
Cybersecurity sebagai
Isu Globalisasi Baru:
Risiko Sistemik pada Infrastruktur Digital
Oleh Rudy C Tarumingkeng

Oleh:
Prof Ir Rudy C Tarumingkeng, PhD
Professor of Management NUP: 9903252922
Rektor, Universitas Cenderawasih, Papua (1978-1988, dan
Rektor, Kampus AGRO Manokwari sekarang Universitas Papua Manokwari)
Coordinator, CIDA/DIKTI SFU Burnaby BC Canada 1988-1991
Rektor, Universitas Kristen Krida Wacana, Jakarta (1991-2000)
Ketua Dewan Guru Besar, IPB-University, Bogor (2005-2006)
AI - Data Analyst, dan Ketua Senat Akademik, IBM-ASMI, Jakarta 2024-

---

rudyct75@gmail.com

CYBERSECURITY SEBAGAI ISU GLOBALISASI BARU RISIKO SISTEMIK PADA INFRASTRUKTUR DIGITAL

Globalisasi pada abad ke-20 sering dipahami melalui arus barang, modal, energi, dan manusia. Namun pada abad ke-21, wajah globalisasi berubah secara mendasar: arus data, perangkat lunak, layanan cloud, identitas digital, pembayaran elektronik, dan platform kini menjadi "urat nadi" ekonomi dan tata kelola. Dalam konteks ini, *cybersecurity* tidak lagi sekadar isu teknis milik divisi TI, melainkan telah menjadi isu strategis global—sejajar dengan perdagangan, energi, dan stabilitas keuangan.

Perubahan ini penting dipahami, terutama oleh negara berkembang. Mengapa? Karena banyak negara sedang melakukan lompatan digital (digital leapfrogging): mempercepat layanan publik digital, pembayaran nontunai, interoperabilitas data, dan otomatisasi sektor produktif. Lompatan ini dapat meningkatkan efisiensi, inklusi, dan daya saing. Namun pada saat yang sama, ia juga memperbesar ketergantungan pada infrastruktur digital yang kompleks, saling terhubung, dan sering kali bergantung pada vendor global, jaringan lintas negara, serta rantai pasok perangkat lunak yang tidak sepenuhnya terlihat.

Dengan kata lain, globalisasi digital melahirkan bentuk risiko baru: **risiko sistemik siber**. Risiko ini muncul ketika gangguan pada satu titik—misalnya penyedia cloud, pembaruan perangkat lunak, pusat data, sistem identitas, atau jaringan pembayaran—menimbulkan efek domino lintas sektor dan lintas wilayah. Dalam sistem yang sangat terintegrasi, gangguan tidak harus berupa serangan negara (state-sponsored attack)

untuk menjadi bencana. Bahkan kegagalan non-malicious seperti pembaruan perangkat lunak yang cacat pun dapat melumpuhkan layanan publik, transportasi, rumah sakit, dan operasi bisnis secara serentak. Hal ini terlihat jelas dalam insiden CrowdStrike/Microsoft tahun 2024, yang menurut Microsoft berdampak pada sekitar 8,5 juta perangkat Windows dan menunjukkan betapa luas dampak sosial-ekonominya meskipun persentase perangkat terdampak relatif kecil terhadap total perangkat Windows global. (The Official Microsoft Blog)

Esai ini membahas *cybersecurity* sebagai isu globalisasi baru dengan fokus pada risiko sistemik pada infrastruktur digital. Argumen utamanya adalah sebagai berikut: **semakin digital dan terintegrasi suatu ekonomi, semakin penting pendekatan keamanan siber yang berbasis tata kelola, resiliensi, dan koordinasi lintas sektor—bukan hanya proteksi teknis di level organisasi**. Untuk itu, kita perlu memandang keamanan siber sebagai persoalan ekonomi politik global, manajemen risiko sistemik, dan kapasitas kelembagaan negara, bukan sekadar persoalan firewall, antivirus, atau sertifikasi teknis semata.

---

1. Dari Globalisasi Barang ke Globalisasi Infrastruktur Digital

Pada masa globalisasi klasik, risiko sistemik lebih sering diasosiasikan dengan krisis keuangan, guncangan harga minyak, perang dagang, atau terganggunya jalur pelayaran. Dalam globalisasi digital, "jalur pelayaran" baru adalah jaringan data, kabel, pusat data, perangkat lunak inti, dan layanan digital yang menopang transaksi serta operasi harian. Ketika infrastruktur ini terganggu, pabrik tidak hanya berhenti karena kekurangan bahan baku, tetapi juga karena sistem ERP gagal, pembayaran tidak dapat diproses, atau jaringan logistik kehilangan visibilitas.

Di sinilah *cybersecurity* menjadi isu globalisasi baru. Ia hadir di persimpangan antara tiga perkembangan besar:

Pertama, digitalisasi lintas sektor. Energi, keuangan, kesehatan, transportasi, pemerintahan, pendidikan, dan perdagangan semakin terdigitalisasi. Badan Energi Internasional (IEA) menegaskan bahwa digitalisasi sistem kelistrikan membuka peluang efisiensi besar, tetapi juga memperluas *attack surface* dan meningkatkan paparan terhadap risiko siber. Artinya, transformasi digital tanpa penguatan keamanan dan resiliensi dapat memindahkan efisiensi menjadi kerentanan.

Kedua, integrasi lintas batas. Banyak layanan digital modern berjalan di atas ekosistem global: *cloud services*, perangkat lunak keamanan, *content delivery networks*, API pihak ketiga, sistem kolaborasi, dan *managed services*. Ketergantungan ini membuat satu gangguan berpotensi menyebar cepat ke banyak negara dan sektor secara simultan. IMF menggarisbawahi bahwa ketergantungan pada institusi/penyedia yang tidak mudah digantikan dan keterhubungan teknologi (misalnya banyak firma memakai perangkat lunak yang sama) dapat mempercepat propagasi gangguan dan mengganggu stabilitas sistem. (IMF)

Ketiga, ketimpangan kapasitas siber global. Tidak semua negara, lembaga, dan organisasi memiliki tingkat kesiapan yang sama. World Economic Forum menyoroti peningkatan risiko siber dan kesenjangan ketahanan (*cyber inequity*) antara organisasi besar dan kecil, termasuk tantangan rantai pasok yang semakin berat. (World Economic Forum Reports) Sementara itu, World Bank mencatat dukungannya terhadap penguatan fondasi siber di puluhan negara, namun juga menekankan bahwa negara berpendapatan rendah masih menghadapi kesenjangan kapasitas yang serius—termasuk keterbatasan tim tanggap insiden dan sumber daya kelembagaan. (UnitedHealth Group)

Dalam lanskap ini, globalisasi tidak lagi hanya soal “siapa mengekspor apa”, tetapi juga “siapa mengendalikan lapisan digital kritis”, “siapa

memiliki kapasitas respons saat insiden", dan "seberapa cepat sebuah kegagalan teknis berubah menjadi krisis sosial-ekonomi".

---

2. Infrastruktur Digital sebagai Infrastruktur Kritis Baru

Untuk memahami risiko sistemik siber, kita perlu lebih dulu memahami apa yang dimaksud dengan **infrastruktur digital**. Dalam diskusi publik, istilah ini sering dipersempit menjadi internet atau pusat data. Padahal, secara fungsional, infrastruktur digital mencakup beberapa lapisan yang saling bergantung:

Lapisan fisik: kabel, satelit, pusat data, jaringan listrik pendukung, perangkat jaringan.

Lapisan komputasi dan platform: *cloud infrastructure*, sistem operasi, virtualisasi, layanan identitas.

Lapisan aplikasi dan layanan: sistem pembayaran, e-government, rekam medis, logistik, ERP, platform pendidikan.

Lapisan tata kelola dan proses: kebijakan akses, manajemen identitas, cadangan data, respons insiden, audit, koordinasi.

Lapisan manusia dan organisasi: operator, vendor, regulator, pengguna akhir, pimpinan organisasi, ekosistem pemasok.

Kesalahan umum dalam pengelolaan keamanan siber adalah fokus berlebihan pada satu lapisan (misalnya teknologi) sambil mengabaikan lapisan lain (tata kelola, SDM, proses, ketergantungan vendor). Padahal, insiden besar hampir selalu bersifat *socio-technical*: terjadi karena kombinasi kelemahan teknologi, kelemahan proses, keterlambatan deteksi, desain organisasi yang terfragmentasi, atau kurangnya kejelasan tanggung jawab.

NIST Cybersecurity Framework (CSF) 2.0 membantu melihat isu ini secara lebih utuh. Framework ini menekankan enam fungsi utama—**Govern, Identify, Protect, Detect, Respond, Recover**—dan secara eksplisit menempatkan **Govern** di pusat sebagai dasar pengambilan keputusan dan prioritisasi risiko. (NIST Publications) Ini penting karena keamanan siber pada infrastruktur digital bukan hanya soal "mencegah serangan", melainkan juga soal bagaimana organisasi menetapkan strategi risiko, peran, otoritas, prioritas layanan kritis, dan mekanisme pemulihan saat gangguan tetap terjadi.

Dalam praktik globalisasi digital, infrastruktur digital telah menjadi infrastruktur kritis baru karena ia menopang infrastruktur kritis lainnya. Sebuah bank dapat memiliki gedung dan kas, tetapi tanpa sistem pembayaran, jaringan komunikasi, dan identitas digital, fungsi ekonominya lumpuh. Sebuah rumah sakit dapat memiliki dokter dan obat, tetapi tanpa sistem informasi, penjadwalan, dan jaringan klaim, kapasitas layanannya menurun drastis. Sebuah negara dapat memiliki lembaga pemerintahan yang lengkap, tetapi layanan publik digital yang tidak resilien dapat menggerus kepercayaan warga saat terjadi gangguan.

Karena itu, diskursus keamanan siber modern bergerak dari *asset protection* ke **operational resilience**—kemampuan mempertahankan layanan esensial meskipun terjadi insiden.

---

3. Mengapa Risiko Siber Menjadi Risiko Sistemik?

Tidak semua insiden siber bersifat sistemik. Banyak insiden bersifat lokal, terbatas pada satu organisasi, dan dapat dikelola dengan cepat. Risiko menjadi sistemik ketika memenuhi beberapa karakteristik berikut:

3.1. Ketergantungan Bersama pada Komponen yang Sama

Banyak organisasi menggunakan perangkat lunak, layanan cloud, atau vendor keamanan yang sama. Ketika satu komponen bersama ini gagal atau disusupi, dampaknya dapat menyebar luas. IMF secara eksplisit mengingatkan tentang risiko dari *common vulnerabilities* dan konsentrasi pada penyedia pihak ketiga. (IMF)

Secara manajerial, ini mirip dengan kegagalan pemasok tunggal dalam rantai pasok manufaktur—tetapi dalam dunia digital, propagasinya jauh lebih cepat dan sering serentak.

3.2. Keterhubungan Layanan yang Tinggi

Sistem digital modern saling terhubung melalui API, integrasi data, dan otomatisasi proses. Kelebihannya adalah efisiensi; kelemahannya adalah *cascade effect*. Gangguan pada identitas, autentikasi, atau jaringan inti dapat memblokir banyak aplikasi sekaligus.

3.3. Sulit Digantikan dalam Waktu Singkat

Risiko sistemik muncul saat komponen yang terganggu tidak mudah diganti (*not easily substitutable*). IMF menekankan bahwa serangan pada institusi kunci, infrastruktur pasar keuangan, atau penyedia cloud kunci dapat dengan cepat mengganggu stabilitas. (IMF)

3.4. Dampak terhadap Kepercayaan

Dalam sistem digital, kepercayaan adalah aset publik. Ketika warga atau pelaku usaha meragukan keamanan sistem pembayaran, identitas digital, atau layanan pemerintah, dampaknya tidak berhenti pada gangguan operasional. Ia meluas menjadi biaya reputasi, biaya kepatuhan, perilaku defensif, dan bahkan perlambatan adopsi digital.

3.5. Asimetri Informasi dan Pelaporan

Sering kali organisasi enggan berbagi detail insiden karena alasan reputasi, legal, atau kompetitif. IMF mencatat hambatan berbagi informasi ini sebagai masalah penting dalam pengelolaan risiko siber

sistemik. (IMF) Akibatnya, pembelajaran lintas sektor terlambat, dan regulator sulit memetakan eksposur sistemik secara real time.

---

4. Lanskap Ancaman Global: Dari Serangan terhadap Ketersediaan hingga Ransomware

Lanskap ancaman global memperkuat argumen bahwa *cybersecurity* kini adalah isu globalisasi baru. ENISA dalam *Threat Landscape 2024* mengidentifikasi tujuh ancaman utama, dengan ancaman terhadap **ketersediaan (availability)** berada di urutan teratas, disusul ransomware dan ancaman terhadap data. ENISA juga menekankan bahwa analisisnya didasarkan pada ribuan insiden yang dilaporkan secara publik. (enisa.europa.eu)

Temuan ini sangat relevan untuk diskusi risiko sistemik. Dalam narasi lama keamanan informasi, banyak organisasi terlalu fokus pada kerahasiaan data (*confidentiality*). Namun dalam ekonomi digital yang real-time, **ketersediaan layanan** sering kali menjadi isu paling kritis. Sistem pembayaran, transportasi, rumah sakit, dan layanan publik bisa menimbulkan dampak sosial-ekonomi besar meski tidak ada kebocoran data masif, jika layanan tidak tersedia selama beberapa jam atau hari.

Di sisi lain, ransomware tetap menjadi ancaman sentral karena model bisnisnya menargetkan kelumpuhan operasional dan pemerasan. Ransomware tidak hanya mengeksploitasi kelemahan teknologi, tetapi juga kelemahan tata kelola: cadangan data yang buruk, segmentasi jaringan lemah, manajemen akses yang longgar, dan prosedur pemulihan yang tidak teruji.

World Economic Forum menyoroti meningkatnya risiko siber yang dirasakan organisasi dan adanya *cyber inequity*, yakni kesenjangan ketahanan antara organisasi besar dan kecil, serta tekanan rantai pasok

yang makin berat. (World Economic Forum Reports) Dalam bahasa globalisasi, ini berarti manfaat digitalisasi tersebar lebih cepat daripada kapasitas perlindungannya. Hasilnya adalah "pasar global yang saling terhubung tetapi tidak simetris dalam kemampuan bertahan."

IMF menambahkan dimensi makro-finansial yang sangat penting: jumlah serangan siber meningkat tajam dibanding periode sebelum pandemi, dan meskipun banyak kerugian langsung berukuran kecil, risiko kerugian ekstrem meningkat. IMF juga mencatat bahwa sektor keuangan sangat terekspos dan bahwa gangguan besar dapat menjalar melalui saluran kepercayaan, infrastruktur pembayaran, dan keterhubungan teknologi. (IMF)

Dari sini terlihat bahwa ancaman siber bukan lagi sekadar isu kriminalitas digital. Ia telah menjadi isu stabilitas sistem.

---

5. Narasi Kasus: Ketika Gangguan Siber Menjadi Efek Domino Global

Agar pembahasan tidak berhenti pada konsep, mari kita lihat beberapa narasi kasus yang menunjukkan bagaimana risiko sistemik bekerja dalam praktik.

5.1. Insiden CrowdStrike–Microsoft 2024: Bukan Serangan, tetapi Dampaknya Sistemik

Salah satu pelajaran paling penting tahun 2024 adalah bahwa **dampak sistemik tidak selalu berasal dari serangan siber jahat**. Dalam insiden CrowdStrike, pembaruan perangkat lunak pihak ketiga memicu gangguan luas pada perangkat Windows. Microsoft memperkirakan sekitar 8,5 juta perangkat terdampak—kurang dari 1% dari seluruh mesin Windows—tetapi dampak ekonomi dan sosialnya meluas karena perangkat-perangkat tersebut berada di organisasi yang menjalankan layanan kritis. Microsoft sendiri menekankan bahwa insiden ini

menunjukkan sifat ekosistem teknologi yang saling terhubung (cloud provider, platform, vendor keamanan, pelanggan enterprise) dan pentingnya *safe deployment* serta *disaster recovery*. (The Official Microsoft Blog)

Reuters melaporkan dampaknya terasa di berbagai sektor, termasuk maskapai, media, dan layanan keuangan, memperlihatkan bagaimana ketergantungan yang tersebar dapat menghasilkan gangguan serentak di banyak negara. (Reuters)

Secara manajerial, kasus ini sangat penting karena mengguncang asumsi bahwa "menambah kontrol keamanan otomatis selalu menurunkan risiko." Dalam sistem yang kompleks, kontrol keamanan yang salah konfigurasi atau pembaruan yang bermasalah dapat menjadi sumber gangguan besar. Ini menegaskan perlunya prinsip **resiliensi operasional**, *change management*, *staged rollout*, *rollback capability*, dan segmentasi dampak.

Kasus ini juga memberi pelajaran bagi regulator: pengawasan risiko sistemik siber harus mencakup **vendor dan rantai pasok digital**, bukan hanya operator layanan akhir.

5.2. Change Healthcare (AS) 2024: Serangan terhadap Rantai Proses, Bukan Hanya Satu Entitas

Kasus lain yang menonjol adalah gangguan pada ekosistem layanan kesehatan yang terkait dengan Change Healthcare (UnitedHealth Group). Situs resmi UHG memuat serangkaian pembaruan pemulihan, sementara Reuters menyoroti luasnya dampak terhadap proses klaim dan operasi sektor kesehatan. (UnitedHealth Group)

Mengapa ini penting untuk topik globalisasi? Karena serangan terhadap satu simpul digital dalam ekosistem kesehatan tidak hanya berdampak pada perusahaan target, tetapi juga pada rumah sakit, klinik, apotek, dokter, dan pasien yang bergantung pada proses transaksi dan verifikasi.

Ini adalah contoh klasik dari **risiko sistemik berbasis fungsi**: yang terganggu bukan sekadar "server perusahaan", melainkan fungsi koordinasi ekonomi di sektor kesehatan.

Pelajaran utamanya adalah bahwa pemetaan aset saja tidak cukup. Organisasi dan regulator perlu memetakan **ketergantungan proses kritis** (*critical business services*) dan *third-party dependencies*. OECD juga menekankan pentingnya fokus pada aktivitas kritis dan pengelolaan risiko pihak ketiga sebagai jalan untuk memperkuat ketahanan organisasi. (IEA)

5.3. Indonesia 2024: Layanan Publik Terganggu dan Pelajaran Tata Kelola

Dalam konteks Indonesia, Reuters melaporkan serangan ransomware terhadap pusat data nasional yang mengganggu layanan publik, termasuk layanan imigrasi, dan memicu audit tata kelola data center. Reuters juga melaporkan angka dampak lintas lembaga yang besar serta persoalan cadangan data yang memperburuk pemulihan. (Reuters)

Kasus seperti ini penting dibaca bukan semata sebagai "serangan terhadap server", melainkan sebagai **uji kelembagaan**. Ketika sistem publik terdigitalisasi tetapi tata kelola backup, standar minimum, dan koordinasi antarlembaga belum matang, gangguan siber cepat berubah menjadi krisis layanan publik. Ini menunjukkan bahwa investasi keamanan siber bukan hanya pembelian alat, tetapi juga disiplin organisasi: klasifikasi layanan kritis, standar pemulihan, latihan insiden, dan audit kepatuhan yang benar-benar operasional.

Bagi negara berkembang, pelajaran terbesar dari kasus semacam ini adalah: **transformasi digital pemerintah harus berjalan seiring dengan transformasi tata kelola risiko digital**. Jika tidak, digitalisasi meningkatkan skala manfaat sekaligus skala kegagalan.

---

6. Cybersecurity, Stabilitas Keuangan, dan Ekonomi Politik Global

Salah satu perkembangan paling penting dalam wacana kebijakan global adalah masuknya *cyber risk* ke ranah **stabilitas keuangan** dan **risiko makro**. IMF secara tegas membahas cyber risk sebagai kekhawatiran yang tumbuh bagi stabilitas makrofinansial, serta menyoroti saluran transmisi seperti hilangnya kepercayaan, gangguan layanan pembayaran, dan keterhubungan teknologi serta finansial. (IMF)

Ini berarti *cybersecurity* kini menyentuh inti ekonomi politik global:

Pasar keuangan bergantung pada transaksi digital dan infrastruktur pembayaran.

Perdagangan global bergantung pada logistik digital, dokumen elektronik, dan platform data.

Investasi bergantung pada kepercayaan terhadap ketahanan operasional.

Negara bergantung pada layanan publik digital untuk legitimasi administratif.

Dalam kerangka ini, insiden siber besar dapat menghasilkan biaya ekonomi melalui beberapa jalur:

biaya langsung (pemulihan, forensik, tebusan, litigasi);

biaya operasional (downtime, tertundanya transaksi, gangguan layanan);

biaya reputasi dan kepercayaan;

biaya regulasi/kepatuhan;

biaya makro jika gangguan meluas ke sektor kritis.

Lebih jauh lagi, globalisasi digital menimbulkan pertanyaan baru tentang **kedaulatan fungsional**. Negara boleh saja memiliki kedaulatan hukum atas wilayahnya, tetapi fungsi digital kritisnya mungkin bergantung pada vendor, standar, atau infrastruktur lintas negara. Karena itu, strategi nasional keamanan siber tidak bisa hanya nasionalistik dan tertutup; ia harus menggabungkan kedaulatan, interoperabilitas, kerja sama internasional, dan manajemen ketergantungan.

EU memberikan contoh menarik melalui NIS2 dan DORA. NIS2 memperluas kerangka hukum keamanan siber ke banyak sektor kritis, menetapkan kewajiban strategi nasional, manajemen risiko, pelaporan insiden, serta menekankan akuntabilitas manajemen puncak. (Digital Strategy EU) DORA, di sektor keuangan, menekankan resiliensi operasional digital, risiko pihak ketiga, pelaporan insiden, pengujian, dan pengawasan penyedia pihak ketiga yang kritis; regulasi ini mulai berlaku pada 17 Januari 2025. (ESMA)

Secara akademik, arah kebijakan tersebut menunjukkan pergeseran paradigma: dari *compliance-based security* menuju **systemic resilience governance**.

---

7. Ketimpangan Siber Global dan Tantangan Negara Berkembang

Salah satu aspek yang sering kurang dibahas adalah bahwa globalisasi digital bukan hanya menciptakan konektivitas, tetapi juga **ketimpangan eksposur dan kapasitas**. Negara berkembang sering menghadapi kombinasi tantangan berikut:

Adopsi digital cepat, tetapi kapasitas kelembagaan tertinggal.

Ketergantungan pada vendor/produk global, tetapi negosiasi kontrak dan pengawasan terbatas.

Keterbatasan SDM siber, terutama di sektor publik dan daerah.

Fragmentasi anggaran dan standar, sehingga keamanan menjadi tambahan opsional, bukan prasyarat desain.

Tekanan politik untuk layanan cepat, yang kadang mengorbankan arsitektur resiliensi.

World Bank mencatat dukungan program keamanan siber di 64 ekonomi, yang menunjukkan bahwa isu ini sudah dipandang sebagai bagian dari agenda pembangunan, bukan semata agenda keamanan. Namun World Bank juga menyoroti kesenjangan kapasitas—termasuk rendahnya kesiapan operasional tim tanggap insiden di banyak negara berpendapatan rendah. (UnitedHealth Group)

Di tingkat global, ITU melalui *Global Cybersecurity Index* juga menempatkan isu ini dalam kerangka benchmarking komitmen nasional terhadap keamanan siber di 194 negara anggota. Ini penting karena menunjukkan bahwa *cybersecurity* sudah menjadi indikator kapasitas negara modern—mirip dengan indikator kualitas regulasi, kemudahan berbisnis, atau kesiapan logistik.

Bagi negara berkembang, persoalan utamanya bukan sekadar "mengejar teknologi terbaru", tetapi membangun **kapasitas institusional minimum** yang konsisten:

standar nasional untuk layanan kritis,

kerangka pelaporan insiden,

audit dan backup yang wajib,

latihan simulasi,

koordinasi regulator sektor,

dan pengembangan talenta siber.

Tanpa itu, digitalisasi dapat menghasilkan paradoks: layanan terlihat modern di permukaan, tetapi rapuh di lapisan inti.

---

8. Dari Keamanan Teknis ke Tata Kelola Resiliensi: Agenda Strategis

Jika *cybersecurity* adalah isu globalisasi baru, maka responsnya juga harus melampaui pendekatan teknis semata. Berikut adalah kerangka strategis yang relevan, terutama untuk negara berkembang dan organisasi publik-besar.

8.1. Menjadikan Cybersecurity sebagai Agenda Manajemen Puncak

NIST CSF 2.0 menempatkan fungsi **Govern** sebagai pusat, dan NIS2 juga menegaskan akuntabilitas manajemen puncak. (NIST Publications) Ini berarti dewan, pimpinan kementerian/lembaga, direksi BUMN, dan manajemen puncak perusahaan harus memandang keamanan siber sebagai isu pencapaian misi, bukan isu teknisi belaka.

Pertanyaan strategis yang harus dijawab pimpinan bukan hanya:

"Apakah kita punya firewall?"
tetapi:

"Layanan apa yang paling kritis bagi publik/pelanggan?"

"Berapa lama maksimum layanan boleh berhenti?"

"Apa ketergantungan pihak ketiga yang paling rentan?"

"Apakah kita pernah menguji pemulihan nyata?"

8.2. Fokus pada Layanan Kritis, Bukan Semua Sistem Sekaligus

Pendekatan yang efektif adalah memetakan **critical services** dan ketergantungan prosesnya. OECD menekankan penguatan ketahanan melalui fokus pada aktivitas kritis dan pengelolaan risiko pihak ketiga.

(IEA) Ini lebih realistis daripada mengejar kesempurnaan keamanan di semua aset secara seragam.

Dalam narasi manajemen, ini serupa dengan prinsip Pareto dalam operasi: lindungi dan resilienkan simpul yang efek dominonya paling besar.

8.3. Mengelola Risiko Pihak Ketiga dan Konsentrasi

Banyak insiden besar menunjukkan bahwa risiko terbesar justru berada di luar perimeter organisasi. IMF, DORA, dan OECD sama-sama menekankan pentingnya pengawasan pihak ketiga dan konsentrasi layanan digital. (IMF)

Agenda praktisnya meliputi:

inventaris vendor kritis,

klausul kontrak untuk insiden/pemulihan,

hak audit,

persyaratan pelaporan,

uji kontinuitas bersama,

dan strategi *exit/substitution* untuk fungsi yang sangat vital.

8.4. Membangun Kapasitas Deteksi dan Respons Kolektif

Karena sifat ancaman yang lintas sektor, respons individual tidak cukup. NIS2 menekankan kerja sama lintas negara, jaringan CSIRT, dan mekanisme koordinasi krisis. (Digital Strategy EU) Ini memberi pelajaran bahwa negara perlu membangun ekosistem respons: CERT/CSIRT nasional, CSIRT sektoral, protokol eskalasi, dan latihan gabungan.

8.5. Menyatukan Keamanan Siber dengan Transformasi Digital

Kesalahan paling mahal adalah memperlakukan keamanan sebagai "tambahan" setelah sistem selesai dibangun. Keamanan dan resiliensi

harus menjadi bagian dari desain transformasi digital: arsitektur data, segmentasi layanan, backup, observabilitas, dan *business continuity*.

Dalam bahasa manajemen perubahan, ini berarti *cybersecurity by design* dan *resilience by design*.

---

9. Implikasi bagi Indonesia dan Negara Berkembang: Sebuah Refleksi Kebijakan

Bagi Indonesia dan banyak negara berkembang, tema utama bukan apakah akan melakukan digitalisasi—karena itu sudah menjadi keniscayaan—melainkan **bagaimana melakukan digitalisasi yang aman, tangguh, dan dapat dipercaya**.

Ada beberapa refleksi strategis yang layak digarisbawahi.

9.1. Infrastruktur Digital adalah Infrastruktur Pembangunan

Selama ini, pembangunan sering diukur lewat jalan, pelabuhan, listrik, dan irigasi. Di era ekonomi digital, pusat data, interoperabilitas layanan, keamanan identitas digital, dan ketahanan sistem pembayaran juga harus diperlakukan sebagai infrastruktur pembangunan. Gangguan pada infrastruktur digital dapat menghambat perdagangan, mobilitas, investasi, dan layanan sosial sama nyata dengan kerusakan jalan atau listrik.

9.2. Ketahanan Siber adalah Bagian dari Daya Saing

Dalam globalisasi baru, investor dan mitra bisnis menilai bukan hanya biaya tenaga kerja atau insentif fiskal, tetapi juga reliabilitas operasional digital. Negara atau perusahaan yang sering mengalami gangguan sistemik akan menanggung *risk premium* yang lebih tinggi—baik secara finansial maupun reputasional.

9.3. Tata Kelola Lebih Penting daripada Sekadar Belanja Teknologi

Banyak organisasi membeli alat keamanan, tetapi tidak memiliki inventaris aset yang akurat, prosedur backup yang teruji, atau kejelasan otoritas saat insiden. Pengalaman berbagai negara menunjukkan bahwa kelemahan tata kelola dapat membatalkan manfaat teknologi canggih. IMF juga menyoroti peran pengaturan tata kelola dan pengawasan dalam memperkuat kesiapan. (IMF)

9.4. Perlu Pendekatan Berlapis: Nasional, Sektoral, Organisasi

Risiko sistemik tidak dapat diatasi pada satu level saja. Diperlukan:

Level nasional: strategi, standar minimum, koordinasi krisis, kerangka pelaporan.

Level sektoral: regulasi spesifik layanan kritis (keuangan, energi, kesehatan, transportasi, pemerintahan).

Level organisasi: implementasi kontrol, latihan, pemulihan, dan budaya keamanan.

Pendekatan seperti NIS2 dan DORA memberi contoh bagaimana level-level ini dapat dihubungkan melalui kewajiban tata kelola, pelaporan, pengujian, dan kerja sama. (Digital Strategy EU)

---

10. Penutup: Cybersecurity sebagai Bahasa Baru Kepercayaan dalam Globalisasi

Cybersecurity kini dapat dipahami sebagai **bahasa baru kepercayaan** dalam globalisasi. Jika pada masa lalu kepercayaan global dibangun melalui aturan perdagangan, standar kualitas, dan stabilitas moneter, maka kini ia juga ditentukan oleh ketahanan infrastruktur digital yang menopang aktivitas ekonomi dan sosial.

Esai ini menegaskan bahwa *cybersecurity* telah bertransformasi dari isu teknis menjadi isu strategis global karena tiga alasan utama: (1) digitalisasi telah menjadikan infrastruktur digital sebagai fondasi banyak sektor kritis; (2) interkoneksi global menciptakan risiko sistemik melalui ketergantungan bersama dan konsentrasi pihak ketiga; dan (3) ketimpangan kapasitas siber membuat manfaat globalisasi digital tidak diimbangi oleh ketahanan yang merata. Temuan-temuan dari ENISA, IMF, WEF, ITU, OECD, World Bank, serta perkembangan regulasi seperti NIS2 dan DORA memperlihatkan arah yang sama: dunia sedang bergerak menuju paradigma **resiliensi digital sistemik**. (enisa.europa.eu)

Dalam kerangka akademik manajemen dan kebijakan publik, pelajaran paling penting adalah bahwa keamanan siber tidak boleh lagi diletakkan di pinggir organisasi. Ia harus berada di jantung strategi: terkait desain layanan, struktur tanggung jawab, hubungan dengan vendor, budaya organisasi, dan tata kelola risiko lintas sektor. Insiden seperti CrowdStrike dan gangguan layanan publik di berbagai negara menunjukkan bahwa di era globalisasi digital, yang diuji bukan hanya kemampuan mencegah serangan, tetapi kemampuan sistem untuk tetap berfungsi, pulih, dan menjaga kepercayaan publik ketika gangguan tak terhindarkan terjadi. (The Official Microsoft Blog)

Dengan demikian, agenda ke depan—khususnya bagi negara berkembang—bukan sekadar "go digital", melainkan **go digital with resilience**. Negara, perusahaan, dan institusi pendidikan perlu membangun generasi baru kepemimpinan yang memahami bahwa keamanan siber adalah bagian dari manajemen strategis, ekonomi politik, dan ketahanan nasional. Hanya dengan cara itu, globalisasi digital dapat menjadi sarana kemajuan yang inklusif, bukan sumber kerentanan baru yang terus berulang.

Glosarium

1) Attack Surface (Permukaan Serangan)
Keseluruhan titik masuk potensial yang dapat dieksploitasi penyerang, mencakup perangkat, aplikasi, akun, API, jaringan, dan pihak ketiga.

2) Availability (Ketersediaan)
Prinsip bahwa sistem, layanan, dan data tetap dapat diakses saat dibutuhkan oleh pengguna yang berwenang.

3) Backup (Cadangan Data)
Salinan data yang disimpan terpisah untuk pemulihan ketika terjadi gangguan, korupsi data, atau serangan siber (misalnya ransomware).

4) Botnet
Jaringan perangkat yang telah terinfeksi malware dan dikendalikan penyerang untuk melakukan serangan terkoordinasi, seperti DDoS.

5) Business Continuity (Keberlangsungan Bisnis)
Kemampuan organisasi menjaga operasi minimum kritikal selama dan setelah gangguan.

6) CIA Triad (Confidentiality–Integrity–Availability)
Tiga pilar dasar keamanan informasi: kerahasiaan, integritas, dan ketersediaan.

7) CIRT / CSIRT (Computer Security Incident Response Team)
Tim yang bertugas mendeteksi, menangani, mengoordinasikan respons, dan memulihkan insiden keamanan siber.

8) Critical Infrastructure (Infrastruktur Kritis)
Sektor/layanan yang vital bagi masyarakat dan ekonomi (misalnya energi, kesehatan, transportasi, keuangan, telekomunikasi, air, dan layanan publik).

9) Cyber Hygiene (Higiene Siber)
Praktik dasar keamanan digital yang rutin, seperti update sistem, MFA, backup, manajemen kata sandi, dan kewaspadaan phishing.

10) Cyber Resilience (Ketahanan Siber)
Kemampuan untuk **mencegah, mendeteksi, merespons, dan pulih** dari insiden siber sambil menjaga fungsi penting tetap berjalan.

11) Cyber Risk (Risiko Siber)
Potensi kerugian akibat insiden digital yang mengganggu kerahasiaan, integritas, ketersediaan, operasi, reputasi, atau kepatuhan hukum.

12) Data Breach (Kebocoran Data)
Akses, pengungkapan, atau eksfiltrasi data tanpa otorisasi.

13) Digital Sovereignty (Kedaulatan Digital)
Kemampuan negara/organisasi mengendalikan kebijakan, data, infrastruktur, dan standar digital yang strategis.

14) DDoS (Distributed Denial of Service)
Serangan yang membanjiri layanan dengan trafik dari banyak sumber sehingga layanan menjadi lambat atau tidak tersedia.

15) Defense in Depth (Pertahanan Berlapis)
Pendekatan keamanan dengan banyak lapisan kontrol (teknis, prosedural, manusia, dan tata kelola) agar kegagalan satu lapisan tidak langsung melumpuhkan sistem.

16) Endpoint
Perangkat pengguna atau sistem tepi jaringan yang terhubung ke jaringan (laptop, server, smartphone, workstation, IoT).

17) Exploit
Kode/teknik yang memanfaatkan kerentanan untuk memperoleh akses atau mengeksekusi tindakan tidak sah.

18) Exfiltration (Eksfiltrasi Data)
Pemindahan data keluar dari sistem target secara tidak sah.

19) Governance (Tata Kelola Keamanan Siber)
Pengaturan peran, tanggung jawab, kebijakan, pengawasan, dan akuntabilitas untuk pengelolaan risiko siber di tingkat organisasi.

20) Incident Response (Respons Insiden)
Rangkaian kegiatan terstruktur untuk identifikasi, isolasi, penanganan, eradikasi, komunikasi, dan pemulihan insiden.

21) Integrity (Integritas Data/Sistem)
Jaminan bahwa data dan sistem tetap akurat, utuh, dan tidak dimodifikasi tanpa izin.

22) IoT (Internet of Things)
Perangkat fisik yang terhubung ke internet dan saling bertukar data (sensor, smart meter, kamera, perangkat industri, dsb.).

23) Legacy System (Sistem Lama/Warisan)
Sistem yang masih digunakan tetapi sudah tua, sulit diperbarui, atau tidak lagi didukung optimal sehingga rentan secara keamanan.

24) Malware
Perangkat lunak berbahaya yang dirancang untuk merusak, mencuri data, menyusup, atau mengganggu sistem.

25) MFA (Multi-Factor Authentication)
Metode autentikasi yang memerlukan lebih dari satu faktor (misalnya kata sandi + OTP/biometrik).

26) OT (Operational Technology)
Sistem dan perangkat yang mengendalikan proses fisik/industri (SCADA, PLC, sistem utilitas, manufaktur, energi).

27) Patch Management
Proses mengidentifikasi, menguji, dan menerapkan pembaruan keamanan/perbaikan perangkat lunak secara terkontrol.

28) Phishing
Teknik rekayasa sosial untuk menipu korban agar menyerahkan kredensial, data sensitif, atau menjalankan file berbahaya.

29) Ransomware
Jenis malware yang mengenkripsi data/sistem dan menuntut tebusan untuk pemulihan; kini sering disertai ancaman publikasi data (double extortion). ENISA menempatkan ransomware sebagai salah satu ancaman utama dalam lanskap ancaman 2024. (ENISA)

30) Recovery Time Objective (RTO)
Target waktu maksimum yang dapat diterima untuk memulihkan layanan setelah gangguan.

31) Recovery Point Objective (RPO)
Target jumlah kehilangan data maksimum yang dapat diterima (diukur sebagai jarak waktu dari backup terakhir).

32) Risk Appetite (Selera Risiko)
Tingkat risiko yang bersedia diterima organisasi untuk mencapai tujuannya.

33) Supply Chain Risk (Risiko Rantai Pasok Digital)
Risiko yang muncul dari ketergantungan pada vendor, penyedia cloud, software library, integrator, atau mitra operasional.

34) Systemic Risk (Risiko Sistemik)
Risiko ketika gangguan pada satu entitas/sistem menyebar ke banyak sektor atau wilayah karena interdependensi digital dan ekonomi.

35) Third-Party Risk (Risiko Pihak Ketiga)
Risiko operasional dan keamanan yang bersumber dari vendor/penyedia layanan eksternal.

36) Threat Actor (Aktor Ancaman)
Pihak yang melakukan aktivitas berbahaya, seperti kelompok kriminal, aktor negara, hacktivist, insider, atau pelaku oportunistik.

37) Threat Intelligence
Informasi yang dapat ditindaklanjuti mengenai ancaman, teknik serangan, indikator kompromi, dan perilaku aktor.

38) Vulnerability (Kerentanan)
Kelemahan pada sistem, konfigurasi, proses, atau manusia yang dapat dieksploitasi.

39) Zero-Day
Kerentanan yang belum diketahui atau belum tersedia patch saat mulai dieksploitasi.

40) Zero Trust
Prinsip keamanan "never trust, always verify" — setiap akses harus diverifikasi secara berkelanjutan berdasarkan identitas, konteks, dan kebijakan.

Referensi

A. Referensi Inti (Kerangka, Laporan, dan Regulasi)

NIST (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29).
Relevan untuk kerangka tata kelola dan manajemen risiko siber lintas sektor. CSF 2.0 menegaskan enam fungsi inti (Govern, Identify, Protect, Detect, Respond, Recover) serta penekanan lebih kuat pada governance dan supply chain. (NIST Publications)

International Monetary Fund / IMF (2024). *Global Financial Stability Report (April 2024), Chapter 3: Cyber Risk: A Growing Concern for Macrofinancial Stability.*
Sangat penting untuk memahami hubungan antara risiko siber dan stabilitas makro-keuangan, termasuk paparan tinggi sektor keuangan dan potensi kerugian ekstrem. (IMF)

ENISA (European Union Agency for Cybersecurity) (2024). *ENISA Threat Landscape 2024.*
Rujukan utama untuk tren ancaman, kategori aktor ancaman, dan pola serangan pada periode 2023–2024. Halaman ENISA menegaskan ETL sebagai laporan tahunan dan menyoroti delapan tipe ancaman utama. (ENISA)

World Economic Forum (2025). *Global Cybersecurity Outlook 2025* (with Accenture).
Berguna untuk perspektif globalisasi, interdependensi rantai pasok, ketegangan geopolitik, dan kompleksitas lanskap keamanan siber global. (World Economic Forum)

ITU (International Telecommunication Union) (2024). *Global Cybersecurity Index (GCI), 5th Edition.*
Relevan untuk pemetaan kapasitas/komitmen negara melalui lima pilar: legal, technical, organizational, capacity development, dan cooperation. (ITU)

OECD (2022/halaman topik diperbarui). *Digital Security Risk Management* dan *Recommendation on the Digital Security of Critical Activities.*
Penting untuk tata kelola risiko digital pada aktivitas kritikal, kemitraan berbasis kepercayaan, dan kerja sama lintas negara. (OECD)

European Commission (NIS2) (halaman kebijakan & implementasi, 2024). *NIS2 Directive: securing network and information systems*; serta halaman implementasi terkait.
Menjadi rujukan penting untuk kerangka hukum siber UE, termasuk cakupan sektor kritikal dan tenggat implementasi nasional. (Digital Strategy EU)

ESMA (2023/2025 applicability). *Digital Operational Resilience Act (DORA).*
Rujukan penting untuk ketahanan operasional digital sektor keuangan UE; ESMA menegaskan DORA berlaku mulai 17 Januari 2025. (ESMA)

World Bank (2025). *Enhancing Cyber Resilience in Developing Countries.*
Berguna untuk konteks negara berkembang; World Bank melaporkan dukungan pembangunan ketahanan siber di 64 negara (2014–2024), terutama melalui penguatan CSIRT. (World Bank)

IEA (International Energy Agency) (halaman topik digitalisation). *Digitalisation – Energy System.*
Relevan untuk menunjukkan bahwa digitalisasi sektor energi meningkatkan efisiensi dan resiliensi, namun sekaligus memperluas area risiko yang memerlukan pengamanan siber. (IEA)

B. Referensi Kasus dan Ilustrasi Empiris (Gangguan/Insiden)

Microsoft (2024). *Helping our customers through the CrowdStrike outage* (Official Microsoft Blog, 20 Juli 2024).

Referensi primer untuk estimasi dampak sekitar **8,5 juta perangkat Windows** dan narasi interdependensi ekosistem digital. (The Official Microsoft Blog)

Reuters (2024, 20 Juli). *Microsoft says about 8.5 million of its devices affected by CrowdStrike-related outage.*
Bermanfaat sebagai sumber berita internasional yang merangkum dampak lintas sektor (penerbangan, kesehatan, perbankan, media). (Reuters)

Reuters (2024, 19 Juli). *Explainer: What caused the global cyber outage?*
Memberi konteks cepat tentang skala gangguan global dan sektor-sektor yang terdampak. (Reuters)

Reuters (2024, 24 Juni). *Cyber attack compromised Indonesia data centre, ransom sought.*
Referensi penting untuk konteks Indonesia: gangguan pusat data nasional, dampak pada layanan imigrasi, dan tuntutan tebusan. (Reuters)

Reuters (2024, 26 Juni). *More than 40 Indonesian agencies hit by cyberattack on data centres.*
Menjelaskan dampak awal lintas instansi pemerintah serta gangguan layanan publik. (Reuters)

Reuters (2024, 28 Juni). *Indonesia president orders audit of data centres after cyberattack.*
Relevan untuk aspek tata kelola, backup, dan akuntabilitas kelembagaan pasca-insiden. (Reuters)

UnitedHealth Group (2024, 22 April). *UnitedHealth Group Updates on Change Healthcare Cyberattack.*
Referensi primer untuk contoh gangguan rantai proses kesehatan digital, pemulihan layanan, dan isu data sensitif (PHI/PII). (UnitedHealth Group)

C. Referensi Tambahan yang Dapat Memperkaya Makalah (Opsional)

CISA (U.S. Cybersecurity and Infrastructure Security Agency). Dokumentasi sektor infrastruktur kritis dan advisori insiden. Berguna untuk klasifikasi sektor kritis dan praktik koordinasi lintas lembaga. (CISA)

Basel Committee / liputan Reuters (2024). Pembahasan penguatan prinsip risiko pihak ketiga/outsourcing pada sektor perbankan. Relevan untuk dimensi risiko sistemik berbasis ketergantungan vendor/cloud. (Reuters)

Copilot for this article - Chatgpt 5.2 Thinking. Access date: 25 Februari 2026. Prompting on Writer's account (Rudy C Tarumingkeng)

https://chatgpt.com/c/699ee470-4ef8-839d-a0e1-ec281c28c40d