sangat jauh.

Inilah wajah baru pertahanan negara.

Kedaulatan pada abad digital tidak lagi hanya berbicara tentang daratan, lautan, dan ruang udara. Kedaulatan juga meliputi data, jaringan komunikasi, pusat data, satelit, perangkat lunak, algoritma, identitas digital, infrastruktur kritis, sistem pembayaran, ruang informasi, serta kemampuan negara melindungi warganya dari serangan siber.

Pertanyaannya, apakah negara ini benar-benar menguasai ruang digitalnya sendiri? Ataukah kita hanya menjadi pengguna teknologi, penyimpan data, dan pasar besar bagi sistem yang seluruh kendalinya berada di luar kemampuan nasional?

Perang Digital Tidak Selalu Diumumkan

Perang digital berbeda dengan perang konvensional. Pelakunya dapat berupa negara, kelompok yang didukung negara, organisasi kriminal, peretas bayaran, kelompok ideologis, orang dalam, atau individu yang mengejar keuntungan.

Motifnya juga beragam. Ada yang ingin mencuri uang, memperoleh data, melakukan spionase, melumpuhkan pelayanan, menguji pertahanan, merusak reputasi, memeras lembaga, menciptakan kekacauan, atau memengaruhi keputusan politik.

Serangan dapat berbentuk *phishing*, pencurian identitas, *ransomware*, serangan penolakan layanan, perusakan situs, penyusupan rantai pasok, pencurian data, sabotase sistem industri, manipulasi informasi, hingga rekayasa video dan suara menggunakan kecerdasan buatan.

Tidak semua serangan dapat langsung disebut sebagai tindakan perang. Anomali trafik juga tidak selalu berarti serangan berhasil. Penentuan pelaku membutuhkan penyelidikan teknis, intelijen, bukti hukum, dan kehati-hatian karena penyerang dapat menyembunyikan identitas atau menggunakan infrastruktur pihak lain.

Namun, ketidakjelasan pelaku tidak mengurangi dampaknya. Gangguan pada listrik, komunikasi, keuangan, kesehatan, pemerintahan, pangan, air, transportasi, atau pertahanan dapat menimbulkan kerugian yang setara dengan serangan terhadap infrastruktur fisik.

Karena itu, keamanan siber tidak boleh diperlakukan sebagai urusan teknisi komputer di ruang belakang. Keamanan siber merupakan bagian dari keamanan

nasional, perlindungan warga, keberlanjutan ekonomi, dan kepercayaan masyarakat kepada negara.

Ancaman Sudah Berada di Depan Pintu

Laporan Lanskap Keamanan Siber BSSN 2024 mencatat sekitar 330,5 juta anomali trafik sepanjang tahun tersebut. Di dalamnya teridentifikasi sekitar 26,77 juta aktivitas *phishing*, lebih dari 514 ribu aktivitas *ransomware*, dan sekitar 2,48 juta aktivitas yang berkaitan dengan *Advanced Persistent Threat*. (Lanskap Keamanan Siber BSSN 2024)

BSSN juga menelusuri 241 dugaan insiden kebocoran data. Pemantauan pada jaringan tersembunyi menemukan lebih dari 56 juta temuan paparan data yang berdampak pada 461 pemangku kepentingan. Terdapat pula ribuan kasus perusakan tampilan situs, sebagian besar berkaitan dengan penyusupan konten perjudian daring.

Angka tersebut tidak boleh dibaca hanya sebagai statistik. Setiap upaya *phishing* dapat mengincar pegawai pemerintah, nasabah bank, pekerja perusahaan, mahasiswa, jurnalis, anggota militer, atau masyarakat biasa. Satu akun yang berhasil dikuasai dapat menjadi pintu masuk menuju jaringan yang lebih besar.

Satu perangkat yang tidak diperbarui dapat membuka akses terhadap basis data. Satu kata sandi yang digunakan berulang kali dapat membahayakan beberapa layanan. Satu pegawai yang tertipu membuka lampiran dapat melumpuhkan seluruh organisasi.

Kemajuan juga patut diakui. Dalam Global Cybersecurity Index 2024, International Telecommunication Union menempatkan Indonesia pada kelompok Tier 1 atau *role-modelling*, tingkat tertinggi dalam penilaian komitmen keamanan siber. Penilaian tersebut mencakup aspek hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama. (International Telecommunication Union)

Namun, peringkat yang baik bukan jaminan bahwa sistem telah kebal terhadap serangan. Indeks mengukur komitmen dan kesiapan pada tingkat tertentu, sedangkan ketahanan sebenarnya diuji ketika insiden terjadi.

Negara mungkin memiliki regulasi, lembaga, dan strategi. Pertanyaan sesungguhnya adalah apakah cadangan data tersedia, akses dapat dikendalikan, kerentanan segera diperbaiki, koordinasi berjalan, pelayanan dapat dipulihkan, dan masyarakat memperoleh penjelasan yang jujur.

Pelajaran Mahal dari Serangan PDNS 2

Serangan *ransomware* terhadap Pusat Data Nasional Sementara 2 pada Juni 2024 menjadi pelajaran penting. Gangguan tersebut berdampak pada layanan publik di 239 instansi dari total 282 instansi pengguna. (Kementerian Komunikasi dan Digital)

Peristiwa itu menunjukkan bahwa memusatkan data tidak otomatis meningkatkan

keamanan. Konsolidasi dapat meningkatkan efisiensi, standarisasi, dan pengawasan, tetapi juga menciptakan titik kegagalan yang berdampak luas apabila tidak dilengkapi segmentasi, cadangan, pengendalian akses, serta sistem pemulihan.

Pusat data bukan sekadar gedung berisi komputer. Pusat data nasional harus mempunyai arsitektur ketahanan, lokasi cadangan, replikasi yang aman, pemisahan jaringan, pemantauan berkelanjutan, dan prosedur pemulihan yang diuji.

Mempertahankan Kedaulatan Indonesia di Era Perang Digital

Dalam perang konvensional, masyarakat dapat melihat pesawat tempur, kendaraan lapis baja, kapal perang, dan pasukan yang bergerak melintasi perbatasan. Dalam perang digital, serangan dapat dimulai dari sebuah surat elektronik, perangkat lunak yang tidak diperbarui, kata sandi yang dicuri, pegawai yang tertipu, atau celah pada sistem milik penyedia layanan.

Tidak terdengar ledakan ketika sebuah pusat data disusupi. Tidak terlihat asap ketika informasi pribadi dicuri. Namun, akibatnya dapat melumpuhkan layanan imigrasi, perbankan, rumah sakit, transportasi, pembangkit listrik, pemerintahan, dan komunikasi.

Serangan digital juga dapat menyasar pikiran masyarakat. Video palsu, suara hasil rekayasa kecerdasan buatan, berita bohong, dan propaganda terkoordinasi dapat digunakan untuk memecah persatuan, merusak kepercayaan kepada lembaga, memengaruhi pemilu, atau menciptakan kepanikan.

Perang digital berlangsung tanpa harus diumumkan. Pelakunya tidak selalu mengenakan seragam dan tidak selalu berada di wilayah negara yang menjadi sasaran. Mereka dapat berupa kelompok kriminal, aktor yang didukung negara, peretas bayaran, jaringan propaganda, kelompok ideologis, orang dalam, atau pihak ketiga yang sistemnya telah terlebih dahulu dikuasai.

Karena itu, menjaga kedaulatan pada era digital tidak cukup dilakukan dengan mempertahankan daratan, lautan, dan udara. Negara juga harus menjaga data, jaringan, pusat komputasi, satelit, spektrum, identitas digital, algoritma, sistem pembayaran, infrastruktur informasi vital, serta ruang informasi masyarakat.

Kedaulatan digital bukan pilihan tambahan. Ia telah menjadi bagian dari kedaulatan negara.

Kedaulatan Digital Lebih Luas daripada Lokasi Server

Kedaulatan digital sering disederhanakan menjadi pertanyaan: di mana data disimpan?

Lokasi penyimpanan memang penting karena berkaitan dengan yurisdiksi, akses pemerintah asing, kesinambungan layanan, dan kemampuan negara menegakkan hukum. Namun, menyimpan data di dalam negeri belum otomatis membuat data aman.

Server yang berada di wilayah nasional tetap dapat disusupi apabila pengendalian akses lemah. Pusat data milik pemerintah tetap dapat lumpuh jika tidak memiliki cadangan yang terpisah dan teruji. Perangkat yang dibeli dari perusahaan nasional belum tentu aman apabila komponennya tidak diperiksa. Sebaliknya, penggunaan teknologi asing tidak selalu berarti negara kehilangan seluruh kendali apabila terdapat kontrak, enkripsi, audit, portabilitas data, dan pengawasan yang kuat.

Kedaulatan digital harus diukur dari kemampuan negara menentukan siapa yang dapat mengakses data, untuk tujuan apa, berapa lama data disimpan, di mana cadangannya berada, bagaimana data dipindahkan, siapa yang memeriksa sistem, serta bagaimana layanan dipulihkan setelah serangan.

Negara yang berdaulat secara digital harus mampu membuat keputusan tanpa dikunci oleh satu penyedia teknologi. Pemerintah harus dapat memindahkan data dan layanan ketika kontrak berakhir, melakukan audit keamanan, memperoleh pembaruan, memeriksa komponen perangkat lunak, dan menjalankan sistem penting dalam keadaan darurat.

Dengan demikian, kedaulatan digital bukan isolasi teknologi. Kedaulatan digital adalah kemampuan mengendalikan risiko, melindungi hak warga, menjaga kesinambungan layanan, dan mengambil keputusan strategis secara mandiri.

Ancaman yang Tidak Lagi Dapat Dianggap Gangguan Teknis

Laporan Lanskap Keamanan Siber BSSN 2024 mencatat sekitar 330,5 juta anomali trafik. Di dalamnya terdapat sekitar 2,48 juta aktivitas *Advanced Persistent Threat*, lebih dari 514 ribu aktivitas *ransomware*, serta sekitar 26,77 juta aktivitas *phishing*. BSSN juga menelusuri 241 dugaan insiden kebocoran data dan menemukan lebih dari 56 juta paparan data yang berdampak pada 461 pemangku kepentingan. (Laporan Lanskap Keamanan Siber 2024)

Anomali trafik tidak selalu berarti serangan berhasil. Sebagian merupakan indikasi, pemindaian, percobaan, atau aktivitas yang harus dianalisis lebih lanjut. Namun, skala tersebut menunjukkan bahwa sistem digital nasional terus-menerus menghadapi upaya penyusupan dan penyalahgunaan.

Ancaman tidak hanya menargetkan kementerian atau lembaga besar. Pemerintah daerah, sekolah, rumah sakit, perguruan tinggi, usaha kecil, media, organisasi masyarakat, dan pengguna pribadi dapat menjadi pintu masuk.

Sebuah pemerintah kabupaten mungkin dianggap tidak memiliki data strategis. Namun, sistemnya menyimpan identitas penduduk, data pajak, perizinan, informasi pegawai, dokumen anggaran, dan akses menuju jaringan lain. Rumah

sakit menyimpan rekam medis yang bernilai tinggi. Perguruan tinggi memiliki data mahasiswa dan hasil penelitian. Perusahaan swasta menguasai informasi pelanggan serta rantai pasok.

Dalam perang digital, sasaran yang terlihat kecil dapat menjadi jalan menuju sistem yang lebih besar.

Pelajaran Mahal dari PDNS 2

Serangan *ransomware* terhadap Pusat Data Nasional Sementara 2 pada Juni 2024 menjadi peringatan keras. Gangguan tersebut berdampak terhadap layanan publik pada 239 dari 282 instansi pengguna. (Kementerian Komunikasi dan Digital)

Peristiwa itu memperlihatkan bahwa digitalisasi tanpa ketahanan dapat menciptakan titik kegagalan yang sangat besar. Ketika banyak layanan dipusatkan pada satu infrastruktur, kegagalan pada infrastruktur tersebut dapat menyebar ke berbagai instansi secara bersamaan.

Pemusatan sistem memang dapat meningkatkan efisiensi, standardisasi, dan pengawasan. Namun, pemusatan juga meningkatkan dampak apabila terjadi gangguan.

Karena itu, pusat data nasional tidak boleh dibangun hanya sebagai proyek gedung, server, dan jaringan. Ia harus dilengkapi arsitektur ketahanan, segmentasi, pengendalian identitas, pencadangan, pusat pemulihan bencana, pemantauan sepanjang waktu, pengujian berkala, serta prosedur kesinambungan pelayanan.

Cadangan data tidak cukup hanya dicatat dalam dokumen. Cadangan harus terpisah dari sistem utama, terlindungi dari perubahan, dan diuji melalui pemulihan nyata. Prinsip tiga salinan, dua jenis media, satu salinan di lokasi berbeda, satu salinan *offline* atau tidak dapat diubah, serta nol kesalahan setelah pengujian dapat menjadi acuan.

Sistem dinyatakan memiliki cadangan bukan ketika proses penyalinan selesai, tetapi ketika data berhasil dipulihkan dalam waktu yang telah ditetapkan.

Setiap layanan publik penting juga harus mempunyai target waktu pemulihan dan batas kehilangan data yang dapat diterima. Masyarakat perlu mengetahui kapan layanan kembali berjalan, jalur pelayanan alternatif, serta hak mereka ketika gangguan terjadi.

Kedaulatan tidak terlihat dari seberapa banyak aplikasi dibangun. Kedaulatan terlihat dari kemampuan negara mempertahankan dan memulihkan pelayanan ketika aplikasi tersebut diserang.

Infrastruktur Informasi Vital Harus Diperlakukan sebagai Pertahanan Nasional

Serangan terhadap sistem administrasi mungkin menghambat pelayanan.

Serangan terhadap energi, keuangan, transportasi, telekomunikasi, kesehatan, pangan, air, atau pertahanan dapat mengancam keselamatan masyarakat dan stabilitas negara.

Peraturan Presiden Nomor 82 Tahun 2022 telah memberikan kerangka pelindungan infrastruktur informasi vital. Sementara itu, Peraturan Presiden Nomor 47 Tahun 2023 mengatur Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. (Perpres Nomor 82 Tahun 2022, Perpres Nomor 47 Tahun 2023)

Landasan kebijakan tersebut harus diterjemahkan ke dalam standar operasional yang dapat diuji.

Setiap penyelenggara infrastruktur informasi vital perlu memetakan aset, ketergantungan sistem, jalur komunikasi, pemasok, hak akses, dan risiko terburuk. Pengamanan harus menggunakan prinsip *zero trust*: tidak ada pengguna, perangkat, atau koneksi yang otomatis dipercaya hanya karena berada di dalam jaringan.

Hak akses diberikan seminimal mungkin sesuai tugas. Akun dengan kewenangan tinggi harus dibatasi, diawasi, dan dilindungi autentikasi berlapis. Aktivitas penting dicatat agar dapat diperiksa. Jaringan perlu disegmentasi supaya penyerang yang berhasil memasuki satu bagian tidak mudah bergerak menuju sistem lainnya.

Penilaian keamanan tidak boleh berhenti pada sertifikat kepatuhan. Sistem harus menjalani pengujian penetrasi, simulasi serangan, audit konfigurasi, pemindaian kerentanan, dan latihan pemulihan.

Audit yang hanya memeriksa kelengkapan dokumen dapat menghasilkan rasa aman palsu. Dalam keamanan siber, yang diperlukan bukan bukti bahwa prosedur telah ditulis, melainkan bukti bahwa pertahanan benar-benar bekerja.

Data Warga Bukan Komoditas Tanpa Pemilik

Data pribadi menjadi salah satu sumber kekuasaan pada era digital. Identitas, nomor telepon, lokasi, kesehatan, pendidikan, transaksi, kebiasaan, pilihan politik, dan hubungan sosial dapat digunakan untuk memberikan pelayanan, tetapi juga dapat disalahgunakan untuk penipuan, pemerasan, diskriminasi, manipulasi, dan pengawasan berlebihan.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar hukum bagi pengumpulan, pemrosesan, penyimpanan, pemindahan, dan penghapusan data pribadi. (Database Peraturan Pemerintah)

Namun, hukum akan kehilangan arti apabila lembaga dan perusahaan terus mengumpulkan data sebanyak-banyaknya tanpa memahami risikonya.

Prinsip pertama haruslah pengurangan data. Jika suatu pelayanan hanya membutuhkan nama dan alamat, jangan meminta salinan seluruh dokumen keluarga. Jika data tidak lagi diperlukan, data harus dihapus secara aman. Jika data digunakan untuk tujuan baru, masyarakat harus memperoleh penjelasan

dan dasar hukum yang jelas.

Data sensitif perlu dienkripsi ketika disimpan maupun dikirim. Kunci enkripsi tidak boleh berada pada pihak yang sama tanpa pengawasan. Akses pegawai harus dicabut segera ketika mereka berpindah tugas atau berhenti bekerja.

Setiap kebocoran harus dilaporkan secara cepat kepada pihak berwenang dan orang yang terdampak. Pemberitahuan tidak boleh menggunakan bahasa yang mengecilkan masalah. Warga berhak mengetahui data apa yang bocor, risiko yang mungkin timbul, tindakan yang perlu dilakukan, serta bentuk pertanggungjawaban pengelola sistem.

Ketika data warga bocor, negara tidak boleh hanya menyebutnya sebagai gangguan teknis. Kebocoran data merupakan pelanggaran terhadap keamanan, privasi, dan kepercayaan publik.

Ketergantungan Teknologi Menjadi Risiko Strategis

Transformasi digital nasional masih bergantung pada berbagai teknologi dari luar negeri: semikonduktor, sistem operasi, layanan komputasi awan, perangkat jaringan, satelit, basis data, platform komunikasi, mesin pencari, kecerdasan buatan, dan perangkat keamanan.

Kerja sama global tidak dapat dihindari dan tidak harus dipandang sebagai kelemahan. Tidak ada negara yang membangun seluruh teknologi digitalnya sendiri. Masalah muncul ketika ketergantungan berubah menjadi ketidakberdayaan.

Jika pemerintah tidak dapat memeriksa keamanan produk, tidak memiliki tenaga untuk mengoperasikan sistem, tidak dapat memindahkan data, tidak menguasai konfigurasi, atau tidak memperoleh pembaruan tanpa persetujuan penyedia, maka kendali strategis menjadi lemah.

Setiap pengadaan teknologi perlu mensyaratkan hak audit, portabilitas data, standar terbuka, dokumentasi, pelatihan, pembaruan keamanan, waktu penanganan kerentanan, serta rencana keluar dari penyedia.

Untuk perangkat lunak kritis, pemerintah perlu meminta daftar komponen atau *software bill of materials*. Dengan daftar tersebut, pengelola dapat mengetahui apakah suatu produk menggunakan komponen yang memiliki kerentanan.

Kontrak juga harus mengatur kepemilikan data, lokasi pemrosesan, penggunaan subkontraktor, kewajiban pemberitahuan insiden, penghancuran data setelah kontrak berakhir, dan tanggung jawab atas kerugian.

Produk nasional harus diprioritaskan apabila memenuhi standar keamanan, mutu, dan kinerja. Namun, label buatan dalam negeri tidak boleh menjadi pengganti pengujian. Teknologi lokal juga harus diaudit, diperbarui, dan dibandingkan secara objektif.

Kemandirian teknologi bukan membeli produk nasional tanpa pemeriksaan. Kemandirian berarti membangun kemampuan merancang, menguji, memperbaiki, mengoperasikan, dan mengembangkan teknologi secara berkelanjutan.

Industri Keamanan Siber Nasional Harus Dibangun

Negara membutuhkan industri keamanan siber yang kuat, bukan hanya pengguna produk asing.

Perguruan tinggi, lembaga riset, perusahaan teknologi, BUMN, perusahaan rintisan, komunitas peretas etis, dan sektor pertahanan perlu dihubungkan dalam ekosistem riset dan produksi.

Kebutuhan nasional mencakup sistem deteksi ancaman, enkripsi, identitas digital, keamanan komputasi awan, forensik, analisis *malware*, keamanan perangkat IoT, perlindungan teknologi operasional, dan alat pemeriksaan konten sintetis.

Pemerintah dapat menggunakan pengadaan sebagai instrumen pembangunan industri. Namun, pengadaan harus disertai standar teknis, pengujian independen, dan persaingan yang sehat agar tidak menciptakan monopoli baru.

Perusahaan rintisan membutuhkan akses terhadap laboratorium, data uji yang aman, sertifikasi, pendanaan, dan kesempatan menerapkan produknya. Lembaga riset harus memperoleh dukungan untuk menghasilkan paten, prototipe, standar, serta teknologi yang dapat digunakan industri.

Negara juga perlu membangun kemampuan produksi dan pemeliharaan komponen strategis secara bertahap. Tidak semua komponen harus dibuat sendiri, tetapi negara harus mengetahui titik ketergantungan yang paling berisiko dan memiliki rencana jika rantai pasok terganggu.

Kedaulatan teknologi dibangun melalui puluhan tahun pendidikan, penelitian, produksi, dan keberanian membeli hasil karya bangsa sendiri yang telah terbukti aman.

Kekurangan Talenta Sama Berbahayanya dengan Kekurangan Perangkat

Peralatan keamanan yang mahal tidak akan banyak membantu apabila tidak ada orang yang mampu mengoperasikan, memantau, dan menindaklanjuti peringatannya.

Masalah keamanan siber sering bukan ketiadaan teknologi, melainkan kekurangan tenaga, pembagian tanggung jawab yang tidak jelas, konfigurasi yang salah, serta peringatan insiden yang diabaikan.

International Telecommunication Union menempatkan Indonesia dalam kelompok Tier 1 atau *role-modelling* pada Global Cybersecurity Index 2024. Penilaian

tersebut mengukur komitmen negara melalui lima pilar: hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama. (International Telecommunication Union)

Pencapaian tersebut patut diapresiasi. Namun, kategori tinggi tidak berarti negara kebal terhadap serangan. Indeks mengukur komitmen dan kematangan kebijakan, sedangkan pertahanan nyata ditentukan oleh pelaksanaan pada ribuan lembaga, perusahaan, dan perangkat.

Pemerintah perlu membangun peta kebutuhan talenta secara nasional. Sekolah dapat mengenalkan keamanan digital sejak dini. Perguruan tinggi perlu memperkuat program keamanan siber, kriptografi, forensik, kecerdasan buatan, dan tata kelola teknologi.

Pelatihan tidak hanya ditujukan kepada teknisi. Pimpinan lembaga harus memahami risiko siber karena keputusan mengenai anggaran, prioritas, dan penerimaan risiko berada pada mereka. Pegawai administrasi perlu mengenali *phishing*. Tim hukum harus memahami kewajiban pelaporan dan perlindungan data. Bagian pengadaan harus mampu menilai risiko pemasok.

Keamanan siber bukan urusan satu unit teknologi informasi. Ia merupakan tanggung jawab organisasi.

Perang Informasi Mengincar Pikiran Masyarakat

Kedaulatan digital tidak hanya berkaitan dengan jaringan dan data. Ia juga menyangkut kemampuan masyarakat mempertahankan penilaian yang rasional di tengah operasi informasi.

Kecerdasan buatan dapat menghasilkan video dan suara yang menyerupai tokoh nyata. Jaringan akun otomatis dapat memperbesar pesan tertentu. Data pribadi dapat digunakan untuk menyusun propaganda yang disesuaikan dengan ketakutan dan kemarahan kelompok tertentu.

Tujuannya tidak selalu membuat masyarakat percaya pada satu kebohongan. Operasi informasi dapat dirancang agar masyarakat tidak lagi percaya kepada siapa pun.

Ketika semua berita dianggap palsu, fakta kehilangan kekuatan. Ketika setiap kritik disebut propaganda, pengawasan publik melemah. Ketika perbedaan pendapat dianggap sebagai serangan negara asing, demokrasi terancam.

Karena itu, menghadapi perang informasi tidak boleh dilakukan dengan membungkam kritik. Kedaulatan digital bukan kewenangan pemerintah mengendalikan seluruh percakapan masyarakat.

Negara harus melawan manipulasi terkoordinasi melalui bukti, transparansi, komunikasi yang cepat, pemeriksaan fakta, dan pendidikan media. Platform digital perlu membuka informasi mengenai iklan politik, jaringan akun tidak autentik, konten sintetis, serta cara algoritma mendistribusikan informasi.

Pers yang merdeka harus dilindungi karena jurnalisme profesional membantu

masyarakat memeriksa klaim dan mengawasi kekuasaan. Masyarakat sipil dan akademisi juga perlu memperoleh akses untuk meneliti operasi informasi tanpa takut dikriminalisasi.

Pertahanan terhadap disinformasi harus memperkuat demokrasi, bukan menjadi pintu menuju pemerintahan yang antikritik.

Koordinasi Nasional Tidak Boleh Berjalan Sektoral

Ancaman siber melintasi batas kementerian, pemerintah daerah, perusahaan, dan negara. Namun, penanganannya sering terpecah berdasarkan kewenangan sektoral.

Ketika insiden terjadi, pertanyaan mendasar dapat menghambat penanganan: siapa yang memimpin, siapa yang boleh mengisolasi sistem, siapa yang memberi tahu masyarakat, siapa yang memeriksa barang bukti, dan siapa yang bertanggung jawab memulihkan layanan?

Strategi nasional harus menetapkan rantai komando yang jelas dalam situasi krisis, tetapi tetap dilengkapi pengawasan hukum dan sipil. BSSN, TNI, Polri, Komdigi, lembaga intelijen, kementerian teknis, pemerintah daerah, serta penyelenggara infrastruktur vital perlu berlatih bersama.

Latihan tidak boleh hanya dilakukan melalui diskusi di ruang rapat. Simulasi harus menguji keadaan nyata: listrik terputus, pusat data tidak dapat diakses, komunikasi terganggu, data bocor, informasi palsu menyebar, dan layanan publik berhenti.

Setelah latihan atau insiden, hasil evaluasi harus menghasilkan tindakan perbaikan dengan penanggung jawab dan tenggat waktu. Temuan kritis tidak boleh berhenti sebagai laporan rahasia yang tidak pernah ditindaklanjuti.

Informasi teknis sensitif memang harus dilindungi. Namun, masyarakat tetap berhak memperoleh laporan agregat mengenai jenis insiden, waktu pemulihan, dampak pelayanan, serta tindakan perbaikan.

Kerahasiaan tidak boleh digunakan untuk menyembunyikan kelalaian.

Agenda Mempertahankan Kedaulatan Digital

Pertama, pemerintah harus memetakan seluruh aset digital dan infrastruktur informasi vital. Negara tidak dapat melindungi sistem yang tidak diketahui keberadaannya.

Kedua, setiap layanan kritis harus memiliki pencadangan yang terpisah, tidak dapat diubah oleh penyerang, dan diuji melalui pemulihan berkala.

Ketiga, prinsip *zero trust*, autentikasi berlapis, hak akses minimum, segmentasi jaringan, pembaruan sistem, serta pemantauan sepanjang waktu harus menjadi standar wajib.

Keempat, pelaporan insiden perlu dilakukan cepat dan terkoordinasi. Organisasi tidak boleh menyembunyikan kebocoran karena takut kehilangan reputasi. Menunda pemberitahuan justru memperbesar kerugian masyarakat.

Kelima, pengadaan teknologi harus memasukkan persyaratan keamanan sejak awal: audit, daftar komponen, pembaruan, portabilitas, dokumentasi, pelatihan, serta rencana keluar dari penyedia.

Keenam, pemerintah harus mengembangkan industri dan talenta keamanan siber nasional melalui pendidikan, penelitian, sertifikasi, pengadaan, pendanaan, dan kerja sama antara perguruan tinggi serta industri.

Ketujuh, program pelaporan kerentanan dan *bug bounty* perlu diperluas. Peneliti keamanan yang bekerja dengan itikad baik harus memperoleh jalur pelaporan yang aman, bukan langsung diperlakukan sebagai pelaku kejahatan.

Kedelapan, pelaksanaan Undang-Undang Pelindungan Data Pribadi harus diperkuat melalui pengawasan, penegakan, mekanisme pengaduan, serta sanksi yang efektif.

Kesembilan, literasi keamanan digital masyarakat harus menjadi gerakan nasional. Penggunaan autentikasi berlapis, pengelola kata sandi, pembaruan perangkat, pencadangan, dan kewaspadaan terhadap tautan mencurigakan dapat mencegah banyak serangan.

Kesepuluh, diplomasi siber perlu diperkuat. Kejahatan digital melintasi yurisdiksi sehingga membutuhkan pertukaran informasi, bantuan hukum, standar bersama, latihan regional, serta kesepakatan mengenai perilaku negara yang bertanggung jawab di ruang siber.

Kedaulatan Bukan Alasan untuk Menutup Diri

Mempertahankan kedaulatan digital tidak berarti memutus hubungan dengan teknologi global. Isolasi justru dapat memperlambat inovasi, meningkatkan biaya, dan membatasi akses terhadap pengetahuan.

Yang dibutuhkan adalah kerja sama dari posisi yang memiliki kemampuan dan pilihan.

Negara harus mengetahui teknologi mana yang strategis, data mana yang sensitif, layanan mana yang tidak boleh berhenti, ketergantungan mana yang berbahaya, serta kemampuan apa yang harus dikuasai sendiri.

Kedaulatan juga tidak boleh dijadikan alasan untuk mengawasi masyarakat secara berlebihan. Negara yang melindungi sistem tetapi melanggar privasi warga belum dapat disebut berdaulat secara digital.

Kedaulatan harus melindungi rakyat, bukan mengendalikan rakyat.

Keamanan nasional, kebebasan berekspresi, perlindungan data, kemerdekaan pers, dan inovasi harus ditempatkan dalam satu keseimbangan. Sistem yang

aman tetapi antikritik akan merusak demokrasi. Sistem yang terbuka tanpa pengamanan akan mudah disalahgunakan.

Benteng Digital Dibangun Sebelum Serangan

Serangan siber tidak dapat dihapus sepenuhnya. Bahkan sistem paling maju masih dapat mengalami insiden. Ukuran keberhasilan bukan hanya tidak pernah diserang, tetapi kemampuan mencegah, mendeteksi, membatasi dampak, memulihkan layanan, mempelajari kesalahan, dan menuntut pertanggungjawaban.

Dalam perang digital, kelalaian kecil dapat menghasilkan dampak nasional. Kata sandi yang lemah, cadangan yang tidak diuji, pegawai yang tidak dilatih, server yang tidak diperbarui, atau kontrak yang mengunci data dapat menjadi celah menuju krisis.

Karena itu, keamanan siber tidak boleh menunggu setelah terjadi serangan. Anggaran keamanan bukan biaya tambahan, melainkan bagian dari biaya setiap layanan digital. Tidak ada transformasi digital tanpa keamanan digital.

Kita boleh membangun ribuan aplikasi, memperluas jaringan, menerapkan kecerdasan buatan, dan menghubungkan seluruh pelayanan. Namun, semakin terhubung suatu negara, semakin besar pula tanggung jawabnya menjaga setiap titik hubungan.

Kedaulatan Indonesia pada abad ke-21 tidak hanya dipertahankan oleh prajurit di perbatasan, kapal di lautan, dan pesawat di udara. Kedaulatan juga dijaga oleh ahli kriptografi, analis ancaman, pengelola pusat data, peneliti, jurnalis, pembuat perangkat lunak, aparat penegak hukum, guru, pegawai, perusahaan, dan masyarakat yang menjaga datanya.

Benteng digital tidak dibangun ketika serangan telah terjadi. Benteng itu dibangun hari ini melalui teknologi yang dapat dipercaya, manusia yang kompeten, hukum yang adil, kepemimpinan yang bertanggung jawab, serta masyarakat yang sadar akan risikonya.

Jika data dikuasai pihak lain, layanan mudah dilumpuhkan, teknologi sepenuhnya bergantung, dan masyarakat dapat diadu melalui manipulasi informasi, maka kedaulatan negara menjadi rapuh.

Mempertahankan kedaulatan di era perang digital berarti memastikan bahwa negara tetap mampu mengambil keputusan, melayani rakyat, menjaga kebenaran, melindungi data, dan memulihkan dirinya ketika diserang.

Itulah wajah baru pertahanan nasional.

Jakarta, 1 Maret 2026

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