

BAGAIMANA NEGARA MENGGUNAKAN AI UNTUK KEPENTINGAN POLITIK, EKONOMI, DAN MILITER

Oleh

Prof Ir Rudy C Tarumingkeng, PhD

www.rudict.com/cv.pdf

Institut Bisnis dan Multimedia (IBM ASMI)

RudyCT Academic Series 2026

SCIENTIFIC ARTICLE

How States Use AI for Political, Economic, and Military Interests



“Artificial intelligence has become a strategic instrument of the modern state—shaping governance, competitiveness, and national security.”

1



Political Governance

Public services, policy analysis, information management.

2



Economic Competitiveness

Innovation, productivity, industrial strategy, digital economy.

3



National Security & Defense

Intelligence, cyber defense, logistics, strategic readiness.

4



Data, Compute & Infrastructure

Data governance, cloud, semiconductors, digital infrastructure.

5



Ethics & Responsible AI

Accountability, human oversight, privacy, legitimacy.



By: Prof Ir Rudy C Tarumingkeng, PhD



www.rudycr.com/cv.pdf



IBM-ASMI (Institut Bisnis dan Multimedia)

Scholar in Technology, Business, and Digital Transformation

Abstrak

Kecerdasan artifisial (Artificial Intelligence/AI) berkembang dari teknologi komputasional menjadi instrumen strategis negara. Pemerintah menggunakan AI untuk meningkatkan kapasitas administratif, menganalisis kebijakan, mengelola pelayanan publik, memperkuat keamanan, membentuk industri masa depan, mengembangkan ilmu pengetahuan, serta menopang kemampuan pertahanan. Pada saat yang sama, AI juga memperbesar kapasitas negara untuk melakukan pengawasan, memengaruhi arus informasi, mengotomatisasi pengambilan keputusan, memperkuat kompetisi industri, dan mempercepat modernisasi militer. Artikel ini membahas secara naratif dan komprehensif bagaimana negara menggunakan AI untuk kepentingan politik, ekonomi, dan militer, dengan menempatkan teknologi tersebut dalam kerangka state capacity, geopolitik, industrial policy, information power, national security, dan responsible AI. Pembahasan mencakup penggunaan AI dalam administrasi dan pelayanan publik; pemilu, komunikasi politik, diplomasi, disinformasi, dan pengawasan; produktivitas, industri strategis, semikonduktor, data, riset, tenaga kerja, dan kedaulatan teknologi; serta intelijen, komando dan kendali, logistik, pertahanan siber, sistem otonom, simulasi, dan dukungan pengambilan keputusan militer. Studi perbandingan mengenai Amerika Serikat, Tiongkok, NATO/Uni Eropa, dan konteks Indonesia menunjukkan bahwa keunggulan AI nasional tidak ditentukan hanya oleh model algoritmik, melainkan oleh ekosistem yang mencakup data, komputasi, semikonduktor, talenta, penelitian, perusahaan teknologi, infrastruktur, regulasi, institusi, dan legitimasi publik. Artikel menegaskan bahwa AI merupakan teknologi dual-use yang dapat memperkuat kesejahteraan dan keamanan sekaligus meningkatkan risiko konsentrasi kekuasaan, bias, manipulasi, eskalasi strategis, dan pelanggaran hak. Karena itu, pemanfaatan AI oleh negara memerlukan governance yang demokratis, human oversight, akuntabilitas, pengujian, perlindungan data, kepatuhan pada hukum nasional dan internasional, serta strategi pembangunan kapabilitas yang konsisten dengan kepentingan publik.

Kata Kunci

Artificial Intelligence; AI negara; state capacity; politik digital; ekonomi digital; industrial policy; geopolitik teknologi; national security; military AI; responsible AI; surveillance; disinformation; data governance; kedaulatan teknologi; Indonesia.

Pendahuluan

Kecerdasan artifisial tidak lagi hanya menjadi perangkat yang digunakan perusahaan untuk mengoptimalkan proses bisnis atau konsumen untuk mencari informasi. Dalam satu dekade terakhir, AI semakin menjadi bagian dari arsitektur kekuasaan negara. Pemerintah menggunakannya untuk memahami populasi, mengelola sumber daya, memprediksi risiko, menyediakan layanan, mendeteksi anomali, mengatur lalu lintas informasi, menilai kondisi ekonomi, dan mempercepat penelitian. Kementerian pertahanan dan angkatan bersenjata mengembangkan AI untuk analisis data, penginderaan, logistik, simulasi, komando dan kendali, keamanan siber, serta sistem otonom. Akibatnya, AI kini berada pada persimpangan antara administrasi publik, kompetisi ekonomi, geopolitik, dan keamanan nasional.

Perubahan tersebut membuat AI berbeda dari banyak gelombang teknologi sebelumnya. Mesin uap, listrik, telekomunikasi, komputer, dan internet juga memiliki dampak strategis, tetapi AI memiliki sifat khusus karena beroperasi langsung pada informasi, klasifikasi, prediksi, bahasa, persepsi, dan keputusan. Negara modern pada dasarnya adalah organisasi informasi: ia mengumpulkan data, menyusun kategori,

menetapkan prioritas, menyalurkan anggaran, memantau kepatuhan, dan membuat keputusan bagi populasi yang sangat besar. Ketika kemampuan untuk memproses informasi meningkat, kapasitas negara juga dapat meningkat. Namun kemampuan yang sama dapat digunakan untuk kontrol yang berlebihan atau intervensi yang sulit diawasi.

Karena itu pertanyaan utama bukan apakah negara akan menggunakan AI, melainkan untuk tujuan apa, dengan institusi apa, berdasarkan data apa, di bawah aturan apa, dan dengan mekanisme koreksi seperti apa. Negara demokratis, negara otoritarian, negara maju, dan negara berkembang dapat menggunakan teknologi yang sama tetapi menghasilkan konfigurasi kekuasaan yang berbeda. Perbedaan tersebut berasal dari sistem politik, institusi hukum, kapasitas birokrasi, struktur ekonomi, ekosistem teknologi, tingkat ancaman, dan norma sosial. Dengan demikian AI harus dibaca sebagai teknologi yang embedded dalam institusi, bukan sebagai agen yang berdiri di luar politik.

Artikel ini menggunakan tiga ranah analisis: politik, ekonomi, dan militer. Ranah politik mencakup administrasi negara, pelayanan publik, komunikasi politik, diplomasi, regulasi informasi, keamanan domestik, dan legitimasi. Ranah ekonomi mencakup produktivitas, industrial policy, pasar tenaga kerja, riset, semikonduktor, komputasi, data center, perusahaan teknologi, investasi, serta posisi dalam rantai nilai global. Ranah militer mencakup intelligence, surveillance and reconnaissance, command and control, logistics, cyber defence, autonomous systems, simulation, training, and decision support. Ketiganya saling berhubungan dan sering menggunakan infrastruktur yang sama.

Sifat dual-use AI menjadi inti pembahasan. Sistem pengenalan pola yang dikembangkan untuk diagnosis kesehatan dapat mempunyai analogi teknologi dengan analisis citra satelit; sistem optimisasi logistik untuk perusahaan dapat diterapkan pada rantai pasok militer; model bahasa yang membantu layanan publik dapat digunakan untuk komunikasi strategis; dan semikonduktor yang menggerakkan pusat data sipil juga mempunyai implikasi keamanan nasional. Karena garis antara sipil dan militer sering kabur, negara-negara memperlakukan AI sebagai bagian dari kebijakan teknologi strategis, bukan hanya sebagai sektor industri biasa.

Namun artikel ini tidak memandang penggunaan AI oleh negara sebagai kompetisi teknis semata. Pertanyaan normatif sama pentingnya: bagaimana menjaga hak warga, bagaimana mencegah discrimination by algorithm, bagaimana memastikan keputusan berisiko tinggi tetap dapat dipertanggungjawabkan, bagaimana menghindari automation bias, bagaimana mencegah penggunaan deepfake untuk manipulasi, dan bagaimana mempertahankan meaningful human control dalam konteks keamanan. Kualitas governance dapat menjadi sumber keunggulan karena sistem yang dipercaya cenderung lebih mudah diadopsi, diperbaiki, dan diintegrasikan secara luas.

Dalam konteks internasional, arah kebijakan memperlihatkan bahwa AI telah masuk secara formal ke strategi keamanan dan pertahanan. NATO merevisi strategi AI pada 2024 untuk merespons kemajuan seperti generative AI dan AI-enabled information tools, sambil menekankan responsible use, interoperability, testing, dan perlindungan terhadap penggunaan AI oleh adversary. Departemen Pertahanan Amerika Serikat telah memiliki Responsible AI Strategy and Implementation Pathway serta strategi adopsi data, analytics, dan AI. Di Uni Eropa, AI Act membangun kerangka berbasis risiko untuk penggunaan sipil, sementara penggunaan yang secara eksklusif untuk militer, pertahanan, atau keamanan nasional berada di luar ruang lingkup regulasi tersebut. Perkembangan ini menunjukkan bahwa governance AI sipil dan militer mulai membentuk rezim yang berbeda namun saling memengaruhi.

Bagi Indonesia, isu ini relevan karena transformasi digital, keamanan siber, modernisasi pertahanan, perlindungan data, pembangunan industri teknologi, dan penguatan kapasitas birokrasi berkembang secara bersamaan. Indonesia perlu menghindari dua jebakan: techno-optimism yang menganggap setiap adopsi AI sebagai kemajuan, dan techno-pessimism yang melihat AI hanya sebagai ancaman. Strategi yang lebih

produktif adalah membangun kapasitas untuk menilai, menggunakan, mengembangkan, dan mengatur AI sesuai kepentingan nasional, Pancasila, konstitusi, demokrasi, hukum, keamanan, dan tujuan pembangunan.

Peta Konseptual: AI sebagai Instrumen Negara

Ranah	Tujuan Negara	Contoh Pemanfaatan AI	Risiko Utama
Politik & Tata Kelola	kapasitas, legitimasi, keamanan, komunikasi	pelayanan publik, analisis kebijakan, pengawasan, komunikasi strategis	bias, surveillance, manipulasi, opacity
Ekonomi	produktivitas, daya saing, kedaulatan teknologi	industrial policy, R&D, semikonduktor, AI services, science	ketimpangan, dependency, market concentration
Militer	deterrence, kesiapan, kecepatan keputusan	ISR, logistics, cyber defence, autonomous systems, simulation	eskalasi, error, accountability, loss of control
Diplomasi	pengaruh, standar, koalisi	AI governance diplomacy, standard-setting, tech alliances	fragmentasi, techno-blocs

1. AI dan Transformasi State Capacity

Pembahasan mengenai ai dan transformasi state capacity perlu dimulai dari kapasitas negara mengumpulkan, memahami, dan menggunakan informasi untuk menjalankan fungsi publik. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Russell & Norvig, 2021).

Tantangan utamanya adalah anggapan bahwa lebih banyak data otomatis menghasilkan pemerintahan lebih baik. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan,

tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dan transformasi state capacity terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan pemerintah yang memiliki banyak dashboard tetapi definisi data antarinstansi tidak konsisten. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2022).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah transformasi AI harus dimulai dari kualitas institusi, data, proses, dan akuntabilitas. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, ai dan transformasi state capacity menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah *capable and accountable state*: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

2. AI dalam Administrasi Publik

Pembahasan mengenai ai dalam administrasi publik perlu dimulai dari otomatisasi tugas administratif, klasifikasi dokumen, pencarian pengetahuan, dan dukungan keputusan. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Floridi et al., 2018).

Tantangan utamanya adalah otomatisasi birokrasi yang hanya mempercepat prosedur lama tanpa menyederhanakan proses. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai dalam administrasi publik terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan instansi memakai chatbot tetapi warga tetap harus mengulang data yang sama pada banyak layanan. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia

menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2023).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI harus disertai redesign pelayanan dan interoperabilitas. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dalam administrasi publik menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

3. AI untuk Analisis dan Perumusan Kebijakan

Pembahasan mengenai AI untuk analisis dan perumusan kebijakan perlu dimulai dari penggunaan data, simulasi, prediksi, dan NLP untuk memahami masalah publik. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap,

kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (NATO, 2024).

Tantangan utamanya adalah risiko mengubah keputusan politik yang normatif menjadi persoalan teknis semata. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI untuk analisis dan perumusan kebijakan terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan model prediksi kemiskinan yang akurat secara statistik tetapi tidak menjawab prioritas kebijakan distributif. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (European Union, 2024).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko,

memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI harus membantu evidence-informed policy tanpa menggantikan deliberasi demokratis. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI untuk analisis dan perumusan kebijakan menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

4. AI dalam Pelayanan Publik

Pembahasan mengenai AI dalam pelayanan publik perlu dimulai dari peningkatan akses, personalisasi, triage, dan efisiensi layanan. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (U.S. Department of Defense, 2022).

Tantangan utamanya adalah digital exclusion dan ketergantungan pada sistem yang sulit dijelaskan. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan,

tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dalam pelayanan publik terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan warga menerima prioritas layanan berdasarkan model yang tidak ia pahami atau tidak dapat banding. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (UNESCO, 2021).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah layanan berisiko tinggi membutuhkan transparansi, akses alternatif, dan grievance mechanism. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, ai dalam pelayanan publik menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah *capable and accountable state*: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

5. AI, Pengawasan, dan Keamanan Domestik

Pembahasan mengenai ai, pengawasan, dan keamanan domestik perlu dimulai dari pengolahan data sensor, video, transaksi, dan pola perilaku untuk keamanan. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (U.S. Department of Defense, 2023).

Tantangan utamanya adalah pergeseran dari *targeted surveillance* menuju *population-scale surveillance*. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas *informational power*. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. *Informational power* dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip *necessity* dan *proportionality* menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai, pengawasan, dan keamanan domestik terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan *compute*, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan *deployment*. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh *technology stack*. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi *bottleneck*. Kebijakan industri menjadi instrumen untuk mengurangi *bottleneck* tersebut, tetapi keberhasilannya bergantung pada disiplin, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan sistem analitik mengidentifikasi pola yang dianggap mencurigakan tetapi menghasilkan *false positives*. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem *socio-technical*. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia

menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (OECD, 2019).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah pengawasan harus memenuhi necessity, proportionality, legality, dan independent oversight. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, ai, pengawasan, dan keamanan domestik menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

6. AI dan Politik Elektoral

Pembahasan mengenai ai dan politik elektoral perlu dimulai dari analitik opini, segmentasi, microtargeting, deteksi isu, dan komunikasi kampanye. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan

kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (European Union, 2024).

Tantangan utamanya adalah manipulasi psikografis, opaque targeting, bot, deepfake, dan asymmetric persuasion. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dan politik elektoral terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan konten sintetik dibuat untuk memengaruhi persepsi pemilih tanpa atribusi jelas. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Kello, 2017).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko,

memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah integritas pemilu memerlukan autentisitas, disclosure, media literacy, dan enforcement. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan politik elektoral menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

7. Generative AI, Deepfake, dan Krisis Kepercayaan Politik

Pembahasan mengenai generative AI, deepfake, dan krisis kepercayaan politik perlu dimulai dari kemampuan menciptakan teks, suara, gambar, dan video sintetik dengan biaya rendah. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (UNESCO, 2021).

Tantangan utamanya adalah liar's dividend: materi autentik dapat ditolak sebagai palsu karena deepfake mudah dibuat. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, otomatisasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan,

tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, generative ai, deepfake, dan krisis kepercayaan politik terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan rekaman asli dibantah sebagai AI-generated dan publik kehilangan dasar bersama untuk menilai bukti. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Horowitz, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah negara dan platform memerlukan provenance, verifikasi, dan komunikasi krisis. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, generative ai, deepfake, dan krisis kepercayaan politik menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah *capable and accountable state*: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

8. AI dalam Diplomasi dan Soft Power

Pembahasan mengenai ai dalam diplomasi dan soft power perlu dimulai dari analisis bahasa, pemantauan isu global, public diplomacy, dan negotiation support. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (OECD, 2019).

Tantangan utamanya adalah otomatisasi komunikasi tanpa sensitivitas budaya atau risiko manipulasi informasi. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai dalam diplomasi dan soft power terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan kedutaan menggunakan AI untuk memahami opini publik lokal namun perlu menjaga validitas dan konteks. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan

sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Scharre, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI diplomasi sebaiknya memperkuat human judgment dan cultural intelligence. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dalam diplomasi dan soft power menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

9. AI, Censorship, dan Information Control

Pembahasan mengenai AI, censorship, dan information control perlu dimulai dari klasifikasi konten, moderation, ranking, filtering, dan surveillance informasi. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan

yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Kello, 2017).

Tantangan utamanya adalah konsentrasi kemampuan menentukan visibilitas dan batas wacana publik. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI, censorship, dan information control terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan sistem menyaring konten secara luas berdasarkan kategori yang tidak transparan. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Taddeo & Floridi, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko,

memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah governance informasi harus membedakan keamanan, moderasi yang sah, dan pembungkaman dissent. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, ai, censorship, dan information control menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

10. AI untuk Deteksi Disinformasi

Pembahasan mengenai ai untuk deteksi disinformasi perlu dimulai dari penggunaan model untuk mengidentifikasi pola koordinasi, bot, media sintetis, dan klaim berisiko. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Horowitz, 2018).

Tantangan utamanya adalah detektor AI tidak sempurna dan dapat menimbulkan false positives serta bias politik. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan,

tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI untuk deteksi disinformasi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan konten satire atau kritik salah ditandai sebagai disinformasi. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Russell & Norvig, 2021).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI detection harus dilengkapi human review, bukti, dan mekanisme koreksi. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI untuk deteksi disinformasi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah *capable and accountable state*: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

11. AI sebagai Kebijakan Industri Strategis

Pembahasan mengenai AI sebagai kebijakan industri strategis perlu dimulai dari negara mendorong AI sebagai general-purpose technology dan sumber produktivitas. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Scharre, 2018).

Tantangan utamanya adalah industrial policy yang berubah menjadi subsidi tanpa discipline, learning, atau competition. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI sebagai kebijakan industri strategis terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan pemerintah mendanai proyek AI tetapi output tidak mencapai adopsi produktif. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa

yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Floridi et al., 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah kebijakan industri harus menghubungkan riset, firm capability, talent, finance, dan diffusion. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI sebagai kebijakan industri strategis menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

12. Semikonduktor dan Compute sebagai Infrastruktur Kekuasaan

Pembahasan mengenai semikonduktor dan compute sebagai infrastruktur kekuasaan perlu dimulai dari ketergantungan AI pada chip canggih, data center, jaringan, energi, dan cloud. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak

lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Taddeo & Floridi, 2018).

Tantangan utamanya adalah bottleneck pada teknologi yang sangat terkonsentrasi secara geografis dan korporat. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, semikonduktor dan compute sebagai infrastruktur kekuasaan terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan negara memiliki data dan talenta tetapi akses compute terbatas. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (NATO, 2024).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko,

memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah strategi AI nasional perlu memahami seluruh stack teknologi. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, semikonduktor dan compute sebagai infrastruktur kekuasaan menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

13. Data sebagai Aset Strategis Negara

Pembahasan mengenai data sebagai aset strategis negara perlu dimulai dari data publik, administratif, geospasial, ilmiah, dan ekonomi sebagai input AI. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Russell & Norvig, 2021).

Tantangan utamanya adalah fragmentasi data, kualitas rendah, privacy risk, dan institutional hoarding. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih

granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, data sebagai aset strategis negara terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan basis data penting tidak interoperabel sehingga model tidak dapat digunakan secara andal. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2022).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah data governance harus mendahului AI at scale. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response;

bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, data sebagai aset strategis negara menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

14. AI dan Produktivitas Nasional

Pembahasan mengenai ai dan produktivitas nasional perlu dimulai dari AI sebagai alat untuk mengurangi biaya pencarian, prediksi, administrasi, dan produksi pengetahuan. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Floridi et al., 2018).

Tantangan utamanya adalah productivity paradox ketika adopsi teknologi tidak disertai perubahan organisasi. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai dan produktivitas nasional terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan banyak pegawai memiliki akses AI tetapi proses kerja dan kewenangan tidak berubah. Pada permukaan, masalah tersebut tampak sebagai persoalan

implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2023).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah produktivitas memerlukan complementary investment dalam skills dan process redesign. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan produktivitas nasional menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

15. AI untuk Riset, Sains, dan Inovasi

Pembahasan mengenai AI untuk riset, sains, dan inovasi perlu dimulai dari AI membantu discovery, simulation, literature analysis, coding, dan desain eksperimen. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya,

mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (NATO, 2024).

Tantangan utamanya adalah ketergantungan pada model tanpa validation dan risiko reproduksi bias data. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI untuk riset, sains, dan inovasi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan peneliti menggunakan AI untuk menghasilkan hipotesis tetapi harus memeriksa sumber dan metodologi. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (European Union, 2024).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to

chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI science memerlukan reproducibility, provenance, dan scientific judgment. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI untuk riset, sains, dan inovasi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

16. AI dan Pasar Tenaga Kerja

Pembahasan mengenai AI dan pasar tenaga kerja perlu dimulai dari otomatisasi tugas, augmentasi pekerjaan, perubahan skill mix, dan produktivitas. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (U.S. Department of Defense, 2022).

Tantangan utamanya adalah displacement yang terkonsentrasi pada kelompok tertentu serta uneven access to reskilling. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dan pasar tenaga kerja terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan administrasi rutin menyusut sementara kebutuhan analytical and relational work meningkat. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (UNESCO, 2021).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah negara perlu menggabungkan innovation policy dengan labor transition policy. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust

terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan pasar tenaga kerja menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

17. AI, UMKM, dan Difusi Teknologi

Pembahasan mengenai AI, UMKM, dan difusi teknologi perlu dimulai dari pemanfaatan AI untuk pemasaran, inventori, customer service, accounting, dan decision support. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (U.S. Department of Defense, 2023).

Tantangan utamanya adalah kesenjangan adopsi antara frontier firms dan perusahaan kecil. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI, UMKM, dan difusi teknologi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan UMKM membeli tools tetapi tidak memiliki data, proses, atau kemampuan mengevaluasi output. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (OECD, 2019).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah program dukungan harus fokus pada capability upgrading, bukan sekadar akses aplikasi. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, ai, umkm, dan difusi teknologi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

18. AI dalam Perpajakan, Bea Cukai, dan Pengawasan Ekonomi

Pembahasan mengenai ai dalam perpajakan, bea cukai, dan pengawasan ekonomi perlu dimulai dari risk scoring, anomaly detection, fraud analytics, dan resource allocation. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (European Union, 2024).

Tantangan utamanya adalah algorithmic opacity dan risiko memperlakukan probabilitas sebagai kesalahan. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai dalam perpajakan, bea cukai, dan pengawasan ekonomi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan wajib pajak mendapat pemeriksaan lebih intensif berdasarkan pola yang sulit dipahami. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of

responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Kello, 2017).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah penggunaan AI harus menjaga due process dan auditability. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dalam perpajakan, bea cukai, dan pengawasan ekonomi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

19. AI dan Kedaulatan Teknologi

Pembahasan mengenai AI dan kedaulatan teknologi perlu dimulai dari kemampuan negara memilih, mengadaptasi, mengevaluasi, dan mengamankan teknologi kritis. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (UNESCO, 2021).

Tantangan utamanya adalah salah kaprah bahwa sovereignty berarti autarky atau isolasi teknologi. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang

secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dan kedaulatan teknologi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan negara menggunakan model global tetapi membutuhkan local evaluation, data governance, dan fallback options. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Horowitz, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah kedaulatan sebaiknya dipahami sebagai strategic capability, bukan self-sufficiency absolut. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua

ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan kedaulatan teknologi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

20. AI dan Geopolitik Standar

Pembahasan mengenai AI dan geopolitik standar perlu dimulai dari kompetisi dalam technical standards, safety norms, data rules, dan model governance. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (OECD, 2019).

Tantangan utamanya adalah fragmentasi global menjadi ekosistem teknologi yang tidak kompatibel. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dan geopolitik standar terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada

level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan perusahaan harus mematuhi aturan berbeda antara yurisdiksi. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Scharre, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah diplomasi AI semakin penting sebagai bagian dari economic statecraft. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan geopolitik standar menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

21. AI dan Modernisasi Militer

Pembahasan mengenai ai dan modernisasi militer perlu dimulai dari pemanfaatan AI untuk meningkatkan sensing, analysis, logistics, readiness, dan decision support. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Kello, 2017).

Tantangan utamanya adalah narasi bahwa AI otomatis memberikan kemenangan tanpa mempertimbangkan doctrine dan organization. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai dan modernisasi militer terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan angkatan bersenjata memiliki algoritma canggih tetapi integrasi data dan command structure lemah. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of

responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Taddeo & Floridi, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah military AI adalah socio-technical transformation, bukan sekadar procurement teknologi. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan modernisasi militer menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

22. Intelligence, Surveillance, and Reconnaissance (ISR)

Pembahasan mengenai intelligence, surveillance, and reconnaissance (ISR) perlu dimulai dari pemrosesan citra, sinyal, sensor, dan data dalam jumlah besar untuk situational awareness. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Horowitz, 2018).

Tantangan utamanya adalah false confidence dan bias ketika output probabilistik diperlakukan sebagai kepastian. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan

diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, intelligence, surveillance, and reconnaissance (ISR) terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan sistem membantu menyaring data sehingga analisis manusia dapat memprioritaskan perhatian. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Russell & Norvig, 2021).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI ISR perlu validation, uncertainty communication, dan human analysis. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi

terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, intelligence, surveillance, and reconnaissance (ISR) menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

23. AI dalam Command and Control

Pembahasan mengenai AI dalam command and control perlu dimulai dari dukungan pemahaman situasi, prioritization, course-of-action analysis, dan decision support. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Scharre, 2018).

Tantangan utamanya adalah compression of decision time yang dapat meningkatkan risiko eskalasi. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dalam command and control terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada

level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan pemimpin menerima rekomendasi cepat dari sistem tetapi harus memahami uncertainty dan assumptions. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Floridi et al., 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah kecepatan harus diimbangi procedural safeguards dan command responsibility. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dalam command and control menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

24. AI untuk Logistik dan Predictive Maintenance

Pembahasan mengenai ai untuk logistik dan predictive maintenance perlu dimulai dari optimisasi pasokan, perawatan, rute, inventori, dan readiness. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Taddeo & Floridi, 2018).

Tantangan utamanya adalah ketergantungan pada data sensor dan risiko failure cascade jika sistem tidak robust. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai untuk logistik dan predictive maintenance terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan AI memperkirakan kebutuhan perawatan armada sehingga downtime dapat dikurangi. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of

responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (NATO, 2024).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah logistics AI memerlukan resilient data, redundancy, dan cyber protection. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI untuk logistik dan predictive maintenance menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

25. AI dalam Cyber Defence

Pembahasan mengenai AI dalam cyber defence perlu dimulai dari deteksi anomali, triage alerts, malware classification, dan incident support. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Russell & Norvig, 2021).

Tantangan utamanya adalah adversarial adaptation, false positives, dan automated escalation. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan

tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dalam cyber defence terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan sistem membantu SOC mengidentifikasi pola serangan lebih cepat tetapi keputusan respons tetap diawasi manusia. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2022).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah AI cyber defence harus dikembangkan dengan rigorous testing dan clear authority. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi

terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dalam cyber defence menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

26. Sistem Otonom dan Human Control

Pembahasan mengenai sistem otonom dan human control perlu dimulai dari penggunaan autonomy dalam navigasi, sensing, support, dan sejumlah fungsi pertahanan. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Floridi et al., 2018).

Tantangan utamanya adalah risiko kehilangan kontrol bermakna, target misidentification, dan accountability gap. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, sistem otonom dan human control terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada

level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan platform otonom menjalankan fungsi tertentu tetapi parameter dan authorization tetap dibatasi. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2023).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah governance harus membedakan tingkat autonomy, context, legal review, dan human responsibility. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, sistem otonom dan human control menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

27. AI, Wargaming, Simulasi, dan Training

Pembahasan mengenai ai, wargaming, simulasi, dan training perlu dimulai dari penggunaan AI untuk scenario generation, synthetic opponents, rehearsal, dan decision learning. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (NATO, 2024).

Tantangan utamanya adalah simulasi yang memberi ilusi realism padahal model mengandung assumptions tertentu. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, ai, wargaming, simulasi, dan training terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan staf menggunakan simulasi AI untuk menguji konsekuensi kebijakan tanpa menganggap output sebagai prediksi pasti. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of

responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (European Union, 2024).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah simulation literacy harus menjadi bagian dari military education. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI, wargaming, simulasi, dan training menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

28. AI dan Informasi dalam Konflik

Pembahasan mengenai AI dan informasi dalam konflik perlu dimulai dari analisis narasi, deteksi manipulasi, strategic communication, dan situational awareness. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (U.S. Department of Defense, 2022).

Tantangan utamanya adalah blurred line antara counter-disinformation dan propaganda. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan

tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI dan informasi dalam konflik terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan negara membalas operasi informasi lawan tetapi harus menjaga kredibilitas jangka panjang. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (UNESCO, 2021).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah kepercayaan publik merupakan strategic asset yang tidak boleh dikorbankan untuk kemenangan narasi sesaat. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu

menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI dan informasi dalam konflik menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

29. AI, Nuclear Stability, dan Risiko Eskalasi

Pembahasan mengenai AI, nuclear stability, dan risiko eskalasi perlu dimulai dari hubungan AI dengan early warning, intelligence analysis, command support, dan strategic stability. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (U.S. Department of Defense, 2023).

Tantangan utamanya adalah automation bias, spoofing, compressed timelines, dan uncertainty pada krisis berisiko tinggi. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, AI, nuclear stability, dan risiko eskalasi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya

berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan sinyal ambigu dianalisis sistem dengan confidence tinggi sehingga pemimpin dapat salah memahami situasi. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (OECD, 2019).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah keputusan strategis ekstrem memerlukan human judgment, redundancy, dan conservative safeguards. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, AI, nuclear stability, dan risiko eskalasi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

30. Responsible AI dalam Pertahanan

Pembahasan mengenai responsible ai dalam pertahanan perlu dimulai dari prinsip responsible, equitable, traceable, reliable, governable, dan accountable. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (European Union, 2024).

Tantangan utamanya adalah kesenjangan antara prinsip dan implementation pada sistem kompleks. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, responsible ai dalam pertahanan terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan organisasi mengadopsi RAI toolkit untuk menguji lifecycle dan risiko sebelum deployment. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of

responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Kello, 2017).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah responsible AI harus menjadi engineering and governance discipline. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, responsible AI dalam pertahanan menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

31. Amerika Serikat: AI sebagai Kapabilitas Strategis

Pembahasan mengenai Amerika Serikat: AI sebagai kapabilitas strategis perlu dimulai dari integrasi data, analytics, AI adoption, responsible AI, innovation ecosystem, dan defence technology. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (UNESCO, 2021).

Tantangan utamanya adalah tantangan koordinasi organisasi besar serta ketergantungan pada private-sector frontier. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan

diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, Amerika Serikat: AI sebagai kapabilitas strategis terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan DoD membangun CDAO dan strategi adopsi AI sambil menekankan responsible AI. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Horowitz, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah pelajaran utama adalah integrasi ecosystem komersial dan negara dengan governance yang terus berkembang. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu

menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, Amerika Serikat: AI sebagai kapabilitas strategis menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

32. Tiongkok: AI, Industrial Upgrading, dan National Power

Pembahasan mengenai Tiongkok: AI, industrial upgrading, dan national power perlu dimulai dari integrasi AI dalam pembangunan ekonomi, science and technology, smart industry, dan strategic capability. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (OECD, 2019).

Tantangan utamanya adalah interaksi erat antara tujuan pembangunan, keamanan, dan kapasitas negara. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, Tiongkok: AI, industrial upgrading, dan national power terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya

berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan rencana pembangunan menempatkan AI, chip, cloud, dan teknologi inti sebagai prioritas. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Scharre, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah pelajaran utama adalah pentingnya long-term coordination dan capability accumulation. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, Tiongkok: ai, industrial upgrading, dan national power menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable

state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

33. NATO dan Uni Eropa: Interoperability, Risk, dan Norms

Pembahasan mengenai nato dan uni eropa: interoperability, risk, dan norms perlu dimulai dari NATO menekankan responsible military AI sedangkan UE membangun regulatory framework sipil berbasis risiko. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Kello, 2017).

Tantangan utamanya adalah ketegangan antara innovation speed, national security, dan rights protection. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, nato dan uni eropa: interoperability, risk, dan norms terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan AI Act mengecualikan penggunaan eksklusif militer/pertahanan/national security namun mengatur civilian high-risk AI. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit

ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Taddeo & Floridi, 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah governance Barat memperlihatkan pemisahan tetapi juga interaksi antara security and rights regimes. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, nato dan uni eropa: interoperability, risk, dan norms menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

34. Negara Menengah dan Negara Berkembang

Pembahasan mengenai negara menengah dan negara berkembang perlu dimulai dari cara negara dengan sumber daya lebih terbatas memilih niche capability dan partnership. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Horowitz, 2018).

Tantangan utamanya adalah risiko menjadi hanya konsumen teknologi tanpa *evaluation capability*. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas *informational power*. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. *Informational power* dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip *necessity* dan *proportionality* menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, negara menengah dan negara berkembang terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan *compute*, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan *deployment*. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh *technology stack*. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi *bottleneck*. Kebijakan industri menjadi instrumen untuk mengurangi *bottleneck* tersebut, tetapi keberhasilannya bergantung pada *discipline*, kompetisi, *learning*, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan negara menggunakan cloud AI global tetapi membangun *local talent*, *datasets*, dan *regulatory competence*. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem *socio-technical*. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan *situational awareness*, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya *uncertainty* tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, *red-teaming*, *human oversight*, dan *chain of responsibility* yang jelas. Pendekatan *responsible AI* di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik *engineering* dan *governance* (Russell & Norvig, 2021).

Aspek strategis lain adalah *dependency*. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai *vendor lock-in*, *supply-chain security*, *cloud concentration*, *access to chips*, *model updates*, dan *jurisdiction*. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi *governance*, implikasinya adalah strategi realistis adalah *selective sovereignty* dan *trusted partnerships*. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari

penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, negara menengah dan negara berkembang menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

35. Indonesia: Peluang dan Kerentanan Strategis

Pembahasan mengenai Indonesia: peluang dan kerentanan strategis perlu dimulai dari AI untuk birokrasi, layanan publik, ekonomi digital, riset, keamanan, dan modernisasi pertahanan. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Scharre, 2018).

Tantangan utamanya adalah fragmentasi data, talent gaps, vendor dependence, cybersecurity, dan governance readiness. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, Indonesia: peluang dan kerentanan strategis terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan instansi mengadopsi berbagai aplikasi AI tetapi membutuhkan standar lintas pemerintah. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (Floridi et al., 2018).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah Indonesia memerlukan strategi nasional yang menghubungkan civilian AI, economic policy, security, and rights. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, Indonesia: peluang dan kerentanan strategis menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya,

governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah *capable and accountable state*: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

36. Arsitektur Tata Kelola AI Nasional

Pembahasan mengenai arsitektur tata kelola ai nasional perlu dimulai dari *policy coordination*, *standards*, *procurement*, *audits*, *data protection*, *cybersecurity*, dan *accountability*. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Taddeo & Floridi, 2018).

Tantangan utamanya adalah *governance* yang terlalu tersebar sehingga tanggung jawab tidak jelas. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas *informational power*. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. *Informational power* dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip *necessity* dan *proportionality* menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, arsitektur tata kelola ai nasional terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan *compute*, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan *deployment*. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh *technology stack*. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi *bottleneck*. Kebijakan industri menjadi instrumen untuk mengurangi *bottleneck* tersebut, tetapi keberhasilannya bergantung pada disiplin, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan insiden AI melibatkan banyak instansi tetapi tidak ada *single incident protocol*. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem *socio-technical*. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (NATO, 2024).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah arsitektur perlu membagi peran secara tegas sekaligus menyediakan koordinasi lintas sektor. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, arsitektur tata kelola AI nasional menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

37. Etika, Hak Asasi, dan Legitimasi

Pembahasan mengenai etika, hak asasi, dan legitimasi perlu dimulai dari hubungan antara AI negara dengan dignity, privacy, equality, due process, dan political freedom. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Russell & Norvig, 2021).

Tantangan utamanya adalah efisiensi administratif yang diperoleh dengan mengorbankan hak dan trust. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, etika, hak asasi, dan legitimasi terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan model menolak akses warga tanpa jalur appeal yang efektif. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2022).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah legitimasi menuntut contestability dan proportionality. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang

memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, etika, hak asasi, dan legitimasi menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya, governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah capable and accountable state: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

38. Masa Depan Kompetisi AI Antarneegara

Pembahasan mengenai masa depan kompetisi AI antarnegara perlu dimulai dari pergeseran kompetisi dari model AI menuju ecosystem, talent, compute, energy, data, institutions, and alliances. AI menjadi relevan bagi negara karena negara bekerja melalui informasi. Ia harus mengetahui keadaan masyarakat, mengalokasikan sumber daya, mengenali risiko, mengawasi pelaksanaan kebijakan, serta merespons perubahan. Sistem AI dapat membantu memproses volume informasi yang tidak mungkin dianalisis secara manual pada kecepatan yang sama. Namun AI tidak menghapus masalah klasik administrasi dan politik. Data dapat tidak lengkap, kategori dapat bias, tujuan kebijakan dapat konflik, dan keputusan publik tetap memiliki dimensi normatif. Karena itu kemampuan AI harus dipahami sebagai tambahan terhadap kapasitas institusional, bukan pengganti institusi (Floridi et al., 2018).

Tantangan utamanya adalah arms-race framing yang dapat mendorong overinvestment dan under-governance. Situasi ini muncul karena pemerintah sering tertarik pada kemampuan teknis yang terlihat—akurasi model, kecepatan pemrosesan, automasi—sementara kualitas input dan tata kelola lebih sulit terlihat. Sistem yang secara teknis kuat dapat menghasilkan dampak buruk jika data mencerminkan diskriminasi historis, jika tujuan tidak didefinisikan dengan jelas, atau jika petugas tidak mempunyai jalur untuk mengoreksi keluaran. Dalam sektor publik, kegagalan semacam itu berbeda dari kesalahan rekomendasi komersial karena keputusan negara dapat menentukan hak, akses layanan, pajak, keamanan, reputasi, atau bahkan kebebasan seseorang.

Dari perspektif politik, AI memperluas informational power. Pemerintah dapat menggabungkan data administratif, sensor, statistik, geospasial, teks, dan media digital untuk memperoleh gambaran yang lebih granular mengenai masyarakat. Informational power dapat memperbaiki pelayanan dan perencanaan, tetapi juga dapat mengubah keseimbangan antara warga dan negara. Ketika pengumpulan data terlalu luas atau penggunaan sekunder tidak transparan, warga sulit mengetahui bagaimana profil mereka dibentuk. Prinsip necessity dan proportionality menjadi penting: kemampuan teknis untuk mengumpulkan data tidak identik dengan legitimasi untuk menggunakannya.

Dalam konteks ekonomi, masa depan kompetisi ai antarnegara terkait dengan kemampuan negara membentuk ekosistem inovasi. AI memerlukan compute, listrik, pusat data, chip, jaringan, software, talenta, riset, dan perusahaan yang mampu melakukan deployment. Karena itu persaingan AI tidak hanya berlangsung pada level model, tetapi pada seluruh technology stack. Negara yang menguasai satu lapisan namun lemah pada lapisan lain dapat menghadapi bottleneck. Kebijakan industri menjadi instrumen untuk mengurangi bottleneck tersebut, tetapi keberhasilannya bergantung pada discipline, kompetisi, learning, evaluasi, dan kemampuan menghentikan program yang tidak memberikan hasil.

Sebuah ilustrasi dapat memperjelas persoalan. Bayangkan negara mempercepat adopsi karena takut tertinggal meskipun evaluation belum matang. Pada permukaan, masalah tersebut tampak sebagai persoalan implementasi teknis. Namun analisis lebih dalam memperlihatkan interaksi antara organisasi, data, hukum, insentif, kompetensi, dan kepercayaan. Inilah sebabnya AI negara merupakan sistem socio-technical. Model hanya satu komponen. Nilai akhir ditentukan oleh bagaimana manusia menggunakan output, siapa yang berwenang mengambil keputusan, bagaimana kesalahan dilaporkan, bagaimana sistem diuji, dan bagaimana warga atau pengguna dapat mengajukan keberatan.

Dalam ranah keamanan dan pertahanan, logika yang sama menjadi lebih kritis. AI dapat mempercepat analisis dan meningkatkan situational awareness, tetapi kecepatan yang terlalu besar dapat mempersempit ruang refleksi. Sistem probabilistik juga dapat menghasilkan output yang tampak pasti ketika sebenarnya uncertainty tinggi. Karena konsekuensi keputusan militer dapat ekstrem, organisasi pertahanan memerlukan standar pengujian, verifikasi, validasi, red-teaming, human oversight, dan chain of responsibility yang jelas. Pendekatan responsible AI di sektor pertahanan pada dasarnya berusaha mengubah prinsip etis menjadi praktik engineering dan governance (U.S. Department of Defense, 2023).

Aspek strategis lain adalah dependency. Negara modern memperoleh banyak kapabilitas AI dari perusahaan swasta dan rantai pasok internasional. Hal ini memberi kecepatan inovasi, tetapi juga menimbulkan pertanyaan mengenai vendor lock-in, supply-chain security, cloud concentration, access to chips, model updates, dan jurisdiction. Kedaulatan teknologi karena itu tidak berarti semua teknologi harus dibuat domestik. Kedaulatan yang realistis adalah kemampuan memahami ketergantungan, menilai risiko, memiliki alternatif, menjaga data sensitif, dan mempertahankan kompetensi untuk bernegosiasi serta mengaudit pemasok.

Dari sisi governance, implikasinya adalah strategic patience dan rigorous governance dapat menjadi keunggulan. Negara membutuhkan klasifikasi risiko yang membedakan penggunaan berisiko rendah dari penggunaan yang memengaruhi hak, keselamatan, atau keamanan nasional. Tidak semua chatbot pemerintah membutuhkan proses audit yang sama dengan sistem biometric identification atau decision support di bidang pertahanan. Pendekatan proporsional membantu menghindari dua ekstrem: regulasi terlalu ringan pada sistem berisiko tinggi dan regulasi terlalu berat pada inovasi berisiko rendah. Governance yang baik mengalokasikan perhatian sesuai potensi dampak.

Bagi pemimpin publik, kompetensi AI juga harus mencakup kemampuan bertanya. Pejabat tidak harus menjadi data scientist, tetapi harus memahami pertanyaan seperti: data apa yang digunakan; apa tujuan model; apa baseline; berapa tingkat kesalahan; kelompok mana paling terdampak; apakah sistem robust terhadap perubahan; siapa yang dapat menghentikan deployment; apa rencana incident response; bagaimana vendor dievaluasi; dan apakah manfaat benar-benar lebih besar daripada alternatif non-AI. Kemampuan mengajukan pertanyaan ini merupakan bagian dari strategic digital literacy.

Akhirnya, masa depan kompetisi ai antarnegara menunjukkan bahwa AI mengubah hubungan antara kapasitas dan tanggung jawab. Semakin besar kemampuan negara untuk melihat, memprediksi, dan bertindak, semakin besar pula kewajiban untuk membangun kontrol yang layak. Kemajuan teknis tanpa kemajuan kelembagaan dapat menghasilkan negara yang lebih kuat tetapi kurang akuntabel. Sebaliknya,

governance tanpa kemampuan teknis dapat membuat negara gagal melindungi warga atau memanfaatkan peluang ekonomi. Tujuan yang lebih seimbang adalah *capable and accountable state*: negara yang mampu menggunakan AI untuk kepentingan publik sambil mempertahankan batas hukum, etika, dan demokratis.

39. Studi Kasus Komparatif: Empat Model Pemanfaatan AI oleh Negara

Kasus A - Pemerintahan Digital Berbasis AI

Kasus A - Pemerintahan Digital Berbasis AI menggambarkan situasi di mana sebuah negara mengintegrasikan chatbot layanan publik, fraud detection, policy analytics, dan identitas digital. Analisis pertama harus membedakan tujuan publik dari instrumen teknis. Tujuan dapat berupa peningkatan pelayanan, pertumbuhan ekonomi, keamanan, atau deterrence. AI hanyalah salah satu cara untuk mencapai tujuan tersebut. Karena itu pertanyaan awal adalah apakah AI memang memberikan *comparative advantage* dibandingkan prosedur alternatif. Pendekatan ini mencegah *technology solutionism*, yaitu kecenderungan memilih teknologi karena tersedia, bukan karena terbukti sesuai dengan masalah.

Dimensi kedua adalah efisiensi, interoperabilitas, privasi, bias, due process, dan public trust. Setiap dimensi mempunyai pemilik risiko yang berbeda. Tim teknis bertanggung jawab pada kualitas sistem; unit kebijakan pada tujuan dan dasar hukum; pimpinan pada risk acceptance; procurement pada vendor; cybersecurity pada resilience; dan oversight bodies pada akuntabilitas. Jika tanggung jawab tidak dipetakan, organisasi mudah mengalami *accountability gap*: semua pihak terlibat tetapi tidak ada satu pihak yang benar-benar dapat dimintai pertanggungjawaban ketika kegagalan terjadi.

Dimensi ketiga adalah lifecycle. Risiko AI tidak berhenti ketika model selesai diuji. Data berubah, perilaku pengguna berubah, adversary beradaptasi, vendor memperbarui model, dan tujuan organisasi dapat bergeser. Karena itu governance harus berlangsung sejak problem definition, data acquisition, model development, testing, deployment, monitoring, incident response, hingga retirement. Sistem berisiko tinggi sebaiknya memiliki log perubahan, batas penggunaan, indikator drift, jalur eskalasi, dan mekanisme suspend apabila perilakunya tidak lagi sesuai asumsi.

Dimensi keempat adalah human-machine relationship. Human oversight tidak efektif jika manusia hanya berfungsi sebagai stempel pada rekomendasi mesin. Operator membutuhkan waktu, informasi, otoritas, dan pelatihan untuk menolak atau menunda keputusan. Sebaliknya, terlalu banyak intervensi manusia dapat menghilangkan manfaat otomasi. Desain yang baik menentukan titik keputusan mana yang membutuhkan judgment manusia, informasi apa yang harus diperlihatkan, dan bagaimana uncertainty dikomunikasikan. Tujuannya bukan memaksimalkan manusia atau mesin, melainkan mengalokasikan fungsi sesuai kekuatan dan keterbatasannya.

Dimensi kelima adalah legitimacy. Dalam sistem politik, penerimaan publik menentukan apakah teknologi dapat digunakan secara berkelanjutan. Sistem yang efisien tetapi tidak dipercaya dapat memicu resistance, litigation, avoidance behavior, dan political backlash. Kepercayaan tidak dibangun melalui slogan AI ethics, melainkan melalui pengalaman konkret: kesalahan diakui, keputusan dapat dipertanyakan, data tidak disalahgunakan, dan pejabat dapat menjelaskan tujuan sistem. Dengan demikian legitimacy merupakan bagian dari performance, bukan faktor eksternal.

Pelajaran dari kasus ini adalah bahwa negara membutuhkan institutional intelligence yang sama besarnya dengan artificial intelligence. Negara harus mampu mengenali risiko teknologi, belajar dari insiden, memperbarui kebijakan, dan menjaga koordinasi lintas kementerian, regulator, militer, industri, akademisi, serta masyarakat sipil. Negara yang hanya membeli teknologi tanpa meningkatkan kapasitas institusional

dapat menjadi lebih tergantung dan lebih rapuh. Sebaliknya, negara yang membangun kemampuan evaluasi dapat memperoleh manfaat dari teknologi global tanpa kehilangan kendali strategis.

Kasus B - Kebijakan Industri AI

Kasus B - Kebijakan Industri AI menggambarkan situasi di mana pemerintah membangun insentif untuk chip, data center, cloud, startup, research labs, dan AI talent. Analisis pertama harus membedakan tujuan publik dari instrumen teknis. Tujuan dapat berupa peningkatan pelayanan, pertumbuhan ekonomi, keamanan, atau deterrence. AI hanyalah salah satu cara untuk mencapai tujuan tersebut. Karena itu pertanyaan awal adalah apakah AI memang memberikan comparative advantage dibandingkan prosedur alternatif. Pendekatan ini mencegah technology solutionism, yaitu kecenderungan memilih teknologi karena tersedia, bukan karena terbukti sesuai dengan masalah.

Dimensi kedua adalah subsidy discipline, competition, strategic dependency, diffusion, dan fiscal sustainability. Setiap dimensi mempunyai pemilik risiko yang berbeda. Tim teknis bertanggung jawab pada kualitas sistem; unit kebijakan pada tujuan dan dasar hukum; pimpinan pada risk acceptance; procurement pada vendor; cybersecurity pada resilience; dan oversight bodies pada akuntabilitas. Jika tanggung jawab tidak dipetakan, organisasi mudah mengalami accountability gap: semua pihak terlibat tetapi tidak ada satu pihak yang benar-benar dapat dimintai pertanggungjawaban ketika kegagalan terjadi.

Dimensi ketiga adalah lifecycle. Risiko AI tidak berhenti ketika model selesai diuji. Data berubah, perilaku pengguna berubah, adversary beradaptasi, vendor memperbarui model, dan tujuan organisasi dapat bergeser. Karena itu governance harus berlangsung sejak problem definition, data acquisition, model development, testing, deployment, monitoring, incident response, hingga retirement. Sistem berisiko tinggi sebaiknya memiliki log perubahan, batas penggunaan, indikator drift, jalur eskalasi, dan mekanisme suspend apabila perilakunya tidak lagi sesuai asumsi.

Dimensi keempat adalah human-machine relationship. Human oversight tidak efektif jika manusia hanya berfungsi sebagai stempel pada rekomendasi mesin. Operator membutuhkan waktu, informasi, otoritas, dan pelatihan untuk menolak atau menunda keputusan. Sebaliknya, terlalu banyak intervensi manusia dapat menghilangkan manfaat otomatisasi. Desain yang baik menentukan titik keputusan mana yang membutuhkan judgment manusia, informasi apa yang harus diperlihatkan, dan bagaimana uncertainty dikomunikasikan. Tujuannya bukan memaksimalkan manusia atau mesin, melainkan mengalokasikan fungsi sesuai kekuatan dan keterbatasannya.

Dimensi kelima adalah legitimacy. Dalam sistem politik, penerimaan publik menentukan apakah teknologi dapat digunakan secara berkelanjutan. Sistem yang efisien tetapi tidak dipercaya dapat memicu resistance, litigation, avoidance behavior, dan political backlash. Kepercayaan tidak dibangun melalui slogan AI ethics, melainkan melalui pengalaman konkret: kesalahan diakui, keputusan dapat dipertanyakan, data tidak disalahgunakan, dan pejabat dapat menjelaskan tujuan sistem. Dengan demikian legitimacy merupakan bagian dari performance, bukan faktor eksternal.

Pelajaran dari kasus ini adalah bahwa negara membutuhkan institutional intelligence yang sama besarnya dengan artificial intelligence. Negara harus mampu mengenali risiko teknologi, belajar dari insiden, memperbarui kebijakan, dan menjaga koordinasi lintas kementerian, regulator, militer, industri, akademisi, serta masyarakat sipil. Negara yang hanya membeli teknologi tanpa meningkatkan kapasitas institusional dapat menjadi lebih tergantung dan lebih rapuh. Sebaliknya, negara yang membangun kemampuan evaluasi dapat memperoleh manfaat dari teknologi global tanpa kehilangan kendali strategis.

Kasus C - AI untuk Keamanan Nasional

Kasus C - AI untuk Keamanan Nasional menggambarkan situasi di mana lembaga keamanan menggunakan AI untuk triage informasi, deteksi anomali, dan situational awareness. Analisis pertama harus membedakan

tujuan publik dari instrumen teknis. Tujuan dapat berupa peningkatan pelayanan, pertumbuhan ekonomi, keamanan, atau deterrence. AI hanyalah salah satu cara untuk mencapai tujuan tersebut. Karena itu pertanyaan awal adalah apakah AI memang memberikan comparative advantage dibandingkan prosedur alternatif. Pendekatan ini mencegah technology solutionism, yaitu kecenderungan memilih teknologi karena tersedia, bukan karena terbukti sesuai dengan masalah.

Dimensi kedua adalah necessity, proportionality, secrecy, oversight, false positives, dan mission creep. Setiap dimensi mempunyai pemilik risiko yang berbeda. Tim teknis bertanggung jawab pada kualitas sistem; unit kebijakan pada tujuan dan dasar hukum; pimpinan pada risk acceptance; procurement pada vendor; cybersecurity pada resilience; dan oversight bodies pada akuntabilitas. Jika tanggung jawab tidak dipetakan, organisasi mudah mengalami accountability gap: semua pihak terlibat tetapi tidak ada satu pihak yang benar-benar dapat dimintai pertanggungjawaban ketika kegagalan terjadi.

Dimensi ketiga adalah lifecycle. Risiko AI tidak berhenti ketika model selesai diuji. Data berubah, perilaku pengguna berubah, adversary beradaptasi, vendor memperbarui model, dan tujuan organisasi dapat bergeser. Karena itu governance harus berlangsung sejak problem definition, data acquisition, model development, testing, deployment, monitoring, incident response, hingga retirement. Sistem berisiko tinggi sebaiknya memiliki log perubahan, batas penggunaan, indikator drift, jalur eskalasi, dan mekanisme suspend apabila perilakunya tidak lagi sesuai asumsi.

Dimensi keempat adalah human-machine relationship. Human oversight tidak efektif jika manusia hanya berfungsi sebagai stempel pada rekomendasi mesin. Operator membutuhkan waktu, informasi, otoritas, dan pelatihan untuk menolak atau menunda keputusan. Sebaliknya, terlalu banyak intervensi manusia dapat menghilangkan manfaat otomasi. Desain yang baik menentukan titik keputusan mana yang membutuhkan judgment manusia, informasi apa yang harus diperlihatkan, dan bagaimana uncertainty dikomunikasikan. Tujuannya bukan memaksimalkan manusia atau mesin, melainkan mengalokasikan fungsi sesuai kekuatan dan keterbatasannya.

Dimensi kelima adalah legitimacy. Dalam sistem politik, penerimaan publik menentukan apakah teknologi dapat digunakan secara berkelanjutan. Sistem yang efisien tetapi tidak dipercaya dapat memicu resistance, litigation, avoidance behavior, dan political backlash. Kepercayaan tidak dibangun melalui slogan AI ethics, melainkan melalui pengalaman konkret: kesalahan diakui, keputusan dapat dipertanyakan, data tidak disalahgunakan, dan pejabat dapat menjelaskan tujuan sistem. Dengan demikian legitimacy merupakan bagian dari performance, bukan faktor eksternal.

Pelajaran dari kasus ini adalah bahwa negara membutuhkan institutional intelligence yang sama besarnya dengan artificial intelligence. Negara harus mampu mengenali risiko teknologi, belajar dari insiden, memperbarui kebijakan, dan menjaga koordinasi lintas kementerian, regulator, militer, industri, akademisi, serta masyarakat sipil. Negara yang hanya membeli teknologi tanpa meningkatkan kapasitas institusional dapat menjadi lebih tergantung dan lebih rapuh. Sebaliknya, negara yang membangun kemampuan evaluasi dapat memperoleh manfaat dari teknologi global tanpa kehilangan kendali strategis.

Kasus D - AI dalam Pertahanan

Kasus D - AI dalam Pertahanan menggambarkan situasi di mana militer mengadopsi AI untuk ISR, logistics, simulation, cyber defence, dan decision support. Analisis pertama harus membedakan tujuan publik dari instrumen teknis. Tujuan dapat berupa peningkatan pelayanan, pertumbuhan ekonomi, keamanan, atau deterrence. AI hanyalah salah satu cara untuk mencapai tujuan tersebut. Karena itu pertanyaan awal adalah apakah AI memang memberikan comparative advantage dibandingkan prosedur alternatif. Pendekatan ini mencegah technology solutionism, yaitu kecenderungan memilih teknologi karena tersedia, bukan karena terbukti sesuai dengan masalah.

Dimensi kedua adalah testing, reliability, human control, doctrine, interoperability, dan escalation risk. Setiap dimensi mempunyai pemilik risiko yang berbeda. Tim teknis bertanggung jawab pada kualitas sistem; unit kebijakan pada tujuan dan dasar hukum; pimpinan pada risk acceptance; procurement pada vendor; cybersecurity pada resilience; dan oversight bodies pada akuntabilitas. Jika tanggung jawab tidak dipetakan, organisasi mudah mengalami accountability gap: semua pihak terlibat tetapi tidak ada satu pihak yang benar-benar dapat dimintai pertanggungjawaban ketika kegagalan terjadi.

Dimensi ketiga adalah lifecycle. Risiko AI tidak berhenti ketika model selesai diuji. Data berubah, perilaku pengguna berubah, adversary beradaptasi, vendor memperbarui model, dan tujuan organisasi dapat bergeser. Karena itu governance harus berlangsung sejak problem definition, data acquisition, model development, testing, deployment, monitoring, incident response, hingga retirement. Sistem berisiko tinggi sebaiknya memiliki log perubahan, batas penggunaan, indikator drift, jalur eskalasi, dan mekanisme suspend apabila perilakunya tidak lagi sesuai asumsi.

Dimensi keempat adalah human-machine relationship. Human oversight tidak efektif jika manusia hanya berfungsi sebagai stempel pada rekomendasi mesin. Operator membutuhkan waktu, informasi, otoritas, dan pelatihan untuk menolak atau menunda keputusan. Sebaliknya, terlalu banyak intervensi manusia dapat menghilangkan manfaat otomatisasi. Desain yang baik menentukan titik keputusan mana yang membutuhkan judgment manusia, informasi apa yang harus diperlihatkan, dan bagaimana uncertainty dikomunikasikan. Tujuannya bukan memaksimalkan manusia atau mesin, melainkan mengalokasikan fungsi sesuai kekuatan dan keterbatasannya.

Dimensi kelima adalah legitimacy. Dalam sistem politik, penerimaan publik menentukan apakah teknologi dapat digunakan secara berkelanjutan. Sistem yang efisien tetapi tidak dipercaya dapat memicu resistance, litigation, avoidance behavior, dan political backlash. Kepercayaan tidak dibangun melalui slogan AI ethics, melainkan melalui pengalaman konkret: kesalahan diakui, keputusan dapat dipertanyakan, data tidak disalahgunakan, dan pejabat dapat menjelaskan tujuan sistem. Dengan demikian legitimacy merupakan bagian dari performance, bukan faktor eksternal.

Pelajaran dari kasus ini adalah bahwa negara membutuhkan institutional intelligence yang sama besarnya dengan artificial intelligence. Negara harus mampu mengenali risiko teknologi, belajar dari insiden, memperbarui kebijakan, dan menjaga koordinasi lintas kementerian, regulator, militer, industri, akademisi, serta masyarakat sipil. Negara yang hanya membeli teknologi tanpa meningkatkan kapasitas institusional dapat menjadi lebih tergantung dan lebih rapuh. Sebaliknya, negara yang membangun kemampuan evaluasi dapat memperoleh manfaat dari teknologi global tanpa kehilangan kendali strategis.

Kasus E - Krisis Deepfake Politik

Kasus E - Krisis Deepfake Politik menggambarkan situasi di mana menjelang pemilu beredar audio sintesis yang tampak berasal dari seorang pejabat tinggi. Analisis pertama harus membedakan tujuan publik dari instrumen teknis. Tujuan dapat berupa peningkatan pelayanan, pertumbuhan ekonomi, keamanan, atau deterrence. AI hanyalah salah satu cara untuk mencapai tujuan tersebut. Karena itu pertanyaan awal adalah apakah AI memang memberikan comparative advantage dibandingkan prosedur alternatif. Pendekatan ini mencegah technology solutionism, yaitu kecenderungan memilih teknologi karena tersedia, bukan karena terbukti sesuai dengan masalah.

Dimensi kedua adalah provenance, rapid verification, platform response, media literacy, dan institutional credibility. Setiap dimensi mempunyai pemilik risiko yang berbeda. Tim teknis bertanggung jawab pada kualitas sistem; unit kebijakan pada tujuan dan dasar hukum; pimpinan pada risk acceptance; procurement pada vendor; cybersecurity pada resilience; dan oversight bodies pada akuntabilitas. Jika tanggung jawab tidak dipetakan, organisasi mudah mengalami accountability gap: semua pihak terlibat tetapi tidak ada satu pihak yang benar-benar dapat dimintai pertanggungjawaban ketika kegagalan terjadi.

Dimensi ketiga adalah lifecycle. Risiko AI tidak berhenti ketika model selesai diuji. Data berubah, perilaku pengguna berubah, adversary beradaptasi, vendor memperbarui model, dan tujuan organisasi dapat bergeser. Karena itu governance harus berlangsung sejak problem definition, data acquisition, model development, testing, deployment, monitoring, incident response, hingga retirement. Sistem berisiko tinggi sebaiknya memiliki log perubahan, batas penggunaan, indikator drift, jalur eskalasi, dan mekanisme suspend apabila perilakunya tidak lagi sesuai asumsi.

Dimensi keempat adalah human-machine relationship. Human oversight tidak efektif jika manusia hanya berfungsi sebagai stempel pada rekomendasi mesin. Operator membutuhkan waktu, informasi, otoritas, dan pelatihan untuk menolak atau menunda keputusan. Sebaliknya, terlalu banyak intervensi manusia dapat menghilangkan manfaat otomasi. Desain yang baik menentukan titik keputusan mana yang membutuhkan judgment manusia, informasi apa yang harus diperlihatkan, dan bagaimana uncertainty dikomunikasikan. Tujuannya bukan memaksimalkan manusia atau mesin, melainkan mengalokasikan fungsi sesuai kekuatan dan keterbatasannya.

Dimensi kelima adalah legitimacy. Dalam sistem politik, penerimaan publik menentukan apakah teknologi dapat digunakan secara berkelanjutan. Sistem yang efisien tetapi tidak dipercaya dapat memicu resistance, litigation, avoidance behavior, dan political backlash. Kepercayaan tidak dibangun melalui slogan AI ethics, melainkan melalui pengalaman konkret: kesalahan diakui, keputusan dapat dipertanyakan, data tidak disalahgunakan, dan pejabat dapat menjelaskan tujuan sistem. Dengan demikian legitimacy merupakan bagian dari performance, bukan faktor eksternal.

Pelajaran dari kasus ini adalah bahwa negara membutuhkan institutional intelligence yang sama besarnya dengan artificial intelligence. Negara harus mampu mengenali risiko teknologi, belajar dari insiden, memperbarui kebijakan, dan menjaga koordinasi lintas kementerian, regulator, militer, industri, akademisi, serta masyarakat sipil. Negara yang hanya membeli teknologi tanpa meningkatkan kapasitas institusional dapat menjadi lebih tergantung dan lebih rapuh. Sebaliknya, negara yang membangun kemampuan evaluasi dapat memperoleh manfaat dari teknologi global tanpa kehilangan kendali strategis.

Kasus F - Persaingan Teknologi Strategis

Kasus F - Persaingan Teknologi Strategis menggambarkan situasi di mana dua kekuatan besar membatasi akses terhadap chip dan teknologi tertentu sambil memperluas investasi domestik. Analisis pertama harus membedakan tujuan publik dari instrumen teknis. Tujuan dapat berupa peningkatan pelayanan, pertumbuhan ekonomi, keamanan, atau deterrence. AI hanyalah salah satu cara untuk mencapai tujuan tersebut. Karena itu pertanyaan awal adalah apakah AI memang memberikan comparative advantage dibandingkan prosedur alternatif. Pendekatan ini mencegah technology solutionism, yaitu kecenderungan memilih teknologi karena tersedia, bukan karena terbukti sesuai dengan masalah.

Dimensi kedua adalah export controls, supply chains, alliances, industrial policy, dan innovation spillovers. Setiap dimensi mempunyai pemilik risiko yang berbeda. Tim teknis bertanggung jawab pada kualitas sistem; unit kebijakan pada tujuan dan dasar hukum; pimpinan pada risk acceptance; procurement pada vendor; cybersecurity pada resilience; dan oversight bodies pada akuntabilitas. Jika tanggung jawab tidak dipetakan, organisasi mudah mengalami accountability gap: semua pihak terlibat tetapi tidak ada satu pihak yang benar-benar dapat dimintai pertanggungjawaban ketika kegagalan terjadi.

Dimensi ketiga adalah lifecycle. Risiko AI tidak berhenti ketika model selesai diuji. Data berubah, perilaku pengguna berubah, adversary beradaptasi, vendor memperbarui model, dan tujuan organisasi dapat bergeser. Karena itu governance harus berlangsung sejak problem definition, data acquisition, model development, testing, deployment, monitoring, incident response, hingga retirement. Sistem berisiko tinggi sebaiknya memiliki log perubahan, batas penggunaan, indikator drift, jalur eskalasi, dan mekanisme suspend apabila perilakunya tidak lagi sesuai asumsi.

Dimensi keempat adalah human-machine relationship. Human oversight tidak efektif jika manusia hanya berfungsi sebagai stempel pada rekomendasi mesin. Operator membutuhkan waktu, informasi, otoritas, dan pelatihan untuk menolak atau menunda keputusan. Sebaliknya, terlalu banyak intervensi manusia dapat menghilangkan manfaat otomasi. Desain yang baik menentukan titik keputusan mana yang membutuhkan judgment manusia, informasi apa yang harus diperlihatkan, dan bagaimana uncertainty dikomunikasikan. Tujuannya bukan memaksimalkan manusia atau mesin, melainkan mengalokasikan fungsi sesuai kekuatan dan keterbatasannya.

Dimensi kelima adalah legitimacy. Dalam sistem politik, penerimaan publik menentukan apakah teknologi dapat digunakan secara berkelanjutan. Sistem yang efisien tetapi tidak dipercaya dapat memicu resistance, litigation, avoidance behavior, dan political backlash. Kepercayaan tidak dibangun melalui slogan AI ethics, melainkan melalui pengalaman konkret: kesalahan diakui, keputusan dapat dipertanyakan, data tidak disalahgunakan, dan pejabat dapat menjelaskan tujuan sistem. Dengan demikian legitimacy merupakan bagian dari performance, bukan faktor eksternal.

Pelajaran dari kasus ini adalah bahwa negara membutuhkan institutional intelligence yang sama besarnya dengan artificial intelligence. Negara harus mampu mengenali risiko teknologi, belajar dari insiden, memperbarui kebijakan, dan menjaga koordinasi lintas kementerian, regulator, militer, industri, akademisi, serta masyarakat sipil. Negara yang hanya membeli teknologi tanpa meningkatkan kapasitas institusional dapat menjadi lebih tergantung dan lebih rapuh. Sebaliknya, negara yang membangun kemampuan evaluasi dapat memperoleh manfaat dari teknologi global tanpa kehilangan kendali strategis.

40. Kerangka Strategis: POLIS-AI

Untuk merangkum hubungan AI dengan kepentingan negara, artikel ini mengusulkan kerangka POLIS-AI: Purpose, Oversight, Legitimacy, Infrastructure, Security, Artificial Intelligence. PURPOSE berarti setiap sistem AI harus dikaitkan dengan tujuan publik atau keamanan yang spesifik dan dapat dievaluasi. Negara tidak seharusnya mengadopsi AI semata karena tekanan modernisasi. Tujuan harus dinyatakan dalam outcome: pelayanan lebih cepat, fraud berkurang, kesiapan meningkat, biaya turun, atau informasi lebih akurat. Tujuan yang kabur membuka ruang mission creep.

OVERSIGHT berarti keputusan dan sistem harus berada dalam rantai akuntabilitas. Dalam administrasi sipil, oversight dapat melibatkan audit internal, regulator, ombudsman, lembaga perlindungan data, parlemen, pengadilan, dan masyarakat. Dalam pertahanan, sebagian informasi bersifat rahasia, tetapi secrecy tidak identik dengan absence of accountability. Military governance dapat menggunakan legal review, command responsibility, testing authorities, inspector functions, dan parliamentary or executive oversight sesuai sistem negara.

LEGITIMACY berarti AI harus konsisten dengan nilai politik dan hukum yang membuat kekuasaan negara dapat diterima. Negara demokratis memerlukan dasar hukum, proportionality, due process, dan contestability. Dalam kebijakan ekonomi, legitimacy juga berkaitan dengan fairness dalam subsidi, persaingan, dan distribusi manfaat. Dalam pertahanan, legitimacy berkaitan dengan international humanitarian law, rules of engagement, dan prinsip responsible use. Teknologi yang kehilangan legitimacy dapat menurunkan strategic effectiveness karena mengurangi trust dan coalition support.

INFRASTRUCTURE mencakup data, compute, semikonduktor, cloud, jaringan, energi, cybersecurity, dan talenta. Banyak strategi AI gagal karena fokus pada aplikasi tanpa memperhatikan fondasi. Negara perlu memahami dependency map: komponen apa yang diproduksi domestik, apa yang diimpor, vendor mana yang kritis, dan bagaimana gangguan geopolitik memengaruhi availability. Resilience memerlukan redundancy, interoperability, trusted suppliers, dan kemampuan berpindah ketika kondisi berubah.

SECURITY berarti AI harus diperlakukan sebagai target sekaligus alat. Model dapat dicuri, data dapat diracuni, input dapat dimanipulasi, supply chain dapat disusupi, dan sistem dapat dieksploitasi melalui social engineering. Karena itu AI security harus terintegrasi dengan cyber security, physical security, personnel security, dan operational security. Pada sistem pertahanan, threat modeling harus mempertimbangkan bahwa lawan secara aktif mencari cara membuat sistem salah, bukan sekadar bahwa error terjadi secara acak.

ARTIFICIAL INTELLIGENCE sebagai komponen terakhir menegaskan bahwa model tetap penting. Negara membutuhkan kompetensi dalam data science, machine learning, model evaluation, AI engineering, systems integration, dan domain adaptation. Tetapi urutan POLIS-AI sengaja menempatkan AI setelah purpose, oversight, legitimacy, infrastructure, dan security untuk menekankan bahwa sophistication algoritmik tidak cukup. Sebuah model sederhana dalam institusi yang kuat dapat lebih bermanfaat daripada model sangat canggih dalam sistem governance yang lemah.

Kerangka POLIS-AI juga dapat digunakan sebagai checklist sebelum deployment. Apakah tujuan jelas? Siapa pemilik keputusan? Apakah penggunaan sah dan legitimate? Apakah data serta compute cukup? Apakah security risk dinilai? Apakah model telah diuji pada kondisi relevan? Bagaimana manusia mengawasi? Bagaimana insiden dilaporkan? Bagaimana sistem dihentikan? Pertanyaan-pertanyaan tersebut membantu mengubah AI governance dari deklarasi prinsip menjadi proses keputusan.

Pada tingkat nasional, POLIS-AI menunjukkan bahwa strategi AI adalah strategi pembangunan institusi. Kebijakan tidak cukup berhenti pada talent program atau investasi data center. Negara juga membutuhkan procurement reform, data standards, legal capacity, audit professions, public-sector digital leadership, research networks, testing facilities, standards participation, cyber resilience, dan public communication. Keunggulan kompetitif AI pada akhirnya merupakan keunggulan ekosistem.

41. Agenda Strategis Indonesia 2026-2045

Pertama, Indonesia memerlukan integrasi yang lebih kuat antara agenda AI sipil, ekonomi digital, keamanan siber, perlindungan data, dan modernisasi pertahanan. Saat ini berbagai institusi dapat mengembangkan kebijakan berdasarkan mandat masing-masing, tetapi teknologi AI bersifat lintas sektor. Model yang sama dapat digunakan oleh bank, rumah sakit, pemerintah daerah, perusahaan pertahanan, dan lembaga keamanan. Karena itu dibutuhkan common principles, risk taxonomy, standard evaluation, dan mekanisme koordinasi agar standar minimum tidak berbeda secara ekstrem.

Kedua, fondasi data pemerintah harus diperkuat. Interoperabilitas, data quality, metadata, data ownership, access control, dan privacy merupakan prasyarat AI. Tanpa fondasi tersebut, proyek AI akan bergantung pada data ad hoc dan sulit diskalakan. Upaya membangun satu data pemerintah perlu dikaitkan dengan readiness for AI: data tidak hanya tersedia tetapi harus dapat dipercaya, terdokumentasi, aman, dan sesuai tujuan.

Ketiga, Indonesia perlu membangun AI evaluation capability nasional. Kemampuan menggunakan model tersedia secara luas, tetapi kemampuan menilai reliability, bias, robustness, security, hallucination, dan domain suitability lebih langka. Laboratorium evaluasi yang melibatkan pemerintah, universitas, industri, dan lembaga standardisasi dapat membantu procurement dan deployment. Evaluasi khusus bahasa Indonesia dan bahasa daerah juga penting karena performa model global tidak selalu sama pada konteks lokal.

Keempat, kebijakan industri harus fokus pada strategic complementarities. Indonesia tidak harus memproduksi seluruh technology stack, tetapi harus memilih area yang mempunyai economic and strategic leverage. Ini dapat mencakup data center, energy infrastructure, cloud services, local-language AI, applied

AI in natural resources, maritime systems, health, agriculture, logistics, manufacturing, and public services. Kriteria pemilihan sebaiknya mencakup capability spillover, export potential, resilience, dan kebutuhan nasional.

Kelima, perguruan tinggi harus menjadi pusat talent sekaligus pusat critical capability. Pendidikan AI tidak cukup berupa coding. Indonesia membutuhkan ahli machine learning, data engineering, cybersecurity, semiconductors, law, ethics, public policy, military studies, human factors, and management. Interdisciplinary programs menjadi penting karena masalah AI negara tidak dapat diselesaikan satu disiplin. Universitas juga dapat berfungsi sebagai independent evaluator yang menjaga kualitas bukti.

Keenam, penggunaan AI dalam pertahanan perlu dibangun di atas prinsip responsible adoption. Indonesia dapat memanfaatkan AI untuk non-kinetic dan support functions seperti logistics, maintenance, intelligence analysis, simulation, disaster response, maritime domain awareness, and cyber defence, sambil mengembangkan doctrine, testing, legal review, dan human oversight. Pendekatan bertahap membantu organisasi memperoleh pengalaman sebelum menerapkan sistem pada konteks dengan konsekuensi lebih tinggi.

Ketujuh, Indonesia perlu memperkuat public trust. Penggunaan AI dalam pemerintah harus disertai pemberitahuan yang memadai pada konteks berisiko, jalur pengaduan, mekanisme koreksi, dan pengawasan perlindungan data. Warga perlu mengetahui ketika keputusan penting sangat dipengaruhi oleh automated system. Transparansi tidak selalu berarti membuka source code, tetapi setidaknya menjelaskan tujuan, faktor utama, pihak yang bertanggung jawab, dan cara mengajukan keberatan.

Kedelapan, strategi AI nasional perlu memperhitungkan geopolitical risk. Export controls, trade restrictions, cloud policy, supply-chain disruption, dan techno-bloc formation dapat memengaruhi akses teknologi. Indonesia perlu diversified partnerships dan diplomatic engagement agar tidak terlalu tergantung pada satu ekosistem. Politik luar negeri bebas-aktif dapat diterjemahkan dalam teknologi sebagai kemampuan bekerja dengan berbagai mitra sambil menjaga kepentingan nasional dan standar keamanan.

Kesembilan, pengembangan AI harus dihubungkan dengan penciptaan pekerjaan berkualitas dan peningkatan produktivitas. Jika AI hanya meningkatkan keuntungan pada sedikit perusahaan tanpa meningkatkan capability pekerja dan UMKM, dampak pembangunan akan terbatas. Program reskilling, digital extension services, SME upgrading, and sectoral innovation systems perlu menjadi bagian dari strategi. Tujuannya bukan sekadar AI adoption rate, tetapi productivity and welfare outcomes.

Kesepuluh, Indonesia perlu membangun budaya strategic patience. Kompetisi AI sering menciptakan tekanan untuk mengumumkan model, supercomputer, atau proyek besar. Namun kekuatan nasional dibangun melalui investasi konsisten pada pendidikan, penelitian, organisasi, data, cybersecurity, procurement, standards, dan institutions. Keunggulan yang tahan lama tidak berasal dari satu aplikasi viral, melainkan dari kemampuan negara belajar dan memperbaiki diri secara terus-menerus.

Penutup

AI telah menjadi instrumen penting bagi negara karena memperluas kemampuan memahami, memprediksi, mengoordinasikan, dan bertindak. Dalam politik dan tata kelola, AI dapat meningkatkan efisiensi administrasi, membantu analisis kebijakan, memperluas pelayanan publik, serta memperkuat kemampuan mendeteksi risiko. Pada saat yang sama, AI dapat memperbesar surveillance, censorship, manipulation, dan asymmetric informational power. Oleh karena itu pertanyaan politik utama bukan seberapa canggih teknologi negara, tetapi apakah peningkatan kapasitas tersebut dibatasi dan diarahkan oleh hukum, hak, dan mekanisme akuntabilitas.

Dalam ekonomi, AI telah menjadi bagian dari industrial policy dan kompetisi teknologi. Keunggulan tidak hanya ditentukan oleh model terbaik, tetapi oleh kombinasi compute, chips, data, cloud, electricity, talent, research, capital, firms, management, and institutions. Negara yang membangun seluruh ekosistem akan lebih mampu mengubah AI menjadi productivity growth. Bagi negara berkembang, strategi yang realistis bukan meniru setiap komponen frontier, melainkan memilih capability yang memberikan leverage sambil menjaga akses terhadap jaringan global.

Dalam militer, AI dapat meningkatkan situational awareness, logistics, maintenance, cyber defence, simulation, and decision support. Namun manfaat tersebut datang bersama risiko khusus: compressed decision time, adversarial manipulation, automation bias, opaque failure, and escalation. Karena itu military AI membutuhkan testing, verification, validation, legal review, doctrine, human responsibility, dan chain of command yang jelas. Responsible AI bukan hambatan bagi kemampuan militer; ia merupakan cara untuk meningkatkan reliability dan strategic control.

Pada akhirnya, negara yang paling berhasil menggunakan AI mungkin bukan negara yang paling cepat mengotomatisasi segala sesuatu. Keunggulan yang lebih tahan lama muncul ketika teknologi ditempatkan dalam institusi yang mampu belajar, diawasi, memperbaiki kesalahan, dan mempertahankan legitimasi. AI memperbesar kapasitas yang sudah ada. Jika institusi kuat, AI dapat memperkuat pelayanan, pertumbuhan, dan keamanan. Jika institusi lemah atau kekuasaan tidak terkendali, AI dapat memperbesar ketidakadilan dan risiko.

Bagi Indonesia, pilihan strategisnya adalah membangun capable, innovative, secure, and accountable AI state. Ini membutuhkan keseimbangan antara keterbukaan dan kedaulatan, inovasi dan kehati-hatian, efisiensi dan hak, serta keamanan dan demokrasi. AI harus menjadi sarana bagi tujuan nasional, bukan tujuan itu sendiri. Prinsip tersebut penting agar transformasi digital memperkuat manusia, institusi, ekonomi, dan ketahanan bangsa menuju Indonesia 2045.

Satu aspek yang sering diabaikan adalah komunikasi publik mengenai AI negara. Ketika pemerintah menggunakan istilah seperti smart government, predictive analytics, atau autonomous systems, masyarakat dapat menafsirkan kemampuan teknologi secara berlebihan. Komunikasi yang bertanggung jawab perlu menghindari anthropomorphism dan klaim seolah sistem memahami dunia seperti manusia. Pejabat harus menjelaskan bahwa sebagian besar sistem bekerja secara probabilistik, bergantung pada data, dan mempunyai batas konteks. Penjelasan semacam ini penting agar publik tidak memberikan kepercayaan berlebihan maupun ketakutan yang tidak proporsional. Literasi publik menjadi bagian dari governance karena legitimasi teknologi dipengaruhi oleh pemahaman warga terhadap manfaat dan batasnya.

Selain itu, negara perlu membangun mekanisme koordinasi antara innovation speed dan institutional caution. Unit inovasi biasanya didorong bergerak cepat, sedangkan unit hukum, keamanan, audit, dan procurement cenderung bergerak lebih hati-hati. Konflik tersebut tidak harus diselesaikan dengan memilih salah satu. Model governance yang baik menggunakan staged deployment: eksperimen dilakukan pada ruang terbatas dengan data yang sesuai, hasil diukur, risiko dievaluasi, kemudian skala diperluas secara bertahap. Dengan cara ini organisasi memperoleh kecepatan belajar tanpa mengorbankan kontrol. Prinsip tersebut berlaku mulai dari chatbot pelayanan publik sampai decision-support system yang digunakan dalam lingkungan keamanan.

Pada tingkat geopolitik, Indonesia juga perlu aktif dalam pembentukan norma internasional. Negara-negara besar mempunyai kepentingan dan sumber daya untuk memengaruhi standar teknis, definisi responsible AI, export controls, dan aturan data. Negara menengah dapat memperbesar pengaruh melalui koalisi, ASEAN, forum multilateral, standard-setting bodies, serta diplomasi teknologi. Kepentingan Indonesia meliputi akses yang adil terhadap teknologi, keamanan dan perlindungan data, ruang bagi inovasi domestik,

bahasa dan budaya lokal, serta pencegahan penggunaan AI yang meningkatkan ketidakstabilan strategis. Diplomasi AI karena itu perlu melibatkan tidak hanya diplomat, tetapi juga ilmuwan, regulator, militer, pelaku bisnis, dan universitas.

Akhirnya, keberhasilan strategi AI nasional harus dinilai dari outcome, bukan dari jumlah proyek atau besarnya investasi saja. Dalam politik dan pelayanan publik, indikatornya adalah apakah layanan lebih adil, cepat, mudah diakses, dan dapat dipertanggungjawabkan. Dalam ekonomi, indikatornya adalah produktivitas, inovasi, kualitas pekerjaan, kemampuan perusahaan domestik, dan difusi teknologi. Dalam pertahanan, indikatornya adalah readiness, resilience, decision quality, interoperability, dan strategic control. Dengan indikator semacam ini, AI ditempatkan kembali sebagai sarana. Negara tidak mengejar kecerdasan artifisial demi prestise, melainkan menggunakan teknologi secara terukur untuk memperkuat kapasitas manusia dan institusi.

Glossarium

Artificial Intelligence (AI): Sistem komputasional yang melakukan fungsi seperti pengenalan pola, prediksi, pemrosesan bahasa, persepsi, dan dukungan pengambilan keputusan.

Algorithmic governance: Penggunaan algoritma dan sistem data untuk mendukung atau mengotomatisasi fungsi pemerintahan.

Automation bias: Kecenderungan manusia terlalu mempercayai keluaran sistem otomatis.

Autonomous system: Sistem yang dapat melakukan fungsi tertentu dengan tingkat intervensi manusia yang terbatas setelah diaktifkan.

Command and control (C2): Proses dan sistem yang memungkinkan pemimpin mengarahkan, mengoordinasikan, dan mengendalikan operasi.

Compute: Kapasitas komputasi yang digunakan untuk melatih atau menjalankan model AI.

Data governance: Aturan, peran, standar, dan proses untuk mengelola kualitas, akses, keamanan, dan penggunaan data.

Deepfake: Media sintesis atau dimanipulasi dengan AI sehingga tampak atau terdengar autentik.

Deterrence: Upaya mencegah tindakan lawan dengan memengaruhi kalkulasi biaya, manfaat, dan risiko.

Dual-use technology: Teknologi yang memiliki aplikasi sipil dan militer.

Explainability: Kemampuan memberikan penjelasan yang bermakna mengenai cara atau alasan sistem menghasilkan output tertentu.

Human oversight: Pengawasan manusia yang mempunyai informasi dan kewenangan nyata untuk memeriksa, mengoreksi, atau menghentikan sistem.

Industrial policy: Kebijakan negara untuk membentuk struktur, kemampuan, dan daya saing sektor industri.

Information operations: Aktivitas yang berkaitan dengan pengaruh, perlindungan, atau pengelolaan lingkungan informasi dalam konteks strategis.

ISR: Intelligence, Surveillance, and Reconnaissance; kegiatan pengumpulan dan analisis informasi untuk situational awareness.

Meaningful human control: Konsep bahwa manusia tetap memiliki kontrol substansial dan tanggung jawab terhadap keputusan berkonsekuensi penting.

Military AI: Penggunaan AI untuk fungsi pertahanan seperti analisis intelijen, logistik, simulasi, cyber defence, decision support, atau sistem otonom.

Model drift: Penurunan performa model karena lingkungan, data, atau perilaku berubah dari kondisi ketika sistem diuji.

National security: Keamanan negara dan masyarakat terhadap ancaman strategis, militer, siber, ekonomi, atau lainnya.

Provenance: Informasi mengenai asal-usul dan riwayat pembuatan atau perubahan data/konten.

Responsible AI: Pendekatan pengembangan dan penggunaan AI yang memperhatikan reliability, accountability, fairness, traceability, security, dan governance.

State capacity: Kemampuan negara merancang, melaksanakan, dan menegakkan kebijakan serta menyediakan fungsi publik.

Strategic autonomy: Kemampuan mempertahankan pilihan dan tindakan strategis tanpa ketergantungan yang tidak dapat dikelola.

Surveillance: Pengamatan atau pengumpulan informasi sistematis mengenai individu, kelompok, ruang, atau aktivitas.

Technology stack: Rangkaian lapisan teknologi yang menopang sistem AI, termasuk chip, compute, cloud, data, models, software, dan applications.

Verification and validation: Proses memastikan sistem dibangun dengan benar dan sesuai dengan tujuan serta kondisi penggunaannya.

Daftar Pustaka

- Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives*, 33(2), 3–30. <https://doi.org/10.1257/jep.33.2.3>
- Allen, G. C. (2019). Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security. Center for a New American Security.
- Buchanan, B., & Miller, T. (2017). Machine learning for policymakers: What it is and why it matters. Belfer Center for Science and International Affairs.
- Dafoe, A. (2018). AI governance: A research agenda. Centre for the Governance of AI.
- European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.
- Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28, 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36–57.
- Kello, L. (2017). The virtual weapon and international order. Yale University Press.
- NATO. (2021). Summary of the NATO artificial intelligence strategy. North Atlantic Treaty Organization.
- NATO. (2024). Summary of NATO's revised artificial intelligence (AI) strategy. North Atlantic Treaty Organization.

- OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD.
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 33–44. <https://doi.org/10.1145/3351095.3372873>
- Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
- Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton.
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751–752. <https://doi.org/10.1126/science.aat5991>
- UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO.
- U.S. Department of Defense. (2022). Responsible Artificial Intelligence Strategy and Implementation Pathway. Department of Defense.
- U.S. Department of Defense. (2023). Data, Analytics, and Artificial Intelligence Adoption Strategy. Department of Defense.
- U.S. Department of Defense. (2023). Responsible Artificial Intelligence Toolkit. Chief Digital and Artificial Intelligence Office.
- World Bank. (2021). World development report 2021: Data for better lives. World Bank. <https://doi.org/10.1596/978-1-4648-1600-0>
- Zeng, Y., Lu, E., & Huangfu, C. (2019). Linking artificial intelligence principles. Proceedings of the AAAI Workshop on Artificial Intelligence Safety.

Catatan Penulis

Artikel ini ditujukan untuk tujuan akademik dan pendidikan. Pembahasan militer disajikan pada tingkat strategis, kelembagaan, kebijakan, etika, dan tata kelola. Artikel tidak dimaksudkan sebagai panduan operasional. Kebijakan, regulasi, doktrin, dan perkembangan teknologi AI berubah cepat sehingga pembaca perlu merujuk naskah resmi terbaru ketika menggunakan artikel untuk analisis kebijakan.

Lampiran Analitis: Matriks Risiko dan Keputusan AI Negara

Pemanfaatan AI oleh negara dapat dinilai melalui matriks dua dimensi: besarnya dampak keputusan dan tingkat otonomi sistem. Sistem dengan dampak rendah dan otonomi rendah, seperti pencarian dokumen internal atau penyusunan ringkasan, memerlukan kontrol dasar. Sistem dengan dampak tinggi tetapi otonomi rendah, seperti decision support untuk bantuan sosial atau analisis keamanan, membutuhkan validasi lebih ketat karena rekomendasi dapat memengaruhi hak atau keselamatan. Sistem dengan dampak tinggi dan otonomi tinggi memerlukan standar tertinggi karena konsekuensi kesalahan dapat berskala besar dan sulit dipulihkan. Matriks ini membantu mencegah pendekatan one-size-fits-all dalam regulasi maupun procurement.

Dimensi kedua adalah reversibility. Kesalahan chatbot informasi publik dapat diperbaiki relatif cepat, sedangkan kesalahan dalam penegakan hukum, kebijakan kesehatan, atau keamanan nasional dapat meninggalkan dampak yang jauh lebih sulit dibalik. Semakin rendah reversibility suatu keputusan, semakin besar kebutuhan akan human review, dokumentasi, legal basis, dan conservative thresholds. Prinsip ini juga relevan bagi pertahanan. Keputusan yang terkait pemeliharaan aset atau perencanaan logistik memiliki

profil risiko berbeda dari keputusan yang berkaitan dengan penggunaan kekuatan. Governance seharusnya menyesuaikan ketatnya kontrol terhadap irreversibility.

Dimensi ketiga adalah observability. Beberapa kesalahan AI mudah terlihat, misalnya chatbot memberikan jawaban faktual yang salah. Kesalahan lain tersembunyi dalam distribusi statistik: kelompok tertentu secara sistematis menerima skor lebih rendah, wilayah tertentu lebih sering ditandai berisiko, atau jenis ancaman tertentu terabaikan karena data pelatihan tidak representatif. Sistem pemerintah karena itu perlu monitoring yang mampu melihat aggregate effects, bukan hanya insiden individual. Audit fairness, performance by subgroup, drift analysis, dan outcome monitoring dapat menemukan pola yang tidak tampak dalam penggunaan harian.

Dimensi keempat adalah adversarial exposure. Sistem publik yang terbuka menghadapi pengguna yang mungkin mencoba mengeksploitasi kelemahan, sedangkan sistem keamanan menghadapi lawan yang sengaja beradaptasi untuk menipu sensor, data, atau model. Karena itu reliability pada lingkungan benign tidak sama dengan reliability pada lingkungan adversarial. Pertahanan dan keamanan memerlukan threat-informed testing: sistem diuji dengan asumsi adanya aktor yang aktif mencari cara membuatnya gagal. Namun pengujian tersebut harus tetap berada dalam prosedur aman dan tidak menyebarkan teknik operasional yang dapat disalahgunakan.

Dimensi kelima adalah dependency criticality. Bila sebuah sistem AI gagal, apakah fungsi negara masih dapat berjalan? Ketergantungan penuh pada satu model, vendor, cloud, atau jalur konektivitas dapat menciptakan single point of failure. Negara perlu merancang graceful degradation: kemampuan kembali ke mode manual, menggunakan model alternatif, atau mempertahankan fungsi minimum ketika sistem utama terganggu. Konsep ini sangat penting untuk layanan publik kritis dan pertahanan karena resilience sering lebih penting daripada efisiensi maksimum.

Dimensi keenam adalah temporal pressure. AI sering dipromosikan karena dapat mempercepat keputusan. Namun pada situasi krisis, kecepatan dapat menjadi sumber risiko. Sistem yang mendorong pemimpin merespons sebelum informasi diverifikasi dapat meningkatkan kemungkinan miscalculation. Sebaliknya, AI dapat digunakan untuk memperlambat secara cerdas dengan menyaring noise, menampilkan uncertainty, dan mengidentifikasi kebutuhan verifikasi. Desain terbaik bukan selalu fastest decision, melainkan fastest reliable decision yang masih menyediakan ruang bagi judgment ketika stakes tinggi.

Dimensi ketujuh adalah contestability. Dalam negara hukum, warga atau organisasi yang terkena dampak keputusan berisiko tinggi perlu memiliki cara yang nyata untuk mempertanyakan hasil. Contestability membutuhkan penjelasan minimum, identifikasi otoritas yang bertanggung jawab, akses pada proses banding, dan kemampuan manusia untuk menilai kembali kasus. Sistem yang tidak dapat dipertanyakan cenderung mengubah output probabilistik menjadi kekuasaan administratif yang absolut. Karena itu right to contest merupakan komponen penting responsible public-sector AI.

Dimensi kedelapan adalah public-private boundary. Banyak kapabilitas AI terdepan dikembangkan oleh perusahaan swasta, sedangkan negara mempunyai kewenangan publik yang tidak dimiliki perusahaan. Ketika pemerintah menggunakan model komersial, perlu dijelaskan pembagian tanggung jawab: siapa mengontrol data, siapa melakukan update, bagaimana logging dilakukan, siapa bertanggung jawab ketika model berubah, dan bagaimana kontrak menangani security incident. Procurement AI harus berkembang dari pembelian software menjadi governance of continuously changing services.

Dimensi kesembilan adalah international interdependence. Compute, chip fabrication, advanced equipment, cloud services, open-source software, research publications, dan skilled labor tersebar lintas negara. Karena itu bahkan negara besar menghadapi interdependensi. Kebijakan yang terlalu menekankan decoupling dapat menimbulkan biaya inovasi, sedangkan ketergantungan tanpa strategi dapat menciptakan vulnerability. Pendekatan yang lebih seimbang adalah mapping dependencies, identifying critical nodes,

diversifying suppliers, building domestic competence, dan mempertahankan international scientific collaboration pada bidang yang memungkinkan.

Dimensi kesepuluh adalah democratic resilience. AI dapat meningkatkan kemampuan negara merespons disinformasi, tetapi juga dapat digunakan untuk memantau atau mengarahkan opini. Demokrasi membutuhkan kapasitas menghadapi manipulasi tanpa menciptakan kementerian kebenaran yang menentukan seluruh narasi publik. Pendekatan yang lebih sehat mengutamakan transparency, independent fact-checking ecosystems, provenance, media literacy, access to plural information, dan enforcement terhadap tindakan ilegal yang jelas. Tujuannya adalah memperkuat kemampuan warga menilai informasi, bukan mengganti penilaian warga dengan klasifikasi negara.

Dimensi kesebelas adalah institutional memory. Proyek AI sering bergantung pada beberapa orang yang memahami sistem. Ketika mereka pindah, pengetahuan tentang asumsi, limitasi, dan data dapat hilang. Negara perlu dokumentasi model, decision logs, standard operating procedures, training materials, dan communities of practice. Institutional memory menjadi sangat penting karena lifecycle AI panjang dan vendor dapat berganti. Tanpa dokumentasi, organisasi dapat terus menggunakan sistem yang tidak lagi dipahami secara memadai.

Dimensi kedua belas adalah sunset mechanism. Tidak semua sistem AI harus digunakan selamanya. Kondisi kebijakan, data, teknologi, dan risiko dapat berubah. Sistem yang awalnya bermanfaat dapat menjadi tidak relevan atau berbahaya. Karena itu kontrak dan kebijakan sebaiknya memiliki periodic review dan criteria for retirement. Kemampuan menghentikan sistem merupakan tanda maturity, bukan kegagalan. Negara yang mampu menutup program yang tidak efektif menunjukkan bahwa teknologi tetap menjadi alat kebijakan, bukan simbol prestise.

Pada tingkat strategis, matriks risiko ini mengajarkan bahwa AI governance bukanlah usaha mencari satu daftar prinsip universal yang langsung menyelesaikan semua kasus. Governance adalah kemampuan institusi mengklasifikasikan konteks, menetapkan kontrol yang sesuai, dan memperbarui keputusan ketika bukti berubah. Sistem untuk pendidikan, kesehatan, perpajakan, polisi, diplomasi, dan pertahanan mempunyai tujuan dan tingkat risiko berbeda. Common principles tetap penting, tetapi implementation harus sector-specific.

Matriks juga membantu memahami perbedaan antarnegara. Negara dengan rule of law kuat dapat memiliki lebih banyak mekanisme appeal dan judicial review. Negara dengan kapasitas digital tinggi dapat melakukan monitoring lebih detail. Negara dengan ancaman keamanan akut mungkin menerima tingkat secrecy yang lebih besar. Namun tidak ada konteks yang menghapus kebutuhan akuntabilitas. Perbedaannya terletak pada bentuk dan intensitas kontrol, bukan pada apakah kontrol diperlukan sama sekali.

Bagi Indonesia, pendekatan matriks dapat diterapkan dalam procurement pemerintah. Setiap proyek AI dapat dinilai pada impact, autonomy, reversibility, observability, adversarial exposure, dependency, temporal pressure, dan contestability. Skor tersebut dapat menentukan persyaratan minimal: dokumentasi, audit, human review, security testing, privacy assessment, legal review, atau independent evaluation. Dengan demikian kebijakan menjadi lebih konkret daripada hanya meminta semua sistem mematuhi prinsip etika secara umum.

Dalam pertahanan, matriks membantu membangun escalation-aware AI governance. Sistem pendukung logistik dapat diberi ruang otomasi lebih besar daripada sistem yang terhubung dengan keputusan penggunaan kekuatan. Decision support yang menyangkut situasi strategis dapat dirancang untuk menampilkan uncertainty dan competing hypotheses, bukan satu rekomendasi tunggal. Redundancy dapat digunakan agar satu sensor atau model tidak menjadi sumber kebenaran tunggal. Semua pendekatan ini mengurangi risiko bahwa kecepatan komputasional mengalahkan kehati-hatian strategis.

Dalam ekonomi, matriks membantu membedakan critical AI infrastructure dari aplikasi umum. Negara dapat memberikan perhatian khusus pada data center strategis, cloud pemerintah, cyber systems, chip supply, model yang digunakan sektor keuangan atau energi, serta platform dengan skala masyarakat besar. Sementara itu aplikasi productivity berisiko rendah dapat diberi ruang eksperimen lebih luas. Diferensiasi semacam ini mendukung innovation-friendly regulation karena sumber daya pengawasan diarahkan ke area yang paling berisiko.

Secara keseluruhan, matriks risiko menegaskan satu prinsip: semakin besar kemampuan AI mengubah kondisi kehidupan manusia atau keseimbangan kekuasaan, semakin tinggi tuntutan governance. Ini berlaku dalam politik, ekonomi, dan militer. AI yang kuat tidak boleh menjadi alasan mengurangi kontrol; justru kekuatan teknologi meningkatkan kebutuhan pada institusi yang mampu mengarahkan, menguji, dan membatasinya.

Sintesis Akhir

Bila seluruh pembahasan diringkas dalam satu proposisi, AI memperbesar kapasitas negara untuk mengubah informasi menjadi tindakan. Dalam politik, informasi menjadi pelayanan, pengawasan, komunikasi, dan legitimasi. Dalam ekonomi, informasi menjadi produktivitas, inovasi, koordinasi pasar, dan industrial capability. Dalam militer, informasi menjadi situational awareness, kesiapan, keputusan, dan deterrence. Karena itu AI memperkuat karakter dasar negara sebagai organisasi informasi sekaligus organisasi kekuasaan.

Namun kekuatan AI tidak berdiri sendiri. Kapabilitas nasional bergantung pada manusia yang mampu menilai, organisasi yang mampu belajar, infrastruktur yang resilient, data yang dapat dipercaya, perusahaan yang inovatif, universitas yang kuat, regulasi yang legitimate, dan hubungan internasional yang memberi akses sekaligus mengelola ketergantungan. Negara yang hanya mengejar model paling canggih tanpa membangun sistem pelengkap akan menghadapi implementation gap.

Tantangan abad ke-21 adalah memastikan bahwa intelligence advantage tidak berubah menjadi accountability deficit. Kemampuan memprediksi warga tidak boleh menghilangkan hak warga untuk diperlakukan sebagai manusia, bukan sekadar skor. Kemampuan mengotomatisasi keputusan tidak boleh menghapus tanggung jawab pejabat. Kemampuan mempercepat respons militer tidak boleh menghilangkan judgment dan kontrol. Kemampuan memengaruhi informasi tidak boleh menghancurkan kepercayaan publik yang justru menjadi sumber ketahanan nasional.

Dengan demikian strategi AI negara harus menggabungkan tiga tujuan: capability, competitiveness, dan constitutional responsibility. Capability memastikan negara dapat menjalankan fungsi dan melindungi masyarakat. Competitiveness memastikan ekonomi mampu mencipta nilai dalam perubahan teknologi global. Constitutional responsibility memastikan peningkatan kemampuan tetap berada di bawah hukum dan prinsip legitimasi. Ketiganya tidak seharusnya dipertentangkan; negara yang mampu menyeimbangkannya akan memiliki fondasi paling kuat untuk menggunakan AI secara berkelanjutan.

Indonesia memiliki kesempatan membangun modelnya sendiri. Pengalaman negara lain penting sebagai pembandingan, bukan cetak biru. Sistem politik, demografi, geografi kepulauan, struktur ekonomi, kebutuhan pembangunan, dan posisi geopolitik Indonesia menciptakan kebutuhan unik. Fokus pada public service, maritime awareness, disaster response, agriculture, health, education, logistics, cybersecurity, local-language AI, dan industrial upgrading dapat memberi manfaat besar bila dibangun dengan governance yang matang. Dengan pendekatan demikian, AI dapat menjadi sarana memperkuat kapasitas negara tanpa mengorbankan kemanusiaan dan demokrasi.

Rekomendasi Implementasi untuk Pemerintah dan Organisasi Publik

Implementasi AI sebaiknya dimulai dengan inventarisasi use case yang telah dan akan digunakan oleh seluruh lembaga. Inventaris ini tidak cukup berupa daftar aplikasi; setiap sistem perlu mempunyai owner, tujuan, kategori risiko, jenis data, vendor, keputusan yang dipengaruhi, tingkat human oversight, masa penggunaan, serta kontak incident response. Inventarisasi menjadi fondasi governance karena pemerintah tidak dapat mengawasi sistem yang keberadaannya sendiri tidak diketahui secara lengkap. Pendekatan serupa penting ketika unit kerja menggunakan layanan AI publik tanpa proses procurement formal atau tanpa memasukkan sistem tersebut ke arsitektur teknologi organisasi.

Langkah berikutnya adalah membangun tiered assurance. Sistem berisiko rendah dapat melalui self-assessment yang sederhana, sedangkan sistem yang memengaruhi hak, keselamatan, keamanan, atau alokasi sumber daya besar memerlukan independent review. Assurance dapat mencakup data assessment, privacy impact assessment, cyber security review, model evaluation, human-factors testing, legal review, dan operational readiness. Dalam konteks militer, assurance juga harus terhubung dengan doctrine, command authority, dan mission-specific testing. Tujuannya bukan membuat birokrasi baru, tetapi menempatkan kontrol di titik di mana kegagalan paling merugikan.

Pemerintah juga perlu mengembangkan profesi dan kompetensi baru. AI governance membutuhkan penerjemah antara dunia teknis dan dunia kebijakan: pejabat yang memahami machine learning tanpa kehilangan perspektif hukum, manajer yang dapat membaca uncertainty, auditor yang memahami model risk, serta procurement officers yang dapat menilai layanan AI dinamis. Kompetensi tersebut tidak harus selalu berada pada satu jabatan baru; dapat dibangun melalui multidisciplinary teams. Yang penting adalah setiap keputusan besar mempunyai akses pada technical, legal, ethical, security, and domain expertise.

Dalam procurement, kontrak AI perlu memuat kewajiban yang tidak umum pada software tradisional: pemberitahuan perubahan model, lokasi dan perlakuan data, hak audit, logging, incident notification, performance thresholds, exit provisions, portability, intellectual property, dan tanggung jawab vendor. Pemerintah perlu menghindari situasi di mana sistem kritis berubah karena update vendor tanpa evaluation ulang. Procurement juga dapat menjadi instrumen industrial policy dengan mendorong standards, interoperability, cybersecurity, dan keterlibatan perusahaan domestik secara kompetitif.

Terakhir, pemerintah perlu membangun budaya pembelajaran dari insiden. Kesalahan AI tidak boleh selalu disembunyikan karena takut reputasi. Untuk sistem yang tidak terkait informasi rahasia, publikasi incident summaries dapat meningkatkan kepercayaan dan membantu institusi lain belajar. Dalam pertahanan dan keamanan, rincian mungkin harus dibatasi, tetapi mekanisme internal lessons learned tetap penting. Mature AI state bukan negara tanpa kegagalan; ia adalah negara yang menemukan kegagalan lebih cepat, membatasi dampaknya, menjelaskan penyebabnya, dan memperbaiki sistem sebelum masalah berulang.