FSI OPINION
Forumsinologi.id 18 Agustus 2026

Strategi Siber China Kini Ditenagai AI, Asia Tenggara Patut Waspada

Gatra Priyandita

China telah lama menjadi salah satu kekuatan siber ofensif paling mumpuni di dunia. Yang berubah bukanlah skala operasinya, melainkan tujuannya. Kecerdasan buatan, yang dalam bahasa Inggris dikenal sebagai *artificial intelligence* (AI), tengah menggeser aktivitas siber China dari sekadar pengumpulan intelijen menuju pra-pemosisian dan manipulasi yang gigih atas sistem-sistem yang menjadi sandaran negara modern. Asia Tenggara–termasuk juga Indonesia–merupakan salah satu kawasan paling rentan di dunia. Meningkatnya ketergantungan negara-negara kawasan itu pada infrastruktur digital, sebagian besar dipasok China, mempertajam kerentanan itu. Ini bukan persoalan satu dasawarsa ke depan. Ini adalah persoalan masa kini.

Garis besar postur siber China kini mudah dilacak dan ditelaah. Electronic Transactions Development Agency Thailand mencatat sekitar 177 kelompok ancaman tingkat lanjut yang mengakar (*advanced persistent threat*/APT) yang diduga terkait dengan China,[1] sebagian besar terhubung dalam berbagai tingkatan dengan Kementerian Keamanan Negara (MSS) atau Tentara Pembebasan Rakyat (PLA). Selama bertahun-tahun, kerja mereka berfokus pada perolehan keunggulan strategis di ranah informasi,[2] mencuri kekayaan intelektual,[3] memetakan jaringan pemerintah, mengawasi pihak-pihak yang menjadi sasaran. Belakangan, penekanannya bergeser dari pencurian ke pemosisian.

Operasi yang diasosiasikan dengan Volt Typhoon dan Salt Typhoon–kelompok ancaman siber canggih yang terkait dengan China–menyasar infrastruktur telekomunikasi, energi, air, dan transportasi melalui ancaman yang terus-menerus, yaitu secara diam-diam membangun dan mempertahankan akses untuk diaktifkan pada momen strategis tertentu. Doktrin PLA telah lama memperlakukan dominasi informasi sebagai syarat penentu perang modern; *Science of Military*

Strategy edisi 2020 menggambarkan ruang siber sebagai platform dasar untuk melumpuhkan jaringan komando lawan sebelum operasi kinetik dimulai. Dokumen yang bocor pada Februari 2026–yang menggambarkan sebuah *cyber range* milik perusahaan berafiliasi negara China yang dibangun untuk melatih operasi terhadap replika infrastruktur kritis asing–menunjukkan seberapa jauh logika itu telah berkembang.

AI-lah yang membuat ambisi China kini dapat dicapai. AI tidak sekadar mempercepat operasi yang sudah ada; ia mengubah apa yang bisa dilakukan operasi tersebut. Pada November 2025, Anthropic, sebuah perusahan AI yang berpusat di San Fransisco, Amerika Serikat, mengungkap bahwa sebuah kelompok yang disponsori negara China telah memanipulasi perangkat Claude Code, alat coding milik perusahaan tersebut untuk menjalankan kampanye spionase terhadap sekitar tiga puluh target global di sektor teknologi, keuangan, manufaktur kimia, dan pemerintahan, dengan AI menjalankan sekitar 80 hingga 90 persen operasi taktis, sebagian besar secara mandiri.[4] Sebagian besar upaya berhasil dideteksi dan digagalkan, dan hanya segelintir yang berhasil. Akan tetapi, kejadian di atas telah menandakan sebuah niat. AI diperlakukan bukan sebagai perangkat tersendiri untuk satu tugas, melainkan sebagai infrastruktur operasional yang berkesinambungan: terus beradaptasi, memperpendek siklus pengambilan keputusan, dan membuat lingkungan target yang kompleks menjadi terbaca pada skala yang tak mungkin ditandingi tim manusia mana pun. Rencana Lima Tahun ke-15 China, yang mencakup tahun 2026 hingga 2030, memprioritaskan infrastruktur pendukung AI, komputasi kuantum, dan sistem intensif data. Prioritas industri pada setiap rencana sebelumnya secara konsisten memprediksi ke mana spionase siber China akan terkonsentrasi. Jika polanya bertahan, integrasi AI ke dalam operasi ofensif bukanlah improvisasi, melainkan strategi.

Asia Tenggara berada tepat di jalur pergeseran ini. Kawasan ini telah mengalami satu dasawarsa transformasi digital yang sangat cepat, dengan ekonomi internet yang diperkirakan mendekati satu triliun dolar pada 2030, ekosistem *start-up* teknologi yang dinamis, dan sektor AI yang tumbuh pesat. Kondisi dinamis itu sekaligus merupakan kerentanan. Setiap platform, pusat data, dan layanan terhubung yang baru memperluas permukaan serangan, meningkatkan potensi keterpaparan bagi perusahaan, lembaga riset, dan universitas. Biaya akibat *ransomware*–yaitu serangan siber yang mengunci atau mengenkripsi data korban lalu menuntut pembayaran tebusan–dan penipuan daring telah melonjak tajam. Oleh karena spionase China mengikuti ambisi industri pemerintah China sendiri, sektor-sektor yang paling ingin dikembangkan oleh pemerintah Asia Tenggara–manufaktur tingkat lanjut, telekomunikasi, dan AI–justru berpotensi menjadi sasaran pencurian gagasan dan kekayaan intelektual yang bernilai. Bagi Indonesia, dengan digitalisasi yang cepat namun memiliki kematangan siber yang masih timpang, keterpaparan itu terasa akut.

Pelajaran yang lebih berat ada pada isu ketergantungan. Bahayanya bukan lagi sekadar ditembusnya sebuah sistem, melainkan kemungkinan pembentukan secara diam-diam oleh pihak luar. Sistem yang ditenagai AI–termasuk sistem militer–bergantung pada alur data, jaringan sensor,

dan sambungan komunikasi untuk menghasilkan luaran yang menjadi dasar pengambilan keputusan. Lawan yang telah memetakan ketergantungan itu, mempertahankan akses, dan melatih intervensinya tidak perlu sama sekali membobol algoritmanya. Cukup dengan memengaruhi inputnya; sistem tetap bekerja, tetapi perilakunya tidak lagi sesuai dengan kenyataan. Di sinilah ketergantungan Asia Tenggara pada teknologi pasokan China menjadi tidak nyaman secara strategis. Perangkat telekomunikasi, sistem kota pintar dan pengawasan, layanan komputasi awan, kabel bawah laut, dan pusat data yang bersumber dari vendor China bukan sekadar pilihan komersial–semuanya adalah pijakan potensial–dan ketergantungan itu sendiri merupakan permukaan serangan.

Semua ini bukan alasan untuk paranoia, tetapi menuntut perubahan postur. Rezim sertifikasi yang menguji sistem dalam kondisi normal tidak menjelaskan bagaimana sistem akan bekerja ketika menghadapi lawan yang telah lama mempersiapkan medan. Pemerintah di kawasan ini, termasuk Jakarta, harus mendiversifikasi dan menyaring pemasok teknologinya, membangun ketahanan dan jalur alternatif jika sistem utama terganggu pada alur data yang kritis, serta berinvestasi secara serius dalam mendeteksi pra-pemosisian alih-alih menunggu disrupsi. Pertarungan yang akan datang akan ditentukan bukan oleh siapa yang memiliki algoritma lebih baik, melainkan oleh siapa yang lebih lama bersiap dan oleh siapa yang paling keras berpikir tentang kerentanannya sendiri.

Dr. Gatra Priyandita *adalah analis senior di Australian Strategic Policy Institute (ASPI), Canberra, Australia..*

Referensi:

[1] Electronic Transactions Development Agency, “Threat Group Cards: A Threat Actor Encyclopedia,” https://apt.etda.or.th/cgi-bin/aptstats.cgi (diakses 15 Juli 2026).

[2] International Institute for Strategic Studies, “Cyber Capabilities and National Power: A Net Assessment,” 28 Juni 2021, https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/ (diakses 15 Juli 2026).

[3] Australian Strategic Policy Institute, “State-sponsored economic cyber-espionage for commercial purposes: Assessing the preparedness of emerging economies to defend against cyber-enabled IP theft,” 19 Februari 2025, https://www.aspi.org.au/report/state-sponsored-economic-cyber-espionage-commercial-purposes-assessing-preparedness-emerging/ (diakses 15 Juli 2026).

[4] Anthropic, “Disrupting the first reported AI-orchestrated cyber espionage campaign,” November 2025, https://www-cdn.anthropic.com/d7dd50dd1185f59be051b307150d877f2b82bd2c.pdf (diakses 15 Juli 2026).