

AI di Militer

Perang Drone, Keputusan Mesin, dan Jalan Indonesia Menuju
Kemandirian Pertahanan Digital

Onno W. Purbo
onno@indo.net.id
onno@itts.ac.id
Twitter onnowpurbo

Institut Teknologi Tangerang Selatan
OnnoCenter
2026

Lisensi: Karya ini dilisensikan di bawah **Creative Commons Attribution (CC BY) 4.0 International**. Anda bebas menggunakan, membagikan, dan mengadaptasi karya ini untuk tujuan apa pun, termasuk komersial, dengan tetap mencantumkan atribusi yang layak kepada penulis.

Disclaimer: Buku ini disusun untuk tujuan edukasi, dokumentasi, dan refleksi publik berdasarkan sumber-sumber yang dianggap kredibel pada saat penulisan. Penulis telah berupaya menjaga akurasi, namun sangat mungkin masih terdapat kekurangan atau kekeliruan; karena itu, buku ini tidak dimaksudkan sebagai satu-satunya rujukan yang final, dan penulis terbuka terhadap koreksi serta masukan yang membangun.

Kata Pengantar

Alhamdulillahirabbil ‘alamin, puji syukur kehadiran Allah SWT karena atas rahmat dan karunia-Nya buku ini dapat disusun. Penulis juga menyampaikan terima kasih kepada semua pihak yang telah memberi inspirasi, dorongan, dan berbagai masukan dalam proses penulisan buku ini.

Buku ini ditulis karena **AI militer penting dibaca hari ini**. Perang modern tidak lagi hanya ditentukan oleh senjata, tetapi juga oleh **data, drone, sensor, perangkat lunak, dan kecepatan keputusan**. Karena itu, pembahasan AI militer tidak boleh diserahkan hanya kepada militer, teknolog, atau media Barat. Indonesia harus membacanya dengan sudut pandang sendiri, sesuai kebutuhan nasional, kepentingan strategis, dan cita-cita kemandirian bangsa.

Indonesia perlu mulai berpikir lebih serius tentang **perang data, drone, dan keputusan**. Masa depan pertahanan tidak cukup dibangun dengan membeli platform, tetapi harus ditopang oleh kemampuan menguasai data, *mission software*, integrasi sistem, industri teknologi, dan sumber daya manusia. Itulah salah satu alasan utama buku ini ditulis: agar diskusi tentang AI militer menjadi lebih jernih, kritis, dan relevan bagi Indonesia.

Penulis menyadari bahwa buku ini memiliki **keterbatasan sumber**. Banyak informasi tentang AI militer berada di antara fakta resmi, analisis, promosi perusahaan, dan propaganda negara. Karena itu, buku ini disusun dengan komitmen pada **verifikasi** dan sikap **anti-halusinasi**. Buku ini juga ditulis dengan bantuan AI sebagai **alat bantu**, bukan pengganti penulis. Seluruh isi dan tanggung jawab tetap berada pada penulis.

Penulis memohon maaf apabila masih terdapat kekurangan atau kesalahan. Semoga buku ini dapat memberi manfaat dan ikut mendorong **kemajuan bangsa Indonesia**.

Jakarta, April 2026

Penulis

Executive Summary

Pengalaman Ukraina, Iran, dan negara-negara yang berperang menunjukkan satu pelajaran keras: **AI militer bukan lagi proyek masa depan, melainkan inti dari kecepatan keputusan, ketahanan sistem, dan ekonomi perang modern.** Ukraina membuktikan bahwa keunggulan tidak selalu lahir dari platform paling mahal, tetapi dari **integrasi drone murah, data tempur nyata, iterasi cepat dari garis depan ke pabrik, serta kemampuan membuka dan mengolah jutaan citra dan video untuk melatih model dan mempercepat *targeting*, *battlefield awareness*, dan *anti-drone***; bahkan pada 2026 Ukraina membuka akses data tempur bagi sekutu untuk melatih model AI, sementara banyak militer Eropa mulai belajar dari pendekatan itu. Iran memberi pelajaran berbeda tetapi sama pentingnya: **volume, biaya rendah, *resilience*, dan kemampuan tetap menyerang di lingkungan *jamming* sering lebih menentukan daripada teknologi yang paling mewah**; perang terbaru juga mempercepat revolusi *marine drone* dan sistem nirawak murah yang dapat diproduksi massal. Bagi Indonesia, kesimpulannya tegas: **jangan mengejar model terbesar atau simbol teknologi, tetapi bangun ekosistem yang benar-benar *war-ready*** — mulai dari data pertahanan yang rapi dan aman, *mission software*, *command and control*, ISR, *electronic warfare*, *anti-drone*, logistik, maritim, sampai kemampuan uji lapangan dan produksi cepat. Yang harus dikerjakan Indonesia adalah:

1. membangun arsitektur data dan AI pertahanan nasional;
2. menguasai perangkat lunak inti, integrasi sensor, dan edge AI yang tahan gangguan;
3. memperkuat industri drone, elektronik, dan komponen lokal secara bertahap;
4. mereformasi pengadaan agar cepat, adaptif, dan mendorong iterasi;
5. menghubungkan TNI, kampus, BUMN, startup, dan industri swasta dalam satu ekosistem; serta
6. memastikan tata kelola, akuntabilitas manusia, dan kedaulatan data tetap terjaga.

Jika tidak, Indonesia akan terus menjadi pembeli teknologi; jika ya, Indonesia bisa bergerak menuju kemandirian dan kedaulatan pertahanan digital. ([Reuters](#))

Daftar Isi

Kata Pengantar.....	3
Executive Summary.....	4
Daftar Isi.....	5
Metode, Batas Verifikasi, dan Cara Membaca Klaim AI Militer.....	12
Prinsip dasar verifikasi.....	12
Cara membedakan jenis sumber.....	12
1. Fakta resmi.....	12
2. Analisis think tank.....	13
3. Promosi perusahaan.....	13
4. Propaganda negara.....	13
5. Inferensi yang masih diragukan.....	14
Batas verifikasi buku ini.....	14
Cara cepat membaca klaim AI militer.....	14
Mengapa ini penting bagi Indonesia.....	15
Prolog. Dari Hype AI ke Kedaulatan Pertahanan Digital Indonesia.....	16
Mengapa AI di Militer Penting.....	17
Tantangan Indonesia Hari Ini.....	17
Apa yang Harus Dikerjakan Indonesia.....	18
Mandiri dan Berdaulat Bukan Berarti Menutup Diri.....	19
Penutup Prolog.....	19
Bagian I. Kerangka Besar: AI Mengubah Logika Perang.....	20
Bab 1. Dari Revolusi Digital ke AI Militer.....	20
1.1. Dari komputasi, internet, dan data ke AI.....	20
1.2. Mengapa militer tertarik pada AI.....	21
1.3. AI bukan sekadar chatbot.....	22
1.4. Dari otomasi ke keunggulan tempur.....	23
1.5. Pergeseran dari platform ke data, model, dan keputusan.....	24
1.6. Mengapa militer yang lambat membaca perubahan akan tertinggal.....	25
Ringkasan kunci.....	26
Bab 2. OODA Loop, C4ISR, dan Speed of Decision.....	27
2.1. OODA loop sebagai jantung perang modern.....	27
2.2. Dari C2 ke C4ISR.....	28
2.3. ISR dan banjir data.....	29
2.4. Dari melihat ke memahami.....	30
2.5. AI sebagai pengganda kecepatan.....	31
2.6. Mengapa keunggulan tidak lagi hanya di senjata, tetapi di sinkronisasi.....	32
2.7. Bahaya automasi berlebih.....	33
Ringkasan kunci.....	34

Bab 3. Dari Robotik ke Drone Warfare.....	35
3.1. Sejarah singkat UAV dan robotic warfare.....	35
3.2. Dari pesawat tanpa awak ke sistem murah massal.....	36
3.3. ISR, strike, decoy, relay, swarm.....	37
3.4. Mengapa drone murah mengubah ekonomi perang.....	38
3.5. Dari platform mahal ke attritable systems.....	39
3.6. Masa depan perang yang lebih padat, lebih murah, lebih otonom.....	40
Ringkasan kunci.....	40
Bagian II. AI dalam Ekosistem Pertahanan Modern.....	41
Bab 4. AI di Militer Amerika Serikat: Ekosistem, Bukan Produk Tunggal.....	41
4.1. Project Maven dan logika dasar AI pertahanan AS.....	41
4.2. Peran cloud, integrator, dan platform data.....	42
4.3. Frontier model dalam ekosistem pertahanan.....	43
4.4. Anthropic, OpenAI, Palantir, dan negara keamanan nasional.....	44
4.5. Dari eksperimen ke infrastruktur operasional.....	45
4.6. Apa yang bisa dibuktikan dan apa yang harus dicurigai.....	46
Ringkasan kunci.....	47
Bab 5. AI dalam ISR, Command and Control, dan Targeting.....	48
5.1. AI untuk melihat dan menyaring.....	48
5.2. AI untuk menggabungkan data multi-sumber.....	49
5.3. AI untuk prioritas target dan course of action.....	50
5.4. Human-in-the-loop vs human-on-the-loop.....	51
5.5. Risiko false positives dan salah tafsir.....	52
5.6. Mengapa keputusan akhir harus tetap manusia.....	53
Ringkasan kunci.....	54
Bab 6. AI di Luar Medan Tembak: Logistik, Cyber, Maintenance, dan Simulasi.....	55
6.1. Predictive maintenance.....	55
6.2. Logistik prediktif.....	56
6.3. Battle management software.....	57
6.4. AI untuk cyber defense.....	58
6.5. Wargaming dan simulasi.....	59
6.6. Mengapa fungsi non-kinetik sering paling realistis lebih dulu.....	60
6.7. AI sebagai penguat organisasi, bukan hanya senjata.....	61
Ringkasan kunci.....	62
Bagian III. Ukraina: Laboratorium War-Ready AI dalam Kondisi Terbatas.....	63
Bab 7. Ukraina: Dari Korban Invasi ke Ekosistem Defense Tech.....	63
7.1. Mengapa Ukraina menjadi laboratorium perang AI.....	63
7.2. Frontline-driven innovation.....	64
7.3. Startup, bengkel, dan produsen kecil.....	65
7.4. Negara yang belajar sangat cepat.....	66
7.5. Dari improvisasi ke institusionalisasi.....	67
7.6. Mengapa perang memaksa inovasi menjadi praktis.....	68
Ringkasan kunci.....	68
Bab 8. Data Tempur sebagai Aset Strategis Ukraina.....	69

8.1. Video drone, sensor, satelit, dan laporan tempur.....	69
8.2. Data sebagai bahan bakar AI.....	70
8.3. Battlefield awareness dan fusion.....	71
8.4. Mengapa data perang lebih berharga daripada demo laboratorium.....	72
8.5. Politik data, keamanan data, dan nilai industrinya.....	73
Ringkasan kunci.....	74
Bab 9. Industri Drone Ukraina: Murah, Cepat, Tersebar.....	75
9.1. Fast-track procurement.....	75
9.2. Drone murah sebagai tulang punggung tempur.....	76
9.3. FPV, ISR drone, loitering munition, anti-drone.....	77
9.4. EW dan ketahanan terhadap jamming.....	78
9.5. Iterasi cepat dari garis depan ke pabrik.....	79
9.6. Mengapa industri kecil bisa lebih lincah daripada kontraktor besar.....	80
Ringkasan kunci.....	81
Bab 10. Pelajaran Ukraina: Kekuatan, Keterbatasan, dan Relevansi untuk Indonesia....	82
10.1. Kekuatan utama Ukraina.....	82
10.2. Ketergantungan yang masih tersisa.....	83
10.3. Masalah pembiayaan dan scale-up.....	84
10.4. Risiko ketergantungan komponen asing.....	85
10.5. Apa yang relevan untuk Indonesia.....	86
10.6. Apa yang tidak bisa disalin mentah-mentah.....	87
Ringkasan kunci.....	88
Bagian IV. Iran: Ketahanan Asimetris, Volume, dan Otonomi Secukupnya.....	89
Bab 11. Strategi Iran: Murah, Banyak, dan Cukup Efektif.....	89
11.1. Bukan AI paling maju.....	89
11.2. Drone sebagai alat saturasi.....	90
11.3. Volume vs presisi.....	91
11.4. Menekan lawan lewat biaya rendah.....	92
11.5. Produksi massal dan tekanan psikologis.....	93
11.6. Mengapa “cukup baik” bisa sangat berbahaya.....	94
Ringkasan kunci.....	94
Bab 12. AI dan Otonomi dalam Model Perang Iran.....	95
12.1. Otonomi dasar dalam kondisi jamming.....	95
12.2. Navigasi, terminal guidance, dan ketahanan misi.....	96
12.3. Serangan berlapis dan swarm sederhana.....	96
12.4. Komando yang tahan dipukul.....	97
12.5. AI sebagai penguat strategi asimetris, bukan pusat segalanya.....	98
Ringkasan kunci.....	98
Bab 13. Pelajaran Iran: Resilience Lebih Penting daripada Kemewahan.....	99
13.1. Murah tidak berarti primitif.....	99
13.2. Robustness lebih penting daripada spesifikasi tertinggi.....	100
13.3. Mengapa Indonesia perlu belajar soal resilience.....	101
13.4. Apa yang berbahaya bila Indonesia salah membaca Iran.....	102
13.5. Pelajaran yang harus diambil tanpa meniru politiknya.....	103

Ringkasan kunci.....	103
Bagian V. Indonesia: Mengapa Tertinggal, dan Apa yang Harus Diubah.....	104
Bab 14. Titik Lemah Indonesia Hari Ini.....	104
14.1. Terlalu platform-centric.....	104
14.2. Lemah di elektronik pertahanan.....	105
14.3. Lemah di mission software dan data pipeline.....	106
14.4. Pengadaan lambat, prototipe banyak, produksi sedikit.....	107
14.5. Kampus kuat di riset, lemah di transisi ke operasi.....	108
14.6. Industri terfragmentasi.....	109
14.7. Supply chain sebagai titik rapuh strategis.....	110
Penutup Bab: diagnosis yang keras tetapi berguna.....	111
Ringkasan kunci.....	111
Bab 15. Doktrin Indonesia yang Seharusnya: Archipelagic, Networked, Attributable.....	112
15.1. Indonesia harus berangkat dari geografi.....	112
15.2. Negara kepulauan butuh maritime domain awareness.....	113
15.3. Drone udara, laut, dan darat untuk pulau-pulau terluar.....	114
15.4. Pertahanan choke points, pangkalan, dan jalur logistik.....	115
15.5. EW, radar, AIS, satelit, dan AI edge sebagai satu ekosistem.....	116
15.6. Mengapa Indonesia tidak boleh meniru mentah-mentah AS, China, Ukraina, atau Iran.....	117
Penutup Bab: rumusan doktrin yang lebih masuk akal.....	118
Ringkasan kunci.....	118
Bab 16. Apa Itu War-Ready AI versi Indonesia.....	119
16.1. Bukan model terbesar.....	119
16.2. Bukan pula sekedar senjata otonom.....	120
16.3. AI untuk ISR, C2, logistik, EW, anti-drone, dan maritim.....	121
a. AI untuk ISR.....	121
b. AI untuk C2 dan decision support.....	121
c. AI untuk logistik dan maintenance.....	121
d. AI untuk EW dan anti-drone.....	122
e. AI untuk maritim.....	122
16.4. AI edge yang tahan gangguan.....	123
16.5. Sistem yang bisa bekerja saat supply chain terganggu.....	124
16.6. Definisi operasional war-ready AI untuk Indonesia.....	125
Indikator minimum war-ready AI Indonesia.....	125
Rumusan paling singkat.....	126
Penutup Bab: ukuran keberhasilan yang benar.....	126
Bagian VI. Tahapan Indonesia Mengejar Ketinggalan.....	127
Bab 17. Tahap 1: 0–3 Tahun — Bertahan, Belajar, dan Membuat yang Mendesak.....	127
17.1. Jalur cepat pengadaan drone/AI/EW.....	127
17.2. Program nasional autopilot, radio, dan mission computer.....	128
17.3. Fokus pada drone kecil taktis dan counter-drone.....	129
17.4. Pusat data drone dan simulasi tempur.....	130
17.5. Unit operasional sebagai co-developer.....	131

17.6. Latihan GPS-denied dan EW sejak awal.....	132
17.7. Target realistis tiga tahun pertama.....	133
Target minimum tiga tahun pertama.....	133
Target yang jangan dipaksakan di tiga tahun pertama.....	133
Penutup Bab: tiga tahun pertama bukan masa keajaiban, tetapi masa pembentukan watak.....	134
Bab 18. Tahap 2: 3–7 Tahun — Kuasai Elektronik, Integrasi, dan Produksi Rendah Volume.....	135
18.1. PCB ruggedized, power electronics, dan battery systems.....	135
18.2. RF module, crypto, mesh network.....	136
18.3. Camera stack, inertial module, anti-jam navigation.....	137
18.4. Reference design nasional dari kampus dan industri.....	138
18.5. Test range swarm, EW, maritime autonomy.....	139
18.6. Kontrak kecil tapi nyata untuk startup dan vendor lokal.....	140
18.7. Dari prototipe ke produksi awal.....	141
Penutup Bab: Tahap 2 adalah ujian kedewasaan teknis.....	142
Bab 19. Tahap 3: 7–15 Tahun — Mass Autonomy dan Kedaulatan Elektronik Bertahap.....	143
19.1. Design-first strategy, bukan fab-first fantasy.....	143
19.2. ASIC, FPGA, dan mission systems.....	144
19.3. Drone udara-laut-darat yang interoperable.....	145
19.4. Arsenal digital nasional.....	146
19.5. Stockpile komponen kritis dan desain modular.....	147
19.6. Industrial resilience menghadapi cut-off supply chain.....	148
19.7. Dari ketergantungan ke kemandirian bertahap.....	149
Tahap awal.....	149
Tahap menengah.....	149
Tahap lebih matang.....	149
Penutup Bab: Mass autonomy bukan jumlah semata.....	150
Bagian VII. Kampus, Industri, dan Negara: Siapa Harus Mengerjakan Apa.....	151
Bab 20. Peran Kampus: Dari Publikasi ke Reference Design.....	151
20.1. Kampus teknik harus fokus ke apa.....	151
20.2. Chip design, embedded systems, RF, radar, control, vision.....	152
Mengapa enam bidang ini penting.....	152
20.3. Kenapa kampus perlu menghasilkan desain yang bisa diproduksi.....	153
20.4. TRL, spin-off, lisensi, dan pengujian.....	154
20.5. Kurikulum autonomy, AI militer, dan EW.....	155
20.6. Bahaya bila kampus hanya mengejar jurnal.....	156
Bahayanya.....	156
Penutup Bab: kampus sebagai pabrik desain strategis.....	157
Bab 21. Peran Industri Nasional: Dari Vendor ke Mitra Strategis.....	158
21.1. BUMN tidak cukup sendirian.....	158
21.2. Startup dan UKM teknologi harus masuk.....	159
21.3. Produksi massal murah sebagai sasaran.....	160
21.4. Repair, maintenance, dan substitusi komponen.....	161

21.5. Pentingnya standarisasi terbuka terbatas.....	162
21.6. Dari proyek ke kapasitas industri berkelanjutan.....	163
Penutup Bab: industri nasional harus menjadi mesin ketahanan.....	164
Bab 22. Peran Negara dan TNI: Pengarah, Penguji, dan Pembeli Pertama.....	165
22.1. Negara sebagai pembentuk pasar.....	165
22.2. TNI sebagai pengguna dan sumber umpan balik.....	166
22.3. Kemhan sebagai arsitek ekosistem, bukan hanya pembeli.....	167
22.4. Perlunya pusat uji nasional.....	168
22.5. Pendanaan inovasi pertahanan yang cepat.....	169
22.6. Mengapa birokrasi lama harus dipotong.....	170
Penutup Bab: negara dan TNI adalah pengungkit utama.....	171
Bagian VIII. Tata Kelola, Etika, dan Batas Penggunaan.....	172
Bab 23. Responsible Military AI: Kendali Manusia, Akuntabilitas, dan Kepercayaan....	172
23.1. Mengapa etika bukan ornamen.....	172
23.2. Meaningful human control.....	173
23.3. Appropriate levels of judgment and care.....	174
23.4. Explainability, auditability, traceability.....	175
23.5. Tanggung jawab jika sistem salah.....	176
23.6. Mengapa militer butuh AI yang bisa dipercaya, bukan hanya cepat.....	177
Penutup Bab: kepercayaan adalah bagian dari daya tempur.....	178
Bab 24. Hukum, Risiko Sipil, dan Masa Depan Konflik.....	179
24.1. IHL dan tantangan AI.....	179
24.2. Targeting, proportionality, dan distinction.....	180
24.3. Salah sasaran dan dampak sipil.....	181
24.4. Risiko eskalasi, spoofing, dan deception.....	182
24.5. Masa depan hubungan negara, perusahaan, dan perang.....	183
24.6. Mengapa Indonesia perlu aturan operasional sejak dini.....	184
Penutup Bab: hukum bukan rem kemajuan, tetapi rem terhadap bencana.....	185
Penutup.....	186
Bab 25. Penutup: Indonesia Tidak Bisa Lagi Menjadi Penonton.....	186
25.1. AI militer adalah soal organisasi, bukan sekadar algoritma.....	186
25.2. Ukraina menunjukkan pentingnya loop belajar cepat.....	187
25.3. Iran menunjukkan pentingnya resilience dan volume.....	188
25.4. Indonesia harus mulai dari yang bisa dibuat, diuji, dan diproduksi.....	189
25.5. Bukan mengejar yang paling canggih, tetapi yang paling berguna.....	190
25.6. Pertanyaan terakhir: siapa yang berani memulai sekarang?.....	191
Penutup akhir.....	192
Lampiran 1. Kronologi Singkat 2016–2026: AI, Maven, Ukraina, Iran, dan Perang Drone	193
Lampiran 2. Matriks Aktor: negara, militer, integrator, startup, kampus, industri.....	198
Matriks hubungan antar aktor.....	201
Lampiran 3. Matriks Risiko: teknis, operasional, etis, hukum, geopolitik, supply chain..	203
Matriks ringkas: tingkat prioritas risiko untuk Indonesia.....	207

Lampiran 4. Metodologi Verifikasi Sumber dan Anti-Halusinasi.....	209
Glossary.....	213
Referensi.....	218
Tentang Penulis.....	224

Metode, Batas Verifikasi, dan Cara Membaca Klaim AI Militer

Pembahasan AI militer sangat mudah terjebak dalam *hype*, promosi, atau propaganda. Karena itu, bagian ini penting: pembaca harus bisa membedakan **mana fakta, mana analisis, mana promosi, mana propaganda**, dan **mana dugaan yang masih lemah**. Tanpa disiplin ini, pembahasan AI militer akan cepat berubah menjadi pengulangan slogan, bukan pengetahuan yang berguna.

Dalam isu pertahanan, tidak semua klaim bisa diterima mentah-mentah. Ada teknologi yang memang sudah dipakai di lapangan. Ada yang baru diuji coba. Ada juga yang sebenarnya hanya bahasa pemasaran. Karena itu, buku ini memakai satu prinsip sederhana: **yang dinilai bukan bunyi klaimnya, tetapi bukti, fungsi, dan relevansinya**.

Prinsip dasar verifikasi

Beberapa prinsip yang dipakai dalam buku ini adalah:

- **Pisahkan fakta dari tafsir.**
Fakta adalah hal yang bisa ditunjukkan sumbernya. Tafsir adalah cara kita membaca arti strategis dari fakta itu.
- **Lihat fungsi operasionalnya.**
Jangan terpukau istilah seperti *AI-enabled*, *autonomous*, atau *smart*. Tanyakan: ini dipakai untuk apa? ISR, komando, logistik, *anti-drone*, atau hanya tampak canggih di presentasi?
- **Bedakan uji coba dan kemampuan nyata.**
Sistem yang berhasil di laboratorium belum tentu siap dipakai di perang.
- **Jangan menyimpulkan terlalu jauh.**
Jika bukti hanya menunjukkan bantuan analisis data, jangan langsung ditulis seolah mesin sudah mengambil keputusan tempur sendiri.
- **Silangkan sumber bila mungkin.**
Klaim yang penting sebaiknya dicek ke lebih dari satu sumber.

Cara membedakan jenis sumber

1. Fakta resmi

Sumber resmi berasal dari pemerintah, militer, dokumen strategi, anggaran, atau kontrak. Ini penting untuk melihat arah kebijakan dan program yang benar-benar diakui negara.

Tetapi ada batasnya. **Dokumen resmi tidak otomatis membuktikan keberhasilan di lapangan**. Ia menunjukkan niat, struktur, atau prioritas, tetapi belum tentu menunjukkan hasil.

Tanda utamanya:

- berasal dari lembaga resmi,
- tanggal dan konteksnya jelas,
- ada detail program, aturan, atau anggaran.

2. Analisis think tank

Sumber ini berguna untuk membaca makna strategis. Ia membantu menjelaskan mengapa sebuah teknologi penting, apa dampaknya, dan bagaimana membacanya dalam kompetisi militer.

Tetapi tetap harus diingat: **analisis adalah tafsir**, bukan fakta mentah.

Gunanya terutama untuk:

- membaca tren,
- membandingkan antarnegara,
- memahami implikasi strategis.

3. Promosi perusahaan

Vendor dan perusahaan teknologi sering memakai bahasa besar untuk menjual sistem mereka. Kata-kata seperti *revolutionary*, *battle-ready*, atau *decision dominance* harus dibaca hati-hati.

Promosi perusahaan tetap berguna, tetapi hanya untuk melihat:

- apa yang sedang dijual,
- arah pasar,
- posisi perusahaan.

Yang harus ditanya:

- apa buktinya?
- siapa yang menguji?
- apakah sudah dipakai nyata, atau baru demo?

4. Propaganda negara

Negara juga memakai narasi teknologi untuk membangun citra kekuatan, menakut-nakuti lawan, atau mempengaruhi opini publik. Karena itu, klaim negara harus dibaca dengan hati-hati, terutama bila bahasanya terlalu mutlak dan terlalu heroik.

Ciri umumnya:

- klaim sangat besar,
- detail teknis minim,
- bukti independen lemah,
- bahasanya emosional atau absolut.

5. Inferensi yang masih diragukan

Kadang data publik tidak lengkap. Dalam kondisi seperti itu, kita boleh membuat dugaan yang masuk akal. Tetapi dugaan harus tetap ditulis sebagai **kemungkinan**, bukan kepastian.

Bahasa yang sehat misalnya:

- “ini mengindikasikan...”
- “kemungkinan menunjukkan...”
- “ada alasan untuk menduga...”

Batas verifikasi buku ini

Buku ini juga punya batas yang harus dijelaskan dengan jujur.

- **Tidak semua kemampuan militer bisa diketahui publik.**
- **Tidak semua klaim bisa diverifikasi penuh.**
- **Tidak semua program yang diumumkan berarti sudah berhasil.**
- **Tidak semua AI militer berarti LLM atau chatbot.**

Karena itu, buku ini berusaha menulis secara hati-hati: **apa yang sudah jelas dibuktikan, apa yang masih terbatas, dan apa yang masih berupa dugaan.**

Cara cepat membaca klaim AI militer

Setiap kali menemukan klaim tentang AI militer, gunakan pertanyaan berikut:

- **Sumbernya siapa?**
Pemerintah, media, perusahaan, atau analis?
- **Statusnya apa?**
Masih riset, uji coba, pilot, atau sudah operasional?
- **Fungsinya apa?**
Untuk ISR, komando, logistik, *cyber*, *EW*, atau *anti-drone*?
- **Buktinya apa?**
Ada dokumen, kontrak, penggunaan nyata, atau hanya pernyataan?
- **Siapa yang diuntungkan dari narasi itu?**
Vendor, negara, media, atau aktor politik tertentu?

Mengapa ini penting bagi Indonesia

Bagi Indonesia, kemampuan membaca klaim AI militer secara jernih adalah bagian dari strategi nasional. Indonesia tidak boleh membangun pertahanan berdasarkan *hype*, promosi vendor, atau ketakutan sesaat. Yang diperlukan adalah penilaian yang tenang dan keras: **apa yang benar-benar berguna, apa yang bisa diproduksi, apa yang bisa dirawat, dan apa yang bisa dikendalikan sendiri.**

Karena itu, disiplin verifikasi ini penting agar Indonesia tidak hanya menjadi pasar teknologi, tetapi benar-benar bergerak menuju **kemandirian** dan **kedaulatan pertahanan digital**.

Prolog. Dari Hype AI ke Kedaulatan Pertahanan Digital Indonesia

Ada masa ketika kekuatan militer diukur terutama dari jumlah tank, kapal, pesawat tempur, dan rudal. Masa itu belum sepenuhnya berakhir, tetapi medan persaingan telah berubah. Hari ini, kekuatan militer semakin ditentukan oleh **siapa yang lebih cepat melihat, lebih tepat memahami, lebih cepat memutuskan, dan lebih efektif bertindak**. Di titik inilah *artificial intelligence* atau AI menjadi sangat penting. AI bukan sekadar teknologi tambahan. AI mulai menjadi bagian dari logika baru peperangan.

Masalahnya, AI militer sering dipahami secara keliru. Sebagian orang membayangkannya hanya sebagai chatbot canggih berseragam. Sebagian lain langsung mengaitkannya dengan robot pembunuh yang sepenuhnya otonom. Kedua cara pandang ini terlalu sempit. Dalam praktik pertahanan modern, AI jauh lebih luas dari itu. AI hadir dalam pemrosesan citra drone, analisis video, penyaringan sinyal, penggabungan data dari banyak sensor, dukungan keputusan di ruang komando, pemeliharaan prediktif, logistik, *electronic warfare*, *anti-drone*, sampai penguatan ketahanan sistem saat komunikasi terganggu.

Karena itu, inti AI militer bukan pertama-tama soal “mesin menggantikan manusia.” Intinya adalah **membantu negara dan militer bekerja lebih cepat, lebih presisi, lebih hemat, dan lebih tahan terhadap guncangan**. Negara yang mampu memanfaatkan AI dengan benar akan memiliki keunggulan dalam *situational awareness*, kecepatan keputusan, efisiensi operasi, dan kemampuan belajar dari pengalaman tempur. Negara yang gagal memahaminya akan sibuk membeli simbol teknologi, tetapi tetap tertinggal dalam kemampuan nyata.

Bagi Indonesia, pertanyaan tentang AI militer bukan pertanyaan teoritis. Ini adalah pertanyaan strategis. Indonesia adalah negara kepulauan yang luas, dengan ruang laut besar, jalur logistik panjang, wilayah perbatasan yang tersebar, dan ancaman yang semakin kompleks. Dalam konteks seperti itu, Indonesia tidak cukup hanya mengandalkan platform mahal dan sistem impor. Indonesia membutuhkan **arsitektur pertahanan yang cerdas, terhubung, adaptif, murah dioperasikan, dan bisa terus berjalan meskipun rantai pasok terganggu**. Dengan kata lain, Indonesia membutuhkan jalan menuju **kemandirian pertahanan digital**.

Yang harus dipahami sejak awal adalah bahwa **AI militer bukan kemewahan**, melainkan kebutuhan strategis. Tanpa AI, militer modern akan tenggelam dalam banjir data. Drone, radar, satelit, kamera, sinyal komunikasi, logistik, dan laporan lapangan menghasilkan informasi dalam volume yang terlalu besar untuk diproses secara manual. Dalam situasi seperti itu, yang menang bukan selalu yang punya senjata paling mahal, tetapi yang punya *decision loop* paling cepat dan paling jernih.

Mengapa AI di Militer Penting

Ada beberapa alasan mendasar mengapa AI kini menjadi begitu penting dalam dunia militer:

- **AI mempercepat siklus keputusan.**
Dalam perang modern, keunggulan sering lahir dari kemampuan memperpendek jarak antara sensor dan respons.
- **AI membantu menyaring banjir data.**
Tanpa bantuan sistem cerdas, terlalu banyak informasi justru bisa melumpuhkan pengambilan keputusan.
- **AI meningkatkan efisiensi operasi.**
Bukan hanya di medan tembak, tetapi juga dalam logistik, pemeliharaan, simulasi, dan pertahanan siber.
- **AI memperkuat ketahanan sistem.**
Dalam kondisi *jamming*, gangguan komunikasi, atau keterbatasan personel, AI dapat membantu sistem tetap bekerja.
- **AI mengubah ekonomi perang.**
Kombinasi drone murah, sensor, perangkat lunak misi, dan analitik data dapat menghasilkan efek strategis besar dengan biaya yang jauh lebih rendah dibanding platform konvensional.
- **AI menjadi pembeda dalam kompetisi negara.**
Negara yang menguasai data, model, integrasi sistem, dan produksi teknologi akan lebih siap menghadapi konflik masa depan.

Namun penting ditegaskan: **AI tidak boleh dibaca hanya sebagai alat tempur.** AI juga adalah persoalan industri, pendidikan, riset, tata kelola, regulasi, *supply chain*, dan kapasitas negara. Karena itu, pembicaraan tentang AI militer tidak boleh diserahkan hanya kepada teknolog, militer, atau vendor. Ini adalah isu strategis nasional.

Tantangan Indonesia Hari Ini

Indonesia memiliki potensi, tetapi juga menghadapi kelemahan yang tidak kecil. Kita masih terlalu sering berpikir dalam logika pembelian platform, bukan pembangunan ekosistem. Kita lebih mudah membeli alat daripada membangun kemampuan desain, integrasi, perangkat lunak misi, data pipeline, sensor, dan elektronik pertahanan. Akibatnya, banyak proyek berhenti pada prototipe, presentasi, atau demonstrasi, tetapi tidak tumbuh menjadi sistem operasional yang matang.

Sejumlah persoalan besar yang harus diakui secara jujur adalah:

- **Ketergantungan tinggi pada komponen dan sistem asing.**
- **Lemahnya industri elektronik pertahanan nasional.**
- **Terbatasnya kemampuan *mission software* dan integrasi data.**
- **Proses pengadaan yang lambat dan kurang adaptif.**
- **Keterputusan antara kampus, industri, dan kebutuhan operasi.**
- **Belum kuatnya arsitektur nasional untuk drone, *anti-drone*, dan AI pertahanan.**
- **Rapuhnya *supply chain* untuk komponen strategis.**

Kalau kelemahan ini tidak diatasi, Indonesia akan terus menjadi pasar bagi teknologi pertahanan luar. Kita mungkin terlihat modern di permukaan, tetapi sesungguhnya rapuh di dalam. Dalam krisis nyata, ketergantungan seperti ini bisa menjadi titik lemah yang sangat berbahaya.

Apa yang Harus Dikerjakan Indonesia

Karena itu, agenda Indonesia tidak boleh berhenti pada ambisi besar di atas kertas. Yang dibutuhkan adalah langkah yang konkret, realistis, dan bertahap. Fokusnya bukan memburu model AI terbesar, melainkan membangun **AI yang berguna, tahan gangguan, bisa diproduksi, dan cocok untuk kebutuhan Indonesia.**

Beberapa hal yang harus dikerjakan Indonesia adalah:

- **Membangun AI pertahanan yang berorientasi fungsi, bukan sekadar pencitraan.**
Prioritas awal harus diarahkan pada ISR, *command and control*, logistik, *electronic warfare*, *anti-drone*, dan operasi maritim.
- **Membangun ekosistem data pertahanan.**
AI tidak akan berguna tanpa data yang rapi, aman, terintegrasi, dan dapat dipakai untuk latihan, pengujian, dan operasi.
- **Menguasai *mission software* dan integrasi sistem.**
Kedaulatan tidak cukup dicapai dengan merakit perangkat keras. Indonesia harus mampu mengendalikan perangkat lunak inti yang menjalankan operasi.
- **Memperkuat industri drone nasional.**
Yang dibutuhkan bukan hanya drone untuk pameran, tetapi drone yang murah, dapat diproduksi, mudah diperbaiki, tahan terhadap gangguan, dan relevan untuk operasi kepulauan.
- **Memperkuat kemampuan elektronik dan semikonduktor secara bertahap.**
Tanpa penguasaan elektronik, ketahanan pertahanan digital akan selalu rapuh.
- **Mereformasi model pengadaan pertahanan.**
Pengadaan harus memungkinkan iterasi cepat, uji lapangan, perbaikan terus-menerus, dan transisi dari prototipe ke produksi.

- **Menghubungkan kampus, industri, dan pengguna akhir.**
Kampus tidak cukup berhenti pada publikasi. Industri tidak cukup menjadi vendor. TNI tidak cukup menjadi pembeli. Ketiganya harus menjadi bagian dari ekosistem pembelajaran nasional.
- **Menyiapkan talenta nasional.**
Indonesia memerlukan insinyur, pengembang perangkat lunak, analis data, perancang sistem, operator drone, ahli *cyber defense*, dan pengambil kebijakan yang benar-benar memahami AI pertahanan.
- **Membangun tata kelola yang bertanggung jawab.**
Penggunaan AI militer harus tetap berada dalam kendali manusia, akuntabel, dapat diaudit, dan patuh pada hukum.
- **Menjadikan ketahanan *supply chain* sebagai agenda strategis.**
Dalam perang atau krisis, negara tidak bisa menggantungkan seluruh komponen kritis pada pihak luar.

Mandiri dan Berdaulat Bukan Berarti Menutup Diri

Kemandirian pertahanan digital tidak berarti Indonesia harus mengerjakan semuanya sendirian sejak awal. Kemandirian berarti **mampu menentukan arah sendiri, menguasai komponen inti, memahami sistem yang dipakai, dan tidak lumpuh ketika akses luar terganggu**. Kedaulatan berarti negara memiliki kendali atas data, perangkat lunak, arsitektur, dan keputusan strategisnya sendiri.

Karena itu, kerja sama internasional tetap penting. Aliansi riset, transfer teknologi, lisensi, dan kolaborasi industri tetap dapat dimanfaatkan. Tetapi semua itu harus diarahkan untuk memperkuat kapasitas nasional, bukan memperdalam ketergantungan. Indonesia harus belajar bekerja sama tanpa kehilangan kendali.

Penutup Prolog

Pada akhirnya, pembahasan tentang AI militer bukan semata soal teknologi baru. Ini adalah soal **masa depan kedaulatan, ketahanan nasional, dan kemampuan Indonesia untuk tidak selalu berada di posisi penonton**. Di era perang data, drone, sensor, dan keputusan mesin, negara yang tidak membangun kapasitas sendiri akan mudah didikte oleh negara dan industri lain.

Karena itu, tugas Indonesia hari ini bukan mengejar sensasi teknologi, melainkan membangun fondasi yang kokoh: **data, perangkat lunak, elektronik, drone, integrasi sistem, SDM, industri, dan tata kelola**. Dari sanalah lahir pertahanan digital yang benar-benar mandiri. Dari sanalah kedaulatan tidak hanya diucapkan, tetapi diwujudkan.

AI di militer harus dibaca bukan sebagai mode, melainkan sebagai medan baru perebutan kekuatan. Dan bila Indonesia ingin tetap berdaulat di abad ini, maka pembangunan kemampuan AI pertahanan tidak bisa ditunda terlalu lama.

Bagian I. Kerangka Besar: AI Mengubah Logika Perang

Bab 1. Dari Revolusi Digital ke AI Militer

AI militer harus dibaca **bukan sebagai mode teknologi**, tetapi sebagai perubahan dalam cara negara melihat, memahami, memutuskan, dan bertindak di medan perang. Bagian ini fondasi sebelum masuk ke OODA, C4ISR, *drone warfare*, Ukraina, Iran, dan strategi Indonesia. Fokus itu tepat, karena tanpa kerangka besar ini, diskusi AI militer mudah terjebak antara euforia dan ketakutan.

1.1. Dari komputasi, internet, dan data ke AI

AI militer tidak lahir mendadak dari kemunculan *chatbot*. Ia tumbuh dari revolusi yang lebih panjang: komputasi, jaringan, sensor, miniaturisasi elektronik, internet, *cloud*, dan ledakan data. *The AI Wave in Defence Innovation* menegaskan bahwa AI militer adalah bagian dari **konvergensi teknologi** yang lebih luas—AI/ML, *cloud connectivity*, IoT, 5G, *edge processing*, dan sistem nirawak—yang bersama-sama mengubah cara militer mengumpulkan, memproses, dan memakai informasi.

Pada tahap awal, komputasi militer dipakai terutama untuk kalkulasi, komunikasi, dan otomasi prosedur. Internet dan jaringan digital lalu mengubah struktur komando: informasi tidak lagi bergerak lambat dari satu meja ke meja lain, tetapi dapat mengalir lintas unit dan lintas domain hampir secara *real time*. Ketika sensor makin murah dan melimpah—kamera drone, radar, SIGINT, satelit, telemetry—masalah utamanya bukan lagi kekurangan data, melainkan **kelebihan data**. Karena itu DoD Data Strategy 2020 secara eksplisit menegaskan visi DoD sebagai organisasi yang *data-centric* yang memakai data “at speed and scale” untuk keunggulan operasional. ([U.S. Department of War](#))

Di sinilah perubahan penting terjadi. Dalam era industri, keunggulan militer sering diukur dari jumlah platform: kapal, tank, pesawat, meriam. Dalam era digital, platform tetap penting, tetapi nilainya makin ditentukan oleh kemampuannya masuk ke dalam jaringan data. Sebuah drone, radar, kapal, atau baterai pertahanan udara tidak lagi berdiri sendiri; semuanya menjadi *node* dalam ekosistem sensor–data–keputusan–tindakan. Karena itu, AI tidak boleh dipisahkan dari arsitektur data. Tanpa data yang baik, AI hanyalah lapisan tipis di atas sistem yang tetap buta. ([U.S. Department of War](#))

Intinya:

- **AI militer lahir dari revolusi digital yang panjang, bukan dari LLM semata.**
- **Data menjadi aset strategis, bukan produk sampingan operasi.**
- **Platform modern bernilai tinggi bila terhubung ke jaringan informasi yang baik.**

1.2. Mengapa militer tertarik pada AI

Militer tertarik pada AI karena tiga hal: **kecepatan, skala, dan efisiensi**. AI menjanjikan kemampuan untuk menyaring citra, mengenali pola, mendeteksi anomali, memadukan sumber data yang berbeda, dan menyiapkan opsi tindakan bagi komandan. Dalam bahasa yang lebih tajam, AI menjanjikan pemendekan jarak antara **sensor** dan **respons**. Itu sejalan dengan penekanan outline buku ini pada percepatan keputusan, serta dengan *AI at War* yang menempatkan *speed of decision*, *ISR*, *C2*, dan *integrated fires* sebagai poros perang modern.

Ketertarikan ini bukan hanya untuk fungsi kinetik. Banyak aplikasi AI yang paling realistis justru berada di wilayah non-kinetik: logistik prediktif, *maintenance*, pengelolaan data, *wargaming*, *cyber defense*, dan *battle management*. Buku *Responsible Use of AI in Military Systems* menegaskan bahwa AI militer harus dibahas dalam arti luas, **bukan hanya senjata**, karena penggunaannya mencakup banyak fungsi organisasi dan operasional.

Di tingkat strategis, AI menarik karena negara-negara besar melihatnya sebagai pengali daya saing jangka panjang. *The AI Wave in Defence Innovation* menunjukkan bahwa AI tidak dibaca hanya sebagai alat teknis, melainkan sebagai bagian dari kompetisi yang menyentuh industri, tata kelola, interoperabilitas, dan ketahanan nasional. Itu sebabnya AI militer sesungguhnya adalah soal **kapasitas negara**, bukan sekadar soal perangkat lunak.

Mengapa militer tertarik pada AI:

- memproses data lebih cepat daripada analis manusia murni,
- mengurangi beban kognitif dalam lingkungan data yang padat,
- membantu prioritas target dan opsi tindakan,
- meningkatkan efisiensi logistik dan kesiapan sistem,
- dan memperkuat daya saing strategis jangka panjang.

1.3. AI bukan sekadar chatbot

Salah satu kesalahan paling umum dalam diskusi publik adalah menyamakan AI militer dengan *large language model* atau *chatbot*. Ini terlalu sempit. *Chatbot* hanyalah salah satu bentuk antarmuka AI. Dalam konteks pertahanan, AI mencakup *computer vision*, pengenalan pola, *sensor fusion*, analitik prediktif, optimasi logistik, perencanaan misi, *decision support*, *electronic warfare*, sampai otonomi terbatas pada sistem nirawak. Outline buku ini sendiri sudah menegaskan bahwa AI militer bukan terutama soal *chatbot* dan bukan pula semata soal senjata otonom penuh, tetapi tentang kemampuan menghubungkan data, sensor, komando, drone, logistik, dan keputusan.

Karena itu, ketika publik terlalu fokus pada nama model seperti Claude, GPT, atau model lain, diskusinya sering meleset. *Frontier model* memang penting untuk merangkum laporan, membantu sintesis intelijen, simulasi, atau menyiapkan *course of action*. Tetapi dalam perang nyata, AI yang paling berharga sering justru tidak tampil sebagai percakapan teks. Ia hadir sebagai sistem yang membantu melihat lebih cepat, mengklasifikasi objek, memberi peringatan dini, memadukan data multi-sumber, atau mengurangi beban analisis. Reuters melaporkan bahwa Ukraina telah mengumpulkan lebih dari **2 juta jam video tempur** untuk melatih model AI guna identifikasi target, penilaian efektivitas senjata, dan keputusan taktis; ini menunjukkan bahwa AI militer bergerak dari **data visual dan operasional**, bukan dari percakapan semata. ([Reuters](#))

Buku *Wired for War* membantu memberi jarak kritis dari hype sekarang. Sejak lama, perdebatan tentang robotik perang menekankan bahwa tantangan utama bukan hanya “membuat mesin cerdas,” tetapi membuat sistem yang dapat bertindak tepat di lingkungan yang bising, ambigu, berubah cepat, dan berisiko tinggi. Jadi, menyempitkan AI militer menjadi *chatbot* bukan hanya salah secara teknis; itu juga membuat kita gagal melihat medan perang modern yang sesungguhnya.

AI militer yang nyata biasanya hadir sebagai:

- mesin pengolah citra dan video ISR,
- alat fusi data multi-sensor,
- sistem bantuan keputusan di ruang komando,
- AI untuk logistik, *maintenance*, dan *cyber*,
- serta otonomi terbatas pada drone dan sistem nirawak.

1.4. Dari otomasi ke keunggulan tempur

AI militer harus dibaca sebagai kelanjutan—dan percepatan—dari otomasi. Tetapi ada beda penting antara otomasi biasa dan AI. Otomasi klasik menjalankan aturan yang relatif tetap: bila kondisi A terpenuhi, sistem melakukan B. AI, khususnya yang berbasis *machine learning*, berupaya mengenali pola dari data, menyesuaikan model, lalu memberi prediksi, klasifikasi, atau rekomendasi pada situasi yang lebih kompleks. Di sinilah AI bergeser dari alat administrasi menjadi alat keunggulan tempur.

Keunggulan tempur muncul ketika AI tidak hanya menghemat tenaga, tetapi **mengubah tempo operasi**. Jika AI mempercepat analisis ISR, memperbaiki orientasi situasional, menyiapkan opsi tindakan lebih cepat, atau membantu sinkronisasi lintas domain, maka AI mulai mempengaruhi hasil perang. Dokumen *Artificial Intelligence Strategy for the Department of War 2026* secara eksplisit mengarahkan CDAO dan komando tempur untuk mempercepat eksperimen dan integrasi AI ke konsep tempur, agar AI benar-benar mendukung *warfighting concepts* dan bukan berhenti sebagai demonstrasi teknologi. ([U.S. Department of War](#))

Pelajaran dari Ukraina memperlihatkan bentuk keunggulan tempur yang sangat bumi. Drone murah, video tempur, dan analitik data mungkin tidak terlihat glamor seperti jet siluman, tetapi justru di sanalah letak kemampuan untuk melihat musuh, memperbarui model, mengoreksi taktik, dan mempercepat respons. Sementara itu, program Replicator Pentagon menunjukkan bahwa bahkan AS pun bergerak ke arah ribuan drone murah dan “smart,” dengan anggaran sekitar **US\$500 juta per tahun**, karena keunggulan masa depan semakin terkait dengan volume sistem cerdas yang dapat dikerahkan cepat. ([Reuters](#))

Namun, justru di titik ini risikonya meningkat. Sistem yang makin otomatis dapat menggoda organisasi untuk terlalu percaya pada rekomendasi mesin. Buku *Responsible Use of AI in Military Systems* menekankan pentingnya *lawfulness*, *traceability*, *reliability*, dan mitigasi bias agar manusia tidak berubah menjadi stempel yang sekadar melegalkan keputusan mesin.

Dari otomasi ke keunggulan tempur berarti:

- bukan sekadar lebih sedikit tenaga manusia,
- tetapi lebih cepat melihat, memahami, dan bertindak,
- dengan risiko baru jika organisasi terlalu percaya pada mesin.

1.5. Pergeseran dari platform ke data, model, dan keputusan

Salah satu perubahan paling besar dalam peperangan modern adalah bergesernya pusat gravitasi dari platform ke **arsitektur informasi**. Kapal, pesawat, rudal, tank, dan drone tetap penting. Tetapi nilainya makin tergantung pada seberapa baik mereka terhubung dengan sensor, jaringan, data, model, dan pusat keputusan. Karena itu, militer masa kini tidak cukup hanya menghitung jumlah platform; ia juga harus menghitung kualitas *data pipeline*, integrasi sistem, dan kecepatan pengambilan keputusan. Outline buku ini menangkap perubahan itu dengan sangat jelas.

Dalam logika lama, platform unggul karena performa organiknya: lebih cepat, lebih kuat, lebih jauh jangkauannya. Dalam logika baru, platform unggul bila ia menjadi bagian dari jaringan yang bisa melihat lebih jauh, memahami lebih cepat, dan bertindak lebih sinkron. *The AI Wave in Defence Innovation* bahkan menekankan bahwa konvergensi AI, IoT, *cloud*, 5G, dan *edge computing* justru mendorong revolusi persepsi, pemrosesan, dan kognisi dalam ISR serta pengambilan keputusan.

Karena itu, data menjadi aset strategis. Model AI menjadi alat untuk memeras nilai dari data. Dan keputusan—bukan perangkat keras semata—menjadi medan perebutan sesungguhnya. Bab-bab selanjutnya dalam outline buku ini—tentang OODA, C4ISR, Project Maven, Ukraina, Iran, dan Indonesia—semuanya berdiri di atas pergeseran ini.

Bagi Indonesia, pelajaran ini sangat penting. Negara yang terlalu lama berpikir *platform-centric* akan cenderung membeli alat, tetapi kurang membangun ekosistem data, *mission software*, integrasi sensor, dan kemampuan pengambilan keputusan. Tanpa fondasi itu, AI mudah berubah menjadi hiasan presentasi, bukan kekuatan operasional.

Pergeseran intinya:

- dari **platform tunggal** ke **jaringan data dan keputusan**,
- dari **kepemilikan alat** ke **kemampuan mengintegrasikan alat**,
- dari **kekuatan tembak** ke **kualitas sinkronisasi sensor–analisis–aksi**.

1.6. Mengapa militer yang lambat membaca perubahan akan tertinggal

Sejarah militer menunjukkan bahwa teknologi baru tidak otomatis mengubah hasil perang; yang mengubah hasil adalah **kemampuan organisasi untuk memahami, menyerap, dan menyesuaikan diri lebih cepat**. Banyak militer gagal bukan karena sama sekali tidak memiliki teknologi, tetapi karena membaca teknologi baru dengan lensa lama. Mereka membeli alat baru, tetapi mempertahankan doktrin, birokrasi, dan pola pikir lama. Outline buku ini juga menekankan bahwa AI mengubah alat, tetapi belum tentu langsung mengubah tujuan; yang dibutuhkan adalah *force design*, adaptasi organisasi, pendidikan, dan reformasi akuisisi.

Keterlambatan membaca perubahan biasanya muncul dalam tiga bentuk. **Pertama**, terlalu terpukau pada simbol teknologi—misalnya model paling besar atau platform paling mahal—tetapi lemah di data dan integrasi. **Kedua**, terlalu hati-hati sampai inovasi selalu kalah oleh prosedur. **Ketiga**, gagal membangun SDM yang memahami hubungan antara teknologi, operasi, dan organisasi. *The AI Wave in Defence Innovation* menunjukkan bahwa tantangan adopsi AI memang bukan hanya teknis, tetapi juga terkait tata kelola, budaya organisasi, dan kesenjangan antara kecepatan inovasi dan kecepatan institusi.

Kasus Ukraina memperlihatkan sisi sebaliknya: negara yang terdesak bisa justru belajar sangat cepat bila mampu membuka jalur inovasi dari garis depan ke industri, data, dan produksi. Reuters juga menunjukkan bahwa Ukraina kini bahkan membuka akses data tempur bagi sekutu untuk melatih *drone AI software*, menandakan bahwa pengalaman perang sedang diubah menjadi kapital strategis dan industri sekaligus. ([Reuters](#))

Implikasinya bagi Indonesia keras tetapi jelas. **Militer yang lambat membaca perubahan akan tertinggal bukan hanya dari negara besar, tetapi juga dari negara yang lebih miskin namun lebih adaptif**. Jika AI militer terus dipahami hanya sebagai pembelian platform atau narasi *frontier AI*, maka Indonesia akan datang terlambat ke perang yang logikanya sudah berubah. Karena itu, Bab 1 harus dibaca sebagai peringatan: yang sedang berubah bukan sekadar alat perang, tetapi **logika perang itu sendiri**.

Ringkasan kunci

- **AI militer lahir dari revolusi komputasi, internet, sensor, dan data—bukan dari *chatbot* semata.** ([U.S. Department of War](#))
- **Militer tertarik pada AI karena AI menjanjikan kecepatan, skala, dan efisiensi dalam medan perang yang makin padat data.**
- **AI militer jauh lebih luas daripada LLM:** ia mencakup *computer vision*, *sensor fusion*, *decision support*, *logistics*, *cyber*, dan otonomi terbatas. ([Reuters](#))
- **Keunggulan tempur makin ditentukan oleh kemampuan memendekkan jarak antara sensor dan respons,** bukan sekadar oleh kemewahan platform. ([U.S. Department of War](#))
- **Pusat gravitasi perang bergeser dari platform ke data, model, dan keputusan.**
- **Militer yang lambat membaca perubahan akan kalah oleh organisasi yang lebih cepat belajar,** bahkan bila lawannya tidak memiliki teknologi paling mewah. ([Reuters](#))

Bab 2. OODA Loop, C4ISR, dan Speed of Decision

Bab ini berada di jantung buku. OODA, C4ISR, dan kecepatan keputusan ditempatkan sebagai poros utama untuk memahami mengapa AI mengubah perang bukan terutama pada level slogan, tetapi pada level **tempo operasi, kualitas sinkronisasi, dan efektivitas respons**. Itu sejalan dengan penekanan dalam *AI at War* bahwa perang modern makin ditentukan oleh *ISR, command and control, integrated fires*, dan *speed of decision*, serta dengan *The AI Wave in Defence Innovation* yang melihat AI sebagai bagian dari transformasi pertahanan yang menyentuh data, organisasi, operasi, dan persaingan strategis.

2.1. OODA loop sebagai jantung perang modern

OODA adalah singkatan dari *observe, orient, decide, act*. Konsep ini lahir dari pemikiran Kolonel John Boyd dan tetap relevan karena perang pada dasarnya adalah perebutan **siapa yang lebih cepat membaca keadaan, memahami makna, mengambil keputusan, lalu bertindak sebelum lawan menyesuaikan diri**. Dalam konteks AI militer, OODA menjadi semakin penting karena medan perang sekarang menghasilkan data dalam jumlah yang terlalu besar untuk diproses manusia secara manual. *AI at War* secara eksplisit mengaitkan *big data*, ISR, dan OODA loop sebagai satu rangkaian persoalan operasional, bukan tema terpisah.

Yang sering disalahpahami adalah anggapan bahwa OODA hanya soal “cepat.” Padahal inti OODA bukan sekadar kecepatan mekanis, melainkan **kecepatan yang dibarengi orientasi yang benar**. Jika sebuah militer bergerak cepat tetapi salah memahami situasi, maka ia hanya mempercepat kesalahan. Di sinilah AI menjadi penting sekaligus berbahaya. AI dapat membantu mempercepat pengamatan dan orientasi, tetapi juga dapat mempercepat penyebaran salah tafsir bila data buruk, model rapuh, atau operator terlalu percaya pada mesin. *The AI Wave in Defence Innovation* mengingatkan bahwa AI tidak otomatis memberi keunggulan tanpa adaptasi strategis, organisasional, dan operasional yang memadai.

Untuk militer modern, implikasinya tegas:

- **Siapa yang memendekkan OODA lawan akan punya keunggulan tempur.**
- **Siapa yang mempercepat orientasi yang salah akan menciptakan bencana lebih cepat.**
- **AI bernilai bila membantu manusia melihat lebih jernih, bukan sekadar lebih cepat.**

2.2. Dari C2 ke C4ISR

Dalam perang klasik, pusat perhatian sering berada pada C2, *command and control*. Komandan memberi perintah, unit melaksanakan, lalu laporan kembali naik ke atas. Dalam perang modern, struktur ini berkembang menjadi **C4ISR**: *command, control, communications, computers, intelligence, surveillance, and reconnaissance*. Perubahan ini penting karena ia menunjukkan bahwa keputusan militer tidak lagi berdiri di atas perintah dan disiplin saja, tetapi di atas **komunikasi, komputasi, intelijen, pengamatan, dan pengintaian yang terintegrasi**.

Dokumen resmi Departemen Pertahanan AS menunjukkan arah yang sama. DoD Data Strategy menegaskan bahwa perang modern menuntut DoD menjadi organisasi yang *data-centric* dan mampu mengoperasikan data “at speed and scale,” sementara JADC2 dimaksudkan untuk menghubungkan sensor, data, jaringan, dan *automated decision aids* agar *real-time command and control* menjadi mungkin. ([U.S. Department of War](#))

Perubahan dari C2 ke C4ISR berarti tiga hal.

- **Pertama, komando tidak bisa lagi dipisahkan dari arsitektur informasi.** Komandan yang tidak melihat gambaran utuh akan selalu terlambat.
- **Kedua, komunikasi dan komputasi bukan lagi fungsi pendukung, tetapi bagian dari daya tempur.**
- **Ketiga, ISR menjadi fondasi keputusan.** Tanpa ISR yang baik, C2 hanya menjadi ritual birokratis.

Dalam bahasa yang lebih sederhana: dulu militer unggul karena punya senjata lebih kuat. Kini militer juga harus unggul karena **punya cara lebih baik untuk mengetahui apa yang sedang terjadi**.

2.3. ISR dan banjir data

ISR — *intelligence, surveillance, reconnaissance* — dulu identik dengan mata dan telinga militer. Kini ISR telah berubah menjadi **mesin penghasil data raksasa**. Drone, radar, kamera EO/IR, satelit, sensor maritim, SIGINT, *battlefield reports*, telemetry, dan jaringan komunikasi menghasilkan arus data yang sangat besar, cepat, dan terus-menerus. *AI at War* menekankan hubungan langsung antara *big data* dan ISR; sedangkan outline buku ini memang menempatkan “ISR dan banjir data” sebagai subbab tersendiri karena disinilah salah satu inti revolusi AI militer berada.

Kasus Ukraina memberi contoh nyata. Reuters melaporkan bahwa sejak 2022 Ukraina telah mengumpulkan lebih dari **2 juta jam video perang**, terutama dari drone, dan data itu dipakai untuk melatih model AI guna membantu identifikasi target, menilai efektivitas senjata, dan mendukung keputusan taktis maupun strategis. ([Reuters](#))

Masalah utamanya bukan lagi kekurangan data, tetapi **kepadatan data**. Ada tiga konsekuensi langsung:

- **Analisis manusia mudah kewalahan.** Tidak semua video, citra, sinyal, dan laporan bisa dibaca satu per satu.
- **Waktu respons bisa kalah oleh volume data.** Sistem bisa “kaya informasi tetapi miskin keputusan.”
- **Kualitas data menjadi masalah strategis.** Data yang bias, usang, atau salah label dapat menghasilkan keputusan yang juga salah.

Karena itu, dalam perang modern, ISR tidak cukup hanya “mengumpulkan.” ISR harus mampu **mengurutkan prioritas, membersihkan noise, menggabungkan sumber, dan menghasilkan pemahaman yang bisa dipakai bertindak.**

2.4. Dari melihat ke memahami

Inilah lompatan yang paling penting. Melihat belum tentu memahami. Sensor dapat menangkap ribuan objek, tetapi tanpa *orientation* yang benar, semua itu hanya menjadi kebisingan. AI menjadi relevan ketika ia membantu bergerak dari **deteksi** menuju **interpretasi**. Bukan sekadar menemukan titik panas, objek bergerak, atau pola radio, tetapi membantu menjawab: apakah ini ancaman, tipuan, sasaran bernilai tinggi, atau gangguan biasa?

Di medan perang, jarak antara melihat dan memahami sering menentukan hidup-matinya operasi. *The AI Wave in Defence Innovation* mencatat bahwa kombinasi data yang terus bertambah, daya komputasi, dan kapasitas AI untuk menganalisis data dapat memberi *war fighters* visibilitas medan yang belum pernah ada sebelumnya, membantu mengurangi *fog of war* dan mendukung pengambilan keputusan di berbagai tingkat.

Tetapi pemahaman bukan hanya fungsi algoritma. Ia juga tergantung pada:

- **kualitas data input,**
- **konteks taktis dan operasional,**
- **pengalaman operator,**
- **dan kemampuan organisasi menghubungkan hasil AI ke keputusan nyata.**

Karena itu, AI tidak boleh diperlakukan sebagai mesin wahyu. AI hanya berguna bila ia masuk ke dalam *human-machine team* yang sehat. Buku *Responsible Use of AI in Military Systems* menekankan bahwa penggunaan AI yang bertanggung jawab harus memperhatikan *lawfulness, traceability, reliability*, dan mitigasi bias, karena tanpa itu AI sulit dipercaya ketika stakes-nya sangat tinggi.

2.5. AI sebagai pengganda kecepatan

AI disebut *force multiplier* bukan karena ia menggantikan manusia, tetapi karena ia bisa mempercepat banyak tahap dalam rantai keputusan: menyaring data, mengenali pola, memprioritaskan target, memberi peringatan dini, menggabungkan laporan multi-sumber, bahkan menyiapkan *course of action* awal. Itulah sebabnya militer tertarik pada AI. Nilainya bukan pada “kepintaran” abstrak, melainkan pada kemampuannya **memendekkan jarak antara sensor dan tindakan**. Outline buku ini sejak awal sudah menempatkan AI sebagai penghubung data, sensor, komando, drone, logistik, dan keputusan.

Dokumen AI Strategy for the Department of War 2026 menegaskan bahwa CDAO akan memfokuskan ulang sumber daya untuk mempercepat proyek-proyek *war-winning* dan membuka *foundational enablers* secara real-time ke seluruh departemen, sehingga eksekusi dapat dipercepat lintas organisasi. Ini menunjukkan bahwa percepatan keputusan memang dipahami secara resmi sebagai tujuan strategis, bukan hanya janji vendor teknologi. ([U.S. Department of War](#))

Dalam praktik, AI dapat menjadi pengganda kecepatan pada lima titik:

- **deteksi lebih cepat** terhadap objek, pola, atau anomali,
- **klasifikasi lebih cepat** atas sasaran atau aktivitas,
- **fusi data lebih cepat** dari banyak sensor dan satuan,
- **prioritisasi keputusan lebih cepat** untuk komandan,
- **umpan balik lebih cepat** dari hasil operasi ke perbaikan model.

Namun, ada syaratnya: **AI hanya benar-benar mempercepat keputusan bila organisasi siap menerima dan memakai hasilnya**. Jika tidak, AI hanya menambah layer baru dalam birokrasi.

2.6. Mengapa keunggulan tidak lagi hanya di senjata, tetapi di sinkronisasi

Perang modern tidak lagi dimenangkan hanya oleh platform terbaik atau rudal terjauh. Keunggulan makin ditentukan oleh **sinkronisasi**: seberapa baik sensor, jaringan, komando, tembakan, EW, logistik, dan unit manuver bekerja sebagai satu sistem. *AI at War* menekankan *integrated fires, command and control*, dan *battle network* sebagai tema inti. *The AI Wave in Defence Innovation* juga menyoroti bahwa tantangan terbesar justru ada pada kemampuan menghubungkan *sensor-to-shooter loops* dan aliran data antar-matra, antar-platform, dan antar-organisasi secara real time.

Ini berarti sebuah sistem senjata mahal bisa kehilangan nilai bila tidak tersinkronkan dengan baik. Sebaliknya, sistem yang relatif murah bisa sangat mematikan bila terhubung ke jaringan ISR dan keputusan yang bagus. Pelajaran dari Ukraina sering dibaca tepat dari sini: drone murah menjadi mematikan bukan hanya karena harganya rendah, tetapi karena ia masuk ke *kill chain* yang makin cepat dan makin adaptif. Reuters juga menunjukkan bahwa Ukraina tidak hanya mengumpulkan data, tetapi membangun proses agar data itu memberi nilai operasional dan industri. ([Reuters](#))

Maka, keunggulan masa kini semakin bergeser:

- dari **platform tunggal** ke **sistem jaringan**,
- dari **kepemilikan alat** ke **kemampuan mengintegrasikan alat**,
- dari **kekuatan tembak** ke **kualitas sinkronisasi sensor-keputusan-aksi**.

Bagi Indonesia, ini sangat penting. Negara yang masih berpikir *platform-centric* akan cenderung membeli barang, tetapi lemah dalam integrasi, *mission software*, dan *data pipeline*. Itu berarti ia bisa tampak modern di katalog, tetapi tetap lambat di medan nyata.

2.7. Bahaya automasi berlebih

Di sinilah bab ini harus menutup dengan nada waspada. AI memang bisa mempercepat, tetapi **kecepatan yang tidak diawasi dapat berubah menjadi kesalahan yang juga bergerak cepat**. Buku *Responsible Use of AI in Military Systems* menyoroti risiko operasional khas AI: *brittleness*, *unreliability*, *unpredictability*, dan *bias*. Buku itu juga menekankan risiko *automation complacency* atau *over-reliance*, yaitu ketika operator manusia terlalu percaya pada sistem dan tidak lagi cukup kritis saat AI salah.

Bahaya automasi berlebih muncul dalam beberapa bentuk.

- **Pertama, automation bias.** Operator cenderung menerima keluaran mesin sebagai benar, bahkan ketika konteks lapangan sebenarnya meragukannya.
- **Kedua, brittleness.** Model bekerja baik di lingkungan yang dikenalnya, tetapi gagal saat situasi berubah, data bergeser, atau lawan melakukan deception.
- **Ketiga, opacity.** Sistem memberi rekomendasi, tetapi alasan di baliknya tidak cukup dapat dipahami.
- **Keempat, eskalasi cepat.** Mesin mempercepat rantai keputusan dalam situasi yang sebenarnya ambigu.
- **Kelima, tanggung jawab yang kabur.** Saat banyak manusia dan mesin terlibat dalam satu keputusan, pertanyaan “siapa yang bertanggung jawab?” menjadi makin sulit.

Dokumen Political Declaration on Responsible Military Use of AI and Autonomy yang dipimpin AS menekankan bahwa penggunaan militer AI harus berada dalam rantai komando yang bertanggung jawab, dengan *appropriate human judgment* dan langkah-langkah untuk meminimalkan kegagalan yang tidak diinginkan. Deklarasi itu justru penting karena ia mengakui bahwa percepatan teknologi harus dibarengi disiplin operasional dan tanggung jawab manusia. ([State.gov](https://www.state.gov))

Jadi, pelajaran akhirnya sederhana tetapi keras: **AI yang baik bukan AI yang sekadar cepat, melainkan AI yang dapat dipercaya, dipahami batasnya, diuji, dan dipakai dalam proses manusia-mesin yang sehat**. Tanpa itu, *speed of decision* bisa berubah menjadi *speed of error*.

Ringkasan kunci

- **OODA tetap relevan** karena perang modern adalah perebutan siapa yang lebih cepat dan lebih tepat dalam mengubah pengamatan menjadi tindakan.
- **C4ISR menunjukkan bahwa komando modern tidak bisa dipisahkan dari komunikasi, komputasi, intelijen, pengamatan, dan pengintaian.** ([Kantor Pengawas Pertahanan](#))
- **ISR kini menghasilkan banjir data**, dan nilai AI muncul ketika ia membantu menyaring, menggabungkan, dan memprioritaskan data itu. ([Reuters](#))
- **Keunggulan tempur makin ditentukan oleh kemampuan bergerak dari melihat ke memahami**, bukan sekadar oleh kepadatan sensor.
- **AI adalah pengganda kecepatan**, tetapi hanya efektif bila organisasi siap menggunakannya. ([U.S. Department of War](#))
- **Keunggulan tidak lagi hanya di senjata, tetapi di sinkronisasi** lintas sensor, jaringan, komando, dan tembakan.
- **Automasi berlebih adalah risiko nyata**: bias, *brittleness*, *over-reliance*, dan eskalasi salah keputusan harus diperlakukan serius. ([State.gov](#))

Bab 3. Dari Robotik ke Drone Warfare

Setelah menjelaskan AI, OODA, dan C4ISR, langkah berikutnya adalah menunjukkan bagaimana robotik dan UAV berkembang dari teknologi pelengkap menjadi **instrumen inti perang modern**. Outline buku memang menempatkan bab ini sebagai jembatan dari kerangka konseptual menuju realitas operasi: sejarah UAV, transisi ke sistem murah massal, peran ISR dan *strike*, sampai perubahan ekonomi perang dan masa depan sistem yang lebih padat, lebih murah, dan lebih otonom.

3.1. Sejarah singkat UAV dan robotic warfare

Perang robotik tidak lahir kemarin sore. Buku *Unmanned Aerial Vehicles: Robotic Air Warfare 1917–2007* menunjukkan bahwa eksperimen pesawat tanpa awak sudah muncul sejak Perang Dunia I, ketika upaya awal *pilotless aircraft* dikembangkan melalui kendali radio dan sistem navigasi yang masih sangat primitif. Pada masa awal itu, batas antara UAV dan *guided missile* masih sangat dekat, karena keduanya sama-sama menghadapi problem utama: **bagaimana menggantikan pilot manusia dengan sistem kendali buatan**.

Perkembangan UAV kemudian bergerak bertahap. Pada Perang Dunia II, drone dipakai dalam bentuk yang masih kasar, terutama untuk misi serang dan target latihan. Pada era Perang Dingin, fungsinya bergeser kuat ke *reconnaissance*. Vietnam menjadi fase penting karena drone terbang ribuan kali untuk misi pengintaian yang terlalu beresiko bagi pesawat berawak. Sejak itu, jalur evolusinya makin jelas: dari alat pinggiran menjadi komponen operasional yang makin dipercaya.

Buku *Wired for War* membantu membaca sejarah ini dalam skala yang lebih besar. Robotik militer tidak berkembang hanya karena ada “mesin yang lebih pintar,” tetapi karena kombinasi miniaturisasi elektronik, sensor, komputasi, komunikasi, dan kebutuhan militer untuk mengurangi risiko pada personel. Karena itu, *robotic warfare* harus dipahami bukan sebagai keajaiban teknis tunggal, melainkan sebagai hasil akumulasi banyak kemajuan teknologi yang akhirnya bertemu dengan kebutuhan tempur nyata.

Ada tiga pelajaran sejarah yang penting.

- **Pertama**, UAV tidak lahir sebagai alat dominan; ia tumbuh perlahan melalui fungsi-fungsi terbatas yang terbukti berguna.
- **Kedua**, penerimaan militer biasanya datang setelah teknologi mampu menjawab kebutuhan lapangan, bukan hanya memukau laboratorium.
- **Ketiga**, setiap lompatan besar UAV selalu berkaitan dengan kombinasi **sensor, komunikasi, dan kendali**, bukan airframe semata.

3.2. Dari pesawat tanpa awak ke sistem murah massal

Jika sejarah awal UAV adalah kisah tentang pengintaian dan eksperimen, maka perang modern adalah kisah tentang **skala**. Drone tidak lagi dipandang hanya sebagai pesawat kecil tanpa pilot. Ia telah berubah menjadi keluarga sistem yang sangat luas: dari quadcopter murah, *loitering munition*, *FPV drone*, *loyal wingman*, sampai USV dan UUV. Buku *AI at War* menegaskan bahwa militer modern tidak hanya mengejar otonomi pada satu jenis kendaraan, tetapi pada portofolio sistem nirawak lintas domain.

Yang paling mengubah perang justru bukan selalu drone tercanggih, melainkan **drone yang cukup baik, cukup murah, dan bisa diproduksi banyak**. Reuters melaporkan bahwa Pentagon melalui program Replicator menargetkan ribuan drone murah dan “smart” untuk konflik masa depan, dengan anggaran sekitar **US\$500 juta per tahun**, karena mereka melihat keunggulan tidak lagi hanya datang dari beberapa platform mahal, melainkan dari *massed autonomous systems* yang bisa ditugaskan secara berjejaring. ([Reuters](#))

Ukraina memberi bukti paling keras tentang perubahan ini. Reuters melaporkan Ukraina bertaruh besar pada *interceptor drones* murah sebagai *air shield* biaya rendah, karena penggunaan misil pertahanan udara konvensional terlalu mahal dan stoknya terbatas. Dalam logika ini, drone bukan sekadar pengganti pesawat; drone menjadi **alat perang massal** yang mengubah hubungan antara biaya, risiko, dan hasil tempur. ([Reuters](#))

Perubahan ini membawa implikasi strategis yang besar.

- **Produksi massal** menjadi lebih penting daripada performa maksimal beberapa unit.
- **Kecepatan iterasi** menjadi sama pentingnya dengan spesifikasi teknis.
- **Supply chain** menjadi bagian dari kekuatan tempur.
- **Software** dan *mission system* menjadi sama pentingnya dengan airframe.

3.3. ISR, strike, decoy, relay, swarm

Kekuatan drone modern terletak pada fleksibilitas fungsi. Dalam outline buku ini, pemisahan antara ISR, *strike*, *decoy*, *relay*, dan *swarm* sangat tepat karena justru di situlah UAV berubah dari alat tunggal menjadi **arsitektur operasi**.

ISR tetap menjadi fungsi paling mendasar. Drone memberi mata yang murah, persisten, dan dekat ke medan. Mereka dapat memantau garis depan, jalur logistik, pergerakan musuh, perubahan posisi, sampai pola aktivitas harian lawan. Dalam banyak konflik, siapa yang bisa melihat lebih awal sering sudah unggul sebelum tembakan pertama dilepaskan. Reuters menunjukkan bahwa di Ukraina, data video drone dalam skala sangat besar menjadi bahan bakar AI dan pengambilan keputusan, memperlihatkan bagaimana ISR kini langsung terkait dengan analitik dan pembelajaran mesin. ([Reuters](#))

Strike adalah tahap berikutnya. Drone menyerang dengan dua logika utama: *precision* dan *attrition*. Pada satu sisi adaUCAV atau *loitering munition* yang mengincar target bernilai tinggi. Pada sisi lain ada *FPV drones* murah yang dipakai dalam jumlah besar untuk menghantam kendaraan, bunker, antenna, atau personel. Ini berarti kemampuan menyerang tidak lagi dimonopoli platform besar.

Decoy juga makin penting. Drone murah dapat dipakai untuk memancing radar, memaksa pertahanan udara lawan mengungkap posisi, atau menghabiskan rudal intersektor yang jauh lebih mahal. Dalam perang modern, kadang nilai sebuah drone bukan pada sasaran yang dihancurkannya, tetapi pada **reaksi lawan yang dipaksa muncul**.

Relay adalah fungsi yang sering diremehkan tetapi sangat penting. Drone dapat menjadi perpanjangan jaringan komunikasi, penghubung antar-unit, atau simpul data sementara ketika medan menghambat komunikasi langsung. Dalam operasi kepulauan atau medan yang terputus-putus, fungsi ini sangat bernilai.

Swarm adalah tahap yang lebih maju. Bukan sekadar banyak drone terbang bersama, tetapi **sekumpulan sistem yang bisa dikoordinasikan untuk efek kolektif**: pengintaian serempak, saturasi pertahanan, pencarian area luas, atau kombinasi *decoy* dan *strike*. Reuters melaporkan bahwa AS, China, dan Eropa semua bergerak ke arah sistem *swarming* dan *attributable autonomous systems*, meski tingkat kematangannya masih beragam. ([Reuters](#))

Jadi, drone modern tidak boleh dibaca sebagai “pesawat kecil.” Ia adalah **node multifungsi** dalam jaringan perang.

3.4. Mengapa drone murah mengubah ekonomi perang

Inilah titik paling revolusioner. Drone murah mengubah perang karena mereka mengubah **ekonomi kekerasan**. Dulu, menghancurkan target umumnya membutuhkan platform mahal, personel terlatih tinggi, dan rantai logistik besar. Kini, target bernilai tinggi bisa dihantam oleh sistem yang biayanya jauh lebih rendah. Ini bukan berarti platform mahal tidak penting lagi, tetapi artinya **rasio biaya-serangan** telah berubah drastis.

Reuters menulis bahwa drone laut di banyak kasus dipandang sebagai cara relatif murah dan cepat untuk memperluas kekuatan tempur dibanding kapal perang besar, dengan biaya per unit yang jauh lebih rendah daripada platform tradisional. Logika yang sama berlaku di domain udara: drone murah dapat memaksa lawan menembakkan interceptor yang jauh lebih mahal, atau menutup area tertentu karena ancaman terus-menerus. ([Reuters](#))

Ukraina sekali lagi menjadi studi kasus yang kuat. Penggunaan drone murah, termasuk *interceptor drones*, menunjukkan bahwa solusi yang tidak glamor dapat memberi efek sangat strategis jika bisa diproduksi banyak dan dipakai cepat. Bahkan langkah sederhana penggunaan jaring ikan bekas untuk menghambat drone menunjukkan bahwa perang drone tidak hanya soal “high-tech,” tetapi juga tentang **cara murah menurunkan efektivitas sistem murah lawan**. ([Reuters](#))

Ada beberapa perubahan ekonomi perang yang ditimbulkan drone murah.

- **Biaya masuk perang presisi turun.**
- **Biaya pertahanan naik**, karena pencegahan bisa jauh lebih mahal dari serangan.
- **Inovasi menyebar ke aktor kecil**, termasuk startup dan bengkel.
- **Siklus desain-produksi-pakai-revisi menjadi sangat pendek.**
- **Daya tahan industri** menjadi sama pentingnya dengan daya tahan pasukan.

Ini sebabnya negara yang hanya mengejar platform premium bisa terlihat kuat, tetapi justru kewalahan menghadapi volume murah.

3.5. Dari platform mahal ke attritable systems

Istilah *attritable* penting karena menjelaskan logika baru perang drone: sistem yang **memang dirancang untuk bisa hilang, rusak, atau dikorbankan**, tanpa membuat operasi runtuh. Ini berbeda dari logika lama yang sangat melindungi setiap platform karena biaya dan nilainya sangat tinggi. Dalam logika *attritable*, kehilangan unit adalah bagian yang diterima dari desain operasi. ([Reuters](#))

Program Replicator di AS secara terbuka bergerak ke arah ini: bukan membangun beberapa sistem mewah, tetapi membangun portofolio *all-domain attritable autonomous capabilities* yang bisa diproduksi dan dipakai dalam jumlah banyak. Reuters juga melaporkan bahwa Pentagon mendorong ekspansi kapasitas industri untuk drone murah yang dapat dikorbankan, karena kebutuhan tempur masa depan menuntut volume dan ketahanan, bukan hanya kecanggihan elit. ([Reuters](#))

Konsep ini sangat penting karena mengubah cara militer berpikir tentang desain pasukan.

- **Pertama**, nilai sistem tidak lagi diukur hanya dari umur panjangnya, tetapi dari kontribusinya pada misi.
- **Kedua**, kuantitas bisa menjadi kualitas tersendiri bila terhubung dengan baik.
- **Ketiga**, industri harus mampu memulihkan stok dengan cepat.
- **Keempat**, latihan dan doktrin harus menerima kehilangan sistem sebagai hal normal.

Bagi Indonesia, pelajaran ini sangat besar. Negara dengan sumber daya terbatas justru lebih rasional membangun campuran antara beberapa platform mahal dan **banyak sistem murah yang attritable**. Jika tidak, kita akan terlalu rapuh: kuat di katalog, lemah di perang berkepanjangan.

3.6. Masa depan perang yang lebih padat, lebih murah, lebih otonom

Masa depan perang tidak bergerak ke satu arah tunggal, tetapi beberapa tren sudah sangat jelas. Pertama, perang akan **lebih padat** oleh sistem nirawak lintas domain: udara, laut, bawah laut, dan darat. Kedua, perang akan **lebih murah pada level unit**, tetapi belum tentu lebih murah secara keseluruhan karena volume akan meningkat. Ketiga, perang akan **lebih otonom**, walau dalam banyak kasus otonominya masih terbatas dan sangat bergantung pada manusia, software, jaringan, dan konteks misi.

Reuters menunjukkan tren ini dari banyak arah sekaligus: China mendorong *AI drone swarms* dan sistem otonom, AS mencoba membangun armada drone dan sistem *attributable* dalam skala besar, Eropa mulai masuk ke UCAV yang dirancang untuk *swarm* dan *loyal wingman*, sementara Ukraina terus memproduksi dan mengeksport pengetahuan tempur drone. ([Reuters](#))

Tetapi tren ini tidak berarti manusia hilang dari perang. Justru sebaliknya, tantangannya adalah bagaimana manusia tetap memegang penilaian, tanggung jawab, dan orientasi strategis di tengah laju sistem yang makin cepat. Buku *Responsible Use of AI in Military Systems* penting di sini, karena ia mengingatkan bahwa perluasan otonomi dan AI dalam sistem militer menuntut perhatian serius pada *trust*, *accountability*, *traceability*, dan kontrol manusia yang bermakna.

Jadi, masa depan perang kemungkinan bukan perang robot sepenuhnya, melainkan **perang manusia-mesin** dengan ciri-ciri berikut:

- **lebih banyak sensor dan platform murah,**
- **lebih banyak keputusan yang dibantu mesin,**
- **lebih banyak sistem yang dapat dikorbankan,**
- **lebih besar ketergantungan pada data dan software,**
- **dan lebih besar risiko jika integrasi, governance, dan industri tidak siap.**

Ringkasan kunci

- **UAV punya sejarah panjang**, dari eksperimen awal Perang Dunia I sampai pengintaian massal era Vietnam dan drone serang modern.
- **Perubahan terbesar bukan hanya pada bentuk drone, tetapi pada skalanya:** dari alat terbatas menjadi sistem murah yang diproduksi massal. ([Reuters](#))
- **Drone modern menjalankan banyak fungsi sekaligus:** ISR, *strike*, *decoy*, *relay*, dan *swarm*. ([Reuters](#))
- **Drone murah mengubah ekonomi perang** karena dapat memberi efek besar dengan biaya relatif rendah dan memaksa lawan mengeluarkan biaya pertahanan lebih tinggi. ([Reuters](#))
- **Konsep *attributable systems* mengubah desain kekuatan militer:** kehilangan unit menjadi bagian yang diterima dari operasi. ([U.S. Department of War](#))
- **Masa depan perang bergerak ke arah yang lebih padat, lebih murah, dan lebih otonom**, tetapi tetap menuntut kontrol manusia, integrasi sistem, dan daya tahan industri. ([Reuters](#))

Bagian II. AI dalam Ekosistem Pertahanan Modern

Bab 4. AI di Militer Amerika Serikat: Ekosistem, Bukan Produk Tunggal

Bab ini penting karena banyak orang membaca AI militer Amerika Serikat seolah-olah ia ditentukan oleh satu model, satu vendor, atau satu proyek. Padahal yang lebih akurat adalah ini: **AI pertahanan AS bekerja sebagai ekosistem**—gabungan data, cloud, platform analitik, integrator software, kontraktor pertahanan, kantor transformasi digital, dan komando operasional. Titik itu dengan tepat ditangkap ketika menempatkan Project Maven, CDAO, platform data, frontier model, Palantir, Anthropic, dan OpenAI dalam satu rangkaian, bukan sebagai topik yang berdiri sendiri.

4.1. Project Maven dan logika dasar AI pertahanan AS

Untuk memahami AI militer Amerika Serikat, titik masuk terbaik tetap **Project Maven**. Program ini lahir karena Pentagon menghadapi masalah yang sangat mendasar: banjir data ISR dari drone, citra, dan sensor lain jauh lebih cepat daripada kapasitas analis manusia untuk membacanya. Dalam kerangka ini, Maven bukan proyek “robot perang” dalam arti film fiksi ilmiah, melainkan proyek untuk **mempercepat pengolahan, penyaringan, dan pemaknaan data medan tempur**. Inilah logika dasar AI pertahanan AS: membantu manusia melihat lebih cepat, memahami lebih cepat, dan mengambil keputusan lebih cepat.

Reuters melaporkan bahwa pada Mei 2024 Pentagon memberi Palantir kontrak senilai hingga **US\$480 juta** untuk mengembangkan **Maven Smart System**, sebuah prototipe yang membantu intelijen militer mengidentifikasi *points of interest* dari berbagai sumber data dan mempercepat kerja analis. Dua tahun kemudian, Reuters juga melaporkan bahwa melalui memo 9 Maret 2026, Pentagon memutuskan menjadikan Maven sebagai **program of record**, artinya sistem itu tidak lagi diperlakukan sebagai eksperimen sementara, tetapi sebagai bagian inti dari infrastruktur militer jangka panjang. ([Reuters](#))

Dari sini terlihat sesuatu yang sangat penting. **Maven bukan hanya soal AI. Maven adalah cara Pentagon mengubah AI dari demo menjadi alat perang yang terintegrasi ke organisasi, anggaran, dan komando**. Itu sebabnya bab ini harus dibaca dalam bahasa kelembagaan, bukan sekadar bahasa teknologi.

Pokok penting Project Maven:

- lahir dari masalah banjir data ISR,
- berfungsi mempercepat analisis dan *decision support*,
- menjadi jembatan dari eksperimen AI ke infrastruktur pertahanan yang permanen. ([Reuters](#))

4.2. Peran cloud, integrator, dan platform data

Ekosistem AI pertahanan AS tidak bisa berjalan tanpa tiga lapisan penyangga: **cloud, platform data, dan integrator software**. Di sinilah banyak pembaca salah fokus. Mereka melihat model AI, tetapi tidak melihat infrastruktur yang membuat model itu bisa hidup di organisasi sebesar Pentagon.

Pada sisi *cloud*, Departemen Pertahanan AS membangun **Joint Warfighting Cloud Capability (JWCC)** sebagai kendaraan multi-vendor untuk menyediakan layanan *cloud* di berbagai tingkat klasifikasi, dari level enterprise sampai *tactical edge*. AWS menjelaskan bahwa JWCC dirancang agar DoD dapat memakai *cloud* di semua *security domains* untuk misi saat ini dan masa depan. Artinya, *cloud* bukan aksesoris TI; ia adalah **tulang punggung distribusi komputasi dan data** untuk perang modern. ([Amazon Web Services, Inc.](#))

Pada sisi platform data, **Advana** memegang peran kunci. CDAO dan pejabat DoD berulang kali menggambarkan Advana sebagai platform data analitik terbesar di DoD. Pada September 2024, pejabat CDAO menyebut Advana telah mencapai lebih dari **100.000 pengguna** dan menghubungkan lebih dari **500 source systems**. Pada Juli 2023, CDAO juga melaporkan lonjakan penggunaan Advana dan dashboard PULSE untuk mendukung evaluasi kinerja lebih cepat di tingkat pimpinan. Ini menunjukkan bahwa AI militer AS bertumpu pada **arsitektur data enterprise** yang sangat besar, bukan pada model tunggal. ([U.S. Department of War](#))

Pada sisi integrator, perusahaan seperti **Palantir** menjadi penting karena mereka menjahit banyak komponen menjadi sistem yang benar-benar bisa dipakai. Reuters menggambarkan Maven sebagai platform *command-and-control* yang menganalisis data dari satelit, drone, radar, sensor, dan laporan intelijen untuk mengidentifikasi ancaman atau target potensial. Sementara itu, Palantir sendiri memasarkan Maven Smart System sebagai platform AI-enabled untuk **CJADC2**, yakni *combined joint all-domain command and control*. Itu berarti peran integrator bukan sekadar menjual software, tetapi menyatukan data, model, tampilan operasional, *workflow*, dan deployment lintas domain. ([Reuters](#))

Ekosistem ini bekerja dalam logika berikut:

- **cloud** menyediakan komputasi dan lingkungan multi-domain,
- **platform data** menyatukan data dari banyak sumber,
- **integrator** mengubah data dan model menjadi *workflow* operasional yang dipakai komandan dan analis. ([Amazon Web Services, Inc.](#))

4.3. Frontier model dalam ekosistem pertahanan

Masuknya *frontier model* ke pertahanan AS harus dibaca dengan hati-hati. Mereka penting, tetapi bukan pusat tunggal ekosistem. Model besar dipandang menarik karena bisa membantu sintesis dokumen, analisis teks, penyusunan opsi kebijakan, *cyber defense*, ringkasan intelijen, dan interaksi manusia-mesin yang lebih fleksibel. Tetapi model besar hanya berguna bila ada **data, governance, deployment, dan integrasi** yang mendukungnya. Outline buku ini sudah memberi peringatan yang tepat: AI militer harus dibaca dalam konteks *inovasi pertahanan, percepatan keputusan, integrasi data-platform-cloud*, dan tata kelola, bukan sekadar dalam konteks industri AI.

Anthropic mengumumkan pada 14 Juli 2025 bahwa DoD melalui CDAO memberi perusahaan itu **perjanjian prototipe dua tahun dengan plafon US\$200 juta** untuk memprototipekan kapabilitas frontier AI bagi keamanan nasional. Anthropic juga menyatakan bahwa Claude telah diintegrasikan ke *mission workflows* di jaringan rahasia melalui kemitraan dengan Palantir. Beberapa hari sebelumnya, OpenAI meluncurkan **OpenAI for Government** dan mengumumkan pilot pertama dengan CDAO, juga dengan plafon **US\$200 juta**, untuk memprototipekan pemakaian frontier AI pada operasi administratif, data akuisisi, kesehatan, dan *proactive cyber defense*. ([Anthropic](#))

Dari sini tampak bahwa *frontier model* masuk ke pertahanan bukan langsung sebagai “AI penembak,” melainkan sebagai **lapisan kemampuan kognitif** di atas infrastruktur pertahanan yang sudah dibangun: merangkum, menghubungkan, mengusulkan, mempercepat pencarian pola, dan membantu *workflow*. Tetapi penting juga dicatat: penggunaan resmi yang diumumkan OpenAI justru ditekankan pada domain administratif dan *cyber defense*, bukan langsung pada *lethal targeting*. ([Anthropic](#))

Jadi, posisi *frontier model* adalah:

- penting sebagai akselerator analisis dan interaksi,
- tetapi tetap bergantung pada data, integrator, dan governance,
- dan tidak boleh disamakan otomatis dengan senjata otonom. ([Anthropic](#))

4.4. Anthropic, OpenAI, Palantir, dan negara keamanan nasional

Kasus Anthropic, OpenAI, dan Palantir menunjukkan perubahan besar dalam hubungan negara keamanan nasional AS dengan perusahaan teknologi. Dulu, inovasi pertahanan sangat identik dengan kontraktor pertahanan klasik. Kini, ekosistemnya makin mirip gabungan antara **Silicon Valley, cloud hyperscalers, integrator software, dan birokrasi pertahanan**. Itulah sebabnya Palantir, Anthropic, dan OpenAI penting dibaca bukan sebagai perusahaan biasa, tetapi sebagai bagian dari arsitektur kekuasaan teknologi negara.

Palantir berada di posisi yang sangat strategis karena berfungsi sebagai penghubung antara data, AI, dan *workflow* operasional. Reuters mencatat bahwa kontrak Maven Palantir yang semula bernilai US\$480 juta dinaikkan pada 2025 hingga plafon **US\$1,3 miliar**, dan pada 2026 Maven ditetapkan sebagai program inti Pentagon. Itu menunjukkan bahwa peran Palantir bukan perifer, melainkan semakin dekat ke jantung digital militer AS. ([Reuters](#))

Anthropic dan OpenAI berada pada lapisan model dan layanan AI. Anthropic menekankan *responsible AI* dan menyebut model *Claude Gov* serta *Claude for Enterprise* sebagai bagian dari penawarannya ke DoD. OpenAI, melalui OpenAI for Government, menempatkan diri sebagai penyedia model dan dukungan untuk kebutuhan pemerintah di lingkungan aman dan patuh. Secara politik, ini berarti perusahaan AI frontier sekarang tidak lagi berada di pinggir kebijakan keamanan nasional, tetapi masuk ke pusatnya. ([Anthropic](#))

Namun, disinilah juga letak ketegangannya. **Negara ingin fleksibilitas strategis; perusahaan AI membawa guardrails, kebijakan penggunaan, dan pertimbangan reputasi serta etika.** Dalam bahasa buku ini, pertanyaan yang mengemuka bukan hanya “apakah model ini kuat?”, tetapi juga “siapa yang menetapkan batas pemakaiannya, dan sejauh mana negara mau tunduk pada batas itu?”

4.5. Dari eksperimen ke infrastruktur operasional

Perubahan paling penting dalam AI militer AS bukan masuknya satu model tertentu, tetapi perubahan dari **eksperimen** ke **infrastruktur operasional**. Inilah yang membedakan Pentagon hari ini dari banyak militer lain yang masih berada pada level pilot project. Ketika CDAO dibentuk pada 2022, tugas resminya adalah memimpin strategi dan kebijakan DoD untuk data, analitik, dan AI serta menyeleksi solusi digital yang terbukti untuk diskalakan ke penggunaan enterprise dan joint-use. Artinya, sejak awal tujuannya memang bukan membuat banyak demo, tetapi **mengangkat solusi yang terbukti ke skala institusional**. ([U.S. Department of War](#))

Maven adalah contoh paling jelas dari proses itu. Ia lahir dari kebutuhan analisis citra, berkembang menjadi sistem *command-and-control*, lalu dijadikan program of record. Advana juga tumbuh dari platform analitik menjadi tulang punggung data enterprise. JWCC memberi fondasi *cloud*. Integrator seperti Palantir menjahit banyak domain. Frontier model seperti Claude dan model OpenAI masuk sebagai lapisan kemampuan baru. Jika dilihat bersama-sama, ini bukan lagi serangkaian eksperimen yang terpisah, tetapi **arsitektur operasional yang semakin matang**. ([Reuters](#))

Pelajaran strategisnya jelas:

- **AI militer AS maju bukan karena satu teknologi ajaib,**
- **tetapi karena ada proses institusional yang mengubah prototipe menjadi sistem yang dipakai, dibiayai, dan dipelihara,**
- **serta ada jembatan antara data, cloud, software, komando, dan anggaran.**

Bagi Indonesia, ini pelajaran yang sangat penting. Banyak negara mampu membuat prototipe. Jauh lebih sedikit yang mampu mengubah prototipe menjadi **infrastruktur operasional nasional**.

4.6. Apa yang bisa dibuktikan dan apa yang harus dicurigai

Bab ini perlu ditutup dengan disiplin verifikasi, sesuai metode buku yang membedakan fakta resmi, analisis kredibel, promosi perusahaan, dan klaim yang masih indikatif. Komitmen pada verifikasi dan anti-halusinasi harus ditekankan.

Yang bisa dibuktikan dengan cukup kuat:

- **Project Maven** memang lahir sebagai upaya mengatasi banjir data ISR dan kini berkembang menjadi Maven Smart System yang dipakai Pentagon. ([Reuters](#))
- **CDAO** memang memimpin strategi dan adopsi data, analitik, dan AI lintas DoD, dan menyatukan fungsi JAIC, Chief Data Officer, DDS, serta Advana. ([U.S. Department of War](#))
- **Advana** memang merupakan platform data enterprise besar di DoD dengan skala pengguna dan konektivitas sumber data yang signifikan. ([U.S. Department of War](#))
- **Anthropic** memang menerima perjanjian prototipe CDAO dengan plafon US\$200 juta pada Juli 2025. ([Anthropic](#))
- **OpenAI** memang meluncurkan OpenAI for Government dan mengumumkan kontrak/pilot CDAO dengan plafon US\$200 juta pada Juni 2025. ([OpenAI](#))
- **Palantir** memang memegang kontrak besar Maven dan menjadi integrator penting dalam ekosistem tersebut. ([Reuters](#))

Yang harus dicurigai atau diperlakukan hati-hati:

- Klaim bahwa model tertentu **langsung memilih target mematikan** atau menjadi “otak digital” perang secara mandiri perlu diperlakukan hati-hati kecuali ada dokumen resmi atau sumber investigatif yang sangat kuat. Reuters sendiri tetap menulis bahwa Palantir mengatakan manusia tetap bertanggung jawab memilih dan menyetujui target. ([Reuters](#))
- Klaim sensasional dalam file lampiran seperti operasi spesifik, angka akurasi yang presisi, atau rincian penggunaan model tertentu di serangan tertentu **tidak boleh dijadikan fondasi utama** tanpa verifikasi tambahan. Dokumen outline Anda sendiri sudah mengingatkan bahwa beberapa klaim paling sensasional perlu diperlakukan sebagai bahan indikatif, bukan basis utama buku.
- Narasi perusahaan tentang *responsible AI* perlu dibaca bersama kepentingan komersial dan posisi politiknya. **Bahasa etika perusahaan tidak otomatis sama dengan praktik operasional di medan perang.**
- Sebaliknya, tuduhan bahwa AI sudah sepenuhnya menggantikan komandan juga berlebihan. Buku *AI at War* justru memperingatkan bahwa AI pada level strategis penuh masih menghadapi kerentanan serius, dan hilangnya kontrol manusia akan membawa risiko ekstrem.

Ringkasan kunci

- **AI militer AS adalah ekosistem**, bukan produk tunggal. Ia bertumpu pada Project Maven, CDAO, Advana, JWCC, integrator seperti Palantir, dan kini juga *frontier model* dari Anthropic dan OpenAI. ([Anthropic](#))
- **Project Maven** penting karena ia memperlihatkan logika dasar AI pertahanan AS: mempercepat pengolahan ISR dan memendekkan jarak antara data dan keputusan. ([Reuters](#))
- **Cloud, platform data, dan integrator** adalah tulang punggung sebenarnya; tanpa mereka, model AI besar tidak akan menjadi kekuatan operasional. ([Amazon Web Services, Inc.](#))
- **Anthropic dan OpenAI** masuk ke pertahanan AS bukan sebagai pengganti ekosistem lama, tetapi sebagai lapisan baru di atas infrastruktur yang sudah dibangun. ([Anthropic](#))
- **Perubahan paling penting** adalah pergeseran dari pilot project ke infrastruktur operasional yang permanen. ([U.S. Department of War](#))
- **Disiplin verifikasi wajib dijaga**: yang pasti adalah struktur ekosistemnya; yang sensasional tentang operasi tertentu harus tetap diperlakukan dengan hati-hati. ([Reuters](#))

Bab 5. AI dalam ISR, Command and Control, dan Targeting

Bab ini berada di pusat logika perang modern. Bila Bab 4 menjelaskan bahwa AI militer Amerika Serikat bekerja sebagai **ekosistem**, maka Bab 5 menjelaskan **dimana ekosistem itu paling terasa di medan operasi**: ISR, ruang komando, dan proses *targeting*. Bab ini ditempatkan sesudah pembahasan tentang Project Maven, *cloud*, integrator, dan *frontier model*. Sebab pada akhirnya, nilai AI pertahanan bukan diuji di ruang promosi teknologi, melainkan pada pertanyaan ini: **apakah AI membuat militer lihat lebih cepat, memahami lebih baik, memilih sasaran lebih tepat, dan bertindak tanpa kehilangan kendali manusia?**

5.1. AI untuk melihat dan menyaring

Ladang paling subur bagi AI militer hingga hari ini tetap **ISR**: *intelligence, surveillance, reconnaissance*. Alasannya sederhana. Medan perang modern menghasilkan terlalu banyak data untuk diproses manusia secara manual: video drone, citra satelit, radar, SIGINT, laporan lapangan, telemetry, dan *open-source intelligence*. *AI at War* berulang kali menekankan hubungan erat antara *big data*, ISR, dan OODA loop; AI menjadi penting karena ia dapat membantu menyaring, mengurutkan, dan menandai informasi yang bernilai dari lautan data yang terus mengalir.

Di level resmi, JADC2 dirancang justru untuk memungkinkan *Joint Force “sense, make sense, and act”* secara cepat dengan bantuan otomasi, AI, *predictive analytics*, dan *machine learning*. Artinya, DoD sendiri memandang AI sebagai alat untuk **melihat dan menyaring** sebelum ia menjadi alat untuk memutuskan. ([U.S. Department of War](#))

Kasus Ukraina menunjukkan bentuk paling nyata dari logika ini. Reuters melaporkan bahwa Ukraina telah mengumpulkan lebih dari **2 juta jam video perang** sejak 2022, terutama dari drone. Data itu dipakai untuk melatih model AI agar dapat membantu identifikasi target, menilai efektivitas serangan, dan mempercepat pengambilan keputusan. Dalam konteks ini, AI tidak menggantikan pengintai atau analis; ia membantu **mengurangi kebisingan** dan menonjolkan apa yang paling penting. ([Reuters](#))

Makna praktisnya:

- **AI membantu memilah data yang terlalu besar untuk dibaca manusia.**
- **AI mempercepat deteksi pola, objek, dan anomali.**
- **Nilai awal AI di perang nyata sering muncul sebagai alat penyaring, bukan penembak.** ([U.S. Department of War](#))

5.2. AI untuk menggabungkan data multi-sumber

Masalah besar militer modern bukan hanya banyaknya data, tetapi **terpisah-pisahannya data**. Satu sensor melihat gerakan, radar melihat jejak, satelit memberi citra, SIGINT menangkap emisi, drone memberi video, satuan lapangan memberi laporan teks. Secara terpisah, masing-masing berguna; tetapi keputusan yang baik lahir ketika semuanya bisa dibaca bersama. Di sinilah AI berperan dalam **fusi data multi-sumber**. Outline buku ini menyebutnya dengan tepat: dari “melihat” menuju “menggabungkan” dan kemudian “menentukan pilihan tindakan.”

AI at War menjelaskan bahwa masa depan ISR bergerak ke lingkungan *adaptive closed-loop control* yang memungkinkan AI bekerja lintas domain dan lintas platform untuk mengendalikan sensor, merencanakan rute, dan menghasilkan produk intelijen yang lebih terpadu. Ini penting karena perang modern bukan perang satu sensor; ia adalah perang banyak sensor yang harus berbicara dalam bahasa operasional yang sama.

Praktik Pentagon juga mengarah ke sana. Reuters menjelaskan bahwa Maven dirancang untuk **menginject data dari banyak sumber** guna mengidentifikasi *points of interest* dan mempercepat analisis intelijen serta keputusan *targeting*. Dengan kata lain, sistem seperti Maven tidak bernilai hanya karena ia memakai AI, tetapi karena ia menghubungkan sensor yang sebelumnya terpecah menjadi aliran informasi yang lebih siap pakai. ([Reuters](#))

Namun fusi data bukan perkara teknis semata. Ia juga masalah organisasi. *The AI Wave in Defence Innovation* menekankan bahwa interoperabilitas AI, berbagi data, dan penyatuan standar tetap menjadi hambatan serius di banyak militer. Ini berarti kemampuan menggabungkan data bukan hanya soal model, tetapi juga soal **politik data, standar, kepercayaan antar lembaga, dan kesiapan komando**.

Inti subbab ini:

- AI membantu menyatukan potongan-potongan informasi menjadi gambaran situasional.
- Fusi data adalah dasar bagi *command and control* modern.
- Tanpa integrasi organisasi dan standar data, AI sulit memberi nilai strategis. ([U.S. Department of War](#))

5.3. AI untuk prioritas target dan course of action

Setelah data disaring dan digabungkan, pertanyaan berikutnya adalah: **apa yang harus diprioritaskan?** Di sinilah AI mulai masuk ke wilayah yang lebih sensitif: *target prioritization* dan *course of action analysis*. AI dapat membantu menguraikan sasaran yang mungkin paling bernilai, memberi skor ancaman, mengidentifikasi pola gerak, dan menyajikan opsi tindakan kepada komandan. Ini masih berbeda dari “mesin memutuskan perang sendiri.” Yang terjadi lebih sering adalah AI membantu **mengurangi ruang pencarian** dan mempercepat pengambilan keputusan manusia.

Reuters menulis bahwa Maven telah membantu mengidentifikasi titik dan target potensial dari data medan perang, dan Reuters juga mencatat bahwa sistem itu mendukung ribuan *targeted strikes* dalam beberapa minggu terakhir—meski Reuters tetap menyebut bahwa Palantir menegaskan ada **pengawasan manusia** dalam penggunaannya. Ini penting: AI masuk ke rantai *targeting*, tetapi tidak otomatis berarti AI memegang keputusan akhir. ([Reuters](#))

Buku *Responsible Use of AI in Military Systems* dan *AI at War* sama-sama memberi peringatan bahwa AI sangat berguna untuk *decision support systems*, tetapi begitu ia masuk ke proses seleksi sasaran, risiko moral, hukum, dan operasional ikut naik. Karena itu perbedaan antara **dukungan keputusan** dan **senjata otonom** harus dijaga tegas. AI boleh membantu menentukan prioritas dan pilihan tindakan, tetapi proses penggunaan kekuatan harus tetap berada dalam struktur pertanggungjawaban manusia.

Nilai AI pada tahap ini:

- **mempercepat pengurutan prioritas sasaran,**
- **menyajikan *course of action* lebih cepat,**
- **membantu komandan menghadapi kompleksitas multi-domain,**
- **tetapi tetap harus dibatasi sebagai alat bantu, bukan pengambil keputusan akhir.**

5.4. Human-in-the-loop vs human-on-the-loop

Perdebatan paling penting dalam AI militer bukan sekadar “apakah AI dipakai?”, melainkan **di mana manusia berada dalam rantai keputusan**. Istilah *human-in-the-loop* biasanya berarti sistem tidak dapat menggunakan kekuatan tanpa persetujuan manusia pada tahap kritis. Sementara *human-on-the-loop* berarti manusia mengawasi sistem yang dapat bertindak lebih otonom dan masih punya peluang untuk campur tangan atau membatalkan tindakan. Buku *Responsible Use of AI in Military Systems* menjelaskan bahwa berbagai bentuk kontrol manusia dapat tersebar di banyak titik dalam siklus keputusan, baik sebelum aktivasi, selama pengawasan, maupun saat intervensi terakhir sebelum dampak.

Perdebatan ini juga muncul di level kebijakan AS. Menurut buku yang sama, DoD 2023 cenderung memakai istilah “**appropriate levels of human judgment**” ketimbang “*meaningful human control*.” Itu menunjukkan bahwa perdebatan belum selesai. Ada pihak yang menilai kata “control” lebih tepat karena menekankan tindakan nyata manusia, sementara pihak lain ingin memberi ruang pada sistem yang lebih otonom selama tetap sesuai hukum perang dan tata kelola operasional.

Pada tataran publik, Palantir menyatakan sistemnya tetap di bawah *human oversight*, dan deklarasi politik AS tentang penggunaan militer AI dan otonomi juga menekankan bahwa penggunaan AI harus berada dalam rantai komando yang bertanggung jawab dengan penilaian manusia yang sesuai. Jadi, dalam praktik kebijakan resmi, **AS belum menyatakan bahwa AI boleh menggantikan manusia dalam keputusan penggunaan kekuatan mematikan**. ([Reuters](#))

Yang perlu dipahami dengan jernih:

- ***Human-in-the-loop*** memberi rem manusia lebih kuat.
- ***Human-on-the-loop*** memberi AI lebih banyak ruang bertindak cepat.
- **Semakin cepat perang, semakin besar godaan untuk memindahkan manusia dari pusat keputusan ke pinggir pengawasan.**

5.5. Risiko false positives dan salah tafsir

Inilah sisi gelap AI dalam ISR dan *targeting*. Sistem yang pandai mengenali pola belum tentu benar memahami konteks. Model bisa salah mengklasifikasi kendaraan sipil, salah membaca aktivitas rutin sebagai ancaman, atau terlalu percaya diri pada data yang bias. *Responsible Use of AI in Military Systems* menegaskan bahwa bias data, asumsi model yang keliru, dan ketidakmampuan model menjelaskan dirinya dapat menghasilkan ketidakpercayaan atau, lebih buruk, keputusan salah yang tampak meyakinkan.

Masalah ini menjadi serius di perang karena objek tidak selalu tampil rapi seperti di dataset. Ada kamuflase, deception, kondisi cuaca, *sensor noise*, *concept drift*, dan taktik musuh yang memang dirancang untuk mengecoh mesin maupun manusia. *AI at War* sendiri memasukkan *concept drift*, *deception*, dan *black box* ke dalam persoalan penting AI militer. Dengan kata lain, kesalahan AI di medan perang bukan anomali; ia adalah risiko bawaan yang harus diasumsikan sejak awal.

Kesalahan seperti ini berbahaya karena AI cenderung memberi aura objektivitas. Jika operator tidak cukup kritis, keluaran model dapat diterima sebagai “fakta,” padahal ia hanyalah dugaan statistik. Dalam bahasa yang lebih keras: **AI bisa salah, dan kadang salahnya tampak sangat meyakinkan.** Itulah sebabnya *false positives* dalam konteks militer jauh lebih berbahaya daripada dalam konteks komersial biasa. Salah rekomendasi film bukan tragedi; salah identifikasi sasaran bisa memicu kematian, eskalasi, dan pelanggaran hukum perang.

Risiko utama yang harus diingat:

- salah klasifikasi sasaran,
- ketergantungan berlebihan pada model,
- kesalahan yang dipercepat oleh otomasi,
- dan kaburnya tanggung jawab ketika manusia terlalu percaya pada mesin.

5.6. Mengapa keputusan akhir harus tetap manusia

Pada akhirnya, inti bab ini adalah soal tanggung jawab. AI dapat membantu melihat, menyaring, menggabungkan data, memprioritaskan sasaran, bahkan menyusun *course of action*. Tetapi **keputusan akhir tentang penggunaan kekuatan harus tetap manusia**, karena yang dipertaruhkan bukan hanya efisiensi operasional, melainkan hukum, moral, legitimasi, dan pertanggungjawaban negara. Buku *Responsible Use of AI in Military Systems* sangat jelas: perdebatan tentang *meaningful human control* atau *appropriate levels of human judgment* bukan ornamen etis, tetapi inti dari bagaimana penggunaan AI dapat tetap berada dalam kerangka hukum perang dan akuntabilitas manusia.

Ini juga sejalan dengan arah kebijakan resmi AS. Deklarasi politik yang dipimpin AS menekankan perlunya penilaian dan kepedulian manusia yang sesuai dalam penggunaan militer AI dan otonomi. Bahkan ketika AI dipakai untuk mempercepat rantai keputusan, negara tetap mengakui perlunya manusia dalam rantai komando yang bertanggung jawab. ([State Department](#))

Ada alasan strategis mengapa manusia tidak bisa disingkirkan. Mesin bisa mengenali pola, tetapi tidak memikul tanggung jawab moral. Mesin bisa memberi rekomendasi, tetapi tidak memegang legitimasi politik. Mesin bisa menghitung probabilitas, tetapi tidak memahami sepenuhnya *proportionality*, *distinction*, dan konteks kemanusiaan yang selalu berubah di medan perang. Karena itu, semakin AI menjadi pengganda kecepatan, semakin penting pula **disiplin manusia** dalam memeriksa, meragukan, dan mengambil keputusan akhir.

Jadi, keputusan akhir harus tetap manusia karena:

- hanya manusia yang memegang tanggung jawab hukum dan moral,
- hanya manusia yang dapat menilai konteks lebih luas daripada pola data,
- dan hanya manusia yang dapat memikul akibat politik dari penggunaan kekuatan. ([State Department](#))

Ringkasan kunci

- **AI paling cepat memberi nilai di ISR**, terutama untuk melihat, menyaring, dan memprioritaskan data yang terlalu padat untuk diproses manual. ([U.S. Department of War](#))
- **Fusi data multi-sumber adalah inti *command and control* modern**, dan AI membantu menyatukan sensor, laporan, dan sinyal menjadi gambaran situasional yang lebih siap pakai. ([Reuters](#))
- **AI dapat membantu prioritas target dan *course of action***, tetapi itu harus dipahami sebagai *decision support*, bukan otomatisasi penuh penggunaan kekuatan. ([Reuters](#))
- **Perdebatan *human-in-the-loop* vs *human-on-the-loop* tetap terbuka**, tetapi kebijakan resmi AS masih menekankan pengawasan dan penilaian manusia. ([State Department](#))
- **Risiko *false positives*, bias, dan salah tafsir adalah ancaman nyata**, terutama ketika AI tampak meyakinkan padahal konteksnya salah.
- **Keputusan akhir harus tetap manusia**, karena akuntabilitas, hukum perang, dan legitimasi politik tidak bisa didelegasikan penuh ke mesin. ([State Department](#))

Bab 6. AI di Luar Medan Tembak: Logistik, Cyber, Maintenance, dan Simulasi

Salah satu salah paham paling umum tentang AI militer adalah anggapan bahwa nilainya terutama terletak pada *targeting* atau senjata otonom. Padahal dalam banyak organisasi militer, aplikasi AI yang paling cepat matang justru muncul **di belakang garis tembak**: pemeliharaan, logistik, *cyber defense*, *battle management*, dan simulasi. Fungsi non-kinetik dipetakan sebagai bab tersendiri. Itu penting, karena perang tidak dimenangkan hanya oleh siapa yang menembak lebih dulu, tetapi oleh siapa yang **tetap bisa bergerak, memasok, memperbaiki, melindungi jaringan, dan belajar lebih cepat**.

6.1. Predictive maintenance

Predictive maintenance adalah salah satu wilayah paling realistis bagi AI militer. Logikanya sederhana: alih-alih menunggu alat rusak lalu diperbaiki, atau mengganti komponen berdasarkan jadwal kaku, AI dipakai untuk membaca pola sensor, jam terbang, getaran, suhu, histori kerusakan, dan perilaku sistem agar kegagalan bisa diprediksi lebih awal. Ini mengubah *maintenance* dari reaktif menjadi prediktif. Buku *AI at War* dan *The AI Wave in Defence Innovation* sama-sama memberi ruang besar bagi aplikasi AI di sustainment dan kesiapan sistem, karena disinilah AI bisa memberi dampak besar tanpa langsung masuk ke wilayah paling kontroversial.

Di level resmi, rencana penerbangan Korps Marinir AS 2025 menyebut modernisasi “system component monitoring” untuk memungkinkan tindakan *predictive maintenance*. Sementara dokumen anggaran DoD dan DLA menunjukkan adanya jalur riset **Predictive Analytics, Modeling & Simulation** untuk logistik dan sustainment. Ini menunjukkan bahwa *predictive maintenance* bukan lagi jargon vendor, tetapi sudah masuk ke perencanaan kelembagaan. (media.defense.gov) ([Kantor Pengawas Pertahanan](#))

Makna strategisnya besar. Banyak militer sibuk membeli platform baru, tetapi lupa bahwa **kesiapan tempur nyata** ditentukan oleh berapa banyak sistem yang benar-benar siap dipakai hari ini, minggu depan, dan tiga bulan lagi. AI membantu menjawab pertanyaan itu dengan lebih presisi. Bagi negara dengan anggaran terbatas, ini sangat penting, karena setiap peningkatan kesiapan melalui *predictive maintenance* sering kali lebih murah daripada membeli platform baru. ([U.S. Department of War](#))

Nilai praktis *predictive maintenance*:

- mengurangi *downtime*,
- meningkatkan *readiness*,
- menghemat suku cadang dan jam kerja,
- membantu prioritas perbaikan berdasarkan risiko kegagalan. ([U.S. Department of War](#))

6.2. Logistik prediktif

Jika *maintenance* menjaga alat tetap hidup, maka logistik menjaga perang tetap bergerak. AI menjadi penting di sini karena rantai logistik militer sangat kompleks: permintaan amunisi, bahan bakar, suku cadang, obat, makanan, rotasi, distribusi antar-pangkalan, dan kesiapan industri pendukung. Dokumen anggaran DLA untuk FY2024–FY2026 secara eksplisit menyebut *Predictive Analytics, Modeling & Simulation* sebagai lini usaha riset untuk mengembangkan solusi AI/ML yang membantu *demand projection*, pengambilan keputusan, dan efisiensi logistik. Dengan kata lain, AI logistik sudah dipahami sebagai masalah inti, bukan tambahan kosmetik. ([Kantor Pengawas Pertahanan](#))

Ini sejalan dengan arah buku *AI at War*, yang menunjukkan bahwa perang modern sangat ditentukan oleh kemampuan menghubungkan operasi dengan sustainment. Platform yang canggih tetapi tidak ditopang pasokan yang tepat waktu akan cepat kehilangan nilai. Dalam bahasa yang lebih keras: **AI yang membantu suplai tiba tepat waktu bisa lebih strategis daripada AI yang hanya memberi visualisasi bagus di layar komando.**

Laporan Defense Business Board tentang *Supply Chain Illumination in the Department of Defense* pada Januari 2025 juga menunjukkan bahwa DoD masih menghadapi tantangan besar dalam visibilitas rantai pasok, dan merekomendasikan pendekatan yang lebih kuat untuk *decision making* berbasis data dan praktik terbaik sektor swasta. Ini memperlihatkan bahwa bahkan militer terbesar di dunia pun belum otomatis unggul dalam logistik digital; AI di logistik adalah proyek transformasi organisasi, bukan sekadar instalasi perangkat lunak. ([Badan Usaha Pertahanan](#))

AI logistik dipakai untuk:

- memproyeksikan permintaan,
- mengoptimalkan distribusi,
- memperkirakan kelangkaan dan titik putus pasokan,
- membantu *inventory management* dan prioritas pengiriman. ([Kantor Pengawas Pertahanan](#))

6.3. Battle management software

Di antara fungsi non-kinetik, *battle management software* adalah yang paling dekat ke jantung operasi. Perannya bukan menembak, tetapi **menyatukan informasi, menampilkan gambaran situasi, membantu sinkronisasi, dan mempercepat keputusan**. Inilah wilayah abu-abu antara “belakang layar” dan “medan tempur”, karena software seperti ini menghubungkan logistik, ISR, komando, dan aksi. Buku *AI at War* menekankan bahwa AI sangat penting dalam *command and control*, *integrated fires*, dan *battle networks*, bukan sebagai pengganti komandan, tetapi sebagai akselerator koordinasi.

Di level praktik, Reuters mencatat bahwa **Maven Smart System** telah menjadi inti operasi militer AS dalam menggabungkan data dari berbagai sumber untuk menemukan ancaman dan target potensial. Itu berarti *battle management software* bukan sekadar dashboard; ia adalah *workflow engine* yang menghubungkan data, analisis, komandan, dan keputusan. Bahkan ketika perannya masih diklaim sebagai *advisory tool*, dampaknya bisa sangat besar karena ia mempengaruhi ritme dan kualitas koordinasi. ([Reuters](#))

DoD juga menekankan bahwa *software-defined battlespace* menuntut transformasi proses dan budaya, bukan hanya pembelian aplikasi. *Software Modernization Implementation Plan FY25–26* menegaskan bahwa keunggulan kompetitif DoD bergantung pada pengiriman kapabilitas software yang tangguh “at the speed of relevance.” Artinya, *battle management software* adalah instrumen organisasi: nilai utamanya muncul ketika software menyatu dengan proses komando dan operasi, bukan sekadar saat dipresentasikan. ([CIO - U.S. Department of War](#))

Nilai *battle management software*:

- **mempercepat sinkronisasi antar-unit,**
- **mengurangi fragmentasi informasi,**
- **membantu komandan melihat gambaran operasional lebih utuh,**
- **dan menjadi jembatan antara data dan keputusan.** ([Reuters](#))

6.4. AI untuk cyber defense

AI di *cyber defense* sering lebih realistis daripada AI untuk senjata, karena lingkungan siber memang sangat padat data, cepat berubah, dan memerlukan deteksi pola skala besar. Buku *The Future of Violence* dan *The AI Wave in Defence Innovation* sama-sama memperlihatkan bahwa dunia ancaman modern makin kabur batasnya: *hackers*, *drones*, *malware*, dan perang informasi saling terkait. Dalam lingkungan seperti itu, AI berguna untuk **deteksi anomali, klasifikasi ancaman, prioritas respons, dan korelasi sinyal yang terlalu besar untuk dibaca manusia satu per satu**.

OpenAI sendiri, ketika meluncurkan OpenAI for Government dan kerjasamanya dengan CDAO, secara eksplisit menyebut **proactive cyber defense** sebagai salah satu area prototipe. Ini penting karena menunjukkan bahwa penggunaan resmi frontier AI yang paling dapat diterima secara politik justru ada pada wilayah pertahanan siber, bukan langsung di pemilihan target mematikan.

Di luar AS, Reuters melaporkan pada April 2026 bahwa Microsoft akan menginvestasikan **US\$10 miliar** di Jepang untuk memperluas infrastruktur AI dan memperdalam kerjasama *cyber defense* dengan pemerintah Jepang. Ini menunjukkan bahwa integrasi AI dan pertahanan siber telah menjadi agenda strategis lintas negara, bukan hanya urusan laboratorium. ([Reuters](#))

Tetapi AI siber juga membawa risiko baru: serangan bisa menjadi lebih otomatis, *deepfakes* bisa dipakai untuk gangguan komando, dan model AI sendiri bisa menjadi sasaran *prompt injection*, kebocoran data, atau manipulasi. Jadi AI di *cyber defense* adalah pedang bermata dua: ia memperkuat pertahanan, tetapi juga mempercepat perlombaan ancaman. ([Reuters](#))

Peran utama AI di *cyber defense*:

- **deteksi anomali dan pola serangan,**
- **prioritas peringatan dan respons,**
- **analisis lalu lintas dan korelasi insiden,**
- **serta dukungan bagi pembela jaringan yang kewalahan oleh volume ancaman.** ([Reuters](#))

6.5. Wargaming dan simulasi

Wargaming dan simulasi adalah arena penting lain bagi AI, justru karena di sinilah militer dapat menguji ide, doktrin, dan respons tanpa harus menunggu perang nyata. Outline buku ini tepat menempatkan *wargaming* dan simulasi dalam bab non-kinetik, karena AI di sini lebih berfungsi sebagai **mesin pembelajaran organisasi** daripada sebagai alat serang. Buku *AI at War* menempatkan simulasi, pembelajaran, dan adaptasi doktrin sebagai bagian penting dari transformasi AI dalam perang modern.

Secara kelembagaan, pendidikan militer dan pusat *wargaming* tetap menjadi bagian penting dari DoD. Dokumen anggaran FY2025 untuk National Defense University menunjukkan *Wargaming and Simulation* sebagai bagian fungsi inti institusi itu. Ini berarti simulasi tidak berdiri di pinggir, tetapi tetap berada di dalam pabrik intelektual pertahanan AS. ([Kantor Pengawas Pertahanan](#))

AI menambah nilai di sini dengan beberapa cara. Ia dapat membantu:

- membuat lawan simulasi lebih adaptif,
- menguji lebih banyak skenario dalam waktu lebih singkat,
- membaca pola hasil latihan,
- dan membantu mengevaluasi kelemahan organisasi atau konsep operasi.

Di Jerman, Reuters melaporkan pada Maret 2026 bahwa militer Jerman sedang mengembangkan alat AI untuk mempercepat analisis data medan dan memberi dukungan keputusan, dengan pelajaran dari Ukraina dan tetap menekankan bahwa AI akan menjadi alat penasihat, bukan pengganti keputusan manusia. Pola ini memperkuat satu hal: *wargaming* dan simulasi adalah tempat yang relatif aman untuk mematangkan AI sebelum dipakai lebih dalam di operasi nyata. ([Reuters](#))

6.6. Mengapa fungsi non-kinetik sering paling realistis lebih dulu

Banyak negara ingin melompat ke AI untuk penembakan, swarm, atau *autonomous targeting*. Tetapi dalam praktik, **fungsi non-kinetik sering lebih realistis, lebih murah, lebih dapat diterima secara politik, dan lebih mudah diinstitusikan terlebih dahulu**. Ada beberapa alasan.

- **Pertama**, data dan proses pada logistik, *maintenance*, dan *cyber* biasanya lebih terstruktur daripada medan perang terbuka.
- **Kedua**, risiko salah di wilayah ini, meski tetap serius, biasanya lebih bisa ditoleransi daripada salah identifikasi target mematikan.
- **Ketiga**, manfaatnya lebih mudah diukur: *downtime* turun, kesiapan naik, pasokan lebih presisi, insiden siber lebih cepat dideteksi.
- **Keempat**, organisasi lebih mudah menerima AI sebagai alat bantu “belakang layar” daripada sebagai penentu penggunaan kekuatan.

Itulah sebabnya penggunaan resmi frontier AI oleh OpenAI ke DoD ditekankan pada administrasi, akuisisi, kesehatan, dan *proactive cyber defense*, bukan langsung pada *lethal targeting*. Demikian pula banyak dokumen DoD lebih dulu menekankan data, analitik, *decision support*, dan *software modernization* ketimbang mengumumkan AI sebagai senjata otonom utama. ([CIO - U.S. Department of War](#))

Pelajaran strategisnya jelas: **jalan paling masuk akal menuju AI militer yang matang sering dimulai dari fungsi non-kinetik**, lalu baru bergerak ke area yang lebih sensitif. Negara yang memaksa lompatan langsung ke senjata otonom biasanya justru membangun hype lebih cepat daripada kapasitas nyata.

6.7. AI sebagai penguat organisasi, bukan hanya senjata

Bab ini sebaiknya ditutup dengan satu penegasan: AI militer yang paling matang sering bekerja sebagai **penguat organisasi**. Ia membantu organisasi melihat pola, mengalokasikan sumber daya, menjaga kesiapan, menghubungkan data, melindungi jaringan, dan belajar lewat simulasi. Dalam arti ini, AI bukan sekadar tambahan pada senjata, tetapi tambahan pada **kapasitas institusi**. Outline *Onno W. Purbo, AI di Militer, 2026* sangat kuat ketika menekankan AI sebagai penghubung data, sensor, logistik, keputusan, dan organisasi.

Buku *The AI Wave in Defence Innovation* dan *Responsible Use of AI in Military Systems* sama-sama menunjukkan bahwa nilai AI tidak terletak hanya pada kecerdasan algoritmik, tetapi pada kemampuannya dipadukan dengan struktur organisasi, tata kelola, dan tanggung jawab manusia. Tanpa itu, AI hanya menjadi aksesoris presentasi. Dengan itu, AI bisa menjadi alat untuk memperkuat *readiness*, *resilience*, dan *decision superiority*.

Bagi Indonesia, pelajaran ini sangat penting. Negara yang ingin mengejar ketertinggalan tidak harus mulai dari model AI paling besar atau sistem senjata paling glamor. Titik masuk yang lebih realistis justru ada pada:

- **maintenance dan kesiapan alutsista,**
- **logistik dan stok,**
- **cyber defense,**
- **simulasi dan wargaming,**
- **serta battle management software yang menghubungkan semuanya.**

Di situlah AI mulai berubah dari slogan menjadi **kapabilitas nasional yang benar-benar terasa**.

Ringkasan kunci

- **Aplikasi AI militer yang paling cepat matang sering muncul di luar medan tembak**, terutama di *maintenance*, logistik, *cyber defense*, *battle management*, dan simulasi. ([CIO - U.S. Department of War](#))
- **Predictive maintenance penting** karena meningkatkan kesiapan tempur dengan memprediksi kegagalan sebelum sistem rusak. ([U.S. Department of War](#))
- **Logistik prediktif adalah kekuatan strategis**, karena perang dimenangkan juga oleh siapa yang paling mampu menjaga aliran pasokan dan visibilitas rantai pasok. ([Kantor Pengawas Pertahanan](#))
- **Battle management software menjadi jembatan utama antara data dan keputusan**, dan kini makin menjadi inti operasi militer modern. ([Reuters](#))
- **AI untuk cyber defense termasuk wilayah penggunaan paling realistis dan paling berkembang**, tetapi juga membawa risiko ancaman yang makin otomatis. ([Reuters](#))
- **Wargaming dan simulasi** memberi ruang aman untuk menguji konsep, skenario, dan pembelajaran organisasi sebelum masuk ke operasi nyata. ([Reuters](#))
- **Fungsi non-kinetik sering lebih realistis lebih dulu** karena datanya lebih terstruktur, manfaatnya lebih mudah diukur, dan risikonya lebih bisa dikendalikan. ([CIO - U.S. Department of War](#))
- **AI paling berguna ketika ia memperkuat organisasi**, bukan hanya ketika ia dipasang pada senjata.

Bagian III. Ukraina: Laboratorium War-Ready AI dalam Kondisi Terbatas

Bab 7. Ukraina: Dari Korban Invasi ke Ekosistem Defense Tech

Bab ini penting karena Ukraina memberi satu pelajaran yang sangat keras: **negara yang diserang tidak selalu hanya menjadi korban; ia bisa berubah menjadi laboratorium inovasi perang paling cepat di dunia.** Ukraina bukan dibaca sekadar sebagai medan perang, tetapi sebagai contoh bagaimana data tempur, drone murah, AI, pengadaan cepat, dan industri kecil dapat dipadukan menjadi ekosistem pertahanan yang adaptif. Outline buku ini tepat ketika menempatkan Ukraina sebagai jembatan antara teori AI militer dan pelajaran praktis untuk Indonesia.

7.1. Mengapa Ukraina menjadi laboratorium perang AI

Ukraina menjadi laboratorium perang AI bukan karena sejak awal memiliki industri pertahanan paling besar atau AI paling canggih, tetapi karena **perang memaksanya mengubah kebutuhan mendesak menjadi siklus inovasi yang sangat cepat.** Reuters melaporkan bahwa Ukraina telah mengumpulkan lebih dari **2 juta jam video tempur** dari perang, terutama dari drone, dan menjadikannya bahan untuk melatih model AI bagi identifikasi target, evaluasi serangan, dan dukungan keputusan. Pada 2026, Reuters juga melaporkan Ukraina mulai membuka akses ke data tempur itu bagi negara sekutu untuk melatih *drone AI software*, menandakan bahwa pengalaman perang telah berubah menjadi aset strategis yang bisa dipakai untuk membangun kemampuan baru. ([reuters.com](https://www.reuters.com)) ([reuters.com](https://www.reuters.com))

Ada tiga alasan mengapa Ukraina sangat penting dibaca.

- **Pertama**, ia berperang dalam kondisi sangat keras, sehingga hanya teknologi yang benar-benar berguna yang bertahan.
- **Kedua**, ia menggabungkan teknologi sipil, startup, sukarelawan teknis, dan negara dalam satu ekosistem perang.
- **Ketiga**, ia belajar sangat cepat karena umpan balik dari medan tempur datang hampir tanpa jeda.

Karena itu, Ukraina penting bukan semata karena ia memakai AI, tetapi karena ia menunjukkan **bagaimana AI, data, drone, dan organisasi bisa dipaksa bertemu di bawah tekanan perang nyata.** Itulah yang membuat banyak analis Barat melihat Ukraina sebagai *living laboratory* atau laboratorium nyata perang drone dan AI. ([reuters.com](https://www.reuters.com))

7.2. Frontline-driven innovation

Pelajaran paling menonjol dari Ukraina adalah bahwa inovasi tidak lagi bergerak dari laboratorium ke lapangan secara lambat. Di Ukraina, inovasi bergerak dari **garis depan ke bengkel, ke startup, ke jalur produksi, lalu kembali lagi ke garis depan**. Dengan kata lain, kebutuhan tempur langsung memandu desain, iterasi, dan pembelian. Inilah yang dalam banyak analisis disebut *frontline-driven innovation*.

CSIS menekankan bahwa salah satu hal paling penting dari Ukraina adalah bagaimana negara itu membangun kembali sistem akuisisinya di sekitar teknologi komersial, khususnya sistem nirawak, sehingga kebutuhan garis depan dapat diterjemahkan lebih cepat menjadi produk yang benar-benar dipakai. Reuters juga menunjukkan pola yang sama: pengumpulan data tempur, pelatihan AI, uji lapangan, revisi cepat, dan pengembangan produk berjalan hampir bersamaan, bukan bertahap seperti pola birokrasi lama. (csis.org) (reuters.com)

Logika ini membuat Ukraine berbeda dari banyak negara lain. Banyak militer membeli sistem jadi, lalu berusaha menyesuaikan operasi dengan produk yang ada. Ukraina melakukan hal sebaliknya: **produk dipaksa menyesuaikan diri dengan realitas pertempuran**. Itulah sebabnya siklus belajarnya cepat sekali.

Ciri *frontline-driven innovation* Ukraina:

- kebutuhan unit tempur langsung membentuk desain,
- iterasi dilakukan dalam hitungan minggu, bukan tahun,
- data tempur menjadi bahan baku inovasi,
- dan keberhasilan diukur dari kegunaan di lapangan, bukan dari presentasi teknologi. (csis.org)

7.3. Startup, bengkel, dan produsen kecil

Salah satu hal paling penting dari ekosistem Ukraina adalah bahwa inovasi tidak dimonopoli kontraktor pertahanan besar. Reuters melaporkan bahwa sektor pertahanan Ukraina kini terdiri dari **lebih dari 1.000 perusahaan**, banyak diantaranya merupakan perusahaan swasta kecil yang lahir setelah invasi 2022. Ini berarti perang telah membuka ruang bagi *startup*, bengkel, insinyur kecil, dan produsen lokal untuk masuk langsung ke ekosistem pertahanan. ([reuters.com](https://www.reuters.com))

Di sinilah keunggulan Ukraina menjadi sangat khas. Perusahaan kecil sering lebih lambat di pendanaan, tetapi lebih cepat dalam adaptasi. Mereka tidak terikat terlalu kuat pada proses berat, sehingga bisa:

- mengganti komponen cepat,
- memperbaiki desain berdasar umpan balik operator,
- membuat varian baru drone atau *payload*,
- dan menyesuaikan produk dengan kebutuhan misi tertentu.

Reuters juga melaporkan bahwa Ukraina sekarang bukan hanya memproduksi untuk konsumsi sendiri. Pada 2026, Kyiv mulai membuka jalur ekspor resmi untuk produk pertahanannya, termasuk drone, dan bahkan membangun pusat ekspor di Eropa. Ini menandakan bahwa *startup* dan produsen kecil di Ukraina mulai bergerak dari mode bertahan hidup ke mode **pembangunan industri pertahanan yang lebih permanen**. ([reuters.com](https://www.reuters.com))

Bagi pembaca Indonesia, pelajaran ini sangat penting: **inovasi pertahanan yang cepat hampir selalu membutuhkan ruang besar bagi pemain kecil**, bukan hanya BUMN besar atau kontraktor lama.

7.4. Negara yang belajar sangat cepat

Ukraina menarik bukan hanya karena industrinya cepat, tetapi karena **negara dan militernya juga belajar cepat**. Buku *The AI Wave in Defence Innovation* menekankan bahwa keunggulan teknologi militer tidak akan berarti tanpa adaptasi organisasi, operasional, dan strategis. Ukraina adalah contoh paling nyata dari tesis ini: negara yang awalnya berada dalam posisi sangat terdesak mampu bergerak dari improvisasi menuju pembelajaran institusional.

Reuters mencatat bahwa Menteri Pertahanan dan pejabat digital Ukraina mendorong pembukaan data tempur untuk sekutu, pengembangan AI anti-drone, dan pembentukan lingkungan aman seperti **Brave1 Dataroom** untuk melatih model AI pada data perang nyata. Ini menunjukkan bahwa negara Ukraina tidak hanya membeli teknologi, tetapi berusaha membangun *feedback loop* antara medan tempur, data, AI, industri, dan kebijakan. (reuters.com)

Kementerian Pertahanan Ukraina sendiri menyatakan bahwa Brave1 Dataroom diluncurkan untuk menyediakan lingkungan aman bagi pelatihan solusi AI militer, dengan fokus awal pada deteksi otonom dan intersepsi drone udara. Ini memberi sinyal bahwa pembelajaran Ukraina sudah naik kelas: dari improvisasi drone lapangan ke **institusionalisasi data dan model**. (mod.gov.ua)

Mengapa Ukraina terlihat belajar cepat:

- umpan balik tempur datang terus-menerus,
- negara memberi ruang eksperimen,
- data perang dikumpulkan dan dipakai ulang,
- dan struktur kelembagaan mulai dibangun di atas praktik yang terbukti. (mod.gov.ua)

7.5. Dari improvisasi ke institusionalisasi

Pada fase awal perang, banyak inovasi Ukraina lahir dari improvisasi: drone komersial dimodifikasi, *software* sederhana dipakai untuk koordinasi, dan kebutuhan taktis dijawab dengan cara yang sangat pragmatis. Tetapi yang membuat Ukraina berbeda adalah kemampuannya bergerak dari improvisasi itu menuju **institusionalisasi**.

Simbol terpenting dari proses ini adalah **Brave1**, klaster inovasi pertahanan resmi Ukraina. Brave1 berfungsi sebagai simpul yang menghubungkan pemerintah, militer, pengembang, pendanaan, pengujian, dan adopsi. Di luar itu, Reuters melaporkan bahwa Ukraina kini juga mulai menginternasionalisasi basis industrinya: ekspor dibuka, kerjasama produksi dengan Rumania dibahas, dan teknologi Ukraina mulai diposisikan sebagai bagian dari keamanan Eropa. ([reuters.com](https://www.reuters.com))

Transisi ini penting karena banyak negara bisa berimprovisasi saat krisis, tetapi sedikit yang mampu mengubah improvisasi menjadi **sistem nasional yang bertahan**. Ukraina menunjukkan bahwa perang yang memaksa bisa, bila direspons dengan benar, menciptakan empat hal:

- **jalur pengadaan cepat,**
- **ekosistem pengujian dan revisi,**
- **struktur koordinasi inovasi,**
- **dan basis industri yang mulai bisa mengekspor.** ([reuters.com](https://www.reuters.com))

7.6. Mengapa perang memaksa inovasi menjadi praktis

Perang membuat inovasi Ukraina menjadi praktis karena perang tidak memberi hadiah pada teknologi yang sekadar mengesankan. Ia hanya memberi nilai pada teknologi yang:

- benar-benar bekerja,
- cepat diperbaiki saat gagal,
- cukup murah untuk diproduksi banyak,
- dan cukup sederhana untuk dilatih dan dipakai unit di lapangan.

Itulah sebabnya kekuatan Ukraina bukan terutama pada “AI paling maju,” tetapi pada **loop pembelajaran yang sangat cepat**. Dokumen terlampir Anda sendiri merumuskan formula itu dengan tajam: *data tempur nyata* → *startup cepat* → *uji di garis depan* → *revisi mingguan* → *pembelian cepat* → *produksi massal* → *ekspor bersama sekutu*. Itu menangkap esensinya dengan sangat baik.

Reuters juga menegaskan bahwa inovasi Ukraina tidak menghapus masalah klasik perang. Rusia telah mengejar ketertinggalan UAV, memproduksi drone dalam jumlah sangat besar, dan Ukraina tetap menghadapi persoalan personel, amunisi, dan tekanan industri. Jadi pelajaran yang paling jujur adalah ini: **inovasi cepat bukan pengganti semua kelemahan, tetapi ia dapat memperbesar daya tahan dan daya serang secara signifikan.** ([reuters.com](https://www.reuters.com))

Di titik inilah Ukraina menjadi sangat relevan bagi Indonesia. Bukan karena Indonesia harus meniru perang Ukraina, tetapi karena Ukraina menunjukkan satu prinsip universal: **teknologi pertahanan yang paling berharga adalah yang paling cepat dipaksa menjadi berguna.**

Ringkasan kunci

- **Ukraina menjadi laboratorium perang AI** karena perang memaksanya mengubah data tempur, drone, dan AI menjadi kemampuan nyata dengan sangat cepat. ([reuters.com](https://www.reuters.com))
- **Frontline-driven innovation** adalah inti model Ukraina: kebutuhan garis depan langsung membentuk desain, revisi, dan pembelian. ([csis.org](https://www.csis.org))
- **Ekosistemnya ditopang oleh startup, bengkel, dan produsen kecil**, bukan hanya pemain besar. ([reuters.com](https://www.reuters.com))
- **Ukraina belajar cepat sebagai negara**, bukan hanya sebagai industri, dengan membangun *feedback loop* antara data perang, AI, kebijakan, dan pengadaan. ([reuters.com](https://www.reuters.com))
- **Brave1 dan Dataroom menandai transisi dari improvisasi ke institusionalisasi.** (mod.gov.ua)
- **Perang memaksa inovasi menjadi praktis**: yang bertahan bukan teknologi paling glamor, tetapi yang paling berguna, murah, cepat diperbaiki, dan cepat diproduksi. ([reuters.com](https://www.reuters.com))

Bab 8. Data Tempur sebagai Aset Strategis Ukraina

Bab ini berada di pusat pelajaran Ukraina. Jika Bab 7 menjelaskan bagaimana Ukraina membangun ekosistem *defense tech* di bawah tekanan perang, maka Bab 8 menunjukkan **bahan bakar utama ekosistem itu: data tempur**. Ukraina tidak hanya memproduksi drone dan *software*; Ukraina sedang mengubah pengalaman perang menjadi **aset data** yang bisa dipakai untuk AI, operasi, pengadaan, bahkan kerja sama strategis dengan sekutu.

8.1. Video drone, sensor, satelit, dan laporan tempur

Perang Ukraina menghasilkan arus data yang luar biasa besar. Sumber utamanya bukan satu, melainkan campuran **video drone, citra satelit, sensor lapangan, telemetry, laporan unit tempur, dan data pengintaian dari banyak platform**. Reuters melaporkan bahwa sejak 2022 Ukraina telah mengumpulkan lebih dari **2 juta jam video perang**, terutama dari drone. Sistem OCHI yang dibangun sejak 2022 membantu memberi komandan gambaran area tempur dengan menampilkan umpan video dari banyak kru drone secara bersamaan, lalu berkembang menjadi arsip perang yang terus bertambah sekitar **5–6 terabyte per hari**. ([Reuters](#))

Dari sudut pandang teori militer AI, ini sangat masuk akal. *AI at War* menekankan bahwa ISR, *big data*, dan C4ISR kini saling terkait erat; perang modern menghasilkan arus data yang begitu besar sehingga keunggulan tidak lagi hanya ditentukan oleh kemampuan mengumpulkan data, tetapi oleh kemampuan **mengubah data mentah menjadi pemahaman yang siap dipakai**.

Bagi Ukraina, kombinasi sumber data ini menciptakan sesuatu yang jarang dimiliki negara lain: **rekaman perang intensitas tinggi yang terus-menerus, sangat dekat dengan garis depan, dan dikumpulkan dalam skala besar**. Itulah yang menjadikan Ukraina bukan hanya pengguna AI militer, tetapi juga penghasil salah satu kumpulan data tempur paling bernilai di dunia saat ini. ([Reuters](#))

Sumber data utama Ukraina meliputi:

- video drone ISR dan serangan,
- sensor dan telemetry dari operasi tempur,
- citra satelit dan pengamatan jarak jauh,
- laporan tempur manusia dari unit lapangan,
- serta data hasil serangan, intersepsi, dan penilaian efek. ([Reuters](#))

8.2. Data sebagai bahan bakar AI

Kalimat paling penting dalam bab ini adalah: **AI tanpa data tempur yang baik akan cepat jatuh menjadi demo laboratorium.** Buku *AI at War* sangat jelas menyatakan bahwa implementasi AI harus dimulai dengan pertanyaan tentang sumber data: siapa yang memiliki data, apakah datanya cukup, apakah datanya bersih, bagaimana aksesnya, dan bagaimana kualitasnya. Analogi yang dipakai buku itu sangat kuat: data yang salah atau kotor dalam algoritma AI seperti bahan bakar kotor di pesawat—keduanya tidak layak dipercaya untuk performa tinggi.

Ukraina menjadi penting justru karena memiliki “bahan bakar” itu. Reuters melaporkan data perang yang dikumpulkan Ukraina dipakai untuk melatih model AI agar dapat:

- mengidentifikasi target,
- menilai efektivitas senjata,
- membantu keputusan taktis dan strategis,
- serta belajar dari pola tempur nyata. ([Reuters](#))

Di 2026, langkah itu naik kelas. Reuters melaporkan Ukraina membuka akses ke data medan tempurnya bagi negara sekutu untuk melatih *drone AI software*. Ini berarti Ukraina memandang data perang bukan hanya sebagai arsip operasional, tetapi sebagai **kapital teknologi**. Dataset tempur yang terus diperbarui memberi nilai yang sangat tinggi untuk pelatihan model navigasi, deteksi ancaman, pengenalan sasaran, dan otonomi sistem nirawak. ([Reuters](#))

Buku *Responsible Use of AI in Military Systems* juga membantu menjelaskan mengapa ini penting. AI militer yang matang bukan sekadar *machine learning* sempit, tetapi “awan algoritma” yang memadukan berbagai pendekatan untuk menghasilkan *near real-time situation pictures* dari aliran data heterogen. Dengan kata lain, **data bukan pelengkap AI; data adalah syarat keberadaannya.**

Mengapa data menjadi bahan bakar AI Ukraina:

- karena data tempur memberi contoh dunia nyata, bukan contoh sintesis,
- karena model belajar dari pola musuh, lingkungan, dan hasil operasi aktual,
- dan karena data itu terus bertambah, diperbarui, dan divalidasi oleh perang sendiri. ([Reuters](#))

8.3. Battlefield awareness dan fusion

Nilai tertinggi dari data tempur bukan hanya pada jumlahnya, tetapi pada kemampuannya membentuk **kesadaran situasional medan perang**. Reuters menjelaskan bahwa OCHI awalnya dibuat untuk memberi komandan pandangan serentak dari banyak kru drone di satu area. Itu artinya data tidak diperlakukan sekadar sebagai rekaman, tetapi sebagai alat untuk membangun *battlefield awareness* secara operasional. ([Reuters](#))

Secara konseptual, ini sangat dekat dengan apa yang dijelaskan dalam *Responsible Use of AI in Military Systems*: AI memproses sinyal, pengukuran, dan laporan dari banyak sumber heterogen menjadi gambaran situasi yang komprehensif dan hampir *real time*, yang kemudian dipakai komandan untuk memahami keadaan dan status misi. Proses ini pada intinya adalah **data fusion**—menggabungkan potongan-potongan informasi menjadi gambaran medan perang yang lebih utuh.

Dalam praktik Ukraina, *fusion* itu muncul setidaknya pada tiga level:

- **level taktis**, ketika video drone dan laporan unit dipakai untuk keputusan langsung di lapangan;
- **level operasional**, ketika pola serangan, pergerakan, dan efek serangan dianalisis lintas unit;
- **level strategis**, ketika data tempur dikumpulkan sebagai basis pelatihan model dan pengembangan doktrin. ([Reuters](#))

Itulah sebabnya data tempur Ukraina bernilai tinggi. Ia tidak hanya memberi “apa yang terlihat”, tetapi membantu menjawab:

- apa yang bergerak,
- pola apa yang muncul,
- apa yang berhasil dihantam,
- apa yang gagal,
- dan bagaimana lawan beradaptasi.

Dalam perang modern, keunggulan sering lahir bukan dari siapa yang punya lebih banyak sensor, tetapi dari siapa yang **lebih cepat memadukan hasil sensor menjadi pemahaman yang bisa ditindaklanjuti**.

8.4. Mengapa data perang lebih berharga daripada demo laboratorium

Inilah pelajaran paling keras dari Ukraina. Banyak negara dan perusahaan memiliki demo AI yang impresif: *object recognition*, *path planning*, *autonomy*, *dashboard analytics*. Tetapi data perang Ukraina memberi sesuatu yang tidak bisa ditiru mudah di laboratorium: **kekacauan nyata**.

Di medan perang ada:

- cuaca buruk,
- gangguan sinyal,
- kamuflase,
- *deception*,
- sudut pandang kamera yang jelek,
- objek rusak atau sebagian tertutup,
- perubahan pola lawan,
- dan tekanan waktu yang tidak memberi ruang untuk “ideal conditions”.

AI at War mengingatkan bahwa diskusi implementasi AI harus dimulai dari *clean data*, kualitas data, dan akses data. Tetapi perang menambahkan lapisan lain: data tempur justru sangat berharga karena ia memuat **noise, ambiguitas, dan perilaku musuh yang nyata**. Itulah data yang paling dibutuhkan untuk melatih sistem yang benar-benar *war-ready*.

Reuters menulis bahwa minat sekutu pada data Ukraina tinggi karena pengalaman perang Rusia-Ukraina memberi bahan yang relevan untuk membangun sistem AI bagi konflik masa depan. Ini memperlihatkan satu hal: **data perang yang keras lebih bernilai daripada demo laboratorium yang bersih**. Demo bisa menunjukkan potensi. Data tempur menunjukkan apakah sistem akan tetap berguna ketika dunia tidak lagi rapi. ([Reuters](#))

Bagi militer, perbedaan ini sangat penting.

- **Demo laboratorium menunjukkan bahwa model bisa bekerja.**
- **Data perang menunjukkan apakah model tetap bekerja ketika semua hal yang bisa salah benar-benar salah.**

Itu sebabnya data Ukraina dipandang sebagai salah satu komoditas strategis paling bernilai dalam perlombaan AI militer saat ini. ([Reuters](#))

8.5. Politik data, keamanan data, dan nilai industrinya

Begitu data tempur menjadi aset strategis, ia langsung berubah menjadi **objek politik, keamanan, dan industri**. Ukraina sadar bahwa data perang tidak bisa dibuka sembarangan. Karena itu, langkah membuka akses ke sekutu dilakukan melalui platform aman. Reuters melaporkan bahwa Ukraina menyediakan akses melalui kerangka kerja yang aman untuk *joint analytics* dan pelatihan model bersama mitra. ([Reuters](#))

Kementerian Pertahanan Ukraina menyatakan bahwa **Brave1 Dataroom** diluncurkan sebagai lingkungan aman untuk melatih solusi AI militer, dengan kolaborasi antara Kementerian Pertahanan, Angkatan Bersenjata Ukraina, lembaga riset intelijen militer, Brave1, dan Palantir. Fokus awalnya adalah deteksi otonom dan intersepsi UAV musuh. Artinya, Ukraina sedang membangun **rezim keamanan data tempur**, bukan hanya gudang data. ([mod.gov.ua](#))

Dari sisi industri, nilainya juga besar. Platform Brave1 sendiri secara resmi diposisikan sebagai mesin untuk membangun *DefenseTech industry* Ukraina, menarik investasi, dan menghubungkan solusi teknologi dengan kebutuhan pertahanan nyata. Jadi data tempur Ukraina bukan hanya dipakai untuk pertahanan saat ini, tetapi juga untuk:

- **membesarkan industri domestik,**
- **menarik mitra luar negeri,**
- **menciptakan *reference advantage* untuk produk Ukraina,**
- **dan memperkuat posisi Ukraina dalam kerja sama keamanan Eropa dan NATO-adjacent ecosystems.** ([Digital State](#))

Tetapi ada juga sisi gelapnya. Semakin penting data perang, semakin besar pula risikonya:

- kebocoran data sensitif,
- penyusupan data palsu,
- manipulasi dataset,
- dan ketergantungan pada mitra teknologi asing.

Buku *Responsible Use of AI in Military Systems* mengingatkan bahwa hilangnya integritas data dapat menghasilkan gambaran situasi yang salah, keputusan yang salah, dan ruang luas bagi intervensi lawan melalui data menipu. Jadi politik data tempur bukan hanya soal kepemilikan, tetapi juga soal **integritas, kontrol akses, audit, dan ketahanan terhadap manipulasi**.

Ringkasan kunci

- **Ukraina sedang mengubah data tempur menjadi aset strategis nasional.** Video drone, sensor, satelit, dan laporan tempur kini menjadi sumber daya inti bagi AI militer. ([Reuters](#))
- **Data adalah bahan bakar AI.** Tanpa data tempur yang cukup, bersih, dan relevan, AI militer akan berhenti sebagai demo.
- **Nilai tertinggi data tempur terletak pada *battlefield awareness* dan *fusion*.** Data dipakai untuk membangun gambaran situasi yang bisa ditindaklanjuti, bukan sekadar arsip. ([Reuters](#))
- **Data perang lebih berharga daripada demo laboratorium** karena memuat kompleksitas, gangguan, ambiguitas, dan adaptasi musuh yang nyata. ([Reuters](#))
- **Politik data dan keamanan data kini menjadi isu inti.** Brave1 Dataroom menunjukkan bahwa Ukraina sedang membangun bukan hanya dataset, tetapi juga rezim akses aman, kemitraan, dan nilai industri di atasnya. ([Reuters](#))
- **Pelajaran terbesarnya:** di perang modern, yang dikumpulkan bukan hanya senjata dan amunisi, tetapi juga **data yang nantinya membentuk AI, doktrin, dan industri generasi berikutnya.**

Bab 9. Industri Drone Ukraina: Murah, Cepat, Tersebar

Bab ini menjelaskan inti kekuatan Ukraina yang paling sering disalahpahami. Banyak orang melihat drone Ukraina hanya sebagai alat perang murah. Padahal yang lebih penting adalah **arsitektur industrinya**: cepat, tersebar, fleksibel, dan terus belajar dari medan tempur. Bab ini ditempatkan sesudah pembahasan tentang data tempur. Sebab industri drone Ukraina tidak tumbuh di ruang kosong; ia tumbuh dari kombinasi **data perang, kebutuhan garis depan, pengadaan cepat, dan ekosistem perusahaan kecil**.

9.1. Fast-track procurement

Salah satu keunggulan paling khas Ukraina adalah **jalur pengadaan yang dipercepat**. Bukan berarti tanpa seleksi, tetapi produk yang cukup efektif bisa diuji, dipakai, lalu diperbaiki tanpa menunggu siklus pengadaan yang terlalu lambat. Bahan terlampir Anda sudah merumuskan ini dengan tepat: *fast-track procurement* berarti sistem yang sudah “cukup baik” segera dibeli dan dipakai, walau masih terus disempurnakan.

Pelembagaan paling nyata dari logika ini adalah **Brave1 Market**. Pemerintah Ukraina menjelaskan bahwa platform ini memberi satuan militer cara cepat untuk mengakses teknologi, mulai dari drone, robot darat, sistem AI, sampai perangkat *electronic warfare*. Pada tahap awal, pembelian dilakukan dengan anggaran satuan, lalu diperluas dengan skema *combat points* untuk menukar hasil tempur terverifikasi dengan teknologi yang dibutuhkan. Pemerintah Ukraina juga melaporkan bahwa sampai 29 Januari 2026, militer telah memesan **240.000 drone** melalui Brave1 Market menggunakan *combat e-Points*. (digitalstate.gov.ua) (kmu.gov.ua)

Ini penting karena mengubah pengadaan dari model birokrasi tradisional menjadi **putaran umpan balik tempur–pengadaan–produksi**. Unit yang berhasil menghancurkan target tidak hanya mendapat pengakuan, tetapi juga mempercepat akses pada alat yang mereka nilai paling berguna. Dalam bahasa yang lebih tajam, Ukraina sedang mencoba membuat pengadaan **lebih dekat ke kebutuhan nyata daripada ke logika katalog**.

Ciri utama *fast-track procurement* Ukraina:

- produk yang cukup efektif cepat masuk lapangan,
- umpan balik tempur langsung mempengaruhi pembelian berikutnya,
- pasar dan insentif digital dipakai untuk mempercepat akses satuan ke alat yang relevan. (digitalstate.gov.ua) (kmu.gov.ua)

9.2. Drone murah sebagai tulang punggung tempur

Kekuatan utama Ukraina bukan bertumpu pada sedikit platform mewah, tetapi pada **volume sistem murah yang bisa diproduksi, dikorbankan, dan diganti cepat**. Bahan terlampir Anda menekankan hal ini dengan tepat: Ukraina membanjiri ruang tempur dengan *attributable systems*, bukan mengandalkan sedikit platform mahal.

Reuters melaporkan bahwa Ukraina bertaruh besar pada **interceptor drones** sebagai *low-cost air shield*, karena persediaan misil pertahanan udara tradisional terbatas dan mahal. Pada 2025, Presiden Zelenskyy meminta dana **US\$6 miliar** untuk memperbesar produksi *interceptor drones* dengan target **1.000 unit per hari**. Reuters juga menulis bahwa biaya intersepsi dengan drone dapat jauh lebih murah daripada intersepsi dengan misil, dan model ini mulai menjadi lapisan pertahanan yang sangat penting terhadap ancaman pengintaian dan *kamikaze drones*. (reuters.com)

Ini menunjukkan pergeseran ekonomi perang yang sangat besar. Drone murah bukan lagi pelengkap. Mereka sudah menjadi **tulang punggung tempur** untuk:

- pengintaian,
- penargetan,
- serangan,
- perlindungan unit,
- dan pengurangan biaya pertahanan lawan. (reuters.com)

Bahkan dalam ranah laut, Reuters mencatat bahwa pengalaman Ukraina mendorong revolusi *marine drone*, karena sistem murah modular dapat memberi efek strategis terhadap armada yang jauh lebih mahal. Ini menegaskan satu pelajaran penting: **di perang modern, harga rendah per unit bisa menjadi keunggulan strategis bila dikombinasikan dengan volume, software, dan data yang tepat**. (reuters.com)

9.3. FPV, ISR drone, loitering munition, anti-drone

Keunggulan Ukraina juga lahir dari **portofolio drone yang beragam**, bukan satu jenis drone tunggal. Outline buku ini tepat ketika memisahkan FPV, ISR drone, *loitering munition*, dan *anti-drone* sebagai subkategori penting.

FPV drones menjadi simbol paling keras dari perang murah: cepat, lincah, relatif murah, dan dapat dipakai untuk serangan presisi jarak dekat atau menengah. Reuters menulis bahwa *interceptor drones* Ukraina banyak diadaptasi dan diterbangkan seperti model FPV, karena platform ini murah, familiar, dan cepat disebarkan ke unit. (reuters.com)

ISR drones tetap menjadi fondasi. Mereka menyediakan mata bagi artileri, infanteri, dan komando. Tanpa ISR yang murah dan tersebar, FPV dan *loitering munition* kehilangan banyak nilainya, karena *kill chain* menjadi lambat. Bahan terlampir Anda juga menunjukkan bahwa ekosistem AI Ukraina bergerak dari *situational awareness* menuju analisis video otomatis dan *kill chain* yang lebih cepat.

Loitering munitions menambah lapisan baru: drone yang bisa mencari, menunggu, lalu menghantam sasaran saat peluang muncul. Ini penting di lingkungan yang terus berubah dan sangat dipengaruhi kamuflase, pergerakan cepat, dan peluang serangan yang pendek.

Anti-drone kini sama pentingnya dengan drone serang. Reuters melaporkan bahwa Ukraina menjadikan *interceptor drones* sebagai bagian utama pertahanan udara berbiaya rendah. Bahan terlampir Anda juga menyoroti pengembangan *interceptor swarms* dan sistem anti-drone murah sebagai respons terhadap serangan Shahed dan ancaman massal lainnya. (reuters.com)

Jadi, portofolio inti industri drone Ukraina terdiri dari:

- **FPV** untuk serangan murah dan presisi dekat,
 - **ISR drones** untuk pengamatan dan penargetan,
 - ***loitering munitions*** untuk serangan menunggu peluang,
 - **interceptor/anti-drone** untuk pertahanan udara murah,
 - dan makin ke depan, **sistem swarm** untuk koordinasi multi-platform.
- (reuters.com)

9.4. EW dan ketahanan terhadap jamming

Perang drone di Ukraina tidak bisa dipahami tanpa **electronic warfare (EW)**. Drone yang murah dan banyak akan cepat kehilangan nilai jika tidak mampu bertahan dalam lingkungan gangguan sinyal, spoofing, dan *jamming* yang berat. Karena itu, industri drone Ukraina tidak hanya berlomba membuat airframe dan *payload*, tetapi juga mencari cara agar sistem tetap berguna saat komunikasi terganggu.

Bahan terlampir Anda menekankan bahwa AI pada drone Ukraina semakin diarahkan pada *terminal guidance*, navigasi tanpa GPS, dan kemampuan melanjutkan misi saat koneksi terputus. Ini konsisten dengan pelajaran lapangan: *jamming* bukan gangguan tambahan, tetapi kondisi normal.

Reuters juga menunjukkan betapa pentingnya lapisan *anti-drone* murah, dan bahkan laporan sederhana seperti penggunaan jaring bekas perikanan di Ukraina menegaskan bahwa perlindungan terhadap drone kini memadukan **teknologi tinggi dan solusi lapangan yang sangat pragmatis**. Ini mengingatkan bahwa ketahanan terhadap *jamming* dan ancaman drone bukan hanya soal algoritma, tetapi tentang arsitektur pertahanan yang berlapis. ([reuters.com](https://www.reuters.com))

Makna strategisnya jelas:

- drone tanpa ketahanan EW akan cepat turun nilainya,
- industri yang war-ready harus memikirkan navigasi, *failsafe*, dan *graceful degradation*,
- dan pengembangan *anti-drone* harus berjalan sejajar dengan pengembangan drone serang.

9.5. Iterasi cepat dari garis depan ke pabrik

Keunggulan industri Ukraina mungkin paling terlihat pada **kecepatan iterasi**. Dalam banyak industri pertahanan tradisional, siklus dari desain ke produksi ke revisi bisa memakan tahun. Di Ukraina, perang memaksa siklus itu menjadi jauh lebih pendek. Bab sebelumnya sudah menekankan *frontline-driven innovation*; Bab 9 menunjukkan konsekuensi industrinya: **garis depan menjadi laboratorium uji yang brutal, dan pabrik harus belajar merespons cepat.**

Reuters menulis bahwa Ukraina sedang memanfaatkan pengalaman perang untuk membangun ekspor dan produksi bersama, termasuk pembicaraan dengan Romania dan minat besar dari luar negeri terhadap drone serta sistem *jamming*. Itu berarti industri Ukraina tidak hanya belajar bertahan, tetapi juga belajar **menskalakan pengalaman lapangan menjadi kapasitas manufaktur dan produk yang dapat dipasarkan**. ([reuters.com](https://www.reuters.com)) ([reuters.com](https://www.reuters.com))

Siklusnya dapat diringkas seperti ini:

- **unit tempur memakai alat,**
- **alat gagal atau berhasil dalam kondisi nyata,**
- **umpan balik dikirim ke pengembang,**
- **produk direvisi cepat,**
- **produksi dilanjutkan dengan varian baru.**

Inilah salah satu alasan mengapa industri drone Ukraina terlihat jauh lebih hidup dibanding banyak industri pertahanan tradisional: **ia tidak menunggu kesempurnaan; ia bergerak melalui perbaikan terus-menerus.**

9.6. Mengapa industri kecil bisa lebih lincah daripada kontraktor besar

Salah satu pelajaran paling penting dari Ukraina adalah bahwa **industri kecil sering lebih cocok untuk perang drone yang bergerak cepat**. Reuters melaporkan bahwa sektor pertahanan Ukraina kini mencakup **lebih dari 1.000 perusahaan**, banyak diantaranya perusahaan swasta kecil yang lahir setelah invasi 2022. Struktur seperti ini memberi ekosistem yang sangat lincah, walau juga membawa fragmentasi dan tantangan skala. ([reuters.com](https://www.reuters.com))

Perusahaan kecil unggul karena mereka bisa:

- **mengubah desain lebih cepat,**
- **mengambil keputusan lebih pendek,**
- **mengganti komponen dengan fleksibel saat pasokan terganggu,**
- **dan menyesuaikan produk untuk kebutuhan unit atau misi tertentu.**

Bahan terlampir Anda sudah menekankan bahwa Ukraina memanfaatkan *startup* dan perusahaan kecil swasta, bukan hanya kontraktor besar. Itulah inti kelincahan industrinya.

Namun perlu jujur: kelincahan bukan segalanya. Industri kecil juga punya keterbatasan:

- pembiayaan terbatas,
- skala produksi tidak selalu stabil,
- standar kualitas bisa bervariasi,
- dan ketergantungan pada komponen impor masih ada.

Karena itu, kekuatan Ukraina bukan pada industri kecil semata, tetapi pada **ekosistem yang memberi ruang industri kecil untuk bereksperimen, lalu memilih yang terbukti berguna untuk disalurkan ke skala lebih besar**. Disini peran Brave1, skema pasar digital, dan pembukaan jalur ekspor menjadi sangat penting. ([reuters.com](https://www.reuters.com))

Ringkasan kunci

- **Industri drone Ukraina kuat karena cepat, tersebar, dan dekat dengan kebutuhan tempur nyata**, bukan karena satu perusahaan raksasa tunggal.
- **Fast-track procurement dan Brave1 Market** membuat jalur pembelian lebih dekat ke kebutuhan lapangan; pada Januari 2026 militer Ukraina dilaporkan telah memesan **240.000 drone** melalui skema *combat e-Points*. (digitalstate.gov.ua) (kmu.gov.ua)
- **Drone murah menjadi tulang punggung tempur** karena bisa diproduksi banyak, cepat diganti, dan memberi efek operasional besar dengan biaya relatif rendah. (reuters.com)
- **Portofolionya beragam**: FPV, ISR drone, *loitering munition*, *interceptor/anti-drone*, dan menuju sistem swarm.
- **EW dan ketahanan terhadap jamming adalah syarat inti**, bukan tambahan, dalam perang drone Ukraina. (reuters.com)
- **Iterasi cepat dari garis depan ke pabrik** membuat produk Ukraina terus menyesuaikan diri dengan kondisi perang yang berubah. (reuters.com)
- **Industri kecil lebih lincah daripada kontraktor besar** dalam perang drone cepat, tetapi tetap perlu ekosistem koordinasi, pembiayaan, dan skala. (reuters.com)

Bab 10. Pelajaran Ukraina: Kekuatan, Keterbatasan, dan Relevansi untuk Indonesia

Bab ini penting karena Ukraina tidak boleh dibaca secara romantis. Ukraina memang memberi banyak pelajaran yang sangat berharga tentang **war-ready AI, industri drone, data tempur, dan kecepatan inovasi**, tetapi juga menunjukkan batas yang keras: ketergantungan industri, tekanan pembiayaan, keterbatasan skala, dan perlombaan adaptasi dengan lawan. Bab ini memang berfungsi sebagai jembatan: dari studi kasus Ukraina menuju pertanyaan yang lebih penting bagi pembaca Indonesia, yakni **apa yang bisa dipetik, apa yang harus diwaspadai, dan apa yang tidak boleh ditiru mentah-mentah.**

10.1. Kekuatan utama Ukraina

Kekuatan utama Ukraina bukan terletak pada satu teknologi ajaib, melainkan pada **loop belajar yang sangat cepat**. Reuters melaporkan bahwa Ukraina telah mengumpulkan lebih dari **2 juta jam video perang** sejak 2022, terutama dari drone, dan mengubahnya menjadi dasar pelatihan model AI, analisis target, dan pembelajaran taktis. Pada 2026, Ukraina bahkan mulai membuka akses ke data tempurnya bagi sekutu untuk melatih *drone AI software*, yang menunjukkan bahwa pengalaman perang telah berubah menjadi aset strategis lintas negara. ([Reuters](#))

Kekuatan kedua adalah **kemampuan menghubungkan garis depan, industri kecil, dan negara**. Pola Ukraina bukan laboratorium–baru–medan perang, tetapi medan perang–revisi–produksi–medan perang lagi. Itu yang membuat inovasinya terasa hidup. Bahan terlampir Anda juga menekankan bahwa keunggulan Ukraina datang dari kombinasi *frontline-driven innovation, startup*, bengkel, dan negara yang belajar cepat.

Kekuatan ketiga adalah **arsitektur industri yang murah, cepat, dan tersebar**. Reuters mencatat bahwa sektor pertahanan Ukraina kini mencakup lebih dari **1.000 perusahaan**, banyak diantaranya perusahaan swasta kecil yang lahir setelah invasi 2022. Ini memberi Ukraina basis inovasi yang lebih lincah daripada model yang hanya bergantung pada kontraktor besar. ([Reuters](#))

Kekuatan keempat adalah **kemampuan institusional untuk mengubah improvisasi menjadi sistem**. Brave1, Brave1 Market, dan Dataroom menunjukkan bahwa Ukraina tidak berhenti pada kreativitas lapangan, tetapi mulai membangun mekanisme pengadaan, pengujian, pendanaan, dan pengolahan data yang lebih permanen. Pemerintah Ukraina menyebut bahwa melalui Brave1 Market militer sudah memesan **240.000 drone** menggunakan *combat e-Points*. ([Kementerian Pertahanan Ukraina](#))

Ringkasnya, kekuatan utama Ukraina ada pada:

- **loop belajar yang sangat cepat,**
- **integrasi garis depan–industri–negara,**
- **industri drone yang murah dan tersebar,**

- dan kemampuan menginstitusikan inovasi tempur. ([Reuters](#))

10.2. Ketergantungan yang masih tersisa

Namun Ukraina bukan cerita kemandirian penuh. Justru salah satu pelajaran terbesarnya adalah bahwa negara yang sangat inovatif pun tetap memiliki **ketergantungan yang nyata**. Ketergantungan itu muncul pada beberapa level: komponen, pembiayaan, kerja sama industri, akses teknologi, dan dukungan eksternal.

Reuters menunjukkan bahwa walau Ukraina maju cepat, ia tetap membuka ekspor, menjajaki produksi bersama dengan Romania, dan mencari mitra Eropa untuk memperluas basis manufakturnya. Ini menunjukkan bahwa Ukraina menyadari industrinya sendiri belum cukup untuk menutup seluruh kebutuhan dan pertumbuhan masa depan. ([Reuters](#))

Ketergantungan kedua ada pada **ekosistem teknologi dan mitra**. Dataroom sendiri dibangun sebagai lingkungan aman bersama aktor luar seperti Palantir, dan pembukaan data tempur ke sekutu menunjukkan bahwa Ukraina memilih strategi *shared ecosystem*, bukan autarki penuh. Ini cerdas secara strategis, tetapi tetap berarti ada ketergantungan pada mitra yang punya komputasi, modal, pasar, atau teknologi tertentu. ([Reuters](#))

Ketergantungan ketiga bersifat militer-operasional. Drone murah memang memberi keunggulan, tetapi perang tetap membutuhkan lapisan lain: pertahanan udara, artileri, EW, amunisi, logistik, dan personel. Jadi, Ukraina mengajarkan bahwa **drone dan AI dapat mengubah perang, tetapi tidak menghapus seluruh kebutuhan perang klasik**. Poin ini penting agar Indonesia tidak salah membaca Ukraina sebagai kisah “semua masalah selesai oleh drone.”

10.3. Masalah pembiayaan dan scale-up

Ukraina menunjukkan bahwa inovasi cepat tidak otomatis berarti *scale-up* mudah. Justru setelah inovasi terbukti, masalah berikutnya adalah **siapa yang membiayai produksi massal, stok, ekspansi pabrik, standardisasi, dan ekspor**. Reuters menulis bahwa keputusan Ukraina membuka ekspor senjata pada 2026 lahir partly karena industri domestiknya mampu memproduksi lebih banyak daripada yang bisa dibeli pemerintah. Presiden Zelenskyy bahkan menyebut akan ada **10 “export centres”** di Eropa pada 2026 untuk menopang industri tersebut. ([Reuters](#))

Ini menunjukkan paradoks yang menarik. Di satu sisi, perang menciptakan lonjakan permintaan dan inovasi. Di sisi lain, negara yang sedang berperang tidak selalu mampu membeli seluruh output industrinya sendiri. Maka pembiayaan menjadi masalah strategis, bukan sekadar masalah bisnis. Industri butuh kontrak, modal kerja, jalur ekspor, dan kepastian regulasi agar kapasitas yang sudah dibangun tidak menganggur. Reuters juga melaporkan bahwa lisensi ekspor masa perang mulai dikeluarkan untuk produsen Ukraina, menandakan bahwa *scale-up* membutuhkan perubahan kebijakan negara, bukan hanya peningkatan kapasitas pabrik. ([Reuters](#))

Bagi Indonesia, ini pelajaran yang sangat penting. Banyak negara bisa membuat prototipe atau bahkan produk bagus, tetapi gagal di fase berikutnya: **mengubah prototipe menjadi volume, volume menjadi industri, dan industri menjadi kapasitas nasional yang berkelanjutan**. Itulah sebabnya pembiayaan cepat dan kontrak kecil tetapi nyata—seperti yang sudah disorot dalam catatan terlampir Anda—menjadi sangat penting.

10.4. Risiko ketergantungan komponen asing

Inilah salah satu pelajaran paling keras dari Ukraina bagi negara seperti Indonesia. Di perang drone modern, airframe hanyalah sebagian kecil dari persoalan. Titik rapuh justru sering ada pada **komponen**: GNSS module, IMU, kamera thermal, RF front-end, baterai, ESC, motor, *secure data-link*, *payload electronics*, dan chip pengendali. Bahan terlampir Anda sendiri menekankan bahwa untuk Indonesia, pelajaran Ukraina harus diterjemahkan menjadi prioritas pada autopilot, radio, navigasi tahan gangguan, AI *edge*, dan produksi drone murah—bukan obsesi pada GPU kelas tertinggi.

Risiko ini juga tampak pada langkah Ukraina yang terus mencari mitra produksi dan ekspor di Eropa, serta menjadikan teknologi tempurnya sebagai basis kolaborasi regional. Romania dan Ukraina, misalnya, sedang memajukan pembicaraan untuk produksi drone bersama dengan dukungan dana SAFE dari Uni Eropa. Ini menunjukkan bahwa bahkan negara yang sangat adaptif tetap perlu mengamankan *supply chain* dan kapasitas manufaktur lintas batas. ([Reuters](#))

Pelajaran utamanya sederhana: **ketahanan drone dan AI bukan hanya soal software, tetapi soal pasokan komponen dan kemampuan substitusi desain.** Bagi Indonesia, ini berarti strategi yang paling waras adalah membangun beberapa lapis kemandirian: stok komponen kritis, desain modular, *second source*, dan kemampuan mengganti komponen walau performa sedikit turun. Catatan Anda sudah merumuskannya dengan baik: drone yang “sedikit lebih berat tetapi tetap terbang” lebih berharga daripada desain ideal yang mati karena satu chip hilang.

10.5. Apa yang relevan untuk Indonesia

Ada banyak hal dari Ukraina yang sangat relevan untuk Indonesia, justru karena Indonesia juga tidak berada dalam posisi untuk mengejar semuanya sekaligus. Yang paling relevan bukan seluruh konteks geopolitiknya, melainkan **logika organisasional dan industrialnya**.

Pertama, Indonesia perlu belajar bahwa **kecepatan inovasi dan pengadaan sama pentingnya dengan teknologi itu sendiri**. Jalur cepat pengadaan drone/AI/EW yang dipisahkan dari pola alutsista besar adalah salah satu pelajaran paling langsung dari model Ukraina. Dalam bahan terlampir Anda, hal ini sudah dirumuskan sangat jelas untuk horizon 0–3 tahun: *uji lapangan 90 hari → revisi desain → kontrak kecil → produksi awal → evaluasi → scale-up*.

Kedua, Indonesia perlu belajar bahwa **drone, EW, data, dan command software harus diperlakukan sebagai satu ekosistem**. Catatan Anda menegaskan bahwa drone tanpa data-link tahan gangguan akan lumpuh, AI tanpa sensor dan data akan kosong, dan radar tanpa integrasi ke *kill chain* akan lambat. Ini sangat sejalan dengan pelajaran Ukraina.

Ketiga, Indonesia perlu belajar bahwa **industri kecil dan kampus harus masuk ke loop pertahanan nyata**, bukan berhenti di prototipe atau publikasi. Bahan terlampir Anda menekankan perlunya *reference design* yang bisa diproduksi: autopilot board, radio module, *anti-jam navigation stack*, *secure mesh network*, kamera gimbal murah, dan seterusnya. Itu adalah terjemahan Indonesia yang sangat tepat dari pelajaran Ukraina.

Keempat, Indonesia perlu belajar bahwa **data tempur dan data latihan adalah aset strategis**. Ukraina mengajarkan bahwa data bukan hanya laporan setelah kejadian, tetapi bahan baku AI, evaluasi taktik, dan pengembangan industri. Untuk Indonesia, ini berarti kebutuhan akan *Defense Compute & Dataset Center*, *test range* swarm/EW, dan arsip data uji lapangan yang disiplin.

Kelima, Indonesia perlu belajar bahwa **war-ready AI versi negara kepulauan harus berbeda**. Bukan meniru perang parit Ukraina, tetapi menerjemahkan prinsip yang sama ke konteks Indonesia: *maritime domain awareness*, perlindungan pangkalan, pulau kecil terluar, choke points, anti-infiltrasi, logistik terpencil, dan pertahanan udara jarak dekat terhadap drone. Outline Anda sendiri sudah menekankan bahwa Indonesia tidak boleh meniru mentah-mentah AS, China, Ukraina, atau Iran.

Yang paling relevan untuk Indonesia:

- jalur cepat pengadaan dan iterasi,
- ekosistem drone–EW–AI–command software,
- peran industri kecil dan kampus dalam produk nyata,
- dataset pertahanan nasional,
- dan doktrin kepulauan yang *networked* serta *attritable*.

10.6. Apa yang tidak bisa disalin mentah-mentah

Meski Ukraina sangat inspiratif, ada banyak hal yang tidak bisa—dan tidak boleh—disalin mentah-mentah oleh Indonesia.

Pertama, **konteks geografi dan ancamannya berbeda**. Ukraina berperang dalam konflik darat intensitas tinggi dengan garis depan yang relatif terus-menerus. Indonesia adalah negara kepulauan. Maka pelajaran Ukraina harus diterjemahkan, bukan ditiru. Drone, data, dan AI tetap penting, tetapi fokus operasional Indonesia semestinya berbeda: laut, selat, pangkalan, pulau kecil, logistik maritim, dan pertahanan berlapis.

Kedua, **tingkat tekanan perang Ukraina tidak dapat direplikasi secara damai**.

Banyak kecepatan belajar Ukraina lahir karena perang memaksa semua orang bergerak. Indonesia tidak bisa—dan tentu tidak perlu—menunggu perang untuk menciptakan tekanan semacam itu. Yang harus ditiru adalah *loop*-nya: pengujian cepat, umpan balik cepat, pengadaan cepat, dan produksi bertahap. Bukan kekacauan perang itu sendiri.

Ketiga, **jangan salah meniru hasil sambil melupakan fondasinya**. Sangat mudah terpesona pada FPV, swarm, atau *interceptor drones*, tetapi melupakan data pipeline, integrasi software, logistik komponen, dan pembiayaan. Padahal justru fondasi itulah yang membuat Ukraina efektif. Ini sejalan dengan peringatan awal dalam draft Anda bahwa perang modern bergeser dari platform ke data, model, dan keputusan.

Keempat, **jangan menyimpulkan bahwa drone menggantikan seluruh alutsista lain**. Ukraina justru menunjukkan sebaliknya: drone mengubah perang dengan sangat besar, tetapi tidak menghapus kebutuhan pada EW, radar, artileri, pertahanan udara, logistik, dan struktur komando.

Kelima, **jangan mengimpor gaya improvisasi tanpa membangun institusi**.

Ukraina bergerak dari improvisasi ke Brave1, Dataroom, Market, lisensi ekspor, dan produksi bersama. Jika Indonesia hanya meniru improvisasi lapangan tanpa membangun institusi pengujian, pendanaan, dan industrialisasi, hasilnya akan berhenti di demo.

Ringkasan kunci

- **Kekuatan utama Ukraina** ada pada *loop* belajar cepat, integrasi garis depan–industri–negara, industri kecil yang lincah, dan kemampuan menginstitusikan inovasi. ([Reuters](#))
- **Ukraina tetap punya ketergantungan nyata** pada mitra, komponen, pembiayaan, dan lapisan perang lain di luar drone/AI. ([Reuters](#))
- **Masalah pembiayaan dan *scale-up*** sangat penting: inovasi cepat tidak otomatis menghasilkan industri berkelanjutan tanpa kontrak, ekspor, dan kebijakan pendukung. ([Reuters](#))
- **Risiko ketergantungan komponen asing** adalah salah satu pelajaran paling relevan bagi Indonesia; ketahanan sistem bergantung pada stok, desain modular, dan *second source*.
- **Yang relevan untuk Indonesia** adalah logika Ukraina: pengadaan cepat, ekosistem drone–EW–AI, dataset pertahanan, peran industri kecil/kampus, dan doktrin kepulauan yang *networked* serta *attributable*.
- **Yang tidak bisa disalin mentah-mentah** adalah konteks geografis, tekanan perang darat, dan improvisasi tanpa institusi. Ukraina harus diterjemahkan, bukan dicopy-paste.

Bagian IV. Iran: Ketahanan Asimetris, Volume, dan Otonomi Secukupnya

Bab 11. Strategi Iran: Murah, Banyak, dan Cukup Efektif

Bab ini penting karena Iran sering dibaca dengan dua cara yang sama-sama keliru. Ada yang meremehkan Iran karena tidak memiliki teknologi paling mewah. Ada juga yang membesar-besarkan Iran seolah sudah menjadi kekuatan AI militer paling maju. Keduanya tidak tepat. Pelajaran yang lebih berguna adalah ini: **Iran tampaknya membangun model perang yang bertumpu pada volume, biaya rendah, ketahanan, dan efek psikologis-operasional yang cukup besar, meski bukan berbasis AI paling canggih.** Iran ditempatkan sebagai studi tentang *resilience*, *saturation*, dan strategi “cukup efektif” dalam perang modern.

11.1. Bukan AI paling maju

Iran bukan contoh terbaik untuk AI militer paling canggih. Ia tidak berada di posisi Amerika Serikat dalam *cloud*, integrator, *battle network*, atau *frontier model*. Ia juga tidak berada di posisi China dalam skala industri digital dan ambisi integrasi lintas-domain. Tetapi justru di situlah pelajarannya: **Iran tidak menunggu AI paling maju untuk membangun efek tempur yang nyata.** Strateginya lebih sederhana dan lebih pragmatis—membuat sistem yang cukup murah, cukup banyak, cukup akurat, dan cukup tahan untuk menekan lawan terus-menerus.

Reuters melaporkan bahwa dalam pekan pertama konflik 2026, Iran meluncurkan lebih dari **1.000 drone**, dan menurut estimasi yang dikutip Reuters, Iran memiliki kapasitas produksi sekitar **10.000 drone per bulan**. Angka itu penting bukan karena menunjukkan kecanggihan maksimum, tetapi karena menunjukkan skala industrial dan logika operasional Iran: **kuantitas yang dapat diproduksi cepat.** ([Reuters](#))

Dalam kerangka ini, AI Iran—sejauh yang bisa dibaca dari sumber terbuka—lebih mungkin berfungsi sebagai:

- *guidance* yang cukup baik,
- navigasi dan serangan satu arah,
- otonomi dasar saat komunikasi terganggu,
- dan dukungan bagi perang saturasi.

Jadi, bab ini sebaiknya dibaca bukan sebagai kisah “Iran unggul dalam AI”, tetapi sebagai kisah **bagaimana teknologi yang tidak paling maju tetap bisa sangat berbahaya bila dipadukan dengan strategi yang tepat.** ([Reuters](#))

11.2. Drone sebagai alat saturasi

Inti paling jelas dari strategi Iran adalah penggunaan drone sebagai **alat saturasi**. Bukan untuk memenangkan duel teknologi secara elegan, tetapi untuk membanjiri pertahanan lawan, menciptakan tekanan konstan, memaksa lawan mengaktifkan sistem pertahanan, dan membuka celah bagi serangan lain.

Reuters menulis bahwa sejak serangan AS-Israel terhadap Iran, Teheran meluncurkan ratusan misil dan lebih dari **1.000 drone** ke negara-negara Teluk yang bersekutu dengan Washington. Walau banyak yang diintersep, sebagian tetap menimbulkan kerusakan pada bangunan, infrastruktur, dan pangkalan militer AS. Itu menunjukkan bahwa bahkan ketika tingkat intersepsi tinggi, **efek saturasi tetap muncul**: pertahanan dipaksa aktif terus, biaya naik, tekanan psikologis dan ekonomi meluas. ([Reuters](#))

CFR menyebut fenomena ini sebagai “**precise mass**”: penggunaan sistem murah dalam volume tinggi dengan akurasi yang cukup untuk memberi efek tempur dan strategis. Konsep ini penting karena menjelaskan mengapa perang drone Iran tidak perlu sempurna untuk menjadi efektif. Ia cukup membuat lawan sibuk, boros, waspada terus-menerus, dan kadang tetap terkena. ([Council on Foreign Relations](#))

Dalam bahasa yang lebih operasional, drone saturasi Iran dipakai untuk:

- **menguras interseptor lawan,**
- **menciptakan kelelahan pertahanan,**
- **mengganggu ritme operasi,**
- **dan memaksa lawan berpikir lebih defensif daripada ofensif.** ([Reuters](#))

11.3. Volume vs presisi

Salah satu kunci memahami Iran adalah membedakan **presisi tinggi** dari **presisi yang cukup**. Negara seperti AS sering mengejar presisi yang sangat tinggi dan integrasi sistem yang sangat rapat. Iran tampaknya lebih memilih kombinasi yang lain: **volume tinggi dengan presisi yang cukup untuk tetap mengancam**.

Reuters menggambarkan perang 2026 sebagai bukti bahwa drone murah sedang mengubah langit perang. Bahkan jika tidak semua drone menembus pertahanan, biaya pertahanan lawan tetap melonjak, dan sebagian drone tetap bisa lolos atau menimbulkan efek sekunder. Dalam logika ini, volume bukan lawan dari presisi; volume adalah cara untuk mengurangi kebutuhan akan presisi absolut. ([Reuters](#))

CFR juga menekankan bahwa apa yang terlihat di Iran adalah bentuk baru perang: penggunaan *low-cost drones* dalam volume besar sebagai fitur reguler perang masa depan. Ini berarti bahwa di banyak konteks, **“cukup akurat dalam jumlah besar” dapat lebih berbahaya daripada “sangat akurat dalam jumlah kecil.”** ([Council on Foreign Relations](#))

Pelajaran ini penting karena banyak negara terlalu fokus pada platform elit. Iran menunjukkan model lain:

- **lebih baik banyak sistem yang cukup akurat,**
- **daripada sedikit sistem yang sangat mahal tetapi cepat habis,**
- terutama jika tujuan utamanya adalah menguras, menekan, dan memanjangkan beban lawan.** ([Reuters](#))

11.4. Menekan lawan lewat biaya rendah

Kekuatan strategis Iran sangat terkait dengan **unit economics**. Reuters menulis bahwa drone murah sedang memaksa AS dan sekutunya mengeluarkan jutaan dolar untuk menghadapi ancaman yang nilainya hanya sebagian kecil dari biaya intersepsi. Inilah logika yang paling penting: Iran tidak harus menghancurkan seluruh target untuk menang secara taktis. Ia cukup membuat biaya pertahanan lawan melonjak, memaksa distribusi ulang sumber daya, dan menimbulkan rasa tidak aman yang terus-menerus. ([Reuters](#))

Model seperti ini sangat cocok dengan strategi asimetris. Negara yang lebih lemah secara konvensional tidak mencoba menandingi lawan satu banding satu. Ia mencoba:

- **menaikkan biaya lawan,**
- **memaksa lawan membuang stok interseptor,**
- **menciptakan ketidakpastian ekonomi dan psikologis,**
- **dan mempertahankan kemampuan menyerang lebih lama daripada yang diperkirakan lawan.** ([Reuters](#))

Reuters bahkan mengutip analisis bahwa Iran bisa mengganggu lalu lintas di Selat Hormuz selama berbulan-bulan dengan drone, cukup dengan menunjukkan bahwa beberapa tanker masih dapat dihantam sehingga kekhawatiran pasar dan pelayaran bekerja sebagai pengali efek. Di sini terlihat jelas bahwa **biaya rendah bukan sekadar soal hemat uang, tetapi cara untuk menghasilkan pengaruh strategis yang jauh lebih besar dari ongkos produksinya.** ([Reuters](#))

11.5. Produksi massal dan tekanan psikologis

Iran tidak hanya mengandalkan taktik, tetapi juga **kapasitas produksi**. Reuters melaporkan pada Januari 2026 bahwa berbagai cabang angkatan darat Iran menerima batch **1.000 drone**, dengan pernyataan resmi bahwa langkah itu bagian dari upaya memperkuat keunggulan strategis dan respons cepat. Jika dikaitkan dengan estimasi kapasitas produksi **10.000 per bulan** yang dikutip Reuters, terlihat bahwa Iran memang memandang drone sebagai instrumen yang harus tersedia dalam jumlah besar, bukan hanya sebagai aset khusus. ([Reuters](#))

Produksi massal ini punya efek ganda. Yang pertama adalah efek militer langsung: stok cukup untuk menyerang berulang, bukan sekali dua kali. Yang kedua adalah **efek psikologis**: lawan harus hidup dalam kesadaran bahwa serangan berikutnya bisa datang lagi, lagi, dan lagi. Ini penting karena perang modern bukan hanya perebutan target, tetapi juga perebutan ritme, fokus, dan ketahanan mental.

Dalam logika ini, tekanan psikologis tidak muncul hanya dari akurasi drone, tetapi dari:

- **kemungkinan serangan terus-menerus,**
- **ketidakpastian titik serang,**
- **dan kesadaran bahwa stok lawan bisa terkuras lebih cepat daripada stok penyerang.** ([Reuters](#))

Iran tampaknya memahami bahwa dalam perang modern, persepsi bahwa “serangan murah dapat terus datang” sudah merupakan bentuk kekuatan tersendiri.

11.6. Mengapa “cukup baik” bisa sangat berbahaya

Inilah pelajaran paling penting dari Iran. Dalam dunia teknologi, banyak orang terpaku pada sistem terbaik, akurasi tertinggi, dan AI tercanggih. Tetapi perang sering memberi nilai pada sesuatu yang lain: **sistem yang cukup baik, cukup murah, cukup banyak, dan cukup tahan untuk tetap relevan di bawah tekanan.**

CFR menulis bahwa pengalaman Iran dan Ukraina sama-sama menunjukkan lahirnya era *precise mass*—penggunaan volume besar sistem murah yang makin akurat. Reuters menambahkan bahwa heavy *jamming* di Teluk dan Ukraina justru mendorong fokus pada sistem yang bisa bekerja dengan atau tanpa kontrol manusia langsung. Ini berarti bahwa “cukup baik” menjadi berbahaya ketika:

- ia bisa diproduksi massal,
- ia tidak bergantung pada satu rantai komunikasi rapuh,
- ia murah enough untuk dikorbankan,
- dan ia cukup akurat untuk tetap memaksa lawan merespons serius. ([Council on Foreign Relations](#))

Ini juga menjelaskan mengapa negara-negara Barat mulai menyesuaikan diri. Reuters melaporkan bahwa militer AS bahkan mendorong sistem seperti LUCAS—drone murah yang terinspirasi dari Shahed—karena mereka menyadari bahwa ancaman dari sistem murah dan cukup efektif tidak bisa dihadapi hanya dengan platform mahal. Jadi, “cukup baik” bukan label merendahkan. Dalam perang, ia bisa berarti **cukup untuk mengubah kalkulasi biaya, cukup untuk mengganggu operasi, dan cukup untuk menggeser keseimbangan psikologis lawan.** ([Reuters](#))

Ringkasan kunci

- **Iran bukan contoh AI militer paling maju**, tetapi contoh strategi yang sangat pragmatis: murah, banyak, dan cukup efektif. ([Reuters](#))
- **Drone dipakai sebagai alat saturasi**, untuk membanjiri pertahanan, menguras interseptor, dan menekan lawan terus-menerus. ([Reuters](#))
- **Volume sering lebih penting daripada presisi absolut.** Sistem yang cukup akurat dalam jumlah besar bisa lebih berbahaya daripada sistem elit dalam jumlah kecil. ([Reuters](#))
- **Biaya rendah adalah senjata strategis.** Iran menekan lawan dengan memaksa mereka mengeluarkan biaya pertahanan jauh lebih tinggi daripada biaya serangannya. ([Reuters](#))
- **Produksi massal memperkuat tekanan psikologis dan operasional**, karena serangan dapat diulang terus-menerus. ([Reuters](#))
- **“Cukup baik” bisa sangat berbahaya** ketika dipadukan dengan volume, ketahanan, dan logika perang asimetris. ([Reuters](#))

Bab 12. AI dan Otonomi dalam Model Perang Iran

Bab ini harus dibaca dengan hati-hati. Iran sering dibahas dengan dua ekstrem: dianggap sangat tertinggal, atau dianggap sudah memiliki AI perang yang sangat maju. Keduanya terlalu sederhana. Pola yang lebih akurat adalah ini: **Iran tampaknya membangun otonomi yang cukup untuk membuat sistem murah tetap berguna dalam perang nyata**, terutama dalam lingkungan yang padat gangguan, berbiaya rendah, dan menuntut daya tahan. Iran ditempatkan bukan sebagai contoh AI paling maju, tetapi sebagai contoh **ketahanan asimetris, volume, dan otonomi secukupnya**.

12.1. Otonomi dasar dalam kondisi jamming

Pelajaran paling penting dari model Iran adalah bahwa otonomi tidak selalu berarti *full autonomy*. Dalam banyak kasus, yang paling berguna justru **otonomi dasar**: kemampuan sistem untuk tetap melanjutkan misi ketika sinyal terganggu, *link* komando putus, atau lingkungan dipenuhi *jamming*. Reuters menulis bahwa perang di Teluk dan Ukraina sama-sama menunjukkan bahwa *heavy jamming* justru mendorong pengembangan sistem yang dapat beroperasi dengan atau tanpa kendali manusia langsung. Ini sangat relevan untuk membaca Iran. ([Reuters](#))

Buku *Responsible Use of AI in Military Systems* juga memberi petunjuk yang kuat. Bab tentang perang Ukraina menjelaskan bahwa drone tipe Shahed—yang berasal dari Iran—dapat diprogram sebelum peluncuran untuk tugas serangan dan tetap bekerja bahkan ketika sistem pemandu berbasis satelit gagal, dengan beralih ke *inertial navigation system* dan *sensor fusion algorithms* untuk memperkirakan posisi, sikap, dan kecepatan.

Jadi, ketika kita bicara “AI dan otonomi” pada Iran, yang paling masuk akal bukan membayangkan sistem supercanggih ala *frontier AI*, tetapi **otonomi minimum yang cukup tahan terhadap gangguan elektronik**.

Inti subbab ini:

- Iran tampaknya mengejar otonomi yang cukup, bukan otonomi yang paling maju.
- Lingkungan *jamming* membuat otonomi dasar menjadi sangat berharga.
- Nilai strategisnya ada pada kelangsungan misi, bukan kemewahan algoritma. ([Reuters](#))

12.2. Navigasi, terminal guidance, dan ketahanan misi

Pada model perang Iran, dua hal paling penting tampaknya adalah **navigasi** dan **ketahanan misi**. Sistem seperti Shahed menjadi menonjol bukan karena “cerdas” dalam arti luas, tetapi karena bisa diarahkan ke sasaran dengan biaya rendah dan tetap mempertahankan fungsi dasar ketika komunikasi atau GPS terganggu. Buku *Responsible Use of AI in Military Systems* menyebut bahwa ketika *satellite-linked guidance systems* gagal, sistem pemandu Shahed dapat beralih ke navigasi inersial dan mengoreksi lintasan dengan memproses data sensor dinamis.

Inilah inti praktisnya: **ketahanan misi lebih penting daripada presisi absolut**. Sistem yang masih bisa mendekati sasaran, tetap bergerak dalam arah yang benar, dan tidak sepenuhnya buta saat *link* hilang, sudah sangat berharga dalam perang asimetris. Reuters juga menulis bahwa drone murah Iran menjadi ancaman yang bisa bertahan berbulan-bulan terhadap lalu lintas di Selat Hormuz karena jumlah dan ritme serangannya, bukan karena setiap unit memiliki kualitas tertinggi. ([Reuters](#))

Dalam kerangka ini, *terminal guidance* tidak harus dibaca sebagai kecerdasan spektakuler. Ia bisa berarti:

- kemampuan menyesuaikan fase akhir serangan,
- kemampuan tetap menuju sasaran saat jalur komunikasi menurun,
- dan kemampuan mempertahankan misi dalam kondisi tidak ideal.

Pelajaran utamanya: di model Iran, navigasi yang tangguh sering lebih penting daripada AI yang mewah. ([Reuters](#))

12.3. Serangan berlapis dan swarm sederhana

Iran tampaknya tidak mengandalkan satu lapisan serangan tunggal. Polanya lebih dekat ke **serangan berlapis**: kombinasi drone, rudal, dan tekanan berulang untuk membanjiri pertahanan lawan. Reuters menulis bahwa Iran menembakkan ratusan rudal dan lebih dari 1.000 drone dalam konflik 2026, dan banyak analis melihat nilai strategisnya bukan hanya pada kerusakan fisik, tetapi pada kemampuannya memaksa pertahanan lawan tetap aktif, mahal, dan tertekan. ([Reuters](#))

Dalam konteks ini, *swarm* Iran tidak perlu dibayangkan sebagai *swarm intelligence* yang sangat maju. Yang lebih masuk akal adalah **swarm sederhana atau serangan massal terkoordinasi secara cukup**, di mana volume dan waktu peluncuran lebih penting daripada koordinasi canggih antar-unit. Buku *Responsible Use of AI in Military Systems* menyebut Shahed sering diluncurkan dalam kelompok lima sampai belasan atau lebih, dan menekankan bahwa bahkan jika hanya sebagian kecil yang mencapai sasaran, kerusakannya tetap bisa besar.

Jadi, “swarm” pada model Iran lebih tepat dibaca sebagai:

- koordinasi sederhana yang cukup untuk saturasi,
- serangan berlapis untuk menguji dan membuka pertahanan,
- dan pemanfaatan volume sebagai pengganti presisi tinggi. ([Reuters](#))

12.4. Komando yang tahan dipukul

Salah satu hal yang membuat model Iran relevan adalah bukan hanya senjatanya, tetapi **arsitektur komandonya yang mencoba tetap bekerja di bawah tekanan**. Reuters melaporkan bahwa IRGC telah mendelegasikan kewenangan lebih jauh ke bawah menjelang serangan pemenggalan kepemimpinan, agar kampanye drone dan misil tetap bisa berjalan meski komandan senior hilang. Ini bukan “AI” dalam arti sempit, tetapi sangat penting untuk memahami bagaimana otonomi teknis dan otonomi organisasi saling bertemu. ([reuters.com](https://www.reuters.com))

Dalam model seperti ini, sistem tidak harus sepenuhnya dikendalikan dari pusat. Cukup bila:

- **perintah besar sudah ditetapkan,**
- **unit bawah punya ruang menjalankan rencana,**
- **dan sistem teknis bisa tetap bergerak walau koneksi ke pusat terganggu.**

Di sinilah otonomi teknis dan ketahanan komando saling menguatkan. Sistem yang bisa tetap terbang saat *jamming* berat menjadi lebih berbahaya bila dipadukan dengan organisasi yang juga bisa tetap menyerang saat pusat komando terpukul.

Makna strategisnya:

- **komando tahan pukul membuat volume serangan lebih berkelanjutan,**
- **otonomi dasar pada drone mengurangi beban kontrol pusat,**
- **dan keduanya cocok dengan strategi asimetris Iran.** ([reuters.com](https://www.reuters.com))

12.5. AI sebagai penguat strategi asimetris, bukan pusat segalanya

Inilah titik paling penting dari bab ini. Pada model Iran, AI dan otonomi tampaknya **bukan pusat dari seluruh strategi**, melainkan **penguat bagi strategi asimetris yang sudah ada**. Strategi dasarnya tetap sama: menekan lawan dengan biaya rendah, volume tinggi, gangguan berulang, dan tekanan psikologis-operasional. AI dan otonomi hanya membuat strategi itu lebih tajam.

Buku *The AI Wave in Defence Innovation* menekankan bahwa setiap negara memakai AI sesuai struktur insentif strategisnya sendiri. Itu sangat cocok untuk membaca Iran. Iran tidak perlu meniru AS. Ia cukup memakai otonomi dan AI untuk memperkuat apa yang sudah menjadi kekuatan asimetrisnya: drone murah, misil, saturasi, *resilience*, dan kemampuan bertahan di bawah embargo serta tekanan militer.

Karena itu, AI Iran paling berguna bila:

- **membuat sistem murah lebih tangguh,**
- **membuat serangan massal lebih sulit dihentikan,**
- **membuat misi tetap berjalan saat komunikasi terganggu,**
- **dan mendukung perang biaya rendah dalam jangka lebih lama.**

Jadi, membaca Iran dengan kaca mata “berapa canggih AI-nya?” sering meleset. Pertanyaan yang lebih tepat adalah: **sejauh mana AI dan otonomi membuat strategi asimetris Iran menjadi lebih mematikan, lebih tahan, dan lebih murah?** Jawaban paling jujur: cukup jauh untuk membuatnya relevan dan berbahaya, meski bukan sebagai contoh AI militer paling maju. ([Reuters](#))

Ringkasan kunci

- **Otonomi Iran tampaknya terutama berupa otonomi dasar yang tahan gangguan**, bukan AI perang paling maju. ([Reuters](#))
- **Navigasi, *terminal guidance*, dan ketahanan misi** lebih penting daripada kecanggihan model secara abstrak. ([Reuters](#))
- **Serangan Iran lebih tepat dibaca sebagai serangan berlapis dan *swarm* sederhana**, dengan volume sebagai pengganti presisi absolut. ([Reuters](#))
- **Komando yang tahan dipukul** memperkuat nilai otonomi teknis, karena operasi bisa terus berjalan walau pusat terganggu. ([reuters.com](#))
- **AI dalam model Iran berfungsi sebagai penguat strategi asimetris**, bukan pusat seluruh sistem perang. ([Reuters](#))

Bab 13. Pelajaran Iran: *Resilience* Lebih Penting daripada Kemewahan

Bab ini penting karena Iran memberi pelajaran yang tidak nyaman tetapi sangat relevan: **dalam perang modern, sistem yang murah, tahan gangguan, dan bisa diproduksi banyak sering lebih berbahaya daripada sistem yang tampak lebih mewah tetapi rapuh, mahal, dan sulit diganti.** Itu sejalan dengan arah *Onno W. Purbo, AI di Militer, 2026*, yang membaca Iran bukan sebagai model AI militer paling maju, melainkan sebagai studi tentang **ketahanan, volume, dan efek strategis dari teknologi yang “cukup baik.”**

13.1. Murah tidak berarti primitif

Salah satu kekeliruan paling umum adalah menganggap sistem murah pasti primitif. Iran justru menunjukkan sebaliknya. Sistem murah bisa saja sederhana, tetapi tetap efektif bila dirancang untuk fungsi yang jelas: menembus, mengganggu, menguras, dan bertahan. Reuters melaporkan bahwa Iran dapat memproduksi hingga sekitar **10.000 drone per bulan**, dan telah menggunakan lebih dari **1.000 drone** dalam pekan-pekan awal perang 2026. Itu menunjukkan bahwa nilai strategis drone Iran tidak bertumpu pada kecanggihan maksimum per unit, melainkan pada **kemampuan produksi dan keberlanjutan operasi.** ([Reuters](#))

CFR menulis bahwa pengalaman Iran menunjukkan lahirnya era “**precise mass**”: penggunaan drone murah dan *one-way attack drones* dalam jumlah besar dengan akurasi yang cukup untuk tetap mengancam target militer, pangkalan, pelabuhan, dan infrastruktur energi. Dalam logika ini, murah tidak identik dengan tidak serius. Murah justru bisa berarti:

- mudah diproduksi ulang,
- mudah dikorbankan,
- mudah disebarkan banyak unit,
- dan cukup untuk memaksa lawan merespons mahal. ([Council on Foreign Relations](#))

Pelajaran utamanya jelas: **harga rendah per unit bisa menjadi kekuatan tempur bila dikawinkan dengan skala, ketahanan, dan tujuan operasi yang realistis.**

13.2. Robustness lebih penting daripada spesifikasi tertinggi

Iran memberi pelajaran bahwa **ketangguhan sistem dalam kondisi buruk** sering lebih penting daripada spesifikasi tertinggi di atas kertas. Dalam lingkungan perang yang padat *jamming*, gangguan GPS, cuaca buruk, dan tekanan tempo tinggi, sistem yang tetap bisa melanjutkan misi memiliki nilai lebih besar daripada sistem yang unggul di brosur tetapi rapuh di lapangan. Buku *Responsible Use of AI in Military Systems* mencatat bahwa drone tipe Shahed dapat tetap berfungsi ketika *satellite-linked guidance* terganggu dengan beralih ke *inertial navigation* dan pemrosesan sensor lain.

CFR juga menulis bahwa Iran kemungkinan telah mengadopsi penguatan seperti **anti-jamming antennas** dan **EW-resistant navigation** untuk memperkuat sistemnya. Bahkan bila tidak mencapai tingkat kecanggihan tertinggi, penguatan seperti itu sudah cukup untuk meningkatkan peluang misi dalam konflik nyata. ([Council on Foreign Relations](#))

Ini sangat penting bagi Indonesia. Banyak negara berkembang tergoda mengejar spesifikasi tertinggi, padahal yang lebih berguna sering justru:

- navigasi yang tahan gangguan,
- data-link yang tetap hidup di bawah tekanan,
- desain modular saat komponen diganti,
- dan sistem yang tetap bekerja walau performanya turun sedikit.

Dengan kata lain, yang paling penting sering bukan “terbaik”, tetapi “tetap hidup saat semua hal mulai rusak.”

13.3. Mengapa Indonesia perlu belajar soal resilience

Indonesia perlu belajar dari Iran bukan karena harus meniru Iran, tetapi karena Indonesia juga menghadapi pertanyaan yang sama: **apa yang terjadi bila pasokan komponen terganggu, jaringan dipukul, GPS bermasalah, atau perang menuntut operasi murah dan berulang?** Dalam konteks itu, pelajaran Iran sangat relevan. Reuters menunjukkan bahwa kekuatan Iran muncul dari kemampuan mempertahankan tekanan operasi dalam waktu lama dengan biaya yang relatif rendah. ([Reuters](#))

Bagi Indonesia, *resilience* seharusnya dibaca setidaknya pada empat lapis:

- **resilience teknis:** sistem tetap terbang atau beroperasi di tengah *jamming* dan kehilangan sinyal;
- **resilience industri:** ada stok komponen kritis, *second source*, dan kemampuan substitusi desain;
- **resilience organisasi:** unit tetap bisa bertindak walau koneksi ke pusat terganggu;
- **resilience ekonomi perang:** sistem cukup murah untuk diproduksi dan diganti banyak kali.

Disini ditekankan *design-first strategy*, stok komponen kritis, desain modular, *mass autonomy*, dan *industrial resilience* menghadapi *cut-off supply chain*.

Pelajaran kerasnya adalah: **Indonesia tidak cukup hanya membeli sistem canggih; Indonesia harus membangun sistem yang tetap bisa dipakai saat kondisi tidak ideal.**

13.4. Apa yang berbahaya bila Indonesia salah membaca Iran

Ada beberapa salah baca yang sangat berbahaya.

Pertama, menganggap Iran hebat hanya karena jumlah dronanya besar. Ini berbahaya karena membuat orang lupa bahwa volume Iran bekerja karena ada logika operasi, ketahanan, dan tujuan asimetris yang jelas. Meniru volume tanpa arsitektur pendukung hanya akan menghasilkan penumpukan alat, bukan kekuatan. ([Reuters](#))

Kedua, menganggap Iran sebagai model AI militer paling maju. Ini keliru. Iran lebih tepat dibaca sebagai model **otonomi secukupnya** dan **strategi asimetris yang diperkuat teknologi**, bukan sebagai pemimpin frontier AI. Kalau Indonesia salah membaca ini, kita bisa salah prioritas: mengejar cerita sensasional tentang AI sambil melupakan *navigation stack*, radio, EW, autopilot, dan logistik komponen.

Ketiga, mengira bahwa perang murah berarti perang asal-asalan. Ini juga salah. Justru karena murah, sistem seperti itu harus sangat disiplin di desain fungsi dan rantai produksi. Sistem murah yang tidak andal hanya menjadi sampah elektronik.

Keempat, menyimpulkan bahwa drone murah menggantikan semua kebutuhan lain. Reuters menunjukkan bahwa sekalipun drone Iran efektif dalam menciptakan gangguan besar di Hormuz dan kawasan Teluk, perang tetap berkaitan dengan pelabuhan, jalur energi, pertahanan udara, ranjau laut, dan keputusan politik tingkat tinggi. Jadi, drone murah memperkuat strategi, tetapi tidak berdiri sendiri. ([Reuters](#))

13.5. Pelajaran yang harus diambil tanpa meniru politiknya

Indonesia bisa dan perlu belajar dari Iran, tetapi **tanpa meniru politik, orientasi regional, atau model eskalasinya**. Yang perlu diambil adalah pelajaran teknis dan organisasionalnya.

Pelajaran pertama: bangun sistem yang **cukup tangguh** sebelum bermimpi tentang sistem yang paling canggih.

Pelajaran kedua: prioritaskan **navigasi tahan gangguan, radio, EW, dan kemampuan misi minimum saat link putus**.

Pelajaran ketiga: anggap **biaya rendah** sebagai alat strategi, bukan sekadar penghematan anggaran.

Pelajaran keempat: desain organisasi dan komando agar tidak terlalu tergantung pada satu pusat yang rapuh.

Pelajaran kelima: perlakukan *resilience* sebagai ukuran kualitas utama, sejajar dengan akurasi dan jangkauan.

Bila diterjemahkan ke konteks Indonesia, pelajaran Iran bukan “jadilah seperti Iran,” tetapi:

- **bangun sistem yang tetap berguna saat diganggu,**
- **buat desain yang bisa hidup di bawah embargo atau putus pasokan,**
- **dan sadari bahwa perang modern memberi nilai besar pada sistem yang tahan, murah, dan bisa diulang.**

Itu sepenuhnya konsisten dengan arah buku Anda: **Indonesia tidak perlu mengejar yang paling glamor terlebih dahulu; Indonesia harus lebih dulu membangun yang paling tahan dan paling berguna.**

Ringkasan kunci

- **Murah tidak berarti primitif.** Sistem murah bisa sangat berbahaya bila diproduksi massal dan dipakai dengan logika operasi yang tepat. ([Council on Foreign Relations](#))
- **Ketangguhan lebih penting daripada spesifikasi tertinggi.** Sistem yang tetap bekerja di bawah *jamming* dan degradasi sering lebih bernilai daripada sistem elit yang rapuh. ([Council on Foreign Relations](#))
- **Indonesia perlu belajar soal *resilience*** karena tantangan sebenarnya bukan hanya teknologi, tetapi juga *supply chain*, EW, komando, dan biaya perang.
- **Salah membaca Iran berbahaya:** bisa membuat kita memuja volume tanpa arsitektur, atau mengejar AI sensasional sambil melupakan fondasi teknis.
- **Pelajaran yang perlu diambil** adalah *resilience*, modularitas, biaya rendah, dan otonomi secukupnya—**tanpa meniru politik dan strategi regional Iran.** ([Reuters](#))

Bagian V. Indonesia: Mengapa Tertinggal, dan Apa yang Harus Diubah

Bab 14. Titik Lemah Indonesia Hari Ini

Bab ini harus ditulis dengan jujur tetapi tetap adil. Indonesia tidak mulai dari nol. Ada fondasi riset, ada inisiatif semikonduktor, ada pengembangan autopilot dan UAV di BRIN, ada agenda radar nasional, ada arah transformasi digital pertahanan, dan ada kesadaran bahwa drone, satelit, dan AI akan semakin penting. Tetapi jika dibaca dari kebutuhan **war-ready AI** dan industri drone/elektronik yang tahan *cut-off supply chain*, kelemahan Indonesia masih nyata: **terlalu berfokus pada platform, terlalu lemah di elektronik dan mission software, terlalu lambat dalam transisi dari prototipe ke produksi, dan terlalu rapuh pada rantai pasok luar negeri**. Tujuh titik lemah ini ditempatkan sebagai pintu masuk menuju agenda perbaikan nasional.

14.1. Terlalu platform-centric

Kelemahan pertama Indonesia adalah cara berpikir yang masih terlalu **platform-centric**. Dalam logika lama, kekuatan pertahanan sering diukur dari jumlah kapal, pesawat, kendaraan tempur, atau rudal. Padahal bab-bab sebelumnya buku ini sudah menekankan bahwa perang modern bergeser dari platform ke **data, model, integrasi sensor, dan kecepatan keputusan**. Catatan yang sudah Anda bangun juga sangat tegas: negara yang terlalu lama berpikir *platform-centric* cenderung membeli alat, tetapi kurang membangun *data pipeline, mission software, integrasi sensor, dan kemampuan pengambilan keputusan*.

Arah doktrin pertahanan Indonesia sendiri sebenarnya sudah memberi petunjuk ke sana. **Buku Putih Pertahanan** menyebut pentingnya pembangunan kekuatan pertahanan maritim yang didukung teknologi satelit dan sistem drone. Namun secara praktis, titik lemah Indonesia masih tampak pada jarak antara pengakuan konseptual itu dan pembangunan ekosistem yang menyatukan **sensor–fusion–komando–drone–EW–data latihan** menjadi satu sistem tempur yang utuh. (kemhan.go.id)

Masalahnya bukan bahwa platform tidak penting. Platform tetap penting. Masalahnya adalah ketika platform diperlakukan seolah otomatis menghasilkan keunggulan. Dalam perang modern, platform unggul bila:

- terhubung ke jaringan data yang baik,
- punya *mission software* yang matang,
- masuk ke *kill chain* yang cepat,
- dan didukung sistem logistik, EW, serta data yang hidup.

Tanpa itu, platform mudah berubah menjadi simbol modernisasi, bukan kekuatan operasional.

14.2. Lemah di elektronik pertahanan

Kelemahan kedua adalah **elektronik pertahanan**. Indonesia memang punya kemajuan di beberapa wilayah, tetapi titik lemah paling serius justru ada pada subsistem yang menentukan apakah drone, radar, atau sistem otonom benar-benar bisa hidup: *flight control computer*, *RF module*, *inertial module*, *power electronics*, *crypto*, *sensor integration*, dan *mission computer*. Catatan yang sudah Anda susun tepat sekali ketika menegaskan bahwa Indonesia tidak boleh hanya serius pada *airframe* drone, tetapi harus serius pada **PCB ruggedized**, **BMS**, **motor controller**, **autopilot board**, **IMU**, **RF**, **antena**, **kamera EO/IR**, **crypto module**, dan **mission computer**.

Data resmi Indonesia justru mendukung diagnosis itu. BRIN menyatakan komitmen untuk membangun **Flight Control Computer** hasil rancangan nasional dan menempatkan autopilot sebagai teknologi kunci UAV. BRIN juga menegaskan bahwa data satelit navigasi makin esensial dan Indonesia perlu membangun **kemandirian teknologi GNSS**. Ini kabar baik, tetapi sekaligus menandakan bahwa titik-titik itu memang masih menjadi pekerjaan besar, bukan kapabilitas yang sudah mapan. (brin.go.id) (brin.go.id)

KKIP juga menunjukkan hal serupa lewat program radar GCI. Radar telah masuk program industri pertahanan nasional, tetapi hingga 2022 penguasaan kunci masih menyisakan area penting seperti **phased array antenna system** dan **signal processor**. Itu berarti Indonesia menyadari persoalannya, tetapi pekerjaan pada jantung elektronik dan pemrosesan sinyal masih jauh dari selesai. (kkip.go.id)

Titik lemahnya jelas:

- Indonesia lebih mudah membuat purwarupa sistem daripada menguasai subsistem elektronik kunci secara luas.
- Bila elektronik inti masih bergantung pada impor, maka daya tahan perang ikut bergantung pada pihak luar.

14.3. Lemah di mission software dan data pipeline

Kelemahan ketiga adalah yang paling sering tidak terlihat: **software dan data**. Indonesia sudah cukup lama terbiasa membahas alat fisik, tetapi jauh lebih jarang membahas *mission software*, *data architecture*, *compute cluster*, atau *after-action data pipeline*. Padahal justru di sinilah AI pertahanan hidup atau mati.

Catatan dalam dokumen Anda sangat tepat: **drone tanpa data-link tahan gangguan akan lumpuh; AI tanpa sensor dan data akan kosong; radar tanpa integrasi ke kill chain akan lambat**. Karena itu, struktur program pertahanan harus menyatukan **sensor → fusion → command software → jammer → drone → after-action data** dalam satu siklus latihan dan pengadaan.

Fakta di tingkat nasional juga mengarah ke sini. Reuters melaporkan bahwa hingga 2025 Indonesia baru menyusun *roadmap* AI nasional yang pertama dan salah satu masalah yang disebut langsung oleh pemerintah adalah kebutuhan akan **infrastruktur** dan **computational clusters**. Itu memberi sinyal bahwa bahkan di level nasional non-pertahanan, basis *compute* dan data untuk AI masih dalam tahap pembentukan. ([reuters.com](https://www.reuters.com))

Ini berarti kritik terhadap Indonesia bukan bahwa “kita tidak punya AI,” tetapi bahwa:

- AI belum ditopang *mission software* pertahanan yang cukup matang,
- belum ada *data pipeline* pertahanan yang benar-benar jelas dan disiplin,
- dan integrasi dari sensor ke keputusan masih cenderung terpecah.

14.4. Pengadaan lambat, prototipe banyak, produksi sedikit

Kelemahan keempat adalah klasik tetapi sangat menentukan: **siklus dari riset ke pengadaan ke produksi masih lambat dan terputus-putus**. Banyak negara berkembang terlihat produktif di seminar, demo, dan purwarupa, tetapi lemah ketika harus mengubah semuanya menjadi volume produksi yang stabil. Dalam dokumen Anda, masalah ini sudah dirumuskan lugas: Indonesia kuat di prototipe, tetapi lemah di transisi ke operasi; karena itu dibutuhkan *Rapid Prototyping & Low-Rate Production Hub* dan jalur cepat pengadaan drone/AI/EW.

Petunjuk resminya juga ada. BRIN menunjukkan kemajuan dengan uji terbang beberapa pesawat tanpa awak dan pengembangan FCC nasional; artinya fondasi riset memang ada. Tetapi justru karena berita resmi masih menekankan *uji terbang*, *optimalisasi sistem autopilot*, dan langkah menuju kemandirian, terlihat bahwa perjalanan dari riset ke *operational fielding* masih panjang. (brin.go.id) (brin.go.id)

Di sisi pertahanan, Kemhan sendiri dalam dokumen SPBE 2025–2029 memasukkan penguatan belanja TIK, integrasi sistem, dan transformasi digital di lingkungan Kemhan/TNI. Itu penting, tetapi juga menunjukkan bahwa reformasi proses dan arsitektur digital masih berada pada tahap pembangunan, bukan hasil akhir yang sudah matang. (ppid.kemhan.go.id)

Masalah utamanya:

- riset ada,
- purwarupa ada,
- tetapi jembatan ke produksi rendah-volume dan adopsi operasional belum cukup kuat.

14.5. Kampus kuat di riset, lemah di transisi ke operasi

Kelemahan kelima adalah pada kampus. Indonesia punya banyak kemampuan akademik, termasuk di kontrol, autopilot, kendali roket, UAV, dan elektronika. Jejak ini terlihat di ekosistem BRIN dan jurnal-jurnal teknis nasional. Tetapi kekuatan akademik itu belum otomatis berubah menjadi **reference design** yang siap diproduksi dan dipakai satuan operasional.

Catatan Anda sangat tajam di sini: kampus jangan hanya menghasilkan makalah; kampus perlu diberi mandat dan insentif untuk menghasilkan **autopilot board, radio module, anti-jam navigation stack, secure mesh network, camera gimbal murah, drone-in-a-box**, dan sejenisnya. Indikator keberhasilan juga perlu bergeser dari jurnal semata ke **TRL naik, uji lapangan, lisensi IP, spin-off, dan adopsi industri/instansi**.

Kemenperin sebenarnya sudah mulai membuka jalan yang benar lewat **ICDEC**. Pada Januari 2026, Kemenperin menegaskan bahwa langkah realistis menuju kemandirian semikonduktor adalah **desain chip dan pengembangan SDM**, bukan langsung *fab* besar, dan bahwa ICDEC dibangun sebagai simpul kolaborasi pemerintah–industri–akademik dengan dukungan 16 perguruan tinggi. Itu sangat penting, tetapi juga menegaskan bahwa kita masih berada pada tahap membangun fondasi desain dan SDM, belum pada tahap kemandirian manufaktur elektronik canggih. (sippa.kemenperin.go.id)

Kelemahan yang harus diakui:

- riset kampus sering berhenti di artikel atau prototipe,
- insentif untuk menuju produk operasional masih lemah,
- dan hubungan kampus–industri–user militer belum cukup rapat dan ritmis.

14.6. Industri terfragmentasi

Kelemahan keenam adalah **fragmentasi industri**. Indonesia punya BUMN pertahanan, ada perusahaan swasta teknologi, ada startup, ada konsorsium riset, ada BRIN, ada kampus, ada Kemenperin, ada Kemhan, ada KKIP. Tetapi masalahnya bukan ketiadaan aktor; masalahnya adalah **terlalu banyak aktor yang belum terikat dalam satu loop produksi–pengujian–pengadaan yang disiplin**.

KKIP memberi contoh bahwa konsorsium bisa dibangun, misalnya untuk radar GCI, dengan keterlibatan LAPI ITB, RTI, Infoglobal, LEN, Balitbang Kemhan, dan mitra offset asing. Itu model yang baik. Namun justru contoh itu menunjukkan bahwa untuk mencapai sistem matang dibutuhkan koordinasi multipihak yang lama dan berat.

(kkip.go.id)

Kemhan sendiri pada 2025 mendorong sinergi pertahanan–industri pada forum KADIN. Ini pertanda positif, tetapi bila masih perlu terus didorong secara eksplisit, berarti integrasi lintas-aktor memang belum otomatis terjadi. (kemhan.go.id)

Dalam bahasa yang lebih blak-blakan: Indonesia bukan kekurangan pemain; Indonesia kekurangan **orkestrasi**.

Bentuk fragmentasi yang paling terasa:

- riset, industri, dan pengguna belum satu ritme,
- produk sering lahir tanpa jalur adopsi yang jelas,
- dan standar bersama untuk integrasi sistem masih belum kuat.

14.7. Supply chain sebagai titik rapuh strategis

Kelemahan ketujuh adalah yang paling berbahaya bila tidak dibaca sejak awal: **rantai pasok**. Jika perang modern bertumpu pada drone, radio, navigasi, sensor, chip, baterai, dan modul RF, maka ketergantungan pada impor berarti ketergantungan pada keputusan politik dan pasar di luar negeri. Kemenperin sendiri menegaskan bahwa tingginya ketergantungan impor semikonduktor adalah sinyal penting bagi ketahanan industri nasional, dan karena itu strategi awal difokuskan pada desain chip/IP, lalu penguatan material, fabrikasi, serta *assembly*, *testing*, dan *packaging*. (sippa.kemenperin.go.id)

Reuters juga menunjukkan bahwa bahkan agenda AI nasional Indonesia masih sangat bergantung pada investasi, infrastruktur, *compute clusters*, dan pemain global seperti Nvidia dan Microsoft. Ini bagus untuk membangun ekosistem digital nasional, tetapi dari sudut pertahanan juga mengingatkan bahwa **fondasi komputasi dan hardware kita masih rapuh secara strategis**. (reuters.com) (reuters.com) (reuters.com)

Catatan Anda sudah memberi resep yang sangat tepat: stok nasional komponen kritis, *second source*, desain modular, *repair depots*, dan kemampuan tetap produksi walau kualitas turun sedikit. Itu bukan paranoia. Itu adalah logika minimum untuk negara yang ingin punya **war-ready AI** dan industri drone yang tidak lumpuh saat jalur pasok global terganggu.

Titik rapuh strategis Indonesia ada pada:

- **chip dan semikonduktor,**
 - **modul navigasi dan sensor,**
 - **komponen RF dan *power electronics*,**
 - **baterai dan *mission electronics*,**
 - **serta ketergantungan pada *compute* dan ekosistem digital asing.**
- (sippa.kemenperin.go.id)

Penutup Bab: diagnosis yang keras tetapi berguna

Kalau seluruh bab ini diringkas dalam satu kalimat, maka titik lemah Indonesia hari ini bukan terutama pada “kurang semangat bicara AI”, melainkan pada **ketidacukupan fondasi operasional**. Kita sudah punya banyak diskursus, beberapa inisiatif, sejumlah riset, dan sebagian fondasi industri. Tetapi untuk menjadi *war-ready*, Indonesia masih harus menjawab tujuh kelemahan ini secara sistematis:

- kurang keluar dari pola pikir platform,
- kurang kuat di elektronik inti,
- kurang matang di *mission software* dan data,
- kurang cepat mengubah prototipe menjadi produksi,
- kurang baik menghubungkan kampus ke operasi,
- kurang rapi mengorkestrasi industri,
- dan masih terlalu rapuh pada *supply chain*.

Justru karena diagnosisnya keras, bab ini berguna. Sebab tanpa diagnosis yang jujur, strategi nasional akan berubah menjadi daftar mimpi, bukan agenda perubahan.

Ringkasan kunci

- **Indonesia masih terlalu *platform-centric***. Kekuatan sering dibaca dari alat, bukan dari integrasi data, software, dan keputusan.
- **Elektronik pertahanan masih lemah**, terutama pada subsistem inti seperti FCC, IMU, RF, crypto, dan pemrosesan sinyal. (brin.go.id) (kkip.go.id)
- **Mission software dan data pipeline** belum cukup matang sebagai tulang punggung AI pertahanan. (reuters.com)
- **Pengadaan masih lambat**, sementara transisi dari prototipe ke produksi operasional belum cukup kuat. (brin.go.id)
- **Kampus kuat di riset tetapi lemah di transisi ke operasi**, sehingga perlu insentif untuk *reference design*, TRL, *spin-off*, dan uji lapangan. (sippa.kemenperin.go.id)
- **Industri masih terfragmentasi**. Problem Indonesia lebih pada orkestrasi daripada ketiadaan aktor. (kemhan.go.id)
- **Supply chain adalah titik rapuh strategis terbesar**. Kemandirian minimum harus dibangun pada komponen, desain modular, dan regenerasi teknologi dalam negeri. (sippa.kemenperin.go.id)

Bab 15. Doktrin Indonesia yang Seharusnya: Archipelagic, Networked, Attritable

Bab ini adalah titik balik buku. Setelah membaca Amerika Serikat, Ukraina, dan Iran, pertanyaan Indonesia bukan lagi “siapa yang paling canggih?”, tetapi **doktrin seperti apa yang paling cocok untuk negara kepulauan terbesar di dunia**. Indonesia perlu doktrin yang **berangkat dari geografi, bertumpu pada jejaring sensor dan data, serta menerima penggunaan sistem murah yang dapat dikorbankan sebagai bagian normal dari operasi**.

Doktrin seperti itu saya ringkas dalam tiga kata: **archipelagic, networked, attritable**. *Archipelagic* berarti berangkat dari realitas negara kepulauan. *Networked* berarti sensor, komando, data, drone, radar, AIS, satelit, dan EW harus bekerja sebagai satu sistem. *Attritable* berarti Indonesia tidak boleh hanya mengandalkan sedikit platform mahal, tetapi harus mempunyai banyak sistem murah yang bisa diganti cepat saat hilang atau rusak. Arah ini juga sejalan dengan **Buku Putih Pertahanan** yang menegaskan bahwa untuk membangun kekuatan pertahanan maritim, Indonesia perlu dukungan **teknologi satelit dan sistem drone**. ([Kementerian Pertahanan](#))

15.1. Indonesia harus berangkat dari geografi

Kelemahan paling umum dalam perumusan doktrin adalah memulai dari teknologi, bukan dari geografi. Untuk Indonesia, itu akan menjadi kesalahan besar. Indonesia bukan negara kontinental, bukan negara bertetangga garis depan darat panjang seperti Ukraina, dan bukan negara yang bisa meniru mentah-mentah model kekuatan global seperti AS atau China. Indonesia adalah **negara kepulauan** dengan ribuan pulau, jalur laut yang sangat panjang, banyak pulau terluar, selat strategis, dan wilayah maritim yang luas. Karena itu, titik berangkat doktrin pertahanan Indonesia haruslah **laut, pulau, selat, pangkalan, dan jalur logistik**, bukan sekadar daftar alutsista. ([Kementerian Pertahanan](#))

Buku Putih Pertahanan secara eksplisit mengaitkan pembangunan kekuatan pertahanan maritim dengan satelit dan drone. Ini penting, karena artinya secara resmi Indonesia sudah mengakui bahwa pengawasan wilayah dan kekuatan pertahanan maritim tidak bisa lagi hanya bergantung pada kapal patroli dan pos fisik. Tetapi pengakuan doktrinal itu harus diterjemahkan lebih jauh: bukan hanya “punya drone” atau “punya satelit,” melainkan **menjadikan ruang kepulauan sebagai ruang yang terus dipantau, dihubungkan, dan dipertahankan secara berlapis**. ([Kementerian Pertahanan](#))

Artinya, doktrin Indonesia harus berangkat dari pertanyaan ini:

- bagaimana menjaga pulau terluar yang kecil tetapi strategis,
- bagaimana memantau jalur laut yang luas tanpa biaya yang melumpuhkan,
- bagaimana mempertahankan choke points dan pangkalan,

- dan bagaimana tetap beroperasi bila koneksi, GNSS, atau rantai pasok terganggu.

15.2. Negara kepulauan butuh maritime domain awareness

Kalau ada satu kebutuhan yang paling mendesak bagi doktrin Indonesia, itu adalah **maritime domain awareness (MDA)**. Negara kepulauan tidak bisa bertahan dengan baik bila ia tidak melihat lautnya sendiri secara cukup cepat, cukup luas, dan cukup dalam. Ini bukan isu abstrak. Ancaman di perairan Indonesia sangat beragam: pelanggaran wilayah, *illegal fishing*, penyelundupan, intrusi kapal asing, sabotase kabel laut, hingga potensi tekanan militer di kawasan seperti Laut Natuna Utara. Sejumlah kajian Indonesia juga menekankan bahwa pengawasan laut modern harus bertumpu pada **radar, satelit, AIS, drone, dan analitik data** untuk memperluas cakupan pemantauan. ([Jurnal Universitas Padjadjaran](#))

Di sinilah MDA bukan sekadar proyek teknis, tetapi inti doktrin. Tanpa MDA yang kuat, Indonesia akan:

- terlambat melihat intrusi,
- terlambat memahami pola ancaman,
- dan terlambat menghubungkan pengamatan dengan respons.

Bahan yang Anda bangun sebelumnya sangat tepat saat menempatkan **maritime domain awareness** sebagai salah satu fungsi utama *war-ready AI* versi Indonesia. Indonesia tidak perlu memulai dari model AI terbesar. Indonesia perlu memulai dari **kemampuan melihat lautnya sendiri secara terus-menerus dan mengubah pengamatan itu menjadi keputusan operasional**.

Selain radar pantai dan patroli fisik, Indonesia juga mulai mengembangkan jalur satelit. Program **RIDU-Sat** di Unhan, misalnya, ditujukan untuk membangun kompetensi satelit nano dan *ground station*. Dari sisi pertahanan, ini penting bukan karena satu satelit kecil akan langsung menyelesaikan masalah, tetapi karena ia menunjukkan bahwa Indonesia mulai masuk ke **rantai kemampuan ruang angkasa yang relevan untuk pengawasan dan komunikasi**. ([Kementerian Pertahanan](#))

15.3. Drone udara, laut, dan darat untuk pulau-pulau terluar

Doktrin kepulauan tidak boleh hanya memikirkan drone udara. Indonesia perlu memandang drone sebagai **keluarga sistem lintas-domain**: udara, laut, dan darat. Pulau-pulau terluar membutuhkan pengawasan terus-menerus, pengiriman sensor murah, kemampuan *relay*, dan dalam kondisi tertentu kemampuan serang ringan, *counter-drone*, dan logistik jarak dekat. Karena itu, doktrin Indonesia seharusnya tidak bertanya “apakah kita punya drone?”, tetapi **drone jenis apa untuk misi apa, di pulau mana, dalam jaringan seperti apa**.

Untuk pulau-pulau terluar, kombinasi yang paling masuk akal adalah:

- **UAV kecil dan sedang** untuk ISR dan *relay* komunikasi,
- **USV/sea drones** untuk patroli area terbatas, perlindungan perairan sekitar pangkalan, dan pengamatan choke points,
- **UGV ringan** untuk logistik, patroli perimeter, atau dukungan pangkalan kecil.

Arah seperti ini makin masuk akal karena bahkan di internal Kementerian Pertahanan sendiri sudah muncul pembahasan tentang **swarm drone** dan *aerial drone mothership* sebagai bagian transformasi medan tempur, disertai anjuran agar Indonesia memiliki **master plan nasional** 10–15 tahun untuk pengembangan sistem tersebut. ([Kementerian Pertahanan](#))

Bagi Indonesia, nilai terbesarnya bukan pada “drone serang spektakuler,” tetapi pada **drone sebagai pengganda kehadiran**. Pulau kecil yang tidak mungkin dijaga besar-besaran oleh personel bisa tetap “hadir” secara militer bila dilapisi drone, sensor, kamera, AIS, radar, dan *edge AI* yang cukup tangguh.

15.4. Pertahanan choke points, pangkalan, dan jalur logistik

Geografi Indonesia memberi beberapa titik yang nilainya jauh lebih besar daripada ukurannya di peta: selat, pangkalan, pelabuhan, *fuel nodes*, *airstrips*, kabel laut, dan rute logistik ke wilayah terluar. Karena itu, doktrin Indonesia tidak boleh hanya bersifat “wilayah luas”, tetapi juga harus bersifat **fokus pada simpul-simpul kritis**. Dalam konteks perang modern, *choke points* dan pangkalan adalah tempat di mana drone, AI, EW, radar, dan jaringan sensor bisa memberi efek yang sangat besar dengan biaya yang relatif lebih rendah daripada penjagaan konvensional penuh di semua tempat. ([Jurnal Unhas](#))

Pertahanan simpul seperti ini memerlukan logika berlapis:

- **lapisan pengawasan** dengan radar, AIS, satelit, dan drone ISR,
- **lapisan identifikasi** dengan fusi data dan *edge analytics*,
- **lapisan respons** dengan *counter-drone*, patroli cepat, dan sistem intersepsi murah,
- **lapisan fallback** bila komunikasi terganggu atau sensor utama rusak.

Ini sangat penting untuk Indonesia karena jalur logistik antar pulau adalah urat nadi pertahanan. Jika pangkalan kecil, selat, atau node logistik bisa dijaga dengan arsitektur murah dan tersebar, Indonesia akan jauh lebih tahan terhadap gangguan daripada bila hanya mengandalkan sedikit platform besar. Bahan Anda sebelumnya sangat tepat saat menekankan **pertahanan pulau kecil, pangkalan, choke points, dan jalur logistik** sebagai inti doktrin Indonesia yang benar.

15.5. EW, radar, AIS, satelit, dan AI edge sebagai satu ekosistem

Inilah inti kata *networked*. Indonesia tidak akan cukup kuat bila terus memandang radar, AIS, satelit, drone, EW, dan AI sebagai proyek-proyek terpisah. Semuanya harus diperlakukan sebagai **satu ekosistem pertahanan**. Bahan Anda merumuskannya dengan sangat tajam: drone tanpa *data-link* tahan gangguan akan lumpuh; AI tanpa sensor dan data akan kosong; radar tanpa integrasi ke *kill chain* akan lambat.

Dari sisi resmi, Indonesia sudah punya beberapa fondasi yang relevan. **KKIP** menempatkan radar sebagai program industri pertahanan nasional dan masih mengejar penguasaan teknologi kunci seperti *phased array antenna system* dan *signal processor*. **BRIN** menekankan FCC dan GNSS sebagai area kunci untuk kemandirian UAV. **Kemhan** sendiri mengakui pentingnya satelit dan drone untuk pertahanan maritim, sementara pembahasan internal tentang *swarm drone* juga sudah mulai muncul. ([KKIP](#))

Karena itu, doktrin Indonesia yang benar harus memperlakukan:

- **EW** sebagai syarat minimum, bukan pelengkap,
- **radar dan AIS** sebagai mata awal,
- **satelit** sebagai penguat cakupan dan ketahanan,
- **AI edge** sebagai alat pemroses dekat lapangan saat koneksi ke pusat lambat atau terganggu,
- **dan mission software** sebagai lem yang menyatukan semuanya.

Kalau ekosistem ini tidak dibangun, Indonesia akan terus punya “bagian-bagian bagus” yang tidak sepenuhnya berbicara satu sama lain.

15.6. Mengapa Indonesia tidak boleh meniru mentah-mentah AS, China, Ukraina, atau Iran

Bagian ini sangat penting. Indonesia bisa belajar banyak dari negara lain, tetapi **tidak boleh menyalin mentah-mentah**.

Dari **AS**, Indonesia bisa belajar tentang ekosistem data, *cloud*, integrator, dan *battle management software*. Tetapi Indonesia tidak punya sumber daya untuk meniru skala dan arsitektur Pentagon secara langsung.

Dari **China**, Indonesia bisa belajar tentang pentingnya skala industri, *mass autonomy*, dan integrasi sipil-militer. Tetapi Indonesia tidak bisa mengandalkan model negara-industri yang sangat tersentralisasi seperti Beijing.

Dari **Ukraina**, Indonesia bisa belajar tentang *frontline-driven innovation*, pengadaan cepat, industri kecil yang lincah, dan data tempur sebagai aset. Tetapi Indonesia tidak punya geografi, ancaman, dan konteks perang darat seperti Ukraina.

Dari **Iran**, Indonesia bisa belajar bahwa *resilience* sering lebih penting daripada kemewahan, dan bahwa sistem murah yang cukup tangguh bisa sangat berbahaya. Tetapi Indonesia tidak boleh meniru logika eskalasi regional atau strategi asimetris Iran secara politik.

Itulah sebabnya doktrin Indonesia harus unik. Ia harus:

- berangkat dari geografi kepulauan,
- menerima bahwa jumlah personel tak mungkin mengisi semua titik,
- membangun kehadiran melalui jaringan sensor dan sistem murah,
- dan mengaitkan doktrin dengan realitas industri dan rantai pasok nasional.

Dengan kata lain, Indonesia perlu **belajar dari semua pihak, tetapi tunduk pada geografinya sendiri**. Itu satu-satunya cara agar doktrin tidak jatuh menjadi imitasi.

Penutup Bab: rumusan doktrin yang lebih masuk akal

Jika bab ini diringkas ke dalam satu kalimat, maka doktrin Indonesia yang lebih masuk akal adalah ini:

Indonesia memerlukan doktrin pertahanan kepulauan yang berbasis jejaring sensor dan data, didukung drone lintas-domain dan sistem murah yang dapat dikorbankan, untuk menjaga pulau terluar, simpul logistik, dan choke points secara berlapis, bahkan saat konektivitas dan rantai pasok terganggu.

Itu berarti kekuatan Indonesia ke depan tidak boleh diukur hanya dari platform besar yang berhasil dibeli, tetapi juga dari:

- berapa jauh laut kita bisa dipantau secara terus-menerus,
- berapa cepat data bisa diubah menjadi keputusan,
- berapa banyak simpul kritis yang punya lapisan pengawasan dan pertahanan murah,
- dan seberapa tangguh sistem kita saat GNSS, *link*, atau pasokan komponen terganggu.

Di situlah makna **archipelagic, networked, attritable** menjadi sangat konkret.

Ringkasan kunci

- **Indonesia harus memulai dari geografi**, bukan dari daftar teknologi. Negara kepulauan memerlukan doktrin yang lahir dari laut, pulau, selat, pangkalan, dan jalur logistik. ([Kementerian Pertahanan](#))
- **Maritime domain awareness adalah inti**, karena negara kepulauan tidak dapat bertahan baik bila tidak melihat lautnya sendiri secara terus-menerus dan cukup dalam. ([Jurnal Universitas Padjadjaran](#))
- **Drone udara, laut, dan darat** perlu diperlakukan sebagai keluarga sistem untuk pulau terluar, bukan sekadar proyek UAV tunggal. ([Kementerian Pertahanan](#))
- **Choke points, pangkalan, dan jalur logistik** harus menjadi fokus pertahanan berlapis, karena nilai strategisnya jauh lebih besar daripada ukuran fisiknya. ([Jurnal Unhas](#))
- **EW, radar, AIS, satelit, dan AI edge** harus dipadukan dalam satu ekosistem, bukan dibangun sebagai proyek yang berdiri sendiri. ([KKIP](#))
- **Indonesia tidak boleh meniru mentah-mentah AS, China, Ukraina, atau Iran.** Indonesia harus belajar dari semuanya, tetapi tetap tunduk pada logika kepulauan dan keterbatasan industrinya sendiri.

Bab 16. Apa Itu *War-Ready AI* versi Indonesia

16.1. Bukan model terbesar

Indonesia keliru besar jika membayangkan *war-ready AI* sebagai perlombaan memiliki model paling besar, *compute* paling mahal, atau *chatbot* paling canggih. Dalam perang, yang menentukan bukan papan presentasi, melainkan apakah sistem mampu **membaca situasi lebih cepat, memadatkan kekacauan data menjadi pemahaman, dan membantu keputusan operasional dalam waktu yang relevan**. Naskah buku ini sejak awal juga menegaskan bahwa AI militer tidak boleh dibaca sebagai “chatbot berseragam”, tetapi sebagai bagian dari sistem tempur yang menghubungkan data, sensor, komando, drone, logistik, dan keputusan.

Pengalaman Amerika Serikat justru memperlihatkan arah yang lebih bumi. Pentagon tidak bergerak hanya pada model besar, tetapi pada **adopsi data, analitik, AI, dan integrasi lintas komponen** melalui strategi resmi CDAO. Replicator juga tidak dijual sebagai perlombaan model, melainkan sebagai upaya menurunkan ribuan sistem otonom lintas domain dengan *software enabler* yang membuat sistem itu benar-benar berguna di lapangan. ([U.S. Department of War](#))

Bagi Indonesia, maknanya jelas.

- **Lebih penting model yang cukup baik tetapi bisa dipasang di sistem nyata**, daripada model hebat yang hanya hidup di pusat data.
- **Lebih penting data pipeline yang rapi**, daripada demo AI yang tidak terhubung ke operasi.
- **Lebih penting inferensi cepat di tepi jaringan**, daripada ketergantungan penuh pada koneksi ke *cloud*.
- **Lebih penting robust dan dapat dipelihara**, daripada mewah tetapi rapuh.

Jadi, *war-ready AI* Indonesia bukanlah AI yang paling besar. Ia adalah AI yang **cukup cerdas, cukup cepat, cukup hemat, cukup aman, dan cukup tahan untuk dipakai terus-menerus** di lingkungan kepulauan yang luas dan keras.

16.2. Bukan pula sekedar senjata otonom

Kesalahan kedua adalah menyamakan *war-ready AI* dengan **senjata otonom penuh**. Ini terlalu sempit, dan untuk Indonesia bahkan berbahaya. Bila diskusi berhenti pada “robot pembunuh” atau *killer robots*, kita gagal melihat wilayah yang justru paling realistis, paling mendesak, dan paling berguna: **ISR, battle management, sensor fusion, prioritasasi response, logistik, anti-drone, dan ketahanan jaringan**. Naskah buku ini sendiri konsisten menempatkan AI militer sebagai sistem yang mempercepat *decision loop*, bukan semata mesin yang menggantikan manusia dalam penggunaan kekuatan mematikan.

Bahkan di negara yang mendorong AI militer sangat agresif, fokus resminya tetap lebih luas daripada senjata otonom. Strategi Pentagon tentang data, analitik, dan AI menekankan adopsi operasional lintas fungsi, sementara berbagai dokumen dan pernyataan resmi tetap menempatkan akuntabilitas, keandalan, dan peran komando manusia sebagai hal sentral. ([U.S. Department of War](#))

Untuk Indonesia, ini penting karena:

- **kebutuhan pertama bukan robot pembunuh**, tetapi sistem yang membuat satuan lebih cepat melihat dan mengerti;
- **kebutuhan kedua bukan otonomi maksimal**, tetapi otonomi secukupnya di bawah gangguan;
- **kebutuhan ketiga bukan penggantian manusia**, tetapi penguatan kualitas komandan, operator, analisis, dan penembak.

Dengan kata lain, *war-ready AI* Indonesia harus dibangun sebagai **AI untuk memperkuat rantai komando dan efektivitas satuan**, bukan sebagai fantasi pemisahan penuh manusia dari keputusan perang.

16.3. AI untuk ISR, C2, logistik, EW, anti-drone, dan maritim

Di Indonesia, definisi yang paling berguna tentang *war-ready AI* harus dimulai dari fungsi. Pertanyaannya bukan “AI apa yang keren?”, melainkan **fungsi mana yang paling menentukan bila negara kepulauan harus melihat, merespons, bertahan, dan terus beroperasi di ruang laut yang luas**. Arah ini juga sangat sesuai dengan susunan buku yang menekankan OODA, C4ISR, *decision speed*, ekosistem drone, serta kebutuhan MDA untuk negara kepulauan.

a. AI untuk ISR

Inilah wilayah paling realistis dan paling bernilai. Ukraina mengumpulkan lebih dari **2 juta jam video perang** sejak 2022 untuk melatih sistem AI yang membantu identifikasi target, penilaian efektivitas serangan, dan keputusan taktis. Itu menunjukkan bahwa dalam perang modern, data visual dan sensor tempur adalah bahan bakar utama AI. ([Reuters](#))

Untuk Indonesia, AI ISR berarti:

- analitik video drone untuk pantai, pelabuhan, pulau terluar, dan jalur laut;
- deteksi anomali pada lalu lintas maritim dari AIS, radar, citra, dan laporan lapangan;
- klasifikasi objek untuk membedakan ancaman, umpan, kapal sipil, dan pola ilegal;
- *cueing* cepat bagi radar, kapal patroli, pesawat maritim, dan satuan reaksi.

b. AI untuk C2 dan *decision support*

AI tidak harus memerintah perang. Tetapi AI harus bisa **menyusun situasi, memprioritaskan alarm, memberi alternatif tindakan, dan memadatkan banjir data menjadi opsi yang bisa diputuskan manusia**. Inilah bentuk AI yang memperpendek OODA tanpa mencabut otoritas komando. Strategi resmi Pentagon juga bergerak ke arah pengintegrasian AI ke konsep tempur dan dukungan bagi pengambil keputusan, bukan sekadar eksperimen laboratorium. ([U.S. Department of War](#))

c. AI untuk logistik dan maintenance

Untuk Indonesia, logistik bukan isu belakang. Negara kepulauan hidup dan mati pada **rantai suplai, ketersediaan suku cadang, kesehatan baterai, kesiapan armada, dan prediksi gangguan distribusi**. Karena itu, AI untuk *predictive maintenance*, prediksi kebutuhan amunisi, penjadwalan rotasi, dan kesehatan sistem justru bisa lebih cepat matang daripada AI kinetik. Arah ini juga inline dengan bab sebelumnya dalam buku yang menekankan logistik, maintenance, dan fungsi non-kinetik sebagai wilayah paling realistis.

d. AI untuk EW dan anti-drone

Perang drone modern memperlihatkan bahwa masalahnya bukan hanya menyerang, tetapi **bertahan dari gangguan, spoofing, jamming, dan serbuan drone murah**. Reuters melaporkan bahwa Ukraina sudah memakai banyak sistem AI-augmented agar drone tetap bisa mencapai target di lingkungan jamming berat; di sisi lain, Pentagon pada akhir 2024 juga mengeluarkan strategi baru untuk menghadapi dampak sistem nirawak, termasuk ancaman drone kecil. ([Reuters](#))

Bagi Indonesia, AI anti-drone berarti:

- deteksi dini pola terbang dan anomali;
- penggabungan radar kecil, RF sensing, EO/IR, dan akustik;
- prioritas ancaman;
- pemilihan respons paling hemat biaya;
- dan pembelajaran terus-menerus dari insiden lapangan.

e. AI untuk maritim

Untuk negara kontinental, pusat gravitasi bisa darat. Untuk Indonesia, pusat gravitasi tetap **maritim**. Buku Putih Pertahanan Indonesia sudah lama menegaskan pembangunan pertahanan maritim yang didukung teknologi satelit dan sistem drone. NATO dan berbagai institusi maritim pertahanan juga semakin menekankan kombinasi AI, *advanced sensing*, dan sistem nirawak udara-laut untuk pengawasan dan keamanan maritim. ([Kementerian Pertahanan](#))

Karena itu, *war-ready AI* Indonesia harus menjadikan **maritime domain awareness** sebagai jantungnya:

- melihat selat strategis,
- membaca pola kapal dan *dark shipping*,
- menjaga pulau terluar,
- memantau perairan sengketa dan jalur logistik,
- serta menghubungkan laut, udara, dan pantai kesatu gambaran operasional.

16.4. AI *edge* yang tahan gangguan

Kalau ada satu kata yang harus menempel pada *war-ready AI*, itu adalah **tahan gangguan**. AI yang hanya bekerja saat koneksi bagus, GNSS bersih, *bandwidth* longgar, dan pusat data tersedia penuh, belum layak disebut *war-ready*. Pelajaran dari Ukraina sangat keras: AI yang bernilai adalah AI yang tetap berguna di bawah jamming, *signal degradation*, dan friksi medan perang. Reuters melaporkan penggunaan sistem AI pada drone justru berkembang karena kebutuhan beroperasi di area yang dilindungi jamming ekstensif. ([Reuters](#))

Di sinilah pentingnya *edge AI*.

Edge AI berarti kemampuan pemrosesan terjadi **dekat sensor dan platform**, bukan selalu di pusat. Dalam konteks Indonesia, ini jauh lebih masuk akal karena:

- wilayah sangat luas,
- konektivitas tidak merata,
- laut dan pulau membuat latensi menjadi masalah nyata,
- dan musuh yang cerdas akan berupaya memukul link komunikasi lebih dulu.

Maka AI *edge* yang dibutuhkan Indonesia seharusnya memiliki ciri berikut:

- **bisa berjalan pada *mission computer* kecil dan hemat daya;**
- **tetap bekerja saat *backhaul* putus;**
- **mampu melakukan inferensi lokal** untuk klasifikasi, pelacakan, atau alarm dini;
- **punya mode degradasi yang anggun**, bukan gagal total;
- **mudah di-*update* tetapi tidak bergantung terus pada vendor luar.**

Ini juga nyambung langsung dengan diagnosis dalam buku bahwa Indonesia lemah pada elektronik pertahanan, *mission software*, dan *data pipeline*, serta rapuh pada *supply chain*. *War-ready AI* tidak bisa dibangun tanpa membenahi fondasi itu.

16.5. Sistem yang bisa bekerja saat *supply chain* terganggu

Perang modern bukan hanya perang tembak. Ia juga perang **chip, baterai, radio, kamera, GNSS, modul RF, autopilot, enkripsi, dan suku cadang**. Karena itu, sistem AI yang hebat di masa damai belum tentu berguna di masa krisis bila seluruh komponennya bergantung pada rantai pasok yang rapuh. Naskah buku ini sudah tepat ketika menempatkan *supply chain* sebagai salah satu titik lemah strategis Indonesia.

Pelajaran global juga mengarah ke sana. Ukraina memperlihatkan betapa berharganya kemampuan cepat memproduksi, memperbaiki, dan memodifikasi sistem murah dalam jumlah besar; sedangkan Iran sering dibaca sebagai contoh bahwa “**cukup baik**”, **murah, dan tahan gangguan** bisa menciptakan efek strategis meskipun tidak berada di puncak teknologi. Di pihak lain, AS sendiri melalui Replicator menekankan volume, kecepatan lapangan, dan *software enabler*, bukan ketergantungan pada beberapa platform eksotis. ([U.S. Department of War](#))

Bagi Indonesia, ini berarti *war-ready AI* harus dirancang dengan prinsip:

- **modular**, sehingga komponen bisa diganti tanpa membunuh seluruh sistem;
- **interoperable**, sehingga sensor dan platform tidak terkurung vendor;
- **maintainable**, sehingga bengkel, kampus, dan industri lokal bisa ikut menopang;
- **attritable**, sehingga kehilangan platform tidak berarti kehilangan operasi;
- **substitutable**, sehingga ada opsi lokal atau regional saat impor terganggu.

Lebih tajam lagi, Indonesia tidak boleh membangun AI pertahanan yang terlalu bergantung pada:

- *cloud* asing yang tak pasti aksesnya saat krisis;
- API tertutup yang bisa berubah syarat sewaktu-waktu;
- modul radio dan navigasi yang sulit diganti;
- serta platform mahal yang jumlahnya sedikit dan tidak tahan kehilangan.

Sistem yang benar-benar *war-ready* adalah sistem yang **masih bisa bertarung dalam bentuk terdegradasi**, bukan sistem yang hanya mengesankan pada *full configuration*.

16.6. Definisi operasional *war-ready AI* untuk Indonesia

Sesudah semua pembahasan diatas, definisi operasionalnya bisa dirumuskan dengan tegas:

War-ready AI versi Indonesia adalah kemampuan AI yang terintegrasi ke jaringan sensor, komando, drone, logistik, EW, dan sistem maritim nasional; mampu mempercepat ISR dan keputusan; dapat bekerja di edge dalam kondisi konektivitas terganggu; tetap berguna saat GNSS, link, atau supply chain dipukul; serta cukup murah, modular, dan dapat diproduksi, diperbaiki, dan diulang dalam skala yang realistis untuk negara kepulauan.

Definisi ini selaras dengan arah buku bahwa Indonesia harus berpikir dari geografi kepulauan, jaringan sensor-data, sistem murah yang bisa dikorbankan, serta daya tahan saat konektivitas dan pasokan terganggu.

Supaya definisi itu tidak berhenti sebagai slogan, saya sarankan ia dipecah menjadi **indikator operasional** berikut.

Indikator minimum *war-ready AI* Indonesia

- **ISR nyata**
AI mampu mengolah video drone, citra, radar, AIS, RF, atau data lapangan menjadi alarm, klasifikasi, atau *cueing* yang berguna bagi operator. ([Reuters](#))
- **C2 yang dipercepat**
AI membantu memadatkan data multi-sumber menjadi gambaran situasi dan opsi tindakan, tanpa mencabut keputusan akhir dari manusia. ([U.S. Department of War](#))
- **Tahan jamming dan *degraded mode***
Sistem tetap punya fungsi inti meskipun link, GNSS, atau *bandwidth* terganggu. ([Reuters](#))
- **Bisa berjalan di *edge***
Fungsi penting tidak bergantung penuh pada pusat data atau konektivitas stabil.
- **Maritim sebagai inti**
Sistem mendukung MDA, perlindungan pulau terluar, choke points, jalur logistik, dan pangkalan. ([Kementerian Pertahanan](#))
- **Anti-drone dan EW masuk dari awal**
Karena perang drone modern membuat pertahanan terhadap drone sama pentingnya dengan memiliki drone. ([U.S. Department of War](#))
- **Murah, modular, attritable**
Kehilangan satu platform tidak boleh mematikan kemampuan sistem secara keseluruhan. ([U.S. Department of War](#))
- **Bisa dipelihara dan diulang di dalam negeri**
Ada kapasitas lokal untuk integrasi, perbaikan, pengujian, dan peningkatan.
- **Tidak sekadar demo**
Sudah dipakai dalam latihan, simulasi keras, dan skenario gangguan nyata.

- **Punya tata kelola**

Ada *logging*, jejak keputusan, batas penggunaan, dan akuntabilitas komando. ([U.S. Department of War](#))

Rumusan paling singkat

Bila harus diringkas ke satu kalimat:

War-ready AI Indonesia bukan AI paling glamor, melainkan AI yang membuat negara kepulauan ini bisa melihat lebih cepat, memutuskan lebih tepat, bertindak lebih murah, dan tetap bertahan saat jaringan, GNSS, dan pasokan terganggu.

Penutup Bab: ukuran keberhasilan yang benar

Ukuran keberhasilan Indonesia ke depan **tidak boleh lagi hanya jumlah platform besar yang dibeli**. Ukuran yang lebih jujur adalah:

- seberapa jauh laut dan pulau terluar bisa dipantau terus-menerus,
- seberapa cepat data bisa diubah menjadi keputusan,
- seberapa murah sistem dapat diulang dan diganti,
- seberapa tahan operasi berlangsung saat diganggu,
- dan seberapa besar bagian dari sistem itu bisa dipelihara di dalam negeri.

Di situlah *war-ready AI* versi Indonesia menemukan maknanya yang paling konkret: **bukan imitasi Amerika, bukan duplikasi Ukraina, bukan salinan Iran, melainkan AI pertahanan yang tunduk pada geografi kepulauan, realitas industri nasional, dan kebutuhan daya tahan strategis Indonesia**. Itu juga sepenuhnya sejalan dengan arah besar buku ini.

Bagian VI. Tahapan Indonesia Mengejar Ketinggalan

Bab 17. Tahap 1: 0–3 Tahun — Bertahan, Belajar, dan Membuat yang Mendesak

17.1. Jalur cepat pengadaan drone/AI/EW

Dalam tiga tahun pertama, Indonesia tidak boleh memulai dari proyek yang terlalu megah. Tahap awal harus berangkat dari satu prinsip sederhana: **perang modern tidak memberi kemewahan bagi negara yang belajar terlalu lambat**. Masalah Indonesia hari ini bukan terutama kurang seminar tentang AI, melainkan **pengadaan lambat, prototipe banyak, produksi sedikit, dan hubungan yang lemah antara kebutuhan operasi dengan keputusan pembelian**. Itu sudah terbaca jelas dalam diagnosis buku ini.

Karena itu, tiga tahun pertama harus difokuskan pada pembentukan **jalur cepat pengadaan** untuk tiga rumpun yang paling mendesak:

- **drone kecil taktis dan munisi berkeliranan sederhana,**
- **sistem *counter-drone* dan EW taktis,**
- **AI operasional untuk ISR, *tracking*, klasifikasi, dan bantuan keputusan,** bukan AI seremonial.

Pelajaran dari Amerika Serikat justru menarik karena negara sebesar itu pun sekarang menekankan **kecepatan penurunan sistem otonom murah dan attritable**, bukan sekadar platform besar. Inisiatif Replicator diarahkan untuk menurunkan **ribuan sistem otonom lintas domain** dalam rentang waktu singkat, dengan fokus pada kecepatan produksi dan pengiriman ke pengguna. ([U.S. Department of War](#)) Sementara itu, strategi baru DoD untuk menghadapi ancaman sistem nirawak menegaskan bahwa proliferasi drone sudah **mengubah karakter konflik**, sehingga respons tidak bisa lagi lambat dan terpisah-pisah. ([U.S. Department of War](#))

Bagi Indonesia, jalur cepat ini seharusnya berarti:

- **kontrak kecil tetapi nyata**, bukan proyek besar yang terlalu lama matang;
- **uji lapangan cepat**, bukan menunggu spesifikasi sempurna;
- **siklus akuisisi–uji–perbaikan–pengadaan ulang** dalam bulan, bukan tahun;
- **prioritas pada sistem yang bisa dipakai sekarang**, meski belum ideal.

Yang dibutuhkan pada tahap ini bukan kesempurnaan. Yang dibutuhkan adalah **tempo belajar nasional**.

17.2. Program nasional autopilot, radio, dan *mission computer*

Kalau tiga tahun pertama ingin memberi fondasi nyata, maka Indonesia harus memilih subsistem yang paling menentukan. Dalam konteks drone, AI, dan EW, tiga subsistem itu adalah:

- **autopilot,**
- **radio/data link,**
- **mission computer.**

Pilihan ini masuk akal karena buku ini sudah menegaskan bahwa titik lemah Indonesia bukan terutama pada wacana, tetapi pada **elektronik pertahanan, mission software, dan data pipeline**. Tanpa penguasaan minimal atas tiga blok ini, Indonesia akan terus tergantung pada paket impor yang sulit dimodifikasi, sulit diaudit, dan rawan lumpuh ketika akses komponen atau dukungan vendor terganggu.

Program nasional di tahap 0–3 tahun karena itu tidak perlu dimulai dari “chip nasional” yang bombastis. Tahap awal harus lebih membumi:

- membuat **arsitektur referensi autopilot** untuk drone kecil udara dan laut;
- mengembangkan **radio link taktis** yang bisa diuji dalam lingkungan padat gangguan;
- membangun **mission computer** yang cukup kuat untuk *edge inference*, navigasi, dan *payload management*;
- memakai pendekatan **design-first**, bukan mimpi *fab-first* yang terlalu dini.

Arah ini justru konsisten dengan roadmap bab-bab sesudahnya, yang menempatkan penguasaan elektronik, integrasi, *reference design*, dan produksi rendah volume sebagai tahap lanjutan. Maka tiga tahun pertama bukan tahap kemandirian penuh, melainkan tahap **menetapkan desain inti yang bisa terus diperbaiki, diuji, dan direproduksi**.

Prinsip kerjanya harus tegas:

- **modular**, agar komponen bisa diganti;
- **interoperable**, agar tidak terkunci vendor;
- **cukup murah**, agar bisa dipakai massal;
- **cukup terbuka secara teknis**, agar kampus, industri, dan satuan bisa ikut memperbaiki.

Di tahap ini, ukuran keberhasilannya bukan “sudah 100% lokal”, melainkan **sudah punya blok inti yang dipahami, bisa diubah, dan bisa diuji sendiri**.

17.3. Fokus pada drone kecil taktis dan *counter-drone*

Indonesia sering tergoda untuk memulai dari platform yang lebih besar karena kelihatan lebih strategis. Padahal dalam tiga tahun pertama, fokus yang paling rasional justru pada **drone kecil taktis** dan **sistem *counter-drone***. Alasannya sederhana: di situlah kombinasi antara **biaya, kecepatan belajar, nilai operasional, dan frekuensi penggunaan** bertemu.

Pengalaman Ukraina sangat jelas. Reuters melaporkan bahwa penggunaan sistem AI untuk drone berkembang pesat justru untuk membantu penetrasi ke area yang diproteksi jamming, sementara produksi dan penggunaan drone murah terus melonjak dalam skala sangat besar. ([Reuters](#)) Perang modern memperlihatkan bahwa **drone kecil bukan lagi alat tambahan**, tetapi telah menjadi bagian rutin dari pengintaian, koreksi tembakan, serangan murah, *decoy*, dan pengumpulan data tempur.

Karena itu, Indonesia dalam tiga tahun pertama sebaiknya memprioritaskan:

- **quadcopter dan fixed-wing kecil untuk ISR taktis,**
- **drone FPV atau sekelasnya untuk eksperimen attritable,**
- **drone maritim kecil untuk pengawasan area terbatas,**
- **sensor dan senjata hemat biaya untuk *counter-drone*,**
- **integrasi EW ringan untuk menguji ketahanan sistem sendiri dan melemahkan sistem lawan.**

Mengapa *counter-drone* harus masuk sejak awal? Karena ancaman drone kecil tumbuh eksponensial dan kini diakui secara resmi sebagai masalah lintas domain. Fakta lembar strategi DoD 2024 menegaskan bahwa penyebaran sistem nirawak yang cepat telah mengubah konflik dan menuntut pendekatan terpadu untuk melawan ancaman itu. ([U.S. Department of War](#))

Bagi Indonesia, ini berarti satu hal penting: **kita tidak boleh hanya belajar menerbangkan drone; kita juga harus belajar menjatuhkan drone, membutakan drone, menipu drone, dan bertahan dari drone.**

17.4. Pusat data drone dan simulasi tempur

AI militer yang serius tidak lahir dari slogan. Ia lahir dari **data tempur, data sensor, logs, video, telemetri, hasil misi, dan umpan balik kegagalan**. Tanpa itu, AI pertahanan akan tinggal menjadi *PowerPoint intelligence*. Karena itu, salah satu agenda paling penting dalam tiga tahun pertama adalah membangun **pusat data drone dan simulasi tempur**.

Pelajaran Ukraina sangat kuat di sini. Reuters melaporkan bahwa Ukraina telah mengumpulkan **lebih dari 2 juta jam video perang** sejak 2022, terutama dari drone, untuk membantu pelatihan model AI dalam identifikasi target, evaluasi efektivitas senjata, dan pengambilan keputusan. ([Reuters](#)) Ukraina juga membangun ekosistem Brave1, dan pada 2026 meluncurkan **Brave1 Dataroom** sebagai lingkungan aman untuk menguji dan melatih model AI menggunakan data militer nyata, dengan fokus awal pada deteksi dan intersepsi ancaman UAV. ([Defense News](#))

Indonesia tidak harus meniru bentuknya mentah-mentah, tetapi prinsipnya harus diambil.

Tiga tahun pertama harus menghasilkan:

- **repositori nasional video drone, telemetri, dan mission logs;**
- **format data standar minimum** untuk latihan dan evaluasi;
- **lingkungan simulasi dan synthetic training** untuk kondisi jamming, cuaca, laut, dan pulau;
- **mekanisme klasifikasi dan akses bertingkat**, agar data berguna tanpa dibuang ke ruang terbuka;
- **alat evaluasi pasca-misi**, sehingga setiap kegagalan menjadi bahan pembelajaran.

Untuk negara kepulauan seperti Indonesia, pusat data ini harus kuat pada skenario:

- **maritime domain awareness,**
- **pulau terluar,**
- **choke points,**
- **pangkalan dan jalur logistik,**
- **serangan drone ke instalasi vital,**
- **operasi dengan konektivitas buruk.**

Jadi, pusat data drone bukan sekadar gudang video. Ia adalah **mesin belajar nasional**.

17.5. Unit operasional sebagai *co-developer*

Salah satu jebakan terbesar dalam inovasi pertahanan adalah memisahkan pengguna dari pembuat. Akibatnya, kampus dan industri membuat prototipe yang mengesankan, tetapi tidak benar-benar cocok dengan kebutuhan lapangan. Buku ini sudah mengingatkan bahwa Indonesia lemah dalam **transisi dari riset ke operasi** dan terlalu sering terjebak pada prototipe yang tidak menyeberang menjadi kapasitas nyata.

Karena itu, dalam tahap 0–3 tahun, **unit operasional harus diperlakukan sebagai *co-developer***, bukan sekadar penerima akhir. Artinya:

- satuan pengguna ikut menentukan masalah prioritas;
- operator memberikan umpan balik harian;
- pengembang memperbaiki sistem berdasarkan pengalaman lapangan, bukan asumsi laboratorium;
- evaluasi keberhasilan didasarkan pada performa misi, bukan hanya spesifikasi katalog.

Model seperti ini sangat dekat dengan pengalaman Ukraina, di mana inovasi pertahanan berkembang cepat karena ada hubungan intens antara garis depan, tim teknis, produsen kecil, dan negara. Reuters dan berbagai laporan tentang ekosistem Ukraina menunjukkan bahwa kecepatan adaptasi datang dari **iterasi cepat berbasis umpan balik operasional**, bukan dari proyek yang terlalu jauh dari medan.

([Reuters](#))

Bagi Indonesia, ini berarti perlu dibangun:

- **beberapa unit uji operasional khusus,**
- **mekanisme pelaporan cepat dari latihan dan operasi,**
- **siklus revisi perangkat lunak dan konfigurasi yang pendek,**
- **budaya menerima kegagalan sebagai data,** bukan sekadar aib birokrasi.

Ini juga penting secara mental. Negara yang ingin mengejar ketertinggalan harus berhenti melihat inovasi pertahanan sebagai proyek presentasi. Inovasi pertahanan adalah **hubungan kerja yang keras antara pengguna, insinyur, analis data, dan pengambil keputusan.**

17.6. Latihan *GPS-denied* dan EW sejak awal

Salah satu kesalahan paling berbahaya adalah melatih drone dan AI hanya dalam kondisi ideal. Di medan perang nyata, musuh tidak akan membiarkan navigasi mulus, *link* bersih, dan spektrum tenang. Karena itu, dari tahun pertama pun Indonesia harus memulai **latihan *GPS-denied* dan EW**.

Ini sepenuhnya sejalan dengan arah Bab 16, yang menegaskan bahwa *war-ready AI* Indonesia harus bekerja di *edge*, tahan gangguan, dan tetap berguna saat GNSS, jaringan, atau *supply chain* dipukul. Pengalaman Ukraina juga memperkuat hal ini. Reuters melaporkan bahwa integrasi AI pada drone sangat didorong oleh kebutuhan untuk mengatasi **jamming** yang membuat kendali manual makin sulit. ([Reuters](#))

Karena itu, latihan awal tidak boleh nyaman. Ia harus memasukkan:

- **hilangnya GPS/GNSS,**
- **putusnya *data link*,**
- **gangguan radio,**
- **umpan sinyal palsu,**
- **penurunan kualitas sensor,**
- **mode operasi terdegradasi,**
- **keputusan operator di bawah informasi yang tidak lengkap.**

Dari latihan-latihan ini, Indonesia akan belajar pelajaran yang sangat penting:

- sistem mana yang terlalu bergantung pada satu link,
- konfigurasi mana yang paling rapuh,
- operator mana yang mampu beradaptasi,
- perangkat lunak mana yang perlu *failsafe* lebih baik,
- dan subsistem mana yang paling layak diprioritaskan untuk penguatan.

Latihan *GPS-denied* juga memaksa kita jujur: **AI yang hanya hebat saat semua infrastruktur normal, belum layak disebut siap perang.**

17.7. Target realistis tiga tahun pertama

Tahap 0–3 tahun harus dinilai dengan target yang keras tetapi masuk akal. Kesalahan umum negara berkembang adalah menulis target yang terlalu besar di atas kertas, lalu menghasilkan kemajuan kecil di lapangan. Untuk bab ini, target realistisnya sebaiknya bukan “mandiri penuh”, melainkan **siap bertahan, siap belajar cepat, dan siap menghasilkan blok dasar yang bisa diulang**.

Target minimum tiga tahun pertama

- **jalur cepat pengadaan** untuk drone kecil, EW taktis, dan *counter-drone* sudah berjalan;
- **beberapa keluarga drone kecil taktis** sudah dipakai rutin untuk ISR dan latihan;
- **program nasional autopilot, radio, dan *mission computer*** sudah menghasilkan desain referensi yang dapat diuji;
- **pusat data drone** sudah menyimpan video, telemetry, dan *mission logs* dari latihan serta operasi;
- **simulasi tempur dan latihan EW** sudah dilakukan secara berkala;
- **unit operasional uji** sudah terbentuk dan berfungsi sebagai *co-developer*;
- **AI awal untuk klasifikasi objek, *tracking*, dan alarm taktis** sudah dipakai terbatas pada skenario nyata;
- **counter-drone berlapis dasar** untuk pangkalan, aset vital, atau pulau terpilih sudah mulai diuji;
- **mekanisme pembelajaran pasca-misi** sudah menjadi rutinitas organisasi.

Target yang jangan dipaksakan di tiga tahun pertama

- **kemandirian chip penuh,**
- **platform besar yang kompleks terlalu dini,**
- ***frontier model* nasional untuk semua fungsi,**
- **produksi massal besar-besaran tanpa fondasi kualitas,**
- **doktrin sempurna sebelum uji lapangan.**

Yang lebih penting dari semua itu adalah membangun lima hasil strategis berikut:

- **tempo belajar nasional meningkat,**
- **hubungan kampus–industri–satuan mulai nyata,**
- **data mulai dihimpun sebagai aset pertahanan,**
- **ketahanan terhadap gangguan mulai diuji dari awal,**
- **Indonesia berhenti menjadi penonton dan mulai menjadi pembuat.**

Penutup Bab: tiga tahun pertama bukan masa keajaiban, tetapi masa pembentukan watak

Tahap pertama ini harus dibaca dengan disiplin. Dalam tiga tahun, Indonesia tidak akan berubah menjadi kekuatan AI militer utama. Tetapi dalam tiga tahun, Indonesia **bisa menentukan apakah ia sungguh masuk ke jalur pembelajaran perang modern, atau kembali tersesat dalam proyek yang indah di dokumen tetapi lemah di lapangan.**

Karena itu, inti tahap 0–3 tahun bukan kemewahan. Intinya adalah:

- **bertahan dari ketertinggalan yang ada,**
- **belajar lebih cepat daripada siklus birokrasi lama,**
- **dan membuat yang paling mendesak lebih dulu.**

Bila tahap ini berhasil, maka Indonesia akan punya sesuatu yang jauh lebih penting daripada slogan: **basis operasional awal untuk drone, AI, EW, data, dan counter-drone yang benar-benar hidup dalam latihan dan operasi.** Dari situlah tahap kedua baru masuk akal. Tanpa itu, semua pembicaraan tentang kedaulatan elektronik, *mass autonomy*, dan industri pertahanan digital hanya akan menjadi janji yang terlalu dini.

Bab 18. Tahap 2: 3–7 Tahun — Kuasai Elektronik, Integrasi, dan Produksi Rendah Volume

18.1. PCB *ruggedized*, *power electronics*, dan *battery systems*

Pada tiga tahun pertama, Indonesia belajar membuat yang mendesak. Tetapi pada tiga sampai tujuh tahun, ukuran keberhasilannya harus naik: **bukan lagi sekadar bisa menerbangkan drone, melainkan mulai menguasai elektronik yang membuat drone, sensor, dan sistem otonom tetap hidup dalam kondisi keras.** Di sinilah **PCB ruggedized, power electronics, dan battery systems** menjadi fondasi, bukan pelengkap. Ini juga sangat sesuai dengan diagnosis buku bahwa kelemahan Indonesia bukan hanya pada platform, tetapi pada **elektronik pertahanan** dan **rantai pasok komponen**.

Mengapa ini penting? Karena dalam operasi nyata, kegagalan sering bukan dimulai dari algoritma, melainkan dari hal yang lebih kasar dan lebih menentukan:

- papan sirkuit yang tidak tahan getaran, panas, garam, dan kelembapan;
- manajemen daya yang buruk;
- sistem baterai yang cepat turun performanya;
- dan desain listrik yang sulit diperbaiki di lapangan.

Departemen Pertahanan AS sendiri menempatkan **energi dan baterai** sebagai area investasi penting dalam penguatan basis industri pertahanan. Dokumen anggaran pengadaan DoD untuk program *Defense Production Act Purchases* secara eksplisit menyebut investasi untuk mendukung kebutuhan baterai berkapasitas besar dan *energy storage*. ([Comptroller](#)) Sementara strategi investasi Office of Strategic Capital DoD menekankan bahwa penguatan industri pada teknologi kritis harus dibaca sebagai bagian dari **ketahanan basis industri**, bukan sekadar pembelian komponen. ([U.S. Department of War](#))

Bagi Indonesia, pelajaran strategisnya jelas:

- **elektronik yang tahan lapangan lebih penting daripada spesifikasi brosur;**
- **manajemen daya yang efisien lebih penting daripada tenaga puncak sesaat;**
- **baterai yang aman, stabil, dan bisa diganti cepat lebih penting daripada klaim jarak terbang di kondisi ideal.**

Karena itu, Tahap 2 harus menargetkan kemampuan nasional minimal pada:

- **desain PCB ruggedized** untuk drone kecil, radio, *mission computer*, dan modul sensor;
- **power distribution board** yang andal untuk sistem udara, darat, dan laut;
- **battery pack engineering, battery management system**, dan pengujian siklus;
- **proteksi panas, korosi, dan getaran** untuk lingkungan maritim dan tropis.

Negara kepulauan seperti Indonesia tidak akan pernah siap perang hanya dengan *software* bagus diatas perangkat keras rapuh. **Ketangguhan listrik dan elektronik adalah bagian dari kedaulatan tempur.**

18.2. RF module, *crypto*, *mesh network*

Jika Tahap 2 ingin sungguh berarti, maka Indonesia tidak boleh berhenti pada autopilot dan airframe. Fokus berikutnya harus jatuh pada **RF module, *crypto*, dan *mesh network***, karena di sinilah hidup-matinya konektivitas operasional. Buku ini sudah menegaskan bahwa AI dan drone tidak boleh dibangun sebagai proyek berdiri sendiri; mereka harus hidup dalam ekosistem **EW, radar, AIS, satelit, jaringan, dan AI edge**.

Perubahan perang modern juga bergerak ke arah itu. Pada November 2024, Pentagon menjelaskan bahwa Replicator tidak hanya berisi sistem otonom, tetapi juga “**integrated enablers**” yang memungkinkan banyak aset nirawak beroperasi dan berkolaborasi secara otonom dalam lingkungan yang aman dan tetap tangguh terhadap jamming dan tindakan balasan lain. ([U.S. Department of War](#)) Strategi baru DoD untuk menghadapi sistem nirawak juga menekankan bahwa ancaman ini makin **terjangkau, otonom, dan networked**, sehingga respons tidak bisa semata platform-centric. ([U.S. Department of War](#))

Untuk Indonesia, artinya sangat konkret.

Tahap 2 harus mulai menguasai:

- **RF front-end** untuk link taktis jarak pendek dan menengah;
- **radio *software-defined*** atau radio modular yang bisa diubah profilnya;
- **kriptografi operasional** untuk kendali, telemetri, dan distribusi data;
- ***mesh networking*** agar unit tetap saling terhubung tanpa tergantung satu node;
- **mode komunikasi terdegradasi** ketika link utama gagal.

Dokumen konsep C2 Inggris tahun 2025 bahkan secara eksplisit menyebut bahwa ***mesh networking***, satelit orbit rendah, dan teknologi semikonduktor baru perlu dipelajari untuk meningkatkan ketahanan komunikasi militer, sambil tetap mengembangkan alternatif terhadap ketergantungan pada sistem ruang angkasa dan PNT. ([GOV.UK](#)) Ini relevan untuk Indonesia karena geografinya justru membuat komunikasi tersebar, berlapis, dan tahan gangguan menjadi kebutuhan struktural, bukan pilihan.

Inti strategis subbab ini adalah tegas: **siapa yang tidak menguasai radio, enkripsi, dan jaringan, pada akhirnya tidak menguasai drone maupun AI**. Ia hanya membeli terminal dari orang lain.

18.3. *Camera stack, inertial module, anti-jam navigation*

Banyak negara berkembang terlalu cepat bicara AI, padahal sensor dan navigasinya masih rapuh. Itu sebabnya Tahap 2 harus menjadikan **camera stack, inertial module, dan anti-jam navigation** sebagai prioritas. Ini penting karena AI untuk ISR, *tracking*, dan bantuan keputusan baru berguna jika **kamera, timing, orientasi, dan navigasi** bisa dipercaya. Arah ini sepenuhnya inline dengan rumusan buku bahwa *war-ready AI* Indonesia harus bekerja saat jaringan terganggu, saat GNSS dipukul, dan saat *supply chain* terganggu.

Kerentanan GNSS bukan hipotesis. Pemerintah Inggris dalam dokumen *problem statement* 2024 tentang PNT untuk sistem nirawak secara eksplisit menanyakan bagaimana pertahanan dapat mengadopsi **PNT resilience as the norm** untuk sistem nirawak. ([GOV.UK](https://gov.uk)) Di dokumen lain, pemerintah Inggris juga menekankan kebutuhan atas **assured anti-jam capabilities** dan teknologi PNT yang tetap bekerja ketika terminal tidak dapat menerima data GPS. ([GOV.UK](https://gov.uk)) Bahkan kajian kebijakan Inggris tentang GNSS menegaskan bahwa layanan berbasis GNSS rentan terhadap jamming dan gangguan lain. ([GOV.UK](https://gov.uk))

Bagi Indonesia, pelajarannya sangat praktis.

Tahap 2 harus menghasilkan kemajuan pada:

- **kamera EO/IR modular** yang bisa dipasang pada banyak platform;
- **gimbal dan camera pipeline** yang stabil untuk ISR;
- **inertial measurement unit** yang dipahami karakter **error-nya**, bukan hanya dibeli jadi;
- **sensor fusion** antara GNSS, IMU, visual odometry, kompas, radar kecil, atau referensi lain;
- **navigasi tahan gangguan**, setidaknya dalam bentuk *graceful degradation*, bukan kegagalan total.

Yang harus dibangun adalah budaya teknis yang benar:

- bukan sekadar “punya kamera”;
- tetapi **mengerti seluruh camera stack** dari sensor, lensa, kompresi, stabilisasi, sinkronisasi waktu, sampai pemrosesan;
- bukan sekadar “punya modul navigasi”;
- tetapi **mengerti bagaimana sistem tetap pulang atau tetap menjalankan misi saat GNSS buruk**.

Di perang modern, sistem yang tidak bisa menjaga orientasi dan tidak bisa melihat dengan benar akan menjadi benda terbang mahal yang buta.

18.4. *Reference design* nasional dari kampus dan industri

Tahap 2 harus menandai perubahan mental yang besar. Kampus dan industri nasional tidak boleh berhenti sebagai penghasil proposal, prototipe tunggal, atau jurnal. Mereka harus mulai menghasilkan **reference design nasional** yang bisa diproduksi, diuji, dimodifikasi, dan diulang. Outline buku sendiri sudah sangat tegas: peran kampus ke depan adalah bergerak **dari publikasi ke reference design**, dan kampus teknik harus fokus pada **chip design, embedded systems, RF, radar, control, vision**, serta menghasilkan desain yang bisa diproduksi.

Mengapa *reference design* penting? Karena Indonesia tidak bisa masuk ke produksi awal bila setiap vendor memulai dari nol, setiap laboratorium membuat desain yang tak kompatibel, dan setiap program mati setelah demonstrasi. *Reference design* memberi tiga keuntungan sekaligus:

- **bahasa teknis bersama** antara kampus, startup, BUMN, dan pengguna;
- **basis standardisasi terbatas** tanpa membunuh inovasi;
- **jalan cepat dari eksperimen ke produksi kecil.**

Pengalaman DIU di Amerika menarik karena program Blue UAS Framework dibangun justru untuk menyediakan daftar **komponen, sub-komponen, modul, dan perangkat lunak yang interoperable** dan menurunkan risiko bagi pemerintah maupun industri. ([Unit Inovasi Pertahanan](#)) Walau konteks Indonesia berbeda, prinsipnya relevan: **ekosistem tumbuh lebih cepat bila ada blok bangunan yang jelas, kompatibel, dan bisa diintegrasikan.**

Karena itu, Tahap 2 sebaiknya menghasilkan beberapa *reference design* nasional minimal:

- **autopilot + mission computer** untuk drone kecil ISR;
- **radio link dan mesh node** taktis;
- **camera stack modular** untuk pengawasan udara dan maritim;
- **sistem tenaga dan baterai** untuk platform kecil;
- **arsitektur counter-drone dasar** untuk pangkalan atau aset vital.

Yang penting, *reference design* ini jangan diperlakukan sebagai dokumen mati. Ia harus menjadi **objek hidup** yang:

- diuji,
- direvisi,
- diberi umpan balik oleh satuan,
- lalu dipakai sebagai fondasi produksi awal.

18.5. *Test range swarm, EW, maritime autonomy*

Tidak ada kedaulatan teknologi pertahanan tanpa **tempat menguji**. Karena itu, Tahap 2 harus melahirkan **test range** untuk *swarm*, EW, dan *maritime autonomy*. Buku ini sendiri mengarah ke sana lewat kebutuhan akan **pusat uji nasional**, pengujian, dan hubungan erat antara negara, TNI, kampus, dan industri.

Pelajaran internasional menunjukkan pentingnya ruang eksperimen nyata. NATO secara konsisten memakai REPMUS di Portugal sebagai ajang eksperimen sistem nirawak maritim; NATO menyebut REPMUS 24 sebagai latihan eksperimen terdepan dunia untuk sistem nirawak maritim, bertujuan menguji kemampuan sistem otonom untuk beroperasi bersama dan memahami ancaman baru di lingkungan maritim. ([NATO](#)) NATO STO juga menyoroti peran CMRE dalam menyediakan solusi yang telah diuji di lapangan untuk domain maritim dan eksperimen sistem otonom. ([NATO STO](#))

Untuk Indonesia, *test range* ini sebaiknya tidak dibayangkan terlalu mewah pada awalnya. Yang penting adalah fungsi:

- **uji *swarm* kecil dan kolaborasi multi-drone;**
- **uji jamming, spoofing, dan degradasi link;**
- **uji interoperabilitas udara-laut-darat;**
- **uji *maritime autonomy* di perairan pesisir, selat, dan sekitar pangkalan;**
- **uji integrasi sensor, AI edge, dan C2.**

Negara kepulauan sangat membutuhkan *test range maritim* karena banyak masalah hanya muncul ketika sistem bertemu:

- air asin,
- angin pesisir,
- pantulan sinyal,
- ombak,
- dan komunikasi yang tidak stabil.

Tanpa *test range* seperti ini, Indonesia akan terus mengira sistem “sudah jadi” karena berhasil di lapangan terbang yang tenang atau di demo tertutup. Padahal **perang bukan ruang presentasi**.

18.6. Kontrak kecil tapi nyata untuk startup dan vendor lokal

Tahap 2 juga harus memperbaiki ekonomi inovasi pertahanan. Selama startup dan vendor lokal hanya diundang ke lomba, seminar, atau *proof of concept* tanpa kontrak nyata, maka kapasitas industri tidak akan pernah tumbuh. Outline buku ini juga bergerak ke arah yang sama: **startup dan UKM teknologi harus masuk**, dan negara perlu menjadi pembentuk pasar serta pembeli pertama.

Pelajaran dari Amerika di sini sangat penting. DIU menekankan bahwa *Commercial Solutions Opening* memungkinkan DoD bekerja dengan **kontraktor pertahanan non tradisional** melalui proses yang lebih cepat dan fleksibel, biasanya menghasilkan *Other Transaction agreement*. ([Unit Inovasi Pertahanan](#)) Laporan Defense Business Board juga mencatat bahwa Replicator memakai mekanisme kontraktual modern untuk mengakses sistem maritim yang siap diproduksi dari perusahaan non tradisional, justru karena proses seperti ini tidak terikat pada kelemahan proses akuisisi lama. ([Dewan Bisnis Pertahanan](#))

Indonesia tidak perlu menyalin instrumen hukumnya mentah-mentah, tetapi prinsipnya perlu diambil:

- **kontrak kecil lebih berguna daripada hibah besar yang lambat;**
- **volume awal kecil tetapi berulang lebih sehat daripada satu proyek besar yang tak berkelanjutan;**
- **pembayaran harus terkait hasil uji, bukan sekadar dokumen administrasi;**
- **vendor lokal perlu diberi ruang untuk tumbuh melalui masalah nyata, bukan sekadar label TKDN di atas kertas.**

Model kontrak kecil tapi nyata bisa diarahkan ke:

- radio modular,
- *battery pack*,
- autopilot,
- modul kamera,
- *counter-drone* pasif,
- perangkat lunak *tracking* dan klasifikasi,
- *ground control station*,
- atau *maritime payload* sederhana.

Dengan cara ini, Tahap 2 tidak hanya membangun teknologi. Ia juga membangun **pasar pertahanan teknologi skala menengah** yang selama ini terlalu tipis di Indonesia.

18.7. Dari prototipe ke produksi awal

Subbab terakhir ini adalah inti seluruh Tahap 2. Ukuran keberhasilan tiga sampai tujuh tahun bukan lagi “berapa banyak prototipe bisa dipamerkan,” tetapi **berapa banyak desain yang lolos ke produksi awal dalam volume rendah**. Ini sepenuhnya inline dengan struktur roadmap buku: Tahap 2 memang dimaksudkan sebagai fase **elektronik, integrasi, dan produksi rendah volume**, sebelum Tahap 3 berbicara tentang *mass autonomy* dan kemandirian bertahap.

Masalah Indonesia selama ini sudah disebut keras dalam buku: **prototipe banyak, produksi sedikit**. Maka Tahap 2 harus memutus pola itu. Caranya bukan dengan melompat ke produksi massal terlalu cepat, tetapi dengan membangun disiplin produksi awal:

- desain dibekukan pada versi tertentu,
- komponen dikualifikasi,
- pengujian dilakukan berulang,
- *failure modes* dicatat,
- *repair loop* dibangun,
- lalu sistem diproduksi dalam batch kecil yang benar-benar dipakai.

Produksi awal ini harus punya beberapa ciri:

- **jumlah kecil tetapi operasional**, bukan sampel museum;
- **ada dokumentasi manufaktur**, bukan hanya file laboratorium;
- **ada rantai suplai minimum yang dipetakan**, termasuk substitusi komponen;
- **ada umpan balik dari pengguna** untuk revisi generasi berikutnya.

Pelajaran dari penguatan rantai pasok pertahanan di berbagai negara juga konsisten: ketahanan industri lahir dari **visibilitas rantai pasok, keterlibatan usaha kecil, dan kemampuan manufaktur yang bisa dipertahankan**, bukan dari ketergantungan penuh pada satu pemasok atau satu integrator besar. ([U.S. Department of War](#))

Jadi, peralihan dari prototipe ke produksi awal bukan isu teknis semata. Ia adalah **uji kedewasaan ekosistem**. Di titik ini akan terlihat apakah kampus, startup, BUMN, vendor, dan pengguna sungguh membentuk rantai nilai nasional, atau masih hidup sebagai pulau-pulau kecil yang tak tersambung.

Penutup Bab: Tahap 2 adalah ujian kedewasaan teknis

Bila Tahap 1 adalah masa bertahan dan belajar cepat, maka **Tahap 2 adalah ujian kedewasaan teknis Indonesia**. Pada fase ini, negara tidak lagi cukup puas dengan bisa membuat demo. Negara harus mulai bisa:

- merancang elektronik yang tahan lapangan,
- membangun radio dan jaringan yang tangguh,
- memahami navigasi dan sensor secara mendalam,
- menghasilkan *reference design* yang bisa diulang,
- menguji sistem di *range* yang keras,
- memberi kontrak nyata pada startup dan vendor lokal,
- dan mengubah prototipe menjadi produksi awal.

Di sinilah perbedaan antara negara yang sungguh mengejar ketinggalan dan negara yang hanya gemar berbicara tentang kemandirian akan terlihat. **Kemandirian pertahanan digital tidak lahir dari slogan besar, tetapi dari papan sirkuit yang tahan, radio yang aman, baterai yang stabil, navigasi yang tetap hidup saat diganggu, dan batch produksi kecil yang benar-benar sampai ke pengguna.**

Bila Tahap 2 gagal, maka Tahap 3 akan menjadi fantasi. Tetapi bila Tahap 2 berhasil, Indonesia akan punya sesuatu yang jauh lebih berharga daripada klaim: **fondasi elektronik dan integrasi yang cukup kuat untuk melangkah ke otonomi massal secara bertahap.**

Bab 19. Tahap 3: 7–15 Tahun — *Mass Autonomy* dan Kedaulatan Elektronik Bertahap

19.1. *Design-first strategy*, bukan *fab-first fantasy*

Pada tahap ini, Indonesia harus mulai berpikir lebih besar, tetapi tetap waras. Kesalahan terbesar yang sering muncul dalam diskusi kemandirian teknologi adalah melompat terlalu cepat ke mimpi pabrik besar, *fab* nasional, atau simbol manufaktur berat, padahal **desain, arsitektur sistem, mission software, RF, dan integrasi belum kokoh**. Karena itu, rumus yang lebih sehat adalah ***design-first strategy*, bukan *fab-first fantasy***. Arah ini juga sangat selaras dengan garis besar buku yang berkali-kali menekankan kelemahan Indonesia pada elektronik pertahanan, *mission software*, dan *data pipeline*, serta perlunya fokus pada desain modular, stok komponen kritis, dan *industrial resilience*.

Mengapa *design-first* lebih masuk akal? Karena nilai strategis dalam sistem otonom modern tidak hanya terletak pada siapa yang memiliki fasilitas produksi paling besar, tetapi pada siapa yang:

- menguasai **arsitektur sistem**,
- mampu merancang **blok elektronik dan perangkat lunak inti**,
- mengendalikan **integrasi antar modul**,
- dan bisa melakukan **substitusi desain** saat komponen tertentu terputus.

Dokumen resmi DoD tentang digital modernization menegaskan bahwa **advanced microelectronics** adalah teknologi fondasional bagi modernisasi pertahanan, tetapi masalah yang dihadapi justru sangat beragam: dari komponen mutakhir sampai komponen butik dan *legacy*. Itu artinya, penguasaan desain, integrasi, dan pilihan teknologi jauh lebih penting daripada sekadar memiliki satu fasilitas manufaktur simbolik. ([U.S. Department of War](#))

Untuk Indonesia, strategi ini berarti:

- **mulai dari desain yang bisa diproduksi**,
- **membangun perpustakaan desain dan IP inti**,
- **menguasai toolchain desain dan validasi**,
- **memetakan *foundry* dan mitra manufaktur eksternal secara realistis**,
- lalu **naik bertahap** ke proses yang lebih dalam jika volume, kompetensi, dan kebutuhan keamanan sudah cukup.

Jadi, *design-first* bukan berarti menyerah pada impor. Sebaliknya, ia adalah jalan yang lebih dewasa untuk **mengurangi ketergantungan tanpa menjual ilusi**.

19.2. ASIC, FPGA, dan *mission systems*

Pada tahap 7–15 tahun, Indonesia harus mulai masuk lebih serius ke dunia **ASIC, FPGA, dan *mission systems***. Ini bukan berarti semua sistem harus menggunakan chip buatan sendiri secara penuh. Tetapi **arsitektur semikonduktor dan komputasi tertanam** harus mulai dikuasai pada level yang membuat Indonesia bisa memilih, memodifikasi, melindungi, dan mengamankan fungsi-fungsi inti.

Ada alasan kuat mengapa FPGA penting. FPGA memberi kelenturan untuk:

- integrasi sensor,
- pemrosesan sinyal,
- akselerasi inferensi tertentu,
- penggabungan fungsi kendali, RF, dan pengolahan data,
- serta penyesuaian cepat dalam siklus iterasi pertahanan.

Pada Januari 2025, NSA menerbitkan panduan keamanan FPGA yang menegaskan pentingnya pemilihan jenis perangkat, enkripsi file konfigurasi, dan perlindungan terhadap modifikasi atau pencurian konfigurasi. Ini menunjukkan bahwa dalam ekosistem pertahanan modern, FPGA bukan hanya soal performa, tetapi juga **keamanan konfigurasi dan ketahanan desain**. ([U.S. Department of War](#))

Sementara itu, ASIC lebih relevan untuk jangka menengah-panjang bila Indonesia sudah memiliki:

- volume penggunaan yang cukup,
- desain yang relatif stabil,
- kebutuhan daya dan ukuran yang sangat ketat,
- dan kebutuhan keamanan atau performa yang tidak bisa terus bergantung pada komponen umum.

Dalam konteks buku ini, yang paling penting bukan kebanggaan semikonduktor semata, tetapi **penguasaan *mission systems***. Artinya:

- *mission computer*,
- *signal processing chain*,
- modul navigasi,
- perangkat RF,
- *sensor fusion engine*,
- *payload controller*,
- dan lapisan perangkat lunak yang menghubungkan semuanya.

Dengan kata lain, kedaulatan elektronik bertahap dimulai bukan dari slogan “buat chip sendiri”, tetapi dari **menguasai blok-blok misi yang membuat sistem tempur bisa berpikir, melihat, bergerak, dan tetap hidup saat diganggu**. Itu juga inline dengan arah Bab 20 di outline, yang nanti menegaskan pentingnya kampus fokus pada *chip design, embedded systems, RF, radar, control, dan vision*.

19.3. Drone udara-laut-darat yang interoperable

Tahap 3 tidak boleh berhenti pada keluarga platform yang terpisah-pisah. Indonesia harus bergerak ke arah **drone udara-laut-darat yang interoperable**. Ini sangat penting untuk negara kepulauan. Medan Indonesia bukan hanya darat atau hanya laut, melainkan simpul yang menghubungkan:

- pulau terluar,
- pesisir,
- pelabuhan,
- choke point,
- pangkalan,
- jalur logistik,
- dan ruang udara rendah.

Karena itu, *mass autonomy* versi Indonesia harus dibangun sebagai **ekosistem lintas domain**, bukan armada platform tunggal.

Pelajaran internasional mengarah kuat ke sana. REPMUS 24 yang didorong NATO secara eksplisit digunakan untuk menguji kemampuan sistem otonom **beroperasi bersama** dan meningkatkan pemahaman aliansi atas ancaman baru di lingkungan maritim. NATO juga menekankan dalam REPMUS 22 bahwa sekitar **120 aset nirawak** diintegrasikan ke dalam satu jaringan untuk skenario eksperimen yang menekankan interoperabilitas. ([NATO](#))

Untuk Indonesia, interoperabilitas itu harus diterjemahkan secara konkret:

- drone udara memberi **ISR cepat**,
- drone laut memberi **kehadiran murah dan persisten** di perairan,
- drone darat membantu **pengamanan pangkalan, logistik, atau pengintaian lokal**,
- semua masuk ke **jaringan data dan komando yang sama**,
- dan semua bisa berbagi *cueing*, identitas objek, status misi, dan peringatan gangguan.

Di sini prinsip yang harus dijaga adalah:

- **arsitektur terbuka terbatas**,
- **format data yang cukup beragam**,
- **lapisan C2 yang konsisten**,
- dan **interoperabilitas sebagai syarat desain**, bukan tambahan belakangan.

Bila Indonesia gagal di titik ini, maka yang lahir hanyalah koleksi drone yang banyak tetapi **tidak benar-benar menjadi sistem tempur**.

19.4. Arsenal digital nasional

Dalam era *mass autonomy*, istilah arsenal tidak lagi bisa dibaca hanya sebagai gudang senjata fisik. Indonesia harus mulai membangun **arsenal digital nasional**. Yang dimaksud bukan sekadar server atau pusat data, tetapi keseluruhan **stok kemampuan digital tempur** yang bisa diperbarui, dipasang ulang, disebarluaskan cepat, dan dipakai lintas satuan.

Arsenal digital ini setidaknya berisi:

- model visi komputer dan klasifikasi objek,
- pustaka navigasi dan *fallback mode*,
- modul *sensor fusion*,
- *mission software*,
- *ground control stack*,
- *EW profile* tertentu,
- dataset latihan,
- simulasi dan *digital twin*,
- serta *software packages* yang bisa dimuat ulang ke banyak platform.

Kenapa ini penting? Karena dalam perang modern, **keunggulan tidak hanya terletak pada siapa yang punya lebih banyak alat, tetapi siapa yang bisa memperbarui perilaku alat lebih cepat**. DoD dalam strategi adopsi data, analitik, dan AI menekankan pentingnya perpindahan dari eksperimen ke adopsi operasional yang terukur dan terintegrasi. Sementara Replicator sendiri menekankan bukan hanya sistem otonom, tetapi juga *integrated enablers* yang memungkinkan aset bekerja secara efektif sebagai ekosistem. ([U.S. Department of War](#))

Dalam konteks Indonesia, arsenal digital nasional harus menjawab kebutuhan berikut:

- **pembaruan cepat dari pelajaran lapangan,**
- **distribusi *software* yang aman dan terkontrol,**
- **versi yang bisa diaudit,**
- **pemisahan antara lingkungan latihan dan operasional,**
- **kemampuan *rollback* bila ada kegagalan,**
- **dan arsip *battle data* untuk generasi sistem berikutnya.**

Jadi, pada tahap ini Indonesia tidak cukup hanya memiliki pabrik kecil dan gudang komponen. Indonesia juga harus punya **gudang kecerdasan operasional digital**.

19.5. *Stockpile* komponen kritis dan desain modular

Pelajaran yang paling keras dari perang modern adalah ini: **rantai pasok akan dipukul**. Karena itu, negara yang ingin bertahan tidak boleh berpikir hanya dalam logika *just in time*. Ia harus berpikir dalam logika ***stockpile komponen kritis + desain modular + sumber alternatif***. Naskah buku yang Anda lampirkan bahkan sudah menuliskan ini dengan sangat eksplisit saat membahas pelajaran Iran dan relevansinya untuk Indonesia.

Laporan DoD tentang *securing defense-critical supply chains* menegaskan pentingnya strategi untuk baterai lithium, penanganan komponen mikroelektronika, dan pencegahan komponen palsu dalam rantai pasok pertahanan. Artinya, bahkan negara dengan industri pertahanan sangat maju tetap harus memikirkan **stok, jaminan asal, dan ketahanan rantai pasok** secara serius. ([U.S. Department of War](#))

Untuk Indonesia, prinsipnya harus sederhana tetapi disiplin.

Komponen yang layak dipikirkan sebagai *stockpile* strategis antara lain:

- modul RF tertentu,
- IMU dan sensor navigasi,
- kamera dan sensor optik tertentu,
- FPGA atau komponen komputasi tertanam tertentu,
- baterai dan *battery management subsystem*,
- komponen daya,
- enkripsi atau elemen keamanan tertentu,
- dan bagian konektivitas yang menjadi *single point of failure*.

Tetapi *stockpile* saja tidak cukup. Tanpa **desain modular**, stok bisa menjadi tumpukan barang yang tidak kompatibel. Karena itu desain modular harus memastikan:

- komponen bisa diganti tanpa merombak seluruh sistem,
- ada **second source** bila pemasok pertama terputus,
- ada *variant* desain untuk beberapa kelas komponen,
- dan integrasi tetap mungkin walau spesifikasi berubah terbatas.

Dalam bahasa yang lebih tajam: **stok tanpa modularitas adalah gudang; modularitas tanpa stok adalah teori. Indonesia butuh keduanya.**

19.6. *Industrial resilience* menghadapi *cut-off supply chain*

Tahap 3 juga harus membuat Indonesia berpikir seperti negara yang sedang menyiapkan diri untuk krisis panjang, bukan seperti organisasi yang hidup dalam asumsi pasar selalu terbuka. Itulah mengapa **industrial resilience** menjadi kata kunci. Dalam konteks buku ini, pelajaran Iran tidak dibaca sebagai ajakan meniru politik Iran, tetapi sebagai pengingat bahwa **resilience lebih penting daripada kemewahan**, dan bahwa sistem harus tetap bekerja saat GPS, jaringan, atau pasokan terganggu.

Laporan Defense Business Board 2024 tentang kemitraan industri untuk krisis menyoroti bahwa proyek seperti Replicator dapat bergerak cepat justru karena memakai mekanisme modern untuk mengakses sistem siap produksi dari perusahaan nontradisional. Ini memberi pelajaran bahwa ketahanan industri tidak hanya lahir dari pabrik besar, tetapi juga dari **ekosistem pemasok, startup, UKM, dan jalur kontrak yang lincah**. ([Dewan Bisnis Pertahanan](#))

Maka *industrial resilience* Indonesia harus dibangun di atas beberapa lapis:

- **lapis teknis**: desain dapat diubah bila komponen tertentu hilang;
- **lapis manufaktur**: ada lebih dari satu jalur perakitan atau integrasi;
- **lapis pemasok**: ada lebih dari satu sumber penting;
- **lapis organisasi**: ada institusi yang bisa memutuskan substitusi cepat;
- **lapis ekonomi perang**: sistem tetap cukup murah untuk diproduksi dan diganti.

Tahap ini juga mensyaratkan perubahan cara pandang negara.

Negara tidak boleh hanya menjadi pembeli akhir. Negara harus menjadi:

- **pembentuk pasar,**
- **pengarah standardisasi terbatas,**
- **penjamin permintaan minimum,**
- **penguji kualitas,**
- dan **penjaga kesiapan industri saat kondisi normal sekalipun.**

Bila tidak, setiap krisis akan membuat Indonesia mulai dari nol lagi.

19.7. Dari ketergantungan ke kemandirian bertahap

Akhirnya, subbab ini harus mengunci pesan besar roadmap. Indonesia tidak akan berpindah dari ketergantungan ke kemandirian dalam satu lompatan. Itu ilusi. Yang lebih mungkin — dan lebih sehat — adalah **kemandirian bertahap**. Ini juga persis dengan arah outline: bukan “kedaulatan total besok pagi”, tetapi **kedaulatan elektronik bertahap**.

Kemandirian bertahap itu bisa dibaca dalam beberapa level.

Tahap awal

Indonesia masih memakai banyak komponen luar, tetapi:

- mulai menguasai desain,
- integrasi,
- *software stack*,
- dan pengujian.

Tahap menengah

Indonesia mulai:

- punya *reference design* mapan,
- mengendalikan banyak blok elektronik inti,
- memiliki *stockpile* komponen kritis,
- dan mampu melakukan substitusi dengan cepat.

Tahap lebih matang

Indonesia mulai:

- menurunkan biaya produksi lewat skala,
- membangun keluarga sistem lintas domain yang interoperable,
- menguasai sebagian IP elektronik dan komputasi tertanam,
- dan mengurangi ketergantungan pada beberapa pemasok atau modul yang paling sensitif.

Ini adalah arti paling jujur dari kemandirian pertahanan digital: **bukan autarki total, tetapi kemampuan mempertahankan operasi, memperbaiki sistem, memodifikasi desain, dan terus memproduksi kapasitas tempur walau lingkungan eksternal memburuk**. Itu sejalan dengan dokumen-dokumen resmi Barat yang makin menekankan *modular open systems*, interoperabilitas, kompetisi, dan pengurangan biaya siklus hidup sebagai fondasi ketahanan modernisasi sistem. ([U.S. Department of War](#))

Penutup Bab: *Mass autonomy* bukan jumlah semata

Bab ini harus ditutup dengan satu penegasan: ***mass autonomy bukan sekadar punya drone banyak***. Yang dimaksud adalah kemampuan nasional untuk:

- merancang,
- memproduksi,
- memperbarui,
- mengintegrasikan,
- memperbaiki,
- mengganti,
- dan mempertahankan sistem otonom dalam jumlah yang relevan secara strategis.

Bagi Indonesia, itu berarti *mass autonomy* hanya masuk akal bila dibangun di atas:

- **desain yang matang,**
- **semikonduktor dan *mission systems* yang dipahami,**
- **interoperabilitas udara-laut-darat,**
- **arsenal digital nasional,**
- ***stockpile* komponen kritis,**
- dan **ketahanan industri menghadapi putusnya pasokan.** ([U.S. Department of War](#))

Kalau Tahap 1 membentuk insting, dan Tahap 2 membentuk kedewasaan teknis, maka **Tahap 3 membentuk daya tahan strategis**. Pada titik inilah Indonesia mulai bergerak dari negara yang membeli teknologi menjadi negara yang **membangun kapasitas tempur digitalnya sendiri secara bertahap, sadar batas, tetapi tidak lagi pasif**.

Bagian VII. Kampus, Industri, dan Negara: Siapa Harus Mengerjakan Apa

Bab 20. Peran Kampus: Dari Publikasi ke *Reference Design*

20.1. Kampus teknik harus fokus ke apa

Bila Indonesia sungguh ingin membangun kemandirian pertahanan digital, maka kampus teknik tidak boleh menyebar energinya ke terlalu banyak hal yang indah tetapi tipis dampaknya. Kampus harus fokus pada **bidang-bidang yang menjadi bottleneck nyata** dalam perang modern: elektronik, komputasi tertanam, RF, navigasi, sensor, kontrol, visi mesin, dan integrasi sistem. Fokus seperti ini sepenuhnya sejalan dengan roadmap buku, karena titik lemah Indonesia justru ada pada **elektronik pertahanan, mission software, data pipeline, serta lemahnya transisi dari riset ke operasi**.

Artinya, kampus teknik perlu berhenti merasa cukup hanya dengan topik yang “naik daun”. Yang dibutuhkan bukan sekadar riset AI umum, tetapi riset yang langsung menempel pada kebutuhan sistem:

- **autopilot dan kontrol,**
- ***embedded systems* dan *mission computer*,**
- **radio taktis dan *mesh networking*,**
- **sensor fusion,**
- **navigasi *GPS-denied*,**
- **kamera dan visi mesin,**
- **EW dan *counter-drone*,**
- **simulasi, *digital twin*, dan evaluasi performa misi.**

DoD dalam *National Defense Science and Technology Strategy* menegaskan bahwa prioritas ilmu pengetahuan dan teknologi pertahanan harus diarahkan untuk menghasilkan **kapabilitas yang relevan bagi *warfighter*** dan memperkuat ekosistem penelitian, teknik, dan transisi teknologi. ([U.S. Department of War](#))

Jadi, pertanyaan pertama bagi kampus bukan lagi “apa topik riset yang mudah dipublikasikan?”, melainkan “**masalah sistem apa yang paling menghambat kesiapan operasional Indonesia?**” Di situlah fokus seharusnya diletakkan.

20.2. *Chip design, embedded systems, RF, radar, control, vision*

Bab ini dengan tepat menyebut rumpun-rumpun yang harus dikuasai kampus: **chip design, embedded systems, RF, radar, control, vision**. Itu bukan daftar teknis yang kebetulan. Itulah jantung sistem otonom modern. Negara yang lemah pada enam bidang ini akan terus menjadi perakitan pinggir, bukan pembangun sistem.

Mengapa enam bidang ini penting

- **Chip design**

Bukan karena Indonesia harus segera punya *fab* besar, tetapi karena tanpa kemampuan desain, kita tidak akan pernah mengerti bagaimana fungsi kritis dipadatkan, diamankan, dioptimalkan dayanya, atau disubstitusi saat komponen hilang. DoD menyebut **advanced microelectronics** sebagai teknologi fondasional bagi modernisasi pertahanan, dan program Microelectronics Commons dibentuk untuk memperkuat jalur prototyping dan fabrikasi mikroelektronika domestik bagi kebutuhan militer. ([U.S. Department of War](https://www.defense.gov/Newsroom/Record/201808010001))

- **Embedded systems**

Di sinilah perangkat keras dan perangkat lunak bertemu. Drone, radio, *mission computer*, sensor, dan aktuator semuanya bergantung pada *embedded systems* yang tahan gangguan, hemat daya, dan bisa dipelihara.

- **RF dan radar**

Perang drone, EW, *counter-drone*, dan pengawasan maritim semuanya hidup dari spektrum. Bahkan dokumen anggaran DoD beberapa tahun terakhir menunjukkan perhatian besar pada **distributed RF, receiver-sensor technology**, EW, dan sensing untuk lingkungan kontestasi. (comptroller.defense.gov)

- **Kontrol**

Tanpa kontrol yang baik, otonomi hanya slogan. Stabilitas terbang, navigasi, *swarm behavior*, *fault tolerance*, dan mode degradasi semuanya bergantung pada ilmu kontrol.

- **Visi mesin**

Karena AI perang yang paling nyata sering hadir sebagai sistem yang **melihat, mengklasifikasi, melacak, dan memberi peringatan dini**. DARPA bahkan mendanai riset seperti *event-based infrared camera* untuk sensor taktis berlatensi rendah dan hemat daya. ([darpa.mil](https://www.darpa.mil))

Maka, untuk kampus teknik Indonesia, daftar prioritasnya sebaiknya tidak kabur. Ia harus bertumpu pada laboratorium dan kelompok riset yang menghasilkan:

- desain blok elektronik,
- *firmware* dan *embedded stack*,
- sistem RF/radar skala taktis,
- algoritma kontrol untuk sistem nirawak,
- *vision pipeline* untuk ISR,
- dan integrasi semua itu menjadi *reference design*.

20.3. Kenapa kampus perlu menghasilkan desain yang bisa diproduksi

Bila kampus hanya menghasilkan konsep, makalah, atau prototipe laboratorium yang tidak bisa diproduksi, maka ia membantu pengetahuan, tetapi **belum tentu membantu kapasitas negara**. Dalam konteks pertahanan digital, Indonesia membutuhkan kampus yang menghasilkan **desain yang bisa diproduksi**, karena di situlah ilmu berubah menjadi kemampuan nasional.

Mengapa ini penting?

- karena **vendor lokal tidak selalu punya kapasitas R&D mendalam**;
- karena negara perlu **arsitektur referensi** yang bisa diuji dan diulang;
- karena produksi rendah volume memerlukan desain yang **rapi, terdokumentasi, dan dapat dimanufaktur**;
- dan karena tanpa desain yang bisa diproduksi, Indonesia akan terus terjebak pada “**prototipe banyak, produksi sedikit**” — diagnosis yang sudah disebut terang dalam naskah buku.

Program Blue UAS Framework dari DIU memberi pelajaran penting: pemerintah mempercepat adopsi sistem nirawak dengan menyediakan kerangka platform, komponen, sub-komponen, dan perangkat lunak yang sudah dinilai lebih siap untuk integrasi dan penggunaan. Prinsipnya jelas: **ekosistem tumbuh lebih cepat bila ada blok bangunan yang nyata dan interoperable**. ([U.S. Department of War](#))

Karena itu, kampus seharusnya didorong untuk menghasilkan:

- *reference design* autopilot,
- *mission computer* modular,
- desain radio taktis,
- *camera stack* dan *processing pipeline*,
- arsitektur *counter-drone*,
- modul daya dan baterai,
- serta *toolchain* pengujian dan dokumentasi manufaktur.

Jadi, peran kampus bukan menjadi pabrik. Tetapi kampus harus menjadi **mesin pembuat desain yang cukup matang untuk ditangkap industri**.

20.4. TRL, *spin-off*, lisensi, dan pengujian

Di titik ini, kampus harus belajar berbicara bukan hanya dalam bahasa riset, tetapi juga dalam bahasa **kematangan teknologi, transisi, dan pengujian**. Konsep **Technology Readiness Levels (TRL)** berguna justru karena memaksa kita jujur tentang posisi teknologi: masih prinsip dasar, sudah *proof of concept*, sudah diuji di lingkungan relevan, atau sudah siap operasi. NASA menjelaskan bahwa TRL memiliki **sembilan tingkat**, dari TRL 1 yang paling awal sampai TRL 9 yang paling matang. ([NASA](#))

Untuk kampus Indonesia, memakai logika TRL penting karena:

- membantu memilah mana riset dasar dan mana yang layak ditransisikan;
- memaksa laboratorium berpikir tentang **uji lingkungan relevan**, bukan hanya uji meja;
- memudahkan negara dan industri menentukan **skema pendanaan** yang tepat;
- dan membuat evaluasi lebih jujur daripada sekadar menghitung publikasi.

Tetapi TRL saja tidak cukup. Kampus juga perlu jalur nyata ke luar laboratorium:

- ***spin-off*** untuk teknologi yang cocok tumbuh sebagai perusahaan;
- **lisensi** untuk desain yang lebih cocok diserap vendor mapan;
- **kemitraan pengujian** dengan satuan operasional dan pusat uji;
- **transisi bertahap** dari prototipe kampus ke produksi rendah volume.

DARPA melalui skema SBIR/STTR memang membuka ruang bagi **usaha kecil berteknologi tinggi dan institusi akademik** untuk mengusulkan pendekatan radikal terhadap ancaman keamanan nasional; ini menunjukkan bahwa hubungan antara kampus, usaha kecil, dan transisi teknologi memang penting dalam ekosistem pertahanan. ([comptroller.defense.gov](#))

Maka, kampus Indonesia perlu membangun disiplin baru:

- setiap riset terapan punya target **TRL** yang jelas;
- setiap desain strategis punya opsi **lisensi atau spin-off**;
- setiap teknologi penting harus melewati **pengujian keras**, bukan sekadar demonstrasi seminar;
- dan setiap laboratorium yang serius harus punya peta jalan **dari riset ke integrasi**.

20.5. Kurikulum autonomy, AI militer, dan EW

Bila kampus diminta berperan lebih besar, maka kurikulumnya juga harus berubah. Tidak cukup lagi bila mahasiswa hanya kuat di teori umum tetapi asing terhadap medan masalah yang sesungguhnya. Indonesia membutuhkan kurikulum yang mulai mengenalkan **autonomy, AI militer, EW, navigasi tahan gangguan, embedded security, sistem nirawak maritim, dan human-machine teaming**.

Tentu, “AI militer” di kampus tidak harus diajarkan sebagai glorifikasi perang. Ia bisa dan harus diajarkan sebagai:

- studi tentang **sistem otonom dalam lingkungan keras**;
- persoalan **kendali manusia, akuntabilitas, dan bias**;
- teknik **sensor fusion, navigasi, visi mesin, EW, dan C2**;
- serta kaitannya dengan **hukum humaniter, etika, dan keselamatan sipil**.

NATO STO menunjukkan bahwa riset dan pengembangan teknologi pertahanan hari ini memang bergerak di bidang seperti **autonomous cyber defense, maritim nirawak, sensing, jaringan, dan integrasi multi-domain**. Program kerja NATO STO 2024–2025 memperlihatkan perhatian besar pada *autonomy*, maritim, jaringan, AI, dan teknologi pertahanan terkait. ([NATO Sto](#))

Karena itu, kurikulum kampus teknik yang relevan untuk 10–15 tahun ke depan sebaiknya mulai memuat:

- **kontrol dan navigasi sistem nirawak,**
- **embedded systems dan real-time computing,**
- **RF, radar, dan EW dasar,**
- **visi mesin untuk ISR,**
- **AI di edge dan inferensi hemat daya,**
- **keamanan siber untuk sistem fisik,**
- **arsitektur sistem multi-domain,**
- **uji, validasi, dan keselamatan,**
- serta **etika, hukum, dan akuntabilitas AI pertahanan**.

Dengan begitu, kampus tidak hanya menghasilkan skripsi. Ia menghasilkan **tenaga teknik yang mengerti sistem nyata**.

20.6. Bahaya bila kampus hanya mengejar jurnal

Di sinilah kritik paling keras perlu disampaikan. **Kampus yang hanya mengejar jurnal akan tertinggal dari kebutuhan zaman.** Tentu publikasi tetap penting. Negara butuh ilmu dasar, metode, dan reputasi akademik. Tetapi bila seluruh insentif kampus hanya diarahkan pada publikasi, maka beberapa bahaya akan muncul sekaligus.

Bahayanya

- **riset memilih topik yang mudah diterbitkan, bukan yang paling dibutuhkan;**
- laboratorium menghasilkan *demo* yang cantik tetapi tidak tahan uji;
- mahasiswa mahir menulis paper, tetapi tidak terbiasa membuat sistem yang dapat diproduksi;
- kolaborasi dengan industri dan pengguna menjadi lemah;
- dan kampus gagal menjadi bagian dari **arsitektur nasional pertahanan digital.**

Buku ini sudah memberi peringatan yang tepat: **kampus kuat di riset, lemah di transisi ke operasi.** Bila penyakit itu dibiarkan, maka Indonesia akan terus memiliki banyak pengetahuan, tetapi sedikit daya tempur digital yang nyata.

Karena itu, ukuran keberhasilan kampus teknik perlu diperluas. Selain publikasi, ia harus dinilai dari:

- **jumlah *reference design* yang matang,**
- **berapa teknologi naik TRL,**
- **berapa yang lolos uji lapangan,**
- **berapa lisensi atau *spin-off* yang hidup,**
- **berapa kerja sama yang benar-benar dipakai industri atau satuan,**
- dan **berapa lulusan yang siap membangun sistem, bukan hanya menganalisisnya.**

Ini bukan anti-jurnal. Ini adalah upaya menempatkan jurnal pada tempat yang benar: **sebagai salah satu output, bukan satu-satunya horizon.**

Penutup Bab: kampus sebagai pabrik desain strategis

Pada akhirnya, peran kampus dalam roadmap buku ini harus dirumuskan dengan tegas. Kampus tidak menggantikan industri. Kampus juga tidak menggantikan negara atau TNI. Tetapi kampus harus menjadi **pabrik desain strategis, pembentuk talenta teknik, tempat lahirnya *reference design*, dan jembatan antara ilmu dengan kemampuan nasional**. Itu sejalan langsung dengan posisi Bab 20 dalam buku: sesudah roadmap teknologi, kampus dibahas pertama kali karena ia adalah **sumber pengetahuan yang harus diubah menjadi kapasitas**.

Bagi Indonesia, kampus teknik yang relevan di era ini adalah kampus yang:

- fokus pada bottleneck strategis,
- kuat di *chip design*, *embedded systems*, RF, radar, kontrol, dan visi,
- menghasilkan desain yang bisa diproduksi,
- memakai disiplin TRL, lisensi, *spin-off*, dan pengujian,
- memperbarui kurikulum autonomy, AI militer, dan EW,
- dan tidak terjebak dalam ilusi bahwa publikasi saja sudah cukup.

Negara yang ingin berdaulat secara digital tidak cukup memiliki kampus yang pintar. Ia membutuhkan kampus yang sanggup mengubah kepintaran menjadi desain, desain menjadi sistem, dan sistem menjadi kapasitas nasional. Di situlah Bab 20 menemukan makna strategisnya.

Bab 21. Peran Industri Nasional: Dari Vendor ke Mitra Strategis

21.1. BUMN tidak cukup sendirian

BUMN pertahanan tetap penting. Mereka punya aset, hubungan dengan negara, pengalaman program besar, dan kapasitas integrasi tertentu. Tetapi untuk ekosistem AI militer, drone, EW, *mission systems*, dan elektronik pertahanan modern, **BUMN tidak cukup sendirian**. Alasannya sederhana: medan teknologi kini bergerak terlalu cepat, terlalu beragam, dan terlalu dekat dengan inovasi komersial untuk ditangani hanya oleh beberapa pemain besar. Naskah buku ini juga sudah memberi sinyal kuat bahwa Indonesia lemah bukan hanya pada alat, tetapi pada **ekosistem**.

Pengalaman internasional menunjukkan pola yang sama. Laporan **Defense Business Board** mencatat bahwa basis industri pertahanan Amerika terdiri dari **hampir 60.000 perusahaan**, sementara kontrak besar memang banyak mengalir ke integrator utama, tetapi inovasi dan manufaktur tersebar luas di sektor swasta. Laporan itu juga menegaskan bahwa DoD makin bergantung pada industri untuk kemampuan yang dibawa ke medan konflik. Sementara NATO dalam laporan tren sains dan teknologi 2025–2045 menekankan bahwa inovasi pertahanan kini semakin banyak digerakkan oleh pelaku industri, bukan pemerintah semata. ([NATO](#))

Bagi Indonesia, pelajarannya jelas:

- **BUMN harus menjadi integrator dan jangkar ekosistem**, bukan pemain tunggal yang menutup ruang pemain lain.
- **BUMN perlu memimpin standarisasi, integrasi, dan jaminan kualitas**, bukan memonopoli semua lapisan teknologi.
- **BUMN harus membuka rantai pasok dan sub-kontrak bagi vendor lokal, startup, dan UKM**, agar kapasitas nasional benar-benar melebar.

Dengan kata lain, bila BUMN mencoba mengerjakan semuanya sendiri, hasilnya biasanya lambat, mahal, dan tipis pembelajarannya. Tetapi bila BUMN diposisikan sebagai **orkestrator ekosistem**, nilainya jauh lebih besar.

21.2. Startup dan UKM teknologi harus masuk

Dalam perang teknologi modern, banyak inovasi lahir bukan dari organisasi paling besar, tetapi dari tim yang kecil, cepat, dan dekat dengan masalah. Karena itu, **startup dan UKM teknologi harus masuk** ke ekosistem pertahanan nasional. Ini bukan romantisme wirausaha. Ini soal struktur inovasi. Drone kecil, radio modular, *payload*, *vision stack*, *counter-drone*, *edge AI*, *firmware*, dan perangkat uji sering justru lebih cocok dikerjakan oleh perusahaan yang lincah, fokus, dan cepat berinteraksi. Arah ini juga inline dengan bab-bab sebelumnya yang menekankan kontrak kecil tetapi nyata, *reference design*, dan produksi rendah volume.

Di Amerika Serikat, DoD secara terbuka menekankan perluasan partisipasi bisnis kecil. Kantor **Office of Industrial Base Growth / Office of Small Business Programs** menyebut bahwa pada FY24, DoD meningkatkan nilai kontrak untuk usaha kecil sebesar **US\$4,9 miliar**, sambil menegaskan misinya untuk memperluas basis industri, meningkatkan kompetisi, membangun kapasitas, dan membuka jalan agar bisnis berbagai ukuran bisa masuk ke pasar pertahanan. ([Bisnis Pertahanan](#)) Dokumen DLA juga menegaskan bahwa program inovasi industri kecil dipakai untuk mengurangi *single points of failure*, memperkuat rantai pasok, dan menurunkan biaya siklus hidup. ([Kantor Comptroller Pertahanan](#))

Untuk Indonesia, konsekuensinya tegas:

- **startup tidak boleh diperlakukan hanya sebagai peserta lomba inovasi;**
- **UKM teknologi tidak boleh dibatasi pada komponen sederhana tanpa akses ke masalah strategis;**
- **mekanisme masuk ke pasar pertahanan harus dibuat lebih jelas, lebih cepat, dan lebih kecil hambatan awalnya.**

Jenis pemain yang perlu didorong masuk antara lain:

- pembuat radio dan modul RF,
- pengembang autopilot dan *embedded systems*,
- pembuat *ground control software*,
- pengembang visi mesin dan klasifikasi objek,
- pembuat sensor, *payload*, dan *counter-drone* ringan,
- serta perusahaan *repair*, *re-engineering*, dan integrasi subsistem.

Negara yang ingin cepat belajar tidak bisa hanya mengandalkan pemain besar. Ia butuh **banyak bengkel teknologi yang hidup**.

21.3. Produksi massal murah sebagai sasaran

Industri nasional akan salah arah bila terlalu terpaku pada platform mahal dalam jumlah kecil. Untuk konteks Indonesia, terutama pada drone kecil, *counter-drone*, sensor, radio, dan *mission modules*, sasaran yang lebih sehat adalah **produksi massal murah**. Ini sejalan dengan pelajaran dari Ukraina dan Iran yang sudah menjadi tema besar dalam buku: **murah tidak berarti primitif**, dan volume sering lebih menentukan daripada kemewahan.

Arah global juga bergerak ke sana. Replicator dirancang untuk mempercepat penyediaan **ribuan sistem otonom** dan *integrated enablers*, bukan hanya beberapa platform eksotis. ([Defense Business Board](#)) DoD juga secara resmi menekankan bahwa ancaman drone dan sistem nirawak tumbuh karena semakin murah, mudah diakses, dan makin terhubung, sehingga respons tidak bisa berbasis logika lama yang terlalu mahal dan terlalu sedikit. ([Defense Business Board](#))

Untuk Indonesia, sasaran produksi massal murah berarti:

- **harga satuan harus turun seiring batch,**
- **waktu produksi harus dipendekkan,**
- **komponen harus disederhanakan sejauh mungkin,**
- **desain harus mudah dirakit, diuji, dan diperbaiki,**
- **dan kehilangan satu sistem tidak boleh memukul operasi secara strategis.**

Ini penting karena negara kepulauan yang luas akan lebih terbantu oleh:

- drone ISR kecil yang banyak,
- node sensor murah yang bisa ditebar,
- modul radio yang bisa dipasang ulang,
- dan keluarga sistem attritable yang bisa diganti cepat,

daripada segelintir platform yang terlalu mahal untuk dipakai rutin.

Jadi, target industrinya harus jujur: **bukan membangun kemewahan dalam jumlah kecil, tetapi membangun kecukupan tempur dalam volume relevan.**

21.4. *Repair, maintenance*, dan substitusi komponen

Industri pertahanan yang sehat tidak diukur hanya dari kemampuan membuat barang baru. Ia juga diukur dari kemampuan **memperbaiki, merawat, meng-overhaul, dan mengganti komponen ketika akses pasokan terganggu**. Dalam konteks buku ini, hal ini sangat penting karena *supply chain* sudah ditempatkan sebagai titik rapuh strategis Indonesia.

Dokumen resmi DoD makin keras menekankan hal ini. **Acquisition Transformation Strategy 2025** menyebut bahwa akuisisi harus memikirkan kemampuan melakukan **depot-level maintenance, repair, and overhaul** serta fokus pada keberlanjutan desain dan *life cycle sustainment* supaya sistem tetap fleksibel dan hemat biaya selama umur pakai. ([U.S. Department of War](#)) DLA juga menekankan pengurangan *single points of failure*, inovasi rantai pasok, serta mitigasi risiko komponen palsu dan ketersediaan mikroelektronika. ([Kantor Comptroller Pertahanan](#))

Bagi Indonesia, ini berarti industri nasional harus dibangun bukan hanya sebagai **manufaktur awal**, tetapi juga sebagai **jaringan sustainment**. Kemampuan yang harus tumbuh antara lain:

- *repair* papan elektronik dan modul daya,
- penggantian sensor dan kalibrasi ulang,
- pembaruan *firmware* dan *software stack*,
- rekayasa balik terbatas untuk komponen yang hilang,
- substitusi komponen setara,
- *remanufacturing* batch kecil,
- dan dokumentasi *failure modes*.

Subbab ini penting karena negara yang tidak punya kapasitas *repair* dan substitusi akan selalu terjebak pada logika:

- beli lagi,
- tunggu vendor,
- atau berhenti operasi.

Padahal dalam krisis, yang dibutuhkan adalah **kemampuan menjaga sistem tetap hidup walau tidak ideal**.

21.5. Pentingnya standarisasi terbuka terbatas

Indonesia perlu standarisasi, tetapi bukan standarisasi yang mematikan inovasi. Yang dibutuhkan adalah **standarisasi terbuka terbatas**: cukup terbuka untuk memungkinkan interoperabilitas, kompetisi, dan substitusi komponen; cukup terbatas untuk tetap menjaga keamanan, kendali, dan kebutuhan operasional. Arah ini sangat sejalan dengan bab-bab sebelumnya tentang *reference design*, interoperabilitas lintas domain, desain modular, dan pengurangan *vendor lock*.

DoD pada 2025 menegaskan bahwa penerapan **Modular Open Systems Approach (MOSA)** sangat penting untuk mendorong interoperabilitas, kompetisi, penyisipan teknologi baru, peningkatan performa, dan penurunan biaya siklus hidup; strategi itu juga disebut penting untuk menghindari *vendor lock*. ([U.S. Department of War](#)) DIU melalui **Blue UAS Framework** juga memberi contoh yang sangat berguna: pemerintah menilai dan menyusun daftar komponen, sub-komponen, modul, dan perangkat lunak yang **interoperable**, sesuai aturan, dan dapat digunakan secara modular oleh berbagai platform. ([Unit Inovasi Pertahanan](#)) NATO STO bahkan telah menyusun **design guidelines for interoperability** untuk sistem *swarm* dalam arsitektur terbuka dan interoperable.

Untuk Indonesia, prinsip “terbuka terbatas” itu dapat diterjemahkan menjadi:

- antarmuka dan format data inti yang disepakati,
- API atau protokol tertentu yang terdokumentasi,
- slot modular untuk radio, kamera, atau *mission payload*,
- dokumentasi integrasi minimum,
- dan aturan hak kekayaan intelektual yang mencegah penguncian total oleh satu vendor.

Yang harus dihindari adalah dua ekstrem:

- **terlalu tertutup**, sehingga setiap sistem menjadi pulau sendiri;
- **terlalu terbuka tanpa disiplin**, sehingga keamanan dan kendali melemah.

Jalan tengah inilah yang paling masuk akal bagi industri nasional yang masih tumbuh: **cukup standar untuk bisa saling sambung, cukup fleksibel untuk tetap bereksperimen**.

21.6. Dari proyek ke kapasitas industri berkelanjutan

Pada akhirnya, inti Bab 21 adalah perubahan cara berpikir. Industri nasional tidak boleh terus hidup dari **proyek sesaat**. Ia harus bergerak menjadi **kapasitas industri berkelanjutan**. Artinya, yang dibangun bukan hanya pengiriman barang satu kali, tetapi kemampuan nasional yang terus memproduksi, terus belajar, terus memperbaiki, dan tetap hidup di luar satu kontrak. Arah ini juga selaras dengan penutup besar buku: Indonesia harus mulai dari yang bisa **dibuat, diuji, dan diproduksi**, bukan dari simbol yang terlalu besar.

Laporan **Industry Partnerships for Crises** menekankan bahwa basis industri pertahanan yang sehat memerlukan hubungan yang lebih lincah antara pemerintah dan pelaku industri, termasuk perusahaan non tradisional, agar kapasitas bisa tumbuh dan siap dipakai dalam krisis. Kantor pertumbuhan basis industri DoD juga menekankan bahwa tujuan mereka adalah **meningkatkan kompetisi, membangun kapasitas, dan menciptakan jalur yang lebih jelas** agar bisnis bisa masuk dan bertahan di pasar pertahanan. ([Bisnis Pertahanan](#))

Bagi Indonesia, perubahan dari proyek ke kapasitas berarti:

- kontrak tidak hanya menilai barang jadi, tetapi juga kemampuan *support* dan *upgrade*;
- produksi batch kecil dilakukan berulang, bukan sekali;
- ada permintaan minimum yang cukup untuk menjaga lini hidup;
- ada insentif untuk *repairability*, modularitas, dan substitusi;
- dan ada hubungan jangka menengah antara negara, BUMN, startup, UKM, dan kampus.

Ukuran keberhasilannya pun harus berubah. Bukan lagi semata:

- berapa proyek dimenangkan,
- atau berapa persen TKDN tertulis,

melainkan:

- berapa desain yang terus diproduksi,
- berapa vendor lokal yang naik kelas,
- berapa komponen yang bisa diganti tanpa impor penuh,
- berapa sistem yang bisa diperbaiki di dalam negeri,
- dan berapa lama industri bisa bertahan jika pasokan luar terganggu.

Penutup Bab: industri nasional harus menjadi mesin ketahanan

Bab ini pada dasarnya ingin menegaskan satu hal: **industri nasional tidak boleh lagi diposisikan sekadar sebagai vendor pengadaan**. Dalam perang digital modern, industri harus menjadi **mesin ketahanan nasional**. Ia harus mampu memproduksi yang murah, memperbaiki yang rusak, mengganti yang hilang, menyederhanakan desain, menjaga lini pasok, dan terus memasukkan pembelajaran lapangan ke generasi sistem berikutnya. Itu adalah makna sebenarnya dari pergeseran **dari vendor ke mitra strategis**.

Karena itu, industri nasional yang dibutuhkan Indonesia adalah industri yang:

- tidak bertumpu pada BUMN saja,
- membuka ruang nyata bagi startup dan UKM,
- mengejar volume murah yang relevan,
- kuat di *repair, maintenance*, dan substitusi,
- memakai standarisasi terbuka terbatas,
- dan bergerak dari logika proyek ke logika kapasitas.

Negara yang serius membangun pertahanan digital tidak cukup membeli dari industrinya. Ia harus menumbuhkan industrinya sebagai bagian dari daya tahan perang itu sendiri.

Bab 22. Peran Negara dan TNI: Pengarah, Penguji, dan Pembeli Pertama

22.1. Negara sebagai pembentuk pasar

Dalam industri pertahanan digital, pasar tidak tumbuh sendiri. Ia dibentuk. Karena itu, **negara harus bertindak sebagai pembentuk pasar**, bukan sekadar penulis spesifikasi dan pembayar tagihan. Ini penting karena teknologi seperti drone kecil, *counter-drone*, radio taktis, *mission software*, *edge AI*, dan sistem maritim otonom sering belum punya pasar sipil dalam negeri yang cukup besar untuk menopang skala, pembelajaran, dan investasi jangka panjang.

Pengalaman Amerika Serikat menunjukkan hal ini dengan sangat jelas. Kantor **Office of Industrial Base Growth** di bawah DoD secara resmi menyatakan misinya adalah memperluas dan memperkuat basis industri pertahanan melalui pertumbuhan vendor dan kematangan pemasok, dengan tujuan **meningkatkan kompetisi, membangun kapasitas, dan menciptakan jalur yang lebih jelas bagi bisnis untuk masuk dan bertahan di pasar pertahanan**. Pada FY24, DoD juga melaporkan kenaikan **US\$4,9 miliar** dalam nilai kontrak untuk usaha kecil. ([Bisnis Pertahanan](#))

Bagi Indonesia, ini berarti negara harus berani melakukan beberapa hal sekaligus:

- **menentukan area prioritas** yang jelas, seperti drone kecil, EW, *counter-drone*, *mission computer*, dan *maritime awareness*;
- **memberi permintaan awal yang cukup nyata**, meski volumenya kecil;
- **mengurangi ketidakpastian pasar** bagi startup, UKM, dan vendor lokal;
- dan **membentuk standar minimum** agar industri tidak tumbuh liar tetapi juga tidak mati oleh birokrasi.

Negara yang hanya menunggu industri “siap sendiri” biasanya akan terlambat. Dalam sektor ini, **permintaan negara adalah sinyal strategis**. Tanpa sinyal itu, banyak pemain lokal akan tetap hidup di tahap prototipe.

22.2. TNI sebagai pengguna dan sumber umpan balik

Teknologi pertahanan tidak matang di ruang rapat. Ia matang di tangan pengguna. Karena itu, **TNI harus diposisikan bukan hanya sebagai penerima alat, tetapi sebagai pengguna aktif dan sumber umpan balik yang terus-menerus**. Ini sangat sejalan dengan arah bab-bab sebelumnya yang menekankan bahwa unit operasional harus menjadi *co-developer*, bukan sekadar pelanggan pasif.

Fungsi TNI di sini sangat strategis karena hanya pengguna lapangan yang bisa menjawab pertanyaan-pertanyaan paling penting:

- sistem mana yang benar-benar membantu,
- mana yang terlalu rapuh,
- mana yang terlalu rumit,
- mana yang tidak cocok dengan ritme operasi,
- dan mana yang justru harus disederhanakan.

Karena itu, TNI harus menjalankan tiga peran sekaligus:

- **pengguna awal**, yang memakai sistem bahkan saat belum sempurna;
- **penguji realitas**, yang memaksa teknologi keluar dari zona nyaman laboratorium;
- **produsen umpan balik**, yang memberi data kegagalan, kebutuhan baru, dan koreksi desain.

Dalam perang teknologi modern, keunggulan tidak hanya datang dari siapa yang punya alat lebih dulu, tetapi dari siapa yang **belajar lebih cepat dari penggunaan alat itu**. Maka TNI harus dibangun sebagai organisasi pembelajar, bukan sekadar organisasi penerima pengadaan.

22.3. Kemhan sebagai arsitek ekosistem, bukan hanya pembeli

Peran Kementerian Pertahanan tidak boleh dipersempit menjadi lembaga pembeli.

Kemhan harus bertindak sebagai arsitek ekosistem. Artinya, Kemhan harus menyusun arah, memetakan peran aktor, menentukan prioritas teknologi, mendorong integrasi, dan menjaga agar kampus, industri, startup, BUMN, serta TNI bergerak dalam kerangka yang saling menyambung.

Ini juga sesuai dengan sinyal resmi di Indonesia sendiri. Dokumen perencanaan SPBE Kemhan 2025–2029 menunjukkan bahwa Kemhan sedang mendorong **peta rencana SPBE, integrasi sistem, dan transformasi digital** di lingkungannya. Itu penting, tetapi juga menandakan bahwa pembenahan arsitektur digital masih berada pada tahap pembangunan dan perlu diarahkan secara lebih operasional. ([PPID Kementerian Pertahanan](#))

Dalam konteks bab ini, Kemhan perlu berfungsi pada lima lapis:

- **arsitek prioritas**, menentukan mana yang mendesak dan mana yang bisa menunggu;
- **arsitek integrasi**, memastikan sistem tidak lahir sebagai pulau-pulau;
- **arsitek permintaan**, memberi sinyal pasar yang cukup stabil;
- **arsitek pengujian**, menetapkan mekanisme uji yang keras;
- **arsitek transisi**, memastikan hasil riset dan prototipe benar-benar menyeberang ke operasi.

Kalau Kemhan hanya membeli barang jadi, maka yang tumbuh adalah ketergantungan. Tetapi bila Kemhan mengorkestrasi ekosistem, yang tumbuh adalah **kapasitas nasional**.

22.4. Perlunya pusat uji nasional

Salah satu kelemahan terbesar negara berkembang adalah terlalu banyak percaya pada demo, terlalu sedikit percaya pada pengujian keras. Karena itu, Indonesia membutuhkan **pusat uji nasional** untuk drone, EW, *counter-drone*, maritim otonom, navigasi *GPS-denied*, dan integrasi AI *edge*. Kebutuhan ini juga inline dengan roadmap buku yang menempatkan pusat data, pusat uji, dan *test range* sebagai fondasi transisi dari prototipe ke kapasitas nyata.

Pelajaran internasional sangat kuat di sini. NATO memakai **REPMUS** sebagai arena eksperimen sistem nirawak maritim dan interoperabilitas lintas sistem; NATO menyebut REPMUS 2024 sebagai latihan eksperimen terdepan untuk sistem nirawak maritim, dengan tujuan menguji operasi bersama dan memahami ancaman baru di lingkungan maritim. ([U.S. Department of War](#))

Bagi Indonesia, pusat uji nasional bukan sekadar lokasi fisik. Ia harus menjadi **mesin verifikasi nasional** yang memungkinkan:

- uji *swarm* kecil dan besar,
- uji jamming, spoofing, dan gangguan spektrum,
- uji integrasi udara-laut-darat,
- uji sistem maritim otonom di lingkungan pesisir dan selat,
- uji baterai, RF, navigasi, dan *mission software*,
- serta evaluasi pasca-uji yang masuk kembali ke desain.

Tanpa pusat uji nasional, negara akan terus mengira banyak sistem “siap”, padahal baru lolos demo yang nyaman. **Perang tidak akan memberi kondisi nyaman.**

22.5. Pendanaan inovasi pertahanan yang cepat

Teknologi pertahanan tidak akan tumbuh bila semua pendanaan bergerak dengan ritme proyek tahunan yang lambat dan administratif. Karena itu, Indonesia membutuhkan **pendanaan inovasi pertahanan yang cepat, kecil, berulang, dan berbasis hasil uji**. Ini penting terutama untuk startup, UKM, laboratorium kampus, dan vendor yang sedang bergerak dari prototipe ke produksi awal.

Di Amerika Serikat, DoD memakai beberapa jalur untuk mempercepat ini. Program **RISE (Rapid Integrated Scalable Enterprise)** dikelola untuk memberi kendaraan kolaboratif bagi usaha kecil agar teknologi inovatif bisa **cepat dimasukkan ke program akuisisi** yang menjawab kebutuhan pertahanan spesifik. Di tingkat lebih besar, reformasi **PPBE** yang diumumkan DoD pada Januari 2025 juga secara resmi diarahkan untuk **mengurangi silo data, memperbaiki analitik, dan meningkatkan kelincahan alokasi sumber daya**, dengan target implementasi berkelanjutan sampai 2028. ([Bisnis Pertahanan](#))

Untuk Indonesia, prinsip pendanaannya sebaiknya begini:

- **kecil tetapi cepat**, agar banyak ide bisa diuji;
- **bertahap berdasarkan bukti**, bukan dibayar penuh di depan;
- **terhubung ke kebutuhan satuan**, bukan hanya usulan laboratorium;
- **punya pintu lanjut ke produksi awal**, bila lolos uji;
- dan **tidak mensyaratkan administrasi yang membunuh kecepatan**.

Yang harus dihindari adalah pola lama:

- dana riset ada, tetapi terlalu jauh dari pengguna;
- dana pengadaan ada, tetapi datang saat teknologi sudah basi;
- dan dana inovasi terlalu kecil atau terlalu lambat untuk membuat perbedaan.

Inovasi pertahanan yang cepat tidak berarti ceroboh. Artinya justru **berani mendanai pembelajaran lebih awal** sebelum semua hal dibuat terlalu mahal untuk diubah.

22.6. Mengapa birokrasi lama harus dipotong

Bagian ini perlu disampaikan dengan jujur. **Birokrasi lama harus dipotong** karena perang teknologi bergerak lebih cepat daripada meja administrasi. Bila Indonesia tetap memakai logika akuisisi, pengujian, dan keputusan yang terlalu lambat, maka semua bab tentang kampus, industri, dan roadmap teknologi akan berhenti sebagai wacana.

Pelajaran ini bahkan sedang dihadapi Amerika Serikat sendiri. **Acquisition Transformation Strategy** DoD yang diterbitkan November 2025 secara eksplisit menyerukan perubahan dari **culture of compliance** menjadi **culture of speed and execution**, dengan tujuan menempatkan seluruh sistem akuisisi dan basis industri pada pijakan yang lebih siap perang, mempercepat *fielding*, meningkatkan kapasitas produksi, dan menerima lebih banyak risiko yang terukur. Dokumen pendampingnya juga menyebut kebutuhan untuk mempercepat *fielding* kemampuan yang mendesak bagi prajurit. ([U.S. Department of War](#))

Untuk Indonesia, memotong birokrasi lama bukan berarti membuang akuntabilitas. Yang perlu dipotong adalah:

- rantai persetujuan yang terlalu panjang,
- spesifikasi yang dibuat seolah semua hal harus sempurna dari awal,
- pengadaan yang terlalu fokus pada kepatuhan dokumen tetapi lemah pada hasil,
- serta pemisahan terlalu kaku antara riset, uji, pengadaan, dan operasi.

Sebaliknya, yang perlu dibangun adalah:

- **jalur cepat untuk kebutuhan mendesak,**
- **mekanisme prototipe–uji–perbaikan–beli ulang,**
- **kontrak kecil yang bisa naik kelas,**
- **pembelajaran lintas lembaga yang lebih terbuka,**
- **dan keputusan yang berbasis bukti uji, bukan hanya format administrasi.**

Bila birokrasi lama tidak dipotong, maka negara akan kalah bukan karena kekurangan ide, tetapi karena **terlalu lambat mengubah ide menjadi kemampuan.**

Penutup Bab: negara dan TNI adalah pengungkit utama

Bab ini pada dasarnya ingin menegaskan satu hal: **tanpa negara dan TNI yang aktif, ekosistem pertahanan digital nasional tidak akan terkonsolidasi**. Kampus bisa merancang. Industri bisa memproduksi. Startup bisa berinovasi. Tetapi yang membuat semuanya menyatu menjadi kapasitas nasional adalah **negara sebagai pembentuk pasar, Kemhan sebagai arsitek ekosistem, dan TNI sebagai pengguna sekaligus sumber pembelajaran**.

Karena itu, peran negara dan TNI harus dibaca dalam tiga kata kunci:

- **pengarah**, karena tanpa arah pasar dan prioritas teknologi, ekosistem akan terpecah;
- **penguji**, karena tanpa uji keras, inovasi akan berhenti di demo;
- **pembeli pertama**, karena tanpa permintaan awal yang nyata, industri lokal tidak akan tumbuh.

Negara yang serius membangun AI militer dan pertahanan digital bukan negara yang paling banyak berbicara tentang kemandirian, melainkan negara yang paling cepat mengubah riset menjadi uji, uji menjadi kontrak, dan kontrak menjadi kapasitas tempur yang terus belajar.

Bagian VIII. Tata Kelola, Etika, dan Batas Penggunaan

Bab 23. *Responsible Military AI*: Kendali Manusia, Akuntabilitas, dan Kepercayaan

23.1. Mengapa etika bukan ornamen

Dalam diskusi AI militer, etika sering diperlakukan seperti lampiran: penting secara retorik, tetapi terpisah dari soal operasi. Itu keliru. **Etika bukan ornamen. Etika adalah bagian dari desain sistem, disiplin komando, dan keandalan operasi.** Bila AI dipakai untuk ISR, prioritas target, *battle management*, atau fungsi otonom tertentu, maka pertanyaan etis tidak datang belakangan. Ia hadir sejak awal: data apa yang dipakai, siapa yang memutuskan, apa batas mesin, dan bagaimana salah bisa dicegah atau setidaknya diperlambat. Pandangan ini juga sudah sejalan dengan naskah buku Anda yang menegaskan bahwa AI militer harus dibaca sebagai persoalan **akuntabilitas, kepercayaan, dan hukum**, bukan semata teknologi.

Departemen Pertahanan AS dalam *Responsible AI Strategy and Implementation Pathway* menempatkan lima prinsip etika AI—**responsible, equitable, traceable, reliable, dan governable**—bukan sebagai hiasan normatif, tetapi sebagai kerangka implementasi untuk pengembangan dan penggunaan AI di pertahanan. Dokumen itu juga menekankan bahwa integrasi etika sejak awal justru membantu mengurangi keraguan, mempercepat adopsi yang benar, dan menjaga kepercayaan di dalam organisasi serta di antara sekutu. ([U.S. Department of War](#))

Karena itu, bagi militer, etika punya fungsi yang sangat praktis:

- mencegah percepatan salah yang tak terkendali,
- menjaga legitimasi keputusan,
- memaksa sistem diuji dalam kondisi realistis,
- dan memastikan manusia tidak larut menjadi stempel bagi mesin.

Militer yang menganggap etika sebagai ornamen biasanya akan terlambat menyadari bahwa masalah sebenarnya bukan hanya “AI bisa atau tidak”, tetapi **AI salah, lalu siapa yang menanggung akibatnya.**

23.2. *Meaningful human control*

Salah satu istilah paling sering muncul dalam perdebatan global adalah ***meaningful human control***. Istilah ini penting, tetapi mudah disalahpahami. Ia bukan sekadar slogan “manusia tetap di tengah”. Yang lebih penting adalah apakah manusia benar-benar:

- mengerti konteks keputusan,
- memahami batas sistem,
- punya waktu dan otoritas untuk mengintervensi,
- dan tidak terperangkap dalam ritme mesin yang terlalu cepat.

Naskah buku Anda juga mengarah ke sana ketika menekankan bahwa tanggung jawab dan penilaian manusia harus tetap hadir dalam rantai komando dan penggunaan sistem.

Deklarasi politik yang dipimpin AS tentang *Responsible Military Use of Artificial Intelligence and Autonomy* menegaskan bahwa negara harus mempertahankan **rantai komando dan kontrol yang bertanggung jawab**, serta memastikan penggunaan militer AI dan otonomi berada di bawah **appropriate human judgment**. Deklarasi itu juga menekankan bahwa penggunaan tersebut harus sesuai dengan hukum humaniter internasional yang berlaku. ([State.gov](https://www.state.gov))

Masalahnya, *human control* tidak otomatis bermakna hanya karena ada manusia di layar. Kontrol manusia menjadi kosong bila:

- operator tidak memahami bagaimana sistem sampai pada rekomendasinya,
- tempo operasi terlalu cepat untuk penilaian yang sungguh-sungguh,
- pilihan manusia tinggal “setuju atau menghambat” tanpa informasi memadai,
- atau rantai komando membiarkan mesin menjadi sumber otoritas tak resmi.

Karena itu, dalam konteks Indonesia, *meaningful human control* sebaiknya dipahami sebagai:

- **manusia tetap memegang keputusan penggunaan kekuatan,**
- **manusia memahami konteks dan batas sistem,**
- **manusia punya peluang realistis untuk menghentikan, mengubah, atau menolak rekomendasi mesin,**
- **dan desain sistem tidak boleh sengaja mendorong kepatuhan buta pada keluaran AI.**

Jadi, inti persoalannya bukan “ada manusia atau tidak”, tetapi **apakah manusia itu masih sungguh memerintah, atau hanya hadir secara simbolik.**

23.3. *Appropriate levels of judgment and care*

Frasa penting lain dalam tata kelola AI militer adalah ***appropriate levels of judgment and care***. Ini terdengar abstrak, tetapi sebenarnya sangat operasional. Maksudnya: tingkat penilaian manusia, kehati-hatian, pengawasan, dan uji yang diterapkan harus **sebanding dengan risiko, konteks, dan dampak sistem**.

DoD Directive 3000.09 yang diperbarui pada Januari 2023 tetap diarahkan untuk memastikan bahwa **komandan dan operator dapat menjalankan tingkat penilaian manusia yang tepat atas penggunaan kekuatan**, sambil mempertahankan persyaratan uji, tinjauan, dan pengawasan senior atas sistem senjata otonom tertentu. Pernyataan resmi DoD saat pembaruan itu juga menegaskan komitmen untuk mengembangkan dan menggunakan sistem senjata, termasuk yang memiliki fungsi otonom, secara **responsible and lawful**. ([U.S. Department of War](#))

Maknanya bagi Indonesia cukup jelas. Tidak semua AI militer menuntut tingkat kehati-hatian yang sama.

- AI untuk **prediksi perawatan** tentu risikonya berbeda dari AI untuk **prioritisasi target**.
- AI untuk **deteksi anomali logistik** berbeda dari AI untuk **pengambilan keputusan di lingkungan tempur yang ambigu**.
- AI untuk **simulasi** berbeda dari AI yang masuk ke rantai penggunaan kekuatan.

Karena itu, kehati-hatian tidak boleh seragam. Semakin tinggi risiko sistem, semakin besar kebutuhan akan:

- pengawasan manusia,
- pengujian realistis,
- audit,
- pembatasan penggunaan,
- dan kejelasan wewenang.

Di titik ini, *responsible military AI* bukan berarti anti-kecepatan. Artinya adalah **kecepatan yang ditopang oleh kehati-hatian yang proporsional**.

23.4. *Explainability, auditability, traceability*

Militer tidak cukup hanya butuh AI yang akurat. Militer butuh AI yang **bisa dijelaskan secukupnya, bisa diaudit, dan jejak keputusannya bisa ditelusuri**. Dalam naskah buku Anda, unsur **traceability** sudah muncul sebagai salah satu landasan penting penggunaan AI militer yang bertanggung jawab.

DoD menempatkan **traceable** sebagai salah satu prinsip etika AI resminya, yang berarti personel terkait harus memiliki pemahaman memadai tentang teknologi, proses pengembangan, metode operasional, serta sumber data dan dokumentasi yang menyertai kemampuan AI. Dokumen Inggris **JSP 936** juga menegaskan bahwa implementasi AI pertahanan harus diarahkan pada kemampuan yang **safe, robust, and effective**, dengan tingkat pengawasan manusia yang tepat, sambil membangun kepercayaan melalui prinsip seperti **understanding, responsibility, bias and harm mitigation, dan reliability**. ([U.S. Department of War](#))

Dalam bahasa operasional, ini berarti sistem harus memiliki setidaknya:

- **jejak data**: data apa yang dipakai dan dari mana asalnya;
- **jejak model**: model versi berapa, diuji kapan, dengan asumsi apa;
- **jejak keputusan**: rekomendasi apa yang diberikan dan kepada siapa;
- **jejak intervensi manusia**: siapa yang menerima, menolak, atau mengubah keluaran sistem;
- **jejak kegagalan**: kapan sistem meleset, dalam kondisi apa, dan pelajaran apa yang diambil.

Tentu tidak semua sistem bisa dijelaskan sampai tingkat sempurna. Tetapi dalam militer, *opacity* yang total itu berbahaya. Sistem yang tidak cukup dapat dijelaskan akan sulit:

- dipercaya,
- diperbaiki,
- diaudit sesudah insiden,
- dan dipertanggungjawabkan secara hukum maupun komando.

Jadi, **AI yang kuat secara operasional harus juga cukup terang secara tata kelola**.

23.5. Tanggung jawab jika sistem salah

Ini pertanyaan paling keras, dan justru paling penting: **jika sistem salah, siapa yang bertanggung jawab?** Naskah buku Anda sudah mengangkat masalah ini saat membahas bahaya automasi berlebih: ketika banyak manusia dan mesin terlibat dalam satu keputusan, pertanyaan tanggung jawab menjadi semakin kabur.

Deklarasi politik AS menekankan pentingnya **rantai komando yang bertanggung jawab**, sementara DoD dan dokumen Inggris sama-sama menekankan *responsibility*, *reliability*, dan *governability* sebagai fondasi. Intinya sama: **tanggung jawab tidak boleh menguap ke dalam mesin**. ([State.gov](https://www.state.gov))

Dalam praktik, tanggung jawab biasanya tersebar di beberapa lapis:

- **perancang sistem**, bila risiko desain diabaikan;
- **pengembang atau integrator**, bila batas sistem tidak dijelaskan atau diuji dengan buruk;
- **komando**, bila sistem dipakai di luar konteks yang seharusnya;
- **operator**, bila ada kelalaian atau kepatuhan buta pada rekomendasi mesin;
- **organisasi**, bila tata kelola, pelatihan, dan pengawasan dibuat terlalu longgar.

Karena itu, doktrin yang sehat harus menolak dua godaan sekaligus:

- menyalahkan operator sendirian untuk kesalahan yang sebenarnya sistemik;
- atau menyalahkan “AI” secara abstrak seolah mesin adalah subjek moral yang berdiri sendiri.

Untuk Indonesia, pelajaran praktisnya adalah setiap sistem AI pertahanan harus datang dengan:

- batas penggunaan yang jelas,
- matriks wewenang yang jelas,
- log keputusan,
- protokol *fail-safe*,
- serta mekanisme investigasi pasca-insiden.

Tanpa itu, organisasi akan masuk ke wilayah paling berbahaya: **sistem salah, dampak besar, tetapi tanggung jawab menguap di antara vendor, komando, operator, dan mesin**.

23.6. Mengapa militer butuh AI yang bisa dipercaya, bukan hanya cepat

Bagian penutup bab ini harus menegaskan satu hal besar: **militer membutuhkan AI yang bisa dipercaya, bukan hanya cepat**. Naskah buku Anda bahkan sudah merumuskannya dengan tajam: AI yang baik bukan AI yang sekadar cepat, melainkan AI yang **dapat dipercaya, dipahami batasnya, diuji, dan dipakai dalam proses manusia-mesin yang sehat**. Tanpa itu, *speed of decision* bisa berubah menjadi *speed of error*.

DoD menulis secara eksplisit bahwa integrasi etika dan tata kelola yang baik justru membantu **maintain trust** di dalam organisasi dan di antara sekutu. Dokumen Inggris **JSP 936** juga meletakkan tujuan yang sama: mendorong AI pertahanan yang aman, andal, efektif, dan berada di bawah tingkat pengawasan manusia yang tepat. ([U.S. Department of War](#))

Mengapa kepercayaan lebih penting daripada sekadar kecepatan?

- Karena **komandan tidak akan sungguh memakai sistem yang tidak mereka percaya**.
- Karena **operator yang terlalu percaya juga berbahaya**, bila kepercayaan itu buta.
- Karena **sekutu dan mitra akan menilai keseriusan tata kelola**, bukan hanya kemampuan teknis.
- Karena **legitimasi operasi** bergantung bukan hanya pada hasil, tetapi juga pada cara hasil itu dicapai.
- Dan karena dalam konflik nyata, **kesalahan cepat bisa lebih merusak daripada keputusan lambat tetapi terkendali**.

Jadi, AI yang layak bagi militer bukan AI yang paling spektakuler. Ia adalah AI yang:

- cukup cepat,
- cukup andal,
- cukup dapat dijelaskan,
- cukup bisa diaudit,
- dan cukup dipercaya untuk dipakai dalam situasi berisiko tinggi.

Penutup Bab: kepercayaan adalah bagian dari daya tempur

Bab ini pada dasarnya ingin mengatakan bahwa **kepercayaan bukan isu lunak**. Dalam AI militer, kepercayaan adalah bagian dari **daya tempur**. Sistem yang tidak dipercaya akan diabaikan. Sistem yang terlalu dipercaya tanpa kritik akan membawa organisasi ke jurang salah yang lebih cepat. Karena itu, jalan yang benar bukan menolak AI, dan bukan pula menyerah pada AI, melainkan **mendisiplinkan AI**.

Bagi Indonesia, *Responsible Military AI* berarti:

- **kendali manusia yang sungguh bermakna,**
- **tingkat kehati-hatian yang sebanding dengan risiko,**
- **kemampuan audit dan penelusuran yang nyata,**
- **tanggung jawab yang tidak kabur,**
- **dan kepercayaan yang dibangun lewat uji, tata kelola, dan disiplin komando.**

Militer yang matang bukan militer yang paling cepat menyerahkan keputusan pada mesin, melainkan militer yang paling disiplin dalam memastikan bahwa kecepatan mesin tetap tunduk pada penilaian manusia, tanggung jawab hukum, dan kebutuhan untuk tetap dipercaya.

Bab 24. Hukum, Risiko Sipil, dan Masa Depan Konflik

24.1. IHL dan tantangan AI

Perang modern selalu berubah, tetapi **hukum humaniter internasional** atau *International Humanitarian Law (IHL)* tidak menjadi usang hanya karena senjata dan sistem menjadi lebih digital. Yang berubah adalah **cara hukum itu diuji**. Ketika AI dipakai untuk ISR, *targeting support*, navigasi, *battle management*, atau fungsi otonom tertentu, tantangannya bukan sekadar “apakah AI boleh dipakai”, melainkan **apakah penggunaan itu masih bisa tunduk pada aturan perang yang membatasi kekerasan dan melindungi sipil**. Ini juga sangat selaras dengan pijakan dalam naskah buku Anda bahwa AI militer harus dibahas bukan hanya sebagai soal kemampuan teknis, tetapi juga sebagai persoalan **hukum, akuntabilitas, dan kepercayaan**.

ICRC menegaskan pada 2026 bahwa penggunaan *autonomous weapon systems* dan sistem terkait tetap tunduk pada aturan IHL tentang **distinction, proportionality, dan precautions in attack**, tetapi teknologi yang bekerja secara opak, berubah lewat *machine learning*, atau sulit dipahami keluaran dan perilakunya dapat menciptakan kurangnya kontrol atas efek sistem, bahkan berisiko membuat sistem itu **indiscriminate by nature** dalam kondisi tertentu. ([ICRC](#)) ICRC juga menekankan dalam penjelasan terbarunya tentang konflik bersenjata bahwa prinsip distinction mewajibkan pihak yang bertikai selalu membedakan antara kombatan dan warga sipil, serta antara sasaran militer dan objek sipil. ([ICRC](#))

Karena itu, tantangan AI terhadap IHL bukan terutama karena hukum lama “tidak relevan”, melainkan karena AI dapat:

- mempercepat keputusan tanpa memperbaiki mutu penilaian,
- menyembunyikan asumsi dan bias di balik keluaran sistem,
- memperlebar jarak antara pengambil keputusan dan efek nyata di lapangan,
- serta membuat rantai tanggung jawab lebih kabur bila sistem dipakai tanpa batas yang jelas. ([ICRC](#))

Jadi, dalam konteks militer, pertanyaan hukumnya bukan “AI atau bukan AI”, tetapi **apakah sistem itu masih memungkinkan manusia dan organisasi mematuhi hukum perang secara sungguh-sungguh**.

24.2. *Targeting, proportionality, dan distinction*

Di dalam hukum perang, ada tiga kata yang harus terus diingat saat AI mulai masuk ke rantai keputusan: **targeting**, **proportionality**, dan **distinction**. Ketiganya bukan detail teknis. Ketiganya adalah inti perlindungan sipil. Prinsip **distinction** menuntut perbedaan antara target militer dan orang atau objek sipil. Prinsip **proportionality** melarang serangan bila kerugian sipil yang diperkirakan akan berlebihan dibanding keuntungan militer konkret dan langsung yang diharapkan. Prinsip **precautions** mewajibkan langkah-langkah layak untuk menghindari atau setidaknya meminimalkan dampak sipil. ([ICRC](#))

Masalahnya, AI dapat menggoda organisasi untuk memperlakukan *targeting* sebagai persoalan klasifikasi dan kalkulasi semata. Padahal ICRC menekankan bahwa aturan proportionality dan precautions dalam serangan **mengandaikan penilaian yang kontekstual**, bukan sekadar hasil formula. ([ICRC](#)) Artikel terbaru di *International Review of the Red Cross* juga memperingatkan bahwa sistem pendukung keputusan berbasis AI dapat mengikis **humane judgment** dalam *targeting* bila organisasi terlalu mengandalkan logika kuantifikasi dan otomatisasi. ([International Review of the Red Cross](#))

Untuk itu, Indonesia perlu membaca isu ini secara disiplin.

- **AI boleh membantu melihat pola**, tetapi tidak otomatis memahami konteks manusia.
- **AI boleh membantu memprioritaskan alarm**, tetapi tidak boleh menggantikan penilaian hukum dan operasional yang matang.
- **AI boleh mempercepat orientasi**, tetapi tidak boleh membuat proportionality berubah menjadi angka yang tampak objektif padahal menyembunyikan ketidakpastian.

Dengan kata lain, *targeting* bukan sekadar soal “apakah sistem mengenali objek dengan benar”. Ia juga soal **siapa yang ada di sekitar target, apa fungsi objek itu, bagaimana kondisi lapangan berubah, dan apakah serangan itu masih sah serta layak dilakukan**. ([ICRC](#))

24.3. Salah sasaran dan dampak sipil

Risiko paling nyata dari AI militer bukan hanya sistem gagal total. Sering kali risikonya justru lebih halus: **salah sasaran, salah tafsir, salah korelasi, atau keyakinan palsu bahwa sistem “cukup akurat”**. Dalam perang nyata, salah seperti itu tidak tinggal di layar. Ia berujung pada **dampak sipil**: korban jiwa, kerusakan infrastruktur, terganggunya rumah sakit, listrik, air, pelabuhan, jaringan komunikasi, atau aktivitas kemanusiaan. ICRC dalam penjelasan 2025 tentang penggunaan drone menegaskan bahwa drone dalam konflik bersenjata tetap tunduk pada prinsip **distinction, proportionality, dan precaution**, serta semua langkah yang layak harus diambil untuk menghindari atau setidaknya meminimalkan kerugian sipil. ([ICRC](#))

ICRC juga mengingatkan bahwa teknologi baru, dari drone komersial sampai AI dan EW, dapat mengaburkan batas antara domain militer dan sipil, termasuk karena penggunaan infrastruktur sipil untuk tujuan militer atau sebaliknya. ([Blog Palang Merah Internasional](#)) Ini penting karena dalam konflik modern, sistem AI sering bekerja di atas:

- data dari infrastruktur yang juga dipakai sipil,
- citra dan sinyal yang konteksnya tidak selalu bersih,
- serta lingkungan yang sangat padat objek sipil.

Di titik ini, salah sasaran bisa lahir dari beberapa sumber:

- **data latih yang bias atau tidak representatif,**
- **sensor yang terganggu cuaca, jamming, atau sudut pandang,**
- **kesalahan klasifikasi objek ganda fungsi,**
- **model yang terlalu percaya diri,**
- atau **operator yang terlalu percaya pada rekomendasi sistem.** ([ICRC](#))

Itu sebabnya, dalam AI militer, akurasi teknis tidak pernah cukup berdiri sendiri. Yang harus dihitung adalah **risiko salah dalam lingkungan konflik yang kacau**, dan dampaknya terhadap manusia sipil yang sering tidak pernah masuk ke data pelatihan atau presentasi vendor.

24.4. Risiko eskalasi, *spoofing*, dan *deception*

Bab ini juga harus mengingatkan bahwa AI dan sistem otonom tidak hanya menambah kemampuan, tetapi juga **menambah jalur eskalasi**. Ketika sistem menjadi lebih cepat, lebih terhubung, dan lebih otonom, maka ruang untuk salah paham, salah atribusi, dan reaksi berantai juga membesar. Risiko ini sangat nyata di lingkungan yang penuh **jamming, spoofing, cyber interference, decoy, dan deception**.

ICRC menekankan bahwa teknologi yang makin cepat dan kompleks dapat mengubah taktik, geografi, peserta, dan dampak perang, sekaligus berisiko mengaburkan batas-batas yang selama ini penting bagi perlindungan sipil. ([Blog Palang Merah Internasional](#)) UNIDIR juga mencatat bahwa integrasi AI ke lingkungan keamanan internasional memperluas kemungkinan penyalahgunaan, eksploitasi kerentanan infrastruktur kritis, dan destabilisasi. ([UNIDIR → Building a more secure world.](#)) Dalam konteks AI dan *targeting support*, risiko *spoofing* dan *deception* sangat serius karena sistem dapat diberi data palsu, dipancing ke kesimpulan keliru, atau diarahkan untuk membaca *decoy* sebagai ancaman nyata. Itu membuat kecepatan yang seharusnya menjadi kekuatan justru berubah menjadi **akselerator salah**.

Beberapa bentuk resikonya adalah:

- **sensor ditipu** oleh sinyal palsu atau *signature* tiruan,
- **navigasi disesatkan** oleh *spoofing* GNSS,
- **AI vision** salah membaca *decoy* atau objek sipil sebagai target,
- **rantai komando bereaksi terlalu cepat** terhadap alarm yang tidak cukup diverifikasi,
- atau **eskalasi antara pihak** dipicu oleh tindakan sistem yang tidak dipahami penuh. ([ICRC](#))

Karena itu, dalam konflik masa depan, pertahanan terhadap manipulasi informasi dan sinyal akan sama pentingnya dengan kemampuan menyerang. Negara yang hanya fokus pada kecerdasan sistem tetapi mengabaikan kemungkinan **penipuan terhadap sistem** akan membangun mesin yang cepat tetapi mudah diperalat.

24.5. Masa depan hubungan negara, perusahaan, dan perang

Konflik masa depan juga ditandai oleh perubahan aktor. Dulu perang lebih mudah dibaca sebagai urusan negara, militer, dan industri pertahanan tradisional. Kini batas itu makin kabur. Perusahaan teknologi besar, penyedia *cloud*, vendor AI, startup drone, pembuat sensor, analis data, sampai operator infrastruktur digital sipil makin terlibat dalam ekosistem perang. Naskah buku Anda sendiri sudah memotret pergeseran ini ketika membahas integrator, *frontier model*, dan hubungan antara perusahaan AI dengan negara keamanan nasional.

Fakta beberapa tahun terakhir memperlihatkan tren itu dengan terang. Pada Juni 2025, OpenAI meluncurkan **OpenAI for Government** untuk mendukung adopsi AI oleh instansi pemerintah AS. ([OpenAI](#)) Pada Juli 2025, Anthropic mengumumkan perjanjian prototipe dua tahun dengan plafon **US\$200 juta** bersama DoD melalui CDAO untuk memajukan kapabilitas AI bagi keamanan nasional. ([Anthropic](#)) Anthropic juga memperkenalkan **Claude Gov models** untuk pelanggan keamanan nasional AS, dengan klaim penggunaan untuk perencanaan strategis, dukungan operasional, analisis intelijen, dan penilaian ancaman. ([Anthropic](#)) Sementara ICRC pada 2025 mengingatkan bahwa peran perusahaan teknologi dalam kegiatan ICT terkait konflik menimbulkan risiko hukum dan perlindungan baru ketika warga sipil dan entitas sipil makin terseret ke dalam operasi konflik. ([ICRC](#))

Artinya, masa depan konflik akan semakin dipengaruhi oleh hubungan segitiga:

- **negara**, yang menetapkan tujuan dan otoritas penggunaan kekuatan;
- **perusahaan**, yang menyediakan model, infrastruktur, sensor, perangkat lunak, atau layanan;
- **dan militer**, yang mengoperasionalkan teknologi itu di medan nyata.

Hubungan ini membawa manfaat, tetapi juga risiko:

- **ketergantungan pada vendor**,
- **kaburnya batas tanggung jawab**,
- **dorongan komersial yang tidak selalu selaras dengan kehati-hatian hukum**,
- **militerisasi infrastruktur sipil**,
- **dan masuknya warga sipil teknis ke dalam orbit konflik**. ([ICRC](#))

Jadi, masa depan perang bukan hanya soal senjata lebih pintar. Ia juga soal **siapa yang membangun, siapa yang mengendalikan, siapa yang mendapat untung, dan siapa yang akhirnya menanggung risiko**.

24.6. Mengapa Indonesia perlu aturan operasional sejak dini

Semua ini membawa kita ke pertanyaan paling penting bagi Indonesia: **mengapa aturan operasional harus disusun sejak dini?** Jawabannya sederhana: karena jauh lebih mudah membangun disiplin sebelum sistem dipakai luas, daripada memperbaiki kerusakan setelah insiden, salah sasaran, atau kebiasaan buruk tertanam.

Deklarasi politik tentang penggunaan militer AI dan otonomi yang dipimpin AS menekankan pentingnya rantai komando yang bertanggung jawab, penggunaan yang sesuai hukum internasional, dan langkah-langkah untuk mengurangi risiko kegagalan yang tidak diinginkan. ([State.gov](#)) DoD juga menempatkan prinsip **traceable, reliable, governable** sebagai bagian dari kerangka AI pertahanan yang bertanggung jawab. ([State.gov](#)) Bagi Indonesia, pelajaran praktisnya bukan menyalin dokumen asing mentah-mentah, tetapi membangun **aturan operasional nasional** yang sesuai dengan geografi, struktur komando, kapasitas industri, dan kebutuhan pertahanan kita.

Aturan operasional sejak dini penting untuk menetapkan:

- **fungsi AI apa yang boleh dan tidak boleh dipakai** dalam konteks tertentu,
- **siapa yang berwenang mengaktifkan, mengubah, atau menghentikan sistem,**
- **bagaimana verifikasi target dan alarm dilakukan,**
- **apa syarat minimum uji, logging, dan audit,**
- **bagaimana sistem dipakai saat GNSS, link, atau sensor terganggu,**
- **dan bagaimana investigasi insiden dilakukan bila sistem salah.** ([ICRC](#))

Aturan seperti ini bukan penghambat inovasi. Justru sebaliknya. Aturan operasional yang jelas membantu:

- mempercepat adopsi yang sehat,
- mengurangi salah tafsir antar-satuan,
- memberi kepastian bagi industri dan pengembang,
- dan melindungi komandan maupun operator dari kebiasaan yang sembrono.

Untuk negara yang sedang membangun kemampuan, **aturan operasional awal adalah bagian dari pembangunan kapasitas**, bukan beban tambahan.

Penutup Bab: hukum bukan rem kemajuan, tetapi rem terhadap bencana

Bab ini pada dasarnya ingin mengatakan satu hal: **hukum dan tata kelola bukan lawan dari inovasi militer**. Mereka adalah pagar agar inovasi tidak berubah menjadi bencana strategis, bencana kemanusiaan, atau bencana legitimasi. Dalam konflik masa depan, AI dapat mempercepat pengamatan, analisis, dan respons. Tetapi AI juga dapat mempercepat **salah sasaran, dampak sipil, kebingungan komando, penipuan sinyal, dan eskalasi** bila dipakai tanpa disiplin hukum dan operasional. ([ICRC](#))

Bagi Indonesia, pelajaran akhirnya sangat jelas:

- **IHL tetap relevan, justru makin penting;**
- **distinction, proportionality, dan precautions** tidak boleh dilarutkan oleh euforia AI;
- **risiko sipil harus dibaca sebagai inti persoalan, bukan efek samping;**
- **hubungan negara, perusahaan, dan perang akan makin rapat dan makin rumit;**
- **dan aturan operasional harus dibangun sejak awal, sebelum kebiasaan yang salah menjadi normal.** ([State.gov](#))

Negara yang matang bukan negara yang paling cepat mempersenjatai AI, melainkan negara yang paling sadar bahwa kecepatan, hukum, perlindungan sipil, dan kendali operasional harus bergerak bersama.

Penutup

Bab 25. Penutup: Indonesia Tidak Bisa Lagi Menjadi Penonton

25.1. AI militer adalah soal organisasi, bukan sekadar algoritma

Di ujung buku ini, ada satu pelajaran yang harus ditegaskan kembali: **AI militer bukan terutama soal algoritma, melainkan soal organisasi**. Algoritma penting, tetapi ia tidak pernah bekerja sendirian. Nilainya baru muncul ketika ia masuk ke dalam sistem yang memiliki:

- sensor yang relevan,
- data yang cukup bersih,
- rantai komando yang jelas,
- operator yang terlatih,
- logistik yang hidup,
- dan budaya belajar yang tidak lumpuh oleh birokrasi.

Itulah sebabnya negara bisa membeli teknologi mahal tetapi tetap tertinggal. Yang sering kurang bukan “AI”, melainkan **kemampuan organisasi untuk menyerap AI ke dalam keputusan, kesiapan, latihan, dan operasi**. Buku ini sejak awal juga mengingatkan bahwa AI militer harus dibaca sebagai perubahan dalam cara negara **melihat, memahami, memutuskan, dan bertindak**.

Pelajaran yang sama terlihat dalam strategi resmi pertahanan modern. Pentagon, misalnya, menekankan adopsi **data, analytics, dan AI** sebagai bagian dari perubahan organisasi, bukan sekadar pembelian perangkat lunak. Strategi itu menempatkan AI dalam kerangka *decision advantage*, integrasi data, dan kesiapan institusi. ([Unit Inovasi Pertahanan](#))

Karena itu, kesimpulan pertama buku ini harus tegas:

- **AI militer yang kuat lahir dari institusi yang kuat;**
- **AI militer yang rapuh biasanya hanya menjadi dekorasi presentasi;**
- **dan organisasi yang lambat belajar akan kalah bahkan bila membeli alat yang mahal.**

25.2. Ukraina menunjukkan pentingnya *loop* belajar cepat

Bila ada satu laboratorium perang modern yang paling keras, itu adalah Ukraina. Pelajaran terbesarnya bukan sekadar bahwa Ukraina memakai drone atau AI, melainkan bahwa Ukraina menunjukkan nilai **loop belajar cepat**. Reuters melaporkan bahwa Ukraina telah mengumpulkan **lebih dari 2 juta jam video perang** sejak 2022 untuk melatih model AI yang membantu identifikasi target, penilaian efektivitas senjata, dan keputusan di medan perang. ([Reuters](#)) Reuters juga melaporkan bahwa Ukraina memakai **puluhan sistem AI** untuk membantu drone tetap mencapai target di lingkungan jamming berat, menunjukkan bahwa nilai AI muncul ketika sistem dipaksa belajar dalam kondisi nyata, bukan nyaman. ([Reuters](#))

Dari sini, ada beberapa pelajaran besar.

- **Data tempur adalah aset strategis**, bukan limbah operasi.
- **Umpan balik lapangan lebih berharga daripada demo laboratorium**.
- **Kecepatan iterasi** sering lebih menentukan daripada kesempurnaan desain awal.
- **Pengguna, pengembang, dan negara** harus berada dalam satu siklus pembelajaran.

Bagi Indonesia, ini sangat penting. Kita terlalu lama hidup dalam pola:

- prototipe dibuat,
- dipamerkan,
- lalu hilang,
- tanpa menjadi sistem yang dipakai, diuji ulang, dan diperbaiki.

Padahal keunggulan modern sering lahir bukan dari siapa yang punya desain awal terbaik, tetapi dari siapa yang **paling cepat mengubah pengalaman operasional menjadi generasi sistem berikutnya**. Itu sebabnya, Ukraina penting dibaca bukan untuk ditiru mentah-mentah, tetapi untuk memahami bahwa **perang modern memberi hadiah kepada organisasi yang belajar paling cepat**.

25.3. Iran menunjukkan pentingnya *resilience* dan volume

Jika Ukraina memberi pelajaran tentang *learning loop*, Iran memberi pelajaran tentang **resilience** dan **volume**. Buku ini sudah menempatkan Iran sebagai contoh bahwa **murah, banyak, dan cukup efektif** bisa menciptakan efek strategis yang besar. Pelajaran utamanya sederhana tetapi keras: **yang “cukup baik” dan bisa dipakai terus-menerus kadang lebih berbahaya daripada yang sangat canggih tetapi sedikit, mahal, dan rapuh.**

Dalam kerangka pertahanan modern, ini berarti:

- volume bisa menekan lawan,
- biaya rendah bisa memaksa lawan mengeluarkan biaya tinggi,
- otonomi secukupnya bisa cukup efektif,
- dan daya tahan terhadap jamming atau gangguan lebih penting daripada spesifikasi terbaik di atas kertas.

Pelajaran ini juga selaras dengan arah program seperti Replicator di Amerika Serikat, yang menekankan **ribuan sistem otonom attritable** dan *integrated enablers*, bukan beberapa platform eksotis. DIU pada November 2024 juga menegaskan bahwa kontrak Replicator diarahkan untuk mendukung **resilient C2** dan **collaborative autonomy** bagi sistem attritable lintas domain. ([Unit Inovasi Pertahanan](#))

Bagi Indonesia, inti pelajarannya adalah ini:

- **resilience lebih penting daripada kemewahan;**
- **jumlah yang relevan lebih penting daripada simbol kecanggihan;**
- dan **daya tahan sistem saat diganggu** lebih penting daripada performa sempurna di kondisi ideal.

25.4. Indonesia harus mulai dari yang bisa dibuat, diuji, dan diproduksi

Dari seluruh pembahasan buku ini, mungkin inilah kalimat yang paling penting untuk Indonesia: **kita harus mulai dari yang bisa dibuat, diuji, dan diproduksi**. Bukan dari fantasi industri besar yang terlalu dini. Bukan dari obsesi pada model paling besar. Bukan dari platform yang hanya bagus di pameran. Naskah buku ini sudah memberi diagnosis yang sangat jujur: Indonesia terlalu *platform-centric*, lemah di elektronik pertahanan, lemah di *mission software* dan *data pipeline*, lambat dalam pengadaan, dan terlalu sering punya **prototipe banyak, produksi sedikit**.

Itu sebabnya, jalan yang lebih sehat adalah memulai dari:

- drone kecil taktis,
- *counter-drone*,
- radio dan *mesh*,
- *mission computer*,
- kamera, IMU, dan navigasi tahan gangguan,
- pusat data drone,
- *test range* nasional,
- serta desain modular yang bisa diperbaiki dan diulang.

Pendekatan seperti ini tidak glamor. Tetapi justru lebih serius. Negara yang ingin membangun kapasitas tidak boleh jatuh cinta pada simbol. Ia harus jatuh cinta pada **rantai kemampuan**: desain, uji, perbaikan, produksi, pemeliharaan, dan pembelajaran.

Jadi, penutup ini harus menolak dua ilusi sekaligus:

- ilusi bahwa Indonesia harus langsung mengejar puncak teknologi dunia;
- dan ilusi bahwa membeli dari luar sudah cukup untuk membuat kita siap.

Yang lebih mendesak adalah **membangun blok-blok kemampuan yang benar-benar bisa hidup di dalam negeri**.

25.5. Bukan mengejar yang paling canggih, tetapi yang paling berguna

Buku ini sejak awal sudah mengingatkan bahwa AI militer terlalu sering dibaca dari narasi teknologi, bukan logika perang. Itulah sebabnya, penutupnya harus kembali ke prinsip yang sama: **Indonesia tidak perlu pertama-tama mengejar yang paling canggih. Indonesia harus mengejar yang paling berguna.**

“Paling berguna” di sini artinya:

- mempercepat ISR,
- membantu C2,
- memperkuat logistik,
- menaikkan kesiapan,
- mendukung EW dan *counter-drone*,
- menjaga wilayah maritim,
- dan tetap bekerja saat konektivitas, GNSS, atau *supply chain* terganggu.

AI yang seperti itu mungkin tidak terlihat spektakuler. Tetapi justru itulah bentuk AI militer yang paling waras untuk negara kepulauan seperti Indonesia. Pelajaran resmi dan lapangan sama-sama menunjukkan hal ini: AI paling bernilai sering justru muncul sebagai penguat organisasi, pengolah data, dan alat bantu keputusan, bukan sekadar “robot pembunuh”. ([Reuters](#))

Karena itu, ukuran keberhasilan Indonesia ke depan bukan:

- siapa yang paling sering memakai kata AI,
- siapa yang paling cepat mengumumkan proyek,
- atau siapa yang paling mewah spesifikasinya.

Ukuran yang lebih jujur adalah:

- **apa yang benar-benar dipakai,**
- **apa yang benar-benar diuji,**
- **apa yang benar-benar diproduksi,**
- dan **apa yang benar-benar menambah daya tahan organisasi.**

25.6. Pertanyaan terakhir: siapa yang berani memulai sekarang?

Akhirnya, semua strategi kembali ke satu pertanyaan yang tidak teknis tetapi sangat menentukan: **siapa yang berani memulai sekarang?**

Pertanyaan ini penting karena Indonesia sebenarnya tidak kekurangan topik. Kita punya banyak diskusi, seminar, prototipe, riset, dan istilah besar. Yang sering kurang justru:

- keputusan untuk memilih prioritas,
- keberanian untuk memulai dari yang kecil tetapi nyata,
- kemauan untuk memotong birokrasi lama,
- dan disiplin untuk terus belajar dari uji dan kegagalan.

Maka pertanyaan penutup buku ini bukan lagi “apakah AI militer penting?” Jawabannya sudah jelas: penting. Pertanyaan sesungguhnya adalah:

- **siapa di negara ini yang mau bertindak sebagai pengarah?**
- **siapa di TNI yang mau menjadi pengguna awal dan penguji keras?**
- **siapa di kampus yang mau pindah dari jurnal ke *reference design*?**
- **siapa di industri yang mau tumbuh dari vendor ke mitra strategis?**
- **dan siapa di birokrasi yang berani mengganti kebiasaan lama dengan ritme yang lebih cepat?**

Di sinilah arti kalimat penutup buku ini:

Indonesia tidak bisa lagi menjadi penonton.

Menjadi penonton berarti:

- kagum pada perang drone orang lain,
- kagum pada model AI orang lain,
- kagum pada industri pertahanan orang lain,
- lalu tetap lambat membangun kemampuan sendiri.

Sebaliknya, mulai sekarang berarti:

- memilih yang paling berguna,
- mengujinya dengan jujur,
- memproduksi dalam skala yang masuk akal,
- memperbaikinya terus,
- dan mengubah pembelajaran itu menjadi kapasitas nasional.

Penutup akhir

Buku ini pada dasarnya membawa kita ke satu kesimpulan besar: **AI militer adalah ujian organisasi nasional**. Ukraina menunjukkan bahwa **kecepatan belajar** dapat mengubah negara yang tertekan menjadi laboratorium inovasi perang. ([Reuters](#)) Iran menunjukkan bahwa **resilience, volume, dan “cukup baik”** bisa menciptakan efek strategis yang besar. Indonesia, karena itu, tidak perlu mulai dari yang paling canggih. Indonesia harus mulai dari yang **paling bisa dibuat, diuji, dan diproduksi**, lalu menaikkan kemampuannya secara bertahap.

Maka pertanyaan terakhir bukan lagi pertanyaan teknologi. Ia adalah pertanyaan politik, organisasi, dan keberanian:

apakah Indonesia akan terus menonton perubahan ini dari jauh, atau mulai membangun kapasitasnya sendiri sekarang, meski dari langkah yang kecil tetapi nyata?

Itulah pertanyaan yang tidak bisa lagi ditunda.

Lampiran 1. Kronologi Singkat 2016–2026: AI, Maven, Ukraina, Iran, dan Perang Drone

Tahun	Peristiwa kunci	Arti strategis singkat
2016	Fase pra-Maven: AI militer belum menjadi arsitektur besar yang dilembagakan; titik berat masih tersebar pada otomasi, ISR, dan eksperimen AI/ML yang belum terintegrasi penuh di level kementerian pertahanan.	Tahun ini berguna sebagai titik awal dekade percepatan : sebelum AI militer menjadi program besar, institusi pertahanan besar masih berada pada fase awal konsolidasi gagasan. Momentum institusional yang tegas baru terlihat mulai 2017–2018 melalui Project Maven dan JAIC. (Dodcio)
2017	Project Maven dibentuk melalui memo pembentukan <i>Algorithmic Warfare Cross-Functional Team</i> pada 25 April 2017. Fokus awalnya adalah membantu analis memproses video drone dan citra ISR dalam skala besar.	Ini adalah titik lahir institusional AI militer modern di AS: AI tidak lagi dibaca sekadar riset, tetapi mulai dipasang langsung ke rantai ISR dan analisis target. (Dodcio)
2018	JAIC (Joint Artificial Intelligence Center) berdiri pada Juni 2018 untuk mempercepat pengiriman kapabilitas AI dan menyatukan arah AI di Departemen Pertahanan AS.	Dari sini AI militer bergerak dari proyek percontohan ke tata kelola kelembagaan . Artinya, negara mulai sadar bahwa AI perlu kantor pusat, prioritas, dan mekanisme adopsi lintas matra. (U.S. Department of War)
2019	Strategi AI DoD 2018 dipublikasikan ringkas pada Februari 2019 ; JAIC diposisikan sebagai pusat percepatan kapabilitas AI. Pada tahun yang sama, pejabat DoD menjelaskan perbedaan peran Maven sebagai <i>product delivery pipeline</i> dan JAIC sebagai pusat keunggulan AI.	Tahun ini penting karena AI militer mulai dibingkai sebagai kapabilitas departemen , bukan eksperimen intelijen semata. Maven menjadi jalur produk; JAIC menjadi pusat orkestrasi. (U.S. Department of War)
2020	DoD mengadopsi 5 prinsip etika AI: <i>responsible, equitable, traceable, reliable, governable</i> . Pada saat yang sama, perang Nagorno-Karabakh 2020 menarik perhatian luas terhadap efektivitas drone kecil dan murah.	Dua arus besar bertemu: AI butuh tata kelola , dan drone murah mengubah ekonomi perang . Sejak titik ini, diskusi AI militer tidak lagi bisa dipisahkan dari etika, <i>targeting</i> , dan perang drone. (U.S. Department of War)

- 2021** **Memo implementasi *Responsible AI*** DoD menekankan penerapan prinsip etika AI ke proses akuisisi dan penggunaan. Pada Desember 2021, **CDAO diumumkan** untuk menyatukan data, AI, dan digital. AI militer naik satu tingkat: bukan lagi hanya “boleh atau tidak”, tetapi **bagaimana dioperasikan secara bertanggung jawab dan siapa yang memimpin integrasinya.** ([U.S. Department of War](#))
- 2022** **CDAO mencapai *initial operating capability*** pada 1 Februari 2022. Pada musim gugur 2022, **drone Shahed buatan Iran mulai dipakai Rusia secara luas** dalam perang Ukraina; Ukraina kemudian menurunkan hubungan diplomatik dengan Iran. Tahun 2022 menandai dua hal sekaligus: **institusionalisasi AI militer di AS dan normalisasi perang drone murah jarak jauh** di Ukraina. Sejak sini, Iran dan Shahed masuk kuat ke percakapan global tentang *volume warfare*. ([U.S. Department of War](#))
- 2023** **CDAO merayakan tahun pertama** dan menegaskan perannya sebagai pusat kebijakan data dan AI DoD. Pada Agustus 2023, **Task Force Lima** dibentuk untuk menilai penggunaan *generative AI* di DoD. Pada 2023 juga, **Replicator** diumumkan sebagai upaya mempercepat ribuan sistem otonom murah. 2023 menunjukkan pergeseran dari AI analitik klasik ke **AI generatif dan otonomi massal**. Pada saat yang sama, negara mulai terang-terangan mengejar **skala dan tempo**. ([U.S. Department of War](#))
- 2023** **Ukraina mempercepat lokalisasi komponen drone** karena khawatir bergantung pada komponen asing, terutama dari China. Ini penting untuk Indonesia karena menegaskan bahwa perang drone bukan hanya soal airframe, tetapi juga **rantai pasok, komponen, dan kedaulatan elektronik.** ([Reuters](#))
- 2023** **Deklarasi politik tentang penggunaan militer AI dan otonomi secara bertanggung jawab** dipublikasikan dan didorong AS pada akhir 2023. Artinya, AI militer kini bukan hanya urusan teknis atau nasional, tetapi mulai masuk ke **pembentukan norma internasional.** ([State.gov](#))
- 2024** **Replicator mulai diumumkan tranche awalnya**, dan Reuters melaporkan Switchblade-600 sebagai pembelian pertama yang diumumkan secara publik di bawah inisiatif tersebut. Tahun ini menandai pergeseran dari wacana “AI besar” ke **sistem otonom attritable dalam jumlah banyak**. Fokusnya bukan simbol, tetapi *fielding* cepat. ([Reuters](#))
- 2024** **Ukraina menargetkan produksi 1 juta drone FPV pada 2024**; Reuters juga menyoroti bagaimana drone mengubah ekonomi perang di Ukraina. Ini menegaskan bahwa perang drone masuk ke fase **industrialisasi massal**, bukan lagi eksperimen unit khusus.

		Volume menjadi faktor strategis. (Reuters)
2024	Reuters melaporkan Ukraina telah mengumpulkan lebih dari 2 juta jam video perang sejak 2022 untuk melatih model AI bagi identifikasi target, evaluasi serangan, dan keputusan taktis.	Ini adalah salah satu bukti paling jelas bahwa data tempur menjadi aset strategis . AI militer yang matang lahir dari <i>battlefield data</i> , bukan sekadar <i>demo dataset</i> . (Reuters)
2024	Reuters melaporkan Rusia telah meluncurkan 8.060 drone Iran-design sejak invasi dimulai , menurut data Ukraina, terutama Shahed.	Angka ini memperjelas bahwa model Iran–Rusia adalah perang saturasi biaya rendah : bukan harus paling presisi, tetapi cukup murah dan cukup banyak untuk menguras pertahanan lawan. (Reuters)
2024	DoD merilis strategi untuk menghadapi ancaman sistem nirawak dan menegaskan bahwa proliferasi UAS telah mengubah karakter konflik.	Ini menunjukkan bahwa drone tidak lagi dianggap pelengkap, tetapi ancaman inti dan domain utama inovasi serta pertahanan . (Reuters)
2025	Iran menerima batch 1.000 drone baru menurut laporan Reuters yang mengutip Tasnim; pada saat yang sama, Reuters menyoroti murahnya drone Shahed dan ketimpangan biaya antara penyerang dan pencegat.	Tahun ini memperkuat pelajaran Iran: resilience, volume, dan biaya rendah bisa menghasilkan tekanan strategis yang tidak seimbang bagi lawan. (Reuters)
2025	Ukraina dan ekosistem drone-nya mulai dilihat sebagai basis ekspor dan pembelajaran global , terutama di bidang <i>interceptor drone</i> dan <i>counter-UAS</i> .	Artinya, perang tidak hanya menghancurkan; ia juga membentuk industri pertahanan baru berbasis data, iterasi cepat, dan umpan balik lapangan. (Reuters)
2026	Brave1 Dataroom diluncurkan di Ukraina sebagai lingkungan aman untuk melatih dan menguji model AI dengan data militer nyata, bekerja sama dengan Palantir menurut laporan <i>Defense News</i> .	Ini menandai fase baru: dataset perang dikurasi menjadi infrastruktur AI pertahanan . Perang tidak hanya menghasilkan rekaman, tetapi juga platform latihan model . (Defense News)
2026	Reuters melaporkan Iran meluncurkan lebih dari 1.000 drone pada pekan pertama konflik 2026 dan diperkirakan mampu memproduksi sekitar 10.000 drone per bulan .	Ini memperlihatkan secara telanjang logika Iran: kuantitas industrial + biaya rendah + keberlanjutan produksi . Bagi pembaca Indonesia, ini adalah pelajaran tentang <i>industrial</i>

		<i>resilience</i> , bukan sekadar soal teknologi tinggi. (Reuters)
2026	Reuters melaporkan Pentagon akan mengadopsi Maven milik Palantir sebagai <i>core military system</i> , menjadikannya <i>program of record</i> dengan pendanaan jangka panjang.	Ini menutup satu siklus penting: Project Maven yang lahir pada 2017 sebagai tim algoritmik kini berubah menjadi sistem inti militer . Artinya, AI yang bertahan bukan yang paling heboh, tetapi yang benar-benar masuk ke sistem organisasi dan operasi. (Reuters)
2026	Militer Jerman mulai terang-terangan mengejar AI untuk mempercepat keputusan perang, sambil menekankan bahwa AI tidak menggantikan penilaian manusia.	Ini menunjukkan bahwa pelajaran Ukraina telah menyebar: negara-negara Eropa kini melihat AI sebagai alat untuk memecah siklus keputusan lawan , bukan sekadar <i>back-office tool</i> . (Reuters)

Benang merah kronologi

Kalau tabel ini ingin dibaca dalam satu nafas, pola besarnya sangat jelas.

- **2017–2021** adalah fase **institusionalisasi AI militer**: Maven, JAIC, prinsip etika, lalu CDAO. ([Dodcio](#))
- **2022–2024** adalah fase **normalisasi perang drone murah dan perang data**: Shahed di Ukraina, industrialisasi FPV, dan pemanfaatan jutaan jam video tempur untuk AI. ([Reuters](#))
- **2025–2026** adalah fase **skala, industrial resilience, dan normalisasi AI sebagai sistem inti**: Brave1 Dataroom, produksi drone Iran dalam volume sangat besar, dan Maven menjadi *program of record*. ([Defense News](#))

Kalimat penutup lampiran

Pelajaran paling penting dari 2016–2026 adalah ini: AI militer tidak berkembang terutama sebagai perlombaan model terbesar, tetapi sebagai gabungan antara institusi, data tempur, drone murah, volume produksi, dan *loop* belajar yang cepat. Itulah sebabnya kronologi ini sangat penting untuk argumen buku secara keseluruhan.

Lampiran 2. Matriks Aktor: negara, militer, integrator, startup, kampus, industri

Aktor	Peran utama	Kontribusi kunci	Risiko bila lemah / salah arah	Prioritas untuk Indonesia
Negara	Pengarah strategi, pembentuk pasar, penentu prioritas nasional	Menetapkan arah teknologi pertahanan, memilih area prioritas, membentuk permintaan awal, menyediakan regulasi, anggaran, dan tata kelola	Ekosistem terpecah, industri bingung, inovasi hidup sebagai proyek, bukan kapasitas nasional	Tetapkan prioritas jelas: drone kecil, <i>counter-drone</i> , EW, <i>mission systems</i> , maritim, pusat uji, data, dan desain modular
Militer / TNI	Pengguna, penguji, dan sumber umpan balik operasional	Menguji sistem di kondisi nyata, memberi umpan balik ke pengembang, menentukan apa yang benar-benar berguna di lapangan	Teknologi berhenti di demo, sistem tidak cocok dengan operasi, budaya belajar tidak tumbuh	Jadikan satuan operasional sebagai co-developer , bukan penerima pasif
Kemhan / birokrasi pertahanan	Arsitek ekosistem dan penghubung lintas aktor	Menyatukan kampus, industri, BUMN, startup, dan TNI ke dalam kerangka prioritas, pengujian, dan pendanaan	Pengadaan lambat, riset tidak menyeberang ke operasi, tiap aktor bergerak sendiri-sendiri	Bangun mekanisme cepat untuk prototipe–uji–pebaikan–produksi awal
Integrator	Penyatu data, model, sensor, antarmuka, dan workflow operasional	Mengubah komponen yang terpisah menjadi sistem yang bisa dipakai komandan dan analis; menjahit cloud, data, AI, tampilan operasional, dan deployment	Data tetap tercerai-berai, AI hanya menjadi modul terpisah, keputusan tidak terhubung ke operasi	Dorong integrator lokal/nasional yang mampu menyatukan data, AI, C2, drone, dan EW, bukan sekadar menjual <i>software</i>

Startup	Sumber inovasi cepat dan spesialisasi teknis	Mengembangkan subsistem lincah: autopilot, radio, <i>payload</i> , <i>edge AI</i> , visi mesin, <i>counter-drone</i> , <i>firmware</i> , <i>ground control</i>	Inovasi mati di lomba atau inkubasi, tidak pernah masuk pasar pertahanan nyata	Beri kontrak kecil tapi nyata , akses ke masalah operasional, dan jalur naik ke produksi awal
UKM teknologi	Pemasok fleksibel, bengkel inovasi, pembuat komponen dan integrasi kecil	Membuat modul, suku cadang, papan elektronik, <i>repair</i> , <i>retrofit</i> , dan substitusi komponen	Industri terlalu tergantung pada pemain besar; <i>repairability</i> dan adaptasi lapangan lemah	Masukkan UKM ke rantai pasok pertahanan digital sejak awal
Kampus	Sumber pengetahuan, talenta, dan <i>reference design</i>	Menghasilkan desain yang bisa diproduksi, menaikkan TRL, melahirkan <i>spin-off</i> , mengembangkan laboratorium untuk RF, radar, kontrol, visi, <i>embedded systems</i> , dan <i>chip design</i>	Kampus kuat di jurnal tetapi lemah di operasi; prototipe tidak pernah matang; talenta tidak siap sistem nyata	Geser dari publikasi ke <i>reference design</i> dan pengujian yang relevan
BUMN pertahanan	Integrator besar, jangkar industri, dan penghubung dengan negara	Menjaga skala program, integrasi lintas vendor, standarisasi minimum, sertifikasi, dan kesinambungan produksi	Monopoli inovasi, lambat bergerak, menutup ruang pemain kecil, menjadi terlalu proyek-sentris	Posisikan BUMN sebagai orkestra ekosistem , bukan pemain tunggal
Industri nasional non-BUMN	Produsen, pemasok subsistem, dan penguat kapasitas manufaktur	Memproduksi batch kecil hingga volume menengah, mengembangkan komponen, <i>repair</i> , <i>maintenance</i> , dan substitusi	Ketergantungan impor tetap tinggi, produksi sedikit, transisi dari prototipe ke batch operasional gagal	Dorong produksi rendah volume yang berulang , bukan satu kali proyek

Perusahaan AI / model / platform	Penyedia lapisan analitik, model, dan antarmuka kognitif	Membantu sintesis data, analisis teks, <i>workflow intelligence</i> , pencarian pola, dan dukungan keputusan	Hype model menutupi masalah data, governance, dan integrasi; ketergantungan vendor meningkat	Tempatkan model sebagai lapisan pendukung , bukan pusat tunggal ekosistem
Cloud / platform data	Fondasi komputasi, penyimpanan, dan integrasi data	Menyediakan lingkungan untuk analitik, <i>deployment</i> , dan fusi data multi-sumber	AI tidak bisa diskalakan, data tetap silo, sistem tidak bisa hidup lintas domain	Bangun fondasi data dan komputasi yang aman, modular, dan tidak rapuh
Pusat uji / test range	Validator teknis dan operasional	Menguji <i>swarm</i> , EW, navigasi <i>GPS-denied</i> , maritim otonom, <i>counter-drone</i> , dan interoperabilitas	Sistem lolos demo, gagal di lapangan; standar mutu tidak terbentuk	Bangun pusat uji nasional sebagai mesin verifikasi ekosistem
Regulator / auditor / pengawas	Penjaga akuntabilitas, keamanan, dan kepatuhan	Menjaga keamanan, pengendalian, dokumentasi, dan tata kelola AI serta penggunaan sistem	Inovasi liar, akuntabilitas kabur, kepercayaan publik dan institusi melemah	Bangun tata kelola yang cepat tetapi tetap bisa diaudit

Matriks hubungan antar aktor

Agar lampiran ini lebih berguna untuk pembaca buku, berikut versi kedua yang menekankan **hubungan kerja antar aktor**, bukan hanya fungsi tunggal. Ini penting karena naskah buku berkali-kali menegaskan bahwa AI pertahanan harus dibaca sebagai **ekosistem** yang terdiri dari data, cloud, platform, integrator, komando, dan pengguna operasional.

Relasi	Yang diberikan	Yang diterima	Nilai strategis	Risiko jika relasi buruk
Negara ↔ Militer	Negara memberi arah, anggaran, aturan, dan permintaan awal	Militer memberi kebutuhan riil, umpan balik, dan evaluasi penggunaan	Menjaga agar pengadaan relevan dengan operasi	Negara membeli yang tidak dibutuhkan; militer menerima alat yang tidak cocok
Negara ↔ Kampus	Negara memberi prioritas riset, dana, dan akses masalah strategis	Kampus memberi desain, talenta, <i>reference design</i> , dan kenaikan TRL	Mengubah ilmu menjadi kapasitas nasional	Kampus sibuk di jurnal, negara kekurangan desain yang siap ditransisikan
Negara ↔ Industri	Negara memberi pasar awal, kepastian arah, dan kontrak	Industri memberi produksi, <i>repair</i> , substitusi, dan skala	Membentuk basis industri pertahanan digital	Industri hidup dari proyek sesaat, bukan kapasitas jangka panjang
Militer ↔ Startup / UKM	Militer memberi masalah nyata dan umpan balik lapangan	Startup/UKM memberi inovasi cepat dan subsistem lincah	Mempercepat siklus belajar	Inovasi tidak pernah masuk operasi
Kampus ↔ Industri	Kampus memberi desain dan talenta	Industri memberi manufaktur, integrasi, dan umpan balik produksi	Menjembatani riset ke produk	Prototipe mati di laboratorium
Integrator ↔ Semua aktor teknis	Integrator menjahit data, model, antarmuka, sensor, dan <i>workflow</i>	Menerima komponen, data, dan kebutuhan operasional	Mengubah potongan-potongan teknologi menjadi sistem tempur	Semua aktor bekerja, tetapi sistem tetap tidak terhubung

BUMN ↔ Startup / UKM / vendor lokal	BUMN memberi akses program besar, integrasi, dan sertifikasi	Startup/UKM memberi inovasi, subsistem, dan kelincahan	Memperluas kapasitas ekosistem nasional	BUMN menjadi bottleneck; startup mati sebelum tumbuh
Pusat uji ↔ Seluruh ekosistem	Pusat uji memberi validasi, data performa, dan <i>stress test</i>	Semua aktor memberi sistem, desain, dan skenario penggunaan	Menjaga kualitas dan kejujuran teknis	Ekosistem hidup dari klaim, bukan bukti

Ringkasan kunci

Lampiran ini bisa dibaca dengan satu kesimpulan sederhana:

- **negara memberi arah dan pasar,**
- **militer memberi realitas operasional,**
- **integrator memberi penyatuan sistem,**
- **startup dan UKM memberi kecepatan inovasi,**
- **kampus memberi desain dan talenta,**
- **industri memberi produksi, perbaikan, dan skala.**

Kalau salah satu hilang, ekosistem menjadi timpang. Tetapi kalau semuanya bergerak dalam ritme yang sama, maka Indonesia bisa mulai membangun **AI militer dan pertahanan digital sebagai kapasitas nasional, bukan sekadar kumpulan proyek.**

Lampiran 3. Matriks Risiko: teknis, operasional, etis, hukum, geopolitik, *supply chain*

Kategori risiko	Bentuk risiko utama	Dampak strategis	Indikator dini	Mitigasi awal yang disarankan
Teknis	Model salah klasifikasi, <i>sensor fusion</i> gagal, data buruk, navigasi rapuh, <i>software bug</i> , latensi tinggi, sistem gagal saat jamming atau GNSS terganggu	Keputusan salah, misi gagal, salah sasaran, hilangnya kepercayaan operator	Akurasi turun di lapangan, hasil uji tidak konsisten, performa jatuh di cuaca/medan keras, terlalu banyak <i>manual override</i>	Uji keras di kondisi nyata, <i>red teaming</i> , <i>logging</i> , mode degradasi, validasi lintas-sensor, <i>fallback mode</i> non-AI
Teknis	Ketergantungan pada satu model, satu vendor, satu <i>cloud</i> , atau satu komponen inti	Sistem rapuh, sulit diperbaiki, sulit diganti, rentan <i>cut-off</i>	Tidak ada alternatif vendor, dokumentasi minim, antarmuka tertutup	Desain modular, <i>second source</i> , standardisasi terbuka terbatas, dokumentasi teknis minimum
Operasional	Sistem tidak cocok dengan ritme operasi satuan	Teknologi berhenti di demo, dipakai sebentar lalu ditinggalkan	Operator enggan memakai sistem, beban kerja naik, antarmuka membingungkan	Libatkan satuan sejak awal sebagai <i>co-developer</i> , uji dengan skenario operasional, iterasi cepat
Operasional	Terlalu percaya pada mesin (<i>automation bias</i>)	Komando menjadi stempel, kesalahan mesin dipercepat	Operator jarang menantang keluaran sistem, rekomendasi AI diterima mentah	Latihan <i>human-in-the-loop</i> , pelatihan batas sistem, SOP untuk verifikasi manusia

Operasional	Sistem hanya bagus di kondisi ideal	Saat perang nyata, performa runtuh	Uji dilakukan hanya di lingkungan nyaman, tidak ada latihan <i>GPS-denied</i> atau EW	Latihan sejak awal di kondisi jamming, spoofing, putus link, data parsial
Etis	AI dipakai tanpa kendali manusia yang bermakna	Hilangnya akuntabilitas moral dan komando	Tidak jelas siapa memutuskan, manusia hanya klik persetujuan formal	Tetapkan batas fungsi AI, jaga otoritas keputusan penggunaan kekuatan tetap pada manusia
Etis	Bias data atau bias desain	Kelompok, objek, atau pola tertentu lebih sering salah dibaca	Banyak <i>false positive</i> pada lingkungan tertentu, anomali berulang	Audit data, uji lintas konteks, evaluasi bias, pembatasan penggunaan
Etis	Sistem opak dan sulit dipahami	Sulit dipercaya, sulit diperbaiki, sulit diaudit	Operator tidak bisa menjelaskan mengapa sistem memberi rekomendasi tertentu	Bangun <i>explainability</i> secukupnya, dokumentasi model, jejak keputusan, audit berkala
Hukum	Penggunaan AI mengganggu prinsip <i>distinction</i>	Risiko menyerang sasaran sipil atau objek sipil	Sistem sulit membedakan target militer dari sipil di lingkungan padat	Batasi peran AI pada dukungan, bukan pengganti penilaian hukum dan operasional manusia
Hukum	Penggunaan AI mengaburkan <i>proportionality</i>	Kerugian sipil bisa berlebihan dibanding keuntungan militer	Penilaian dampak sipil terlalu disederhanakan menjadi angka mesin	Wajibkan penilaian komandan/manusia, SOP verifikasi dampak sipil, <i>no-strike safeguards</i>

Hukum	Tanggung jawab kabur saat sistem salah	Sulit investigasi, sulit akuntabilitas, legitimasi turun	Tidak ada log, tidak ada rantai kewenangan jelas	Tetapkan matriks tanggung jawab: pengembang, integrator, operator, komando
Risiko sipil	Salah sasaran, <i>false positive</i> , atau salah tafsir konteks	Korban sipil, kerusakan infrastruktur, krisis legitimasi	Banyak alarm palsu, salah identifikasi berulang, uji lapangan buruk	Uji di lingkungan sipil-padatan, verifikasi multi-sumber, pembatasan peran pada konteks berisiko tinggi
Risiko sipil	Infrastruktur sipil terseret ke ekosistem perang digital	Eskalasi dampak ke listrik, komunikasi, pelabuhan, rumah sakit, logistik	Ketergantungan tinggi pada jaringan sipil tanpa proteksi	Pisahkan lapisan kritis, siapkan <i>contingency plan</i> , atur batas integrasi sipil-militer
Geopolitik	Ketergantungan pada vendor, platform, atau <i>cloud</i> asing	Tekanan politik, pembatasan ekspor, <i>service denial</i> , <i>lock-in</i>	Lisensi tidak stabil, akses API berubah, komponen sensitif sulit diperoleh	Diversifikasi pemasok, desain yang bisa dipindah, kemampuan lokal untuk integrasi inti
Geopolitik	Perlombaan otonomi dan eskalasi regional	Negara ikut mengejar simbol, bukan kebutuhan nyata	Anggaran tersedot ke proyek glamor, bukan fondasi	Pegang roadmap bertahap, fokus pada fungsi yang paling berguna untuk Indonesia
Geopolitik	Keterlibatan perusahaan besar dalam ekosistem perang	Kepentingan komersial mempengaruhi arsitektur dan ketergantungan	Ekosistem terlalu dibentuk oleh vendor, bukan kebutuhan negara	Negara pegang arsitektur, standar, dan hak audit minimum

Supply chain	Komponen kritis putus atau dibatasi	Produksi berhenti, <i>maintenance</i> lumpuh, batch operasional macet	Lead time panjang, stok menipis, komponen tunggal sulit diganti	<i>Stockpile</i> komponen kritis, <i>second source</i> , substitusi desain, inventaris prioritas
Supply chain	Komponen palsu atau kualitas tidak seragam	Kegagalan sistem di lapangan, risiko keselamatan, menurunnya kepercayaan	Variasi performa besar antar batch, kegagalan dini, asal komponen tidak jelas	Sertifikasi pemasok, pengujian masuk, pelacakan batch, dokumentasi mutu
Supply chain	Ketergantungan pada bahan, baterai, RF, atau mikroelektronika tertentu	Sistem attritable tidak bisa diproduksi massal	Harga melonjak, pasokan tidak pasti, penggantian komponen merusak desain	Fokus pada desain modular, pengembangan alternatif lokal/regional, prioritas untuk komponen paling rapuh
Integrasi ekosistem	Data, sensor, AI, C2, dan drone tidak benar-benar terhubung	Banyak teknologi, sedikit efek tempur	Sistem bekerja sendiri-sendiri, tidak ada gambaran operasional bersama	Integrator nasional, standar antarmuka minimum, pusat data dan pusat uji nasional
Organisasi / birokrasi	Pengadaan lambat, uji lambat, inovasi kalah oleh administrasi	Negara tertinggal walau punya ide dan prototipe	Siklus keputusan panjang, prototipe menumpuk, produksi sedikit	Jalur cepat inovasi, kontrak kecil tapi nyata, uji-perbaikan-produksi berulang

Matriks ringkas: tingkat prioritas risiko untuk Indonesia

Risiko	Tingkat prioritas	Mengapa penting untuk Indonesia	Respon minimum
Rapuh di elektronik, RF, navigasi, dan komponen inti	Sangat tinggi	Karena titik lemah Indonesia ada pada elektronik pertahanan, <i>mission software</i> , dan <i>supply chain</i>	Desain modular, <i>stockpile</i> , <i>second source</i> , <i>reference design</i>
Pengadaan lambat, prototipe banyak, produksi sedikit	Sangat tinggi	Karena tanpa perubahan ritme, semua roadmap tinggal dokumen	Jalur cepat uji–perbaikan–kontrak kecil
Ketergantungan vendor / platform asing	Sangat tinggi	Karena AI pertahanan mudah jatuh ke <i>lock-in</i> dan <i>cut-off</i>	Arsitektur terbuka terbatas, hak audit, diversifikasi pemasok
Salah sasaran dan dampak sipil	Sangat tinggi	Karena legitimasi, hukum, dan kepercayaan publik bisa runtuh cepat	Kendali manusia bermakna, verifikasi multi-sumber, audit
Sistem gagal di lingkungan EW / GPS-denied	Sangat tinggi	Karena perang nyata tidak memberi kondisi ideal	Latihan jamming, spoofing, dan mode degradasi sejak awal
AI opak dan tidak bisa diaudit	Tinggi	Karena tanpa jejak keputusan, tanggung jawab kabur	<i>Logging</i> , <i>traceability</i> , dokumentasi model dan keputusan
Bias data dan <i>automation bias</i>	Tinggi	Karena operator bisa terlalu percaya, atau model salah baca konteks	Pelatihan, audit bias, SOP verifikasi manusia
Eskalasi geopolitik akibat salah baca atau deception	Tinggi	Karena sistem cepat dapat mempercepat salah dan reaksi berantai	<i>Red teaming</i> , latihan deception, pembatasan fungsi otomatis

Industri lokal tidak tumbuh berkelanjutan	Tinggi	Karena tanpa kapasitas produksi dan repair, ketahanan nasional tipis	Kontrak berulang, dukung startup/UKM, fokus produksi batch nyata
Birokrasi lama menghambat adopsi	Tinggi	Karena melawan perubahan bukan hanya teknologi, tetapi organisasi	Potong rantai persetujuan, ukur hasil uji, bukan hanya dokumen

Ringkasan kunci

Matriks ini memperlihatkan satu pola besar.

- **Risiko teknis** bisa membuat sistem gagal.
- **Risiko operasional** bisa membuat sistem tidak dipakai.
- **Risiko etis dan hukum** bisa membuat sistem kehilangan legitimasi.
- **Risiko geopolitik dan *supply chain*** bisa membuat sistem tidak bertahan lama.
- **Risiko organisasi** bisa membunuh semuanya bahkan sebelum teknologi matang.

Itulah sebabnya, untuk Indonesia, risiko terbesar bukan hanya “AI salah”, tetapi **negara membangun sistem yang tidak tahan gangguan, tidak bisa diaudit, terlalu tergantung pada luar, dan terlalu lambat diperbaiki**. Itu juga sejalan dengan arah keseluruhan buku Anda. ([U.S. Department of War](#))

Lampiran 4. Metodologi Verifikasi Sumber dan Anti-Halusinasi

Unsur metodologi	Prinsip kerja	Cara pakai dalam buku ini	Tanda bahaya / hal yang harus dicurigai
1. Hirarki sumber	Sumber tidak diperlakukan setara. Dokumen resmi negara, regulasi, memo, strategi, dan data primer diletakkan di atas; lalu analisis lembaga kredibel / think tank / jurnal ; lalu laporan media kredibel ; paling bawah klaim perusahaan, unggahan promosi, dan propaganda .	Klaim tentang struktur resmi, kebijakan, kontrak, organisasi, dan doktrin diprioritaskan dari dokumen pemerintah / militer / lembaga resmi . Klaim lapangan diverifikasi silang dengan media kredibel dan, bila ada, dokumen pendukung lain.	Bila satu klaim besar hanya hidup di siaran pers vendor, akun media sosial, atau media partisan , klaim itu tidak dijadikan fondasi utama . DoD sendiri menekankan pentingnya AI yang traceable, reliable, dan governable , yang secara metodologis menuntut jejak sumber dan tata kelola yang jelas. (U.S. Department of War)
2. Pisahkan fakta, analisis, promosi, propaganda, inferensi	Setiap pernyataan harus dikategorikan: fakta terkonfirmasi, analisis, klaim promosi, narasi propaganda , atau inferensi penulis .	Dalam penulisan, fakta dipisahkan dari tafsir. Analisis dipakai untuk membantu membaca makna strategis. Inferensi tetap boleh dipakai, tetapi harus ditulis sebagai inferensi , bukan fakta mentah.	Bahaya utama adalah ketika bahasa promosi atau narasi propaganda menyamar sebagai fakta. Naskah buku ini sendiri sudah mengingatkan perlunya disiplin membedakan kategori-kategori itu.
3. Aturan dua-sumber untuk klaim penting	Klaim yang sangat menentukan sebaiknya didukung minimal dua sumber berbeda , idealnya dari jenis sumber yang berbeda.	Misalnya: satu klaim organisasi/program diverifikasi dari dokumen resmi , lalu disilang dengan media kredibel atau analisis sekunder.	Bila klaim penting hanya muncul sekali dan tidak bisa disilang, klaim itu ditulis sebagai indikatif , bukan konklusif.

4. Utamakan fungsi operasional, bukan hype	Klaim teknologi dibaca dari apa yang benar-benar dapat dibuktikan secara operasional , bukan dari istilah besar atau nama model.	Buku ini menilai AI militer dari hubungannya dengan ISR, C2, logistik, EW, anti-drone, maritim, data, dan keputusan , bukan dari sensasi model terbaru.	Istilah seperti “AI revolusioner”, “game-changing”, “otak perang”, atau “sepenuhnya otonom” harus dicurigai bila tidak ada bukti penggunaan operasional yang jelas.
5. Bedakan “sedang diuji”, “dipakai terbatas”, dan “sudah operasional”	Banyak klaim AI pertahanan mencampuradukkan uji coba, pilot, dan kapabilitas operasional penuh .	Setiap teknologi sebaiknya ditandai statusnya: eksperimen, prototipe, terbatas, dipakai dalam operasi, atau sudah menjadi infrastruktur operasional .	Salah satu sumber halusinasi terbesar adalah memperlakukan pilot project seolah-olah kapabilitas yang sudah mapan .
6. Jangan menyimpulkan lebih jauh daripada bukti	Bila sumber hanya menunjukkan “AI membantu analisis”, jangan ditulis seolah “AI memilih target mematikan”.	Klaim ekstrem tentang AI yang memilih dan menyerang secara mandiri hanya ditulis bila ada dokumen resmi atau investigasi sangat kuat . Naskah buku ini sudah memberi peringatan langsung tentang hal ini.	Frasa yang harus dicurigai: “sepenuhnya otonom”, “tanpa manusia”, “langsung menentukan target”, bila tidak ada bukti kuat. ICRC juga menekankan bahwa sistem otonom dan AI di ranah militer menuntut penilaian yang sangat hati-hati karena isu kontrol manusia, prediktabilitas, dan kepatuhan IHL . (ICRC)

7. Wajib cek konteks hukum dan etika	Klaim kemampuan teknis tidak cukup; harus dibaca bersama IHL, distinction, proportionality, precautions, tanggung jawab komando.	Bila satu sistem tampak “hebat”, penulis tetap menanyakan: siapa mengendalikan, siapa bertanggung jawab, apa risiko sipilnya, dan apakah penggunaannya patuh hukum.	Bahaya muncul ketika buku atau artikel hanya membahas performa teknis tanpa membahas dampak sipil, akuntabilitas, dan batas penggunaan. Deklarasi politik AS juga menekankan penggunaan militer AI harus tetap berada dalam rantai komando yang bertanggung jawab dan sesuai hukum internasional yang berlaku. (State.gov)
8. Tulis ketidakpastian secara jujur	Bila data tidak lengkap, tulis sebagai belum pasti, indikatif, diperkirakan, atau masih diperdebatkan.	Buku ini lebih baik kehilangan sedikit sensasi daripada kehilangan integritas.	Anti-halusinasi gagal bila penulis memaksa semua hal tampak pasti padahal sumbernya tipis.
9. Gunakan AI sebagai alat bantu, bukan sumber otoritas	AI boleh membantu merangkum, memetakan istilah, dan menyusun draf, tetapi tidak boleh menjadi sumber final kebenaran.	Semua klaim penting tetap harus ditambahkan ke dokumen, laporan, atau sumber manusia yang dapat diverifikasi. Naskah buku sejak awal juga menegaskan penggunaan AI sebagai alat bantu, bukan pengganti penulis.	Halusinasi paling berbahaya terjadi ketika teks AI diperlakukan seolah fakta primer.

**10. Prinsip
akhir**

**Lebih baik hati-hati
daripada sensasional.
Lebih baik bertahap
daripada
melebih-lebihkan.**

Buku ini
menempatkan
verifikasi sebagai
bagian dari disiplin
analitis, bukan
lampiran formalitas.

Bila sebuah klaim
terlalu dramatis,
terlalu rapi, atau
terlalu cocok dengan
narasi yang ingin
dipercaya, justru di
situlah verifikasi
harus dibuat lebih
keras.

Catatan penggunaan

Tabel ini dapat dibaca dengan satu prinsip sederhana: **semakin besar konsekuensi sebuah klaim, semakin tinggi standar verifikasinya**. Itu sangat penting untuk topik AI militer, karena wilayah ini dipenuhi **campuran fakta resmi, promosi industri, narasi geopolitik, dan spekulasi teknologi**. Prinsip ini juga sejalan dengan penekanan resmi DoD pada AI yang dapat dilacak dan diaudit, serta perhatian ICRC pada kontrol manusia, prediktabilitas, dan kepatuhan terhadap IHL. ([U.S. Department of War](#))

Glossary

Istilah	Arti singkat	Relevansi dalam dokumen
AI Militer	Penggunaan <i>artificial intelligence</i> dalam fungsi pertahanan, bukan hanya senjata, tetapi juga analisis data, komando, logistik, dan keputusan.	Dokumen menegaskan AI militer bukan sekadar chatbot dan bukan hanya senjata otonom , melainkan sistem yang menghubungkan data, sensor, komando, drone, logistik, dan keputusan.
OODA Loop	Siklus Observe–Orient–Decide–Act : mengamati, memahami, memutuskan, lalu bertindak.	Diposisikan sebagai jantung perang modern ; keunggulan lahir dari kecepatan loop keputusan, bukan hanya dari senjata mahal.
C2 (Command and Control)	Sistem komando dan pengendalian operasi militer.	Menjadi fondasi bagi keputusan dan koordinasi tempur. Dalam dokumen, AI dipakai untuk mempercepat dan memperkuat C2.
C4ISR	<i>Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance</i> .	Kerangka inti perang modern yang menggabungkan komando, komunikasi, komputer, intelijen, pengawasan, dan pengintaian.
ISR	<i>Intelligence, Surveillance, Reconnaissance</i> — intelijen, pengawasan, dan pengintaian.	Salah satu bidang utama pemanfaatan AI: menyaring video, citra, telemetri, dan data sensor dalam jumlah besar.
Speed of Decision	Kecepatan menghasilkan keputusan yang relevan di tengah banjir data dan tekanan waktu.	Dokumen berulang kali menekankan bahwa perang modern ditentukan oleh kecepatan keputusan .
Decision Support	Sistem bantu keputusan yang memberi rekomendasi, prioritas, atau opsi tindakan kepada manusia.	AI militer dipandang bernilai ketika membantu komandan memahami situasi dan memilih tindakan lebih cepat.
Sensor Fusion / Data Fusion	Penggabungan data dari banyak sensor dan sumber menjadi gambaran situasi yang lebih utuh.	Penting karena medan tempur menghasilkan data sangat besar; AI membantu mengubah data mentah menjadi pemahaman operasional.

Targeting	Proses identifikasi, prioritas, dan penetapan target.	Dalam dokumen, AI dapat membantu prioritas target dan <i>course of action</i> , tetapi keputusan akhir tetap harus dijaga oleh manusia.
Course of Action (COA)	Opsi tindakan operasional yang dapat dipilih komandan.	AI diposisikan sebagai alat bantu menyiapkan opsi tindakan, bukan pengganti keputusan manusia.
Drone Warfare	Perang yang memanfaatkan sistem nirawak udara secara luas untuk ISR, serangan, <i>relay</i> , umpan, atau saturasi.	Salah satu tema besar buku; drone murah dipandang mengubah ekonomi perang.
UAV	<i>Unmanned Aerial Vehicle</i> — wahana udara tanpa awak.	Menjadi bagian sejarah dan evolusi menuju perang drone modern.
FPV Drone	<i>First-person view drone</i> , biasanya dikendalikan operator dengan pandangan langsung dari kamera drone.	Disebut sebagai bagian dari ekosistem drone murah, cepat, dan adaptif di perang modern.
Loitering Munition	Senjata/drone yang dapat berkeliling di area sasaran sebelum menyerang.	Mewakili pergeseran ke sistem yang lebih murah, fleksibel, dan responsif.
Swarm	Sekelompok sistem nirawak yang bergerak bersama, serentak, atau berlapis.	Dalam dokumen muncul sebagai bagian dari evolusi perang drone dan strategi saturasi.
Attritable Systems	Sistem yang relatif murah dan “boleh hilang” dalam operasi karena dapat diganti dalam jumlah besar.	Penting untuk logika perang modern: dari platform mahal ke sistem massal yang cukup baik dan bisa diproduksi banyak.
Autonomy / Otonomi	Kemampuan sistem menjalankan fungsi tertentu dengan intervensi manusia yang lebih sedikit.	Dokumen membedakan otonomi praktis/terbatas dari mitos “mesin sepenuhnya mandiri.”
Human-in-the-loop	Manusia tetap berada di dalam rantai keputusan, terutama dalam persetujuan tindakan penting.	Menjadi prinsip penting agar AI tidak mengambil alih keputusan mematikan tanpa kendali manusia.
Human-on-the-loop	Manusia mengawasi sistem yang bekerja lebih otomatis dan dapat campur tangan bila perlu.	Dibahas sebagai model yang lebih berisiko bila pengawasan lemah atau tempo terlalu cepat.

Meaningful Human Control	Kendali manusia yang nyata, bukan formalitas, atas sistem dan keputusan penting.	Terkait isu hukum, etika, akuntabilitas, dan penggunaan AI yang bertanggung jawab.
Project Maven	Program awal pertahanan AS untuk mempercepat analisis citra/video ISR dengan <i>computer vision</i> dan <i>machine learning</i> .	Dokumen menjadikannya contoh awal AI pertahanan yang fokus pada fungsi operasional, bukan sekadar hype.
CDAO	Struktur pertahanan AS yang menggabungkan data, AI, dan analitik dalam satu kantor terpadu.	Menunjukkan bahwa AI militer adalah ekosistem/infrastruktur , bukan produk tunggal.
JAIC	Inisiatif/kantor bersama AI dalam ekosistem pertahanan AS.	Disebut sebagai bagian dari pelembagaan AI pertahanan bersama Maven dan platform data.
Computer Vision	Teknik AI untuk membaca gambar dan video.	Menjadi teknologi utama dalam analisis ISR, identifikasi objek, dan pemrosesan video drone.
Machine Learning	Metode AI yang belajar pola dari data untuk klasifikasi, prediksi, atau deteksi.	Dibedakan dari otomasi biasa; penting untuk pengenalan pola dan analitik tempur.
Big Data	Kumpulan data sangat besar, cepat, dan beragam yang sulit diolah manual.	Medan tempur modern menghasilkan banjir data; AI menjadi penting untuk menyaringnya.
Data-Centric	Pendekatan yang menempatkan data sebagai inti operasi dan keputusan.	Dokumen menekankan bahwa keunggulan tidak lagi hanya pada platform, tetapi pada arsitektur data .
Data Pipeline	Alur pengumpulan, pengiriman, penyimpanan, pemrosesan, dan pemanfaatan data.	Dokumen menilai kelemahan Indonesia juga ada pada mission software dan data pipeline .
Mission Software	Perangkat lunak inti yang menghubungkan sensor, data, platform, dan keputusan dalam operasi.	Sangat penting karena tanpa perangkat lunak misi, platform canggih tidak otomatis efektif.
Battle Management Software	Perangkat lunak untuk membantu pengelolaan pertempuran dan koordinasi operasi.	Ditempatkan sebagai salah satu fungsi AI non-kinetik yang realistis dan berguna.

Predictive Maintenance	Pemeliharaan prediktif berbasis data untuk memprediksi kerusakan sebelum terjadi.	Dokumen menempatkannya sebagai salah satu aplikasi AI paling realistis di luar medan tembak.
Logistik Prediktif	Penggunaan analitik/AI untuk meramalkan kebutuhan logistik dan mendukung kesiapan operasi.	Menunjukkan bahwa AI bernilai besar justru di fungsi non-kinetik dan penguatan organisasi.
Cyber Defense	Penggunaan teknologi, termasuk AI, untuk pertahanan siber.	Masuk sebagai salah satu ruang pemanfaatan AI selain ISR dan targeting.
EW (Electronic Warfare)	<i>Electronic warfare</i> — peperangan elektronik untuk mengganggu, melindungi, atau mengeksploitasi spektrum elektromagnetik.	Penting dalam konteks drone, jamming, anti-drone, dan ketahanan operasi.
Jamming	Gangguan sinyal komunikasi, navigasi, atau kendali elektronik.	Dokumen menekankan ketahanan sistem dalam kondisi jamming sebagai kebutuhan nyata perang modern.
Counter-Drone / Anti-Drone	Upaya mendeteksi, mengganggu, atau menghancurkan drone lawan.	Disebut sebagai salah satu area AI yang paling berguna bagi Indonesia.
War-Ready AI	AI yang benar-benar siap dipakai dalam kondisi operasi, bukan hanya demo atau proyek presentasi.	Menjadi salah satu konsep kunci dokumen, terutama dalam konteks Indonesia yang perlu mengejar yang paling berguna , bukan paling glamor.
Frontline-Driven Innovation	Inovasi yang lahir dari kebutuhan garis depan, lalu diiterasikan cepat ke produksi.	Digunakan untuk membaca pengalaman Ukraina sebagai laboratorium perang nyata.
Fast-Track Procurement	Pengadaan yang dipercepat agar adaptasi teknologi tidak kalah oleh tempo perang.	Relevan karena dokumen menilai birokrasi lambat sebagai salah satu titik lemah.
Supply Chain	Rantai pasok komponen, bahan, perangkat, dan sistem pendukung.	Dalam dokumen, <i>supply chain</i> adalah titik rapuh strategis; AI yang baik harus tetap berguna saat rantai pasok terganggu.
Resilience	Daya tahan sistem, organisasi, atau industri untuk tetap berfungsi saat terganggu.	Menjadi pelajaran penting dari Iran dan sangat relevan bagi Indonesia.

Robustness	Ketangguhan teknis sistem di lingkungan bising, rusak, terganggu, atau tidak ideal.	Dokumen menekankan bahwa dalam perang, <i>robustness</i> sering lebih penting daripada spesifikasi tertinggi.
Archipelagic, Networked, Attritable	Arah doktrin Indonesia yang sesuai dengan karakter negara kepulauan, berjejaring, dan memakai sistem yang bisa diproduksi/disubstitusi massal.	Menjadi salah satu poros doktrin yang diusulkan dalam buku.
Reference Design	Rancangan acuan yang siap dijadikan dasar implementasi nyata.	Dokumen mendorong kampus bergerak dari sekadar publikasi menuju <i>reference design</i> .
Responsible Military AI	Penggunaan AI militer secara bertanggung jawab, dengan kendali manusia, akuntabilitas, dan kepercayaan.	Menjadi tema eksplisit pada bagian tata kelola, etika, dan batas penggunaan.
Traceability	Kemampuan menelusuri bagaimana keputusan, data, atau keluaran sistem dihasilkan.	Penting untuk audit, akuntabilitas, dan pencegahan kesalahan fatal AI.
Reliability	Tingkat keandalan sistem dalam memberikan hasil yang konsisten dan dapat dipercaya.	Menjadi salah satu syarat penggunaan AI militer yang bertanggung jawab.
Bias	Kecenderungan sistem menghasilkan keluaran yang melenceng atau tidak adil karena data/model.	Dokumen mengingatkan mitigasi bias sebagai isu penting dalam AI militer.
Lawfulness	Kesesuaian penggunaan sistem dengan hukum yang berlaku, terutama hukum humaniter internasional.	Menjadi bagian dari batas penggunaan AI militer yang sah dan bertanggung jawab.
Anti-Halusinasi	Disiplin verifikasi agar klaim AI, promosi perusahaan, atau propaganda tidak diterima mentah-mentah sebagai fakta.	Dokumen sejak awal menekankan metode verifikasi, pembedaan fakta–analisis–promosi–propaganda–inferensi.

Referensi

Amazon Web Services. (2022, December 7). *AWS selected for U.S. Department of Defense Joint Warfighting Cloud Capability contract.*

<https://aws.amazon.com/blogs/publicsector/aws-selected-for-u-s-department-of-defense-joint-warfighting-cloud-capability-contract/>

Anthropic. (2025, July 14). *Anthropic and the Department of Defense to advance responsible AI in defense operations.*

<https://www.anthropic.com/news/anthropic-and-the-department-of-defense-to-advance-responsible-ai-in-defense-operations>

Badan Riset dan Inovasi Nasional. (2023, December 7). *PUNA Alap-Alap kembali uji terbang, optimalkan sistem autopilot.*

<https://www.brin.go.id/news/123173/puna-alap-alap-kembali-uji-terbang-optimalkan-sistem-autopilot>

Badan Riset dan Inovasi Nasional. (2024). *Alap-Alap: Langkah strategis BRIN menuju kemandirian teknologi UAV nasional.*

<https://www.brin.go.id/news/123854/alap-alap-langkah-strategis-brin-menuju-kemandirian-teknologi-uav-nasional>

Badan Riset dan Inovasi Nasional. (2024). *Data satelit navigasi kian esensial, Indonesia perlu bangun kemandirian teknologi.*

<https://www.brin.go.id/news/125662/data-satelit-navigasi-kian-esensial-indonesia-perlu-bangun-kemandirian-teknologi>

Badan Riset dan Inovasi Nasional. (2024). *Empat pesawat tanpa awak buatan peneliti BRIN uji terbang, begini hasilnya.*

<https://www.brin.go.id/news/126247/empat-pesawat-tanpa-awak-buatan-peneliti-brin-uji-terbang-begini-hasilnya>

Blum, G., & Wittes, B. (2015). *The future of violence: Robots and germs, hackers and drones.* Basic Books.

Center for Strategic and International Studies. (2025). *Unleashing U.S. military drone dominance: What the United States can learn from Ukraine.*

<https://www.csis.org/analysis/unleashing-us-military-drone-dominance-what-united-states-can-learn-ukraine>

Chief Digital and Artificial Intelligence Office. (2022). *CDAO: New DoD chief digital and artificial intelligence office launches.* U.S. Department of Defense.

<https://www.defense.gov/News/News-Stories/Article/Article/2923986/new-dod-chief-digital-artificial-intelligence-office-launches/>

Chief Digital and Artificial Intelligence Office. (2023). *Dr. Radha Plumb, DoD chief digital and artificial intelligence officer, remarks at the DoD digital symposium.* U.S. Department of Defense.

<https://www.defense.gov/News/Speeches/Speech/Article/3912503/dr-radha-plumb-dod-chief-digital-and-artificial-intelligence-officer-delivers-r/>

Council on Foreign Relations. (2026). *The new era of drone warfare takes root in Iran*.
<https://www.cfr.org/articles/the-new-era-of-drone-warfare-takes-root-in-iran>

Defense Business Board. (2025). *Supply chain illumination in the Department of Defense*.
<https://dbb.defense.gov/Portals/35/Documents/Reports/2025/Final%20Stamped%20-%20DBB%20Supply%20Chain%20Illumination%20-%20201-15-25%20-%20Report.pdf>

Defense Logistics Agency. (2024). *Research, development, test and evaluation budget justification FY2024*. U.S. Department of Defense.
https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/03_RDT_and_E/RDTE_DLA_PB_2024.pdf

Defense Logistics Agency. (2025). *Research, development, test and evaluation budget justification FY2025*. U.S. Department of Defense.
https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/03_RDT_and_E/RDTE_DLA_PB_2025.pdf

Department of Defense. (2020). *DoD data strategy*.
<https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>

Department of Defense. (2021). *Counter-small unmanned aircraft systems strategy*.
<https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF>

Department of Defense. (2022). *Summary of the Joint All-Domain Command and Control (JADC2) strategy*.
<https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF>

Department of Defense. (2023). *Data, analytics, and artificial intelligence adoption strategy*.
https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

Department of Defense. (2024). *Fact sheet: DoD strategy for countering unmanned systems*.
<https://media.defense.gov/2024/Dec/05/2003599149/-1/-1/0/FACT-SHEET-STRATEGY-FOR-COUNTERING-UNMANNED-SYSTEMS.PDF>

Department of Defense. (2025). *2025 Marine Corps aviation plan*.
<https://media.defense.gov/2025/Mar/12/2003665702/-1/-1/1/2025-MARINE-CORPS-AVIATION-PLAN.PDF>

Department of Defense. (2026). *Artificial intelligence strategy for the Department of War*.
<https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF>

Department of Defense Chief Information Officer. (2025). *Software modernization implementation plan FY25–26*.

<https://dodcio.defense.gov/Portals/0/Documents/Library/SW-Mod-I-Plan25-26.pdf>

Digital Transformation Ministry of Ukraine. (n.d.). *Brave1*.

<https://digitalstate.gov.ua/projects/tech/brave1>

Digital Transformation Ministry of Ukraine. (2025). *Brave1 Market: Ukraina zapuskaye marketpleys viyskovykh innovatsiy [Brave1 Market: Ukraine launches a marketplace for military innovations]*.

<https://digitalstate.gov.ua/news/tech/brave1-market-ukrayina-zapuskaye-marketpleys-viyskovykh-innovatsiy>

Kementerian Perindustrian Republik Indonesia. (2026, January 20). *Bangun kemandirian semikonduktor, Kemenperin fokus pengembangan chip & SDM*.

<https://sippa.kemenperin.go.id/news/post/2026/01/20/35/bangun-kemandirian-semikonduktor-kemenperin-fokus-pengembangan-chip-sdm>

Kementerian Pertahanan Republik Indonesia. (2022). *Buku putih pertahanan Indonesia*.

<https://www.kemhan.go.id/wp-content/uploads/2022/08/BUKU-PUTIH.pdf>

Kementerian Pertahanan Republik Indonesia. (2025). *Arsitektur dan peta rencana Sistem Pemerintahan Berbasis Elektronik (SPBE) Kementerian Pertahanan 2025–2029*.

<https://ppid.kemhan.go.id/assets/attachments/20389a4091f2183e101dd6b1024e814a.pdf>

Kementerian Pertahanan Republik Indonesia. (2025, December 1). *Wamenhan dorong sinergi pertahanan–industri pada Rapimnas KADIN Indonesia 2025*.

<https://www.kemhan.go.id/2025/12/01/wamenhan-dorong-sinergi-pertahanan-industri-pada-rapimnas-kadin-indonesia-2025.html>

Komite Kebijakan Industri Pertahanan. (2022, November 30). *Sekilas perkembangan dan rencana industri radar*.

<https://www.kkip.go.id/2022/11/30/sekilas-perkembangan-dan-rencana-industri-radar/>

Ministry of Defence of Ukraine. (2026). *Ministry of Defence launches Brave1 Dataroom, a secure environment for training military AI solutions*.

<https://mod.gov.ua/en/news/ministry-of-defence-launches-brave1-dataroom-a-secure-environment-for-training-military-ai-solutions>

Ministry of Defence of Ukraine. (2026). *Mykhailo Fedorov: 240,000 drones ordered by the military through Brave1 Market*.

<https://mod.gov.ua/en/news/mykhailo-fedorov-240-000-drones-ordered-by-the-military-through-brave1-market>

OpenAI. (2025). *Introducing OpenAI for Government*.

<https://openai.com/global-affairs/introducing-openai-for-government/>

Raska, M. (Ed.). (2023). *The AI wave in defence innovation: Assessing military AI strategies*. Routledge.

Reuters. (2024, April 4). *Nvidia, Indosat plan \$200 mln AI centre investment in Indonesia, government says.*
<https://www.reuters.com/technology/nvidia-indosat-plan-200-mln-ai-centre-investment-indonesia-government-says-2024-04-04/>

Reuters. (2024, April 30). *Microsoft to invest \$1.7 bln in cloud, AI in Indonesia, CEO says.*
<https://www.reuters.com/technology/microsoft-invest-17-bln-cloud-ai-indonesia-ceo-says-2024-04-30/>

Reuters. (2024, May 6). *Pentagon's Replicator selects AeroVironment's Switchblade-600 as first buy.*
<https://www.reuters.com/business/aerospace-defense/pentagons-replicator-selects-aerovironments-switchblade-600-is-first-buy-2024-05-06/>

Reuters. (2024, May 29). *Palantir wins \$480 million U.S. Army deal for Maven prototype.*
<https://www.reuters.com/technology/palantir-wins-480-million-us-army-deal-maven-prototype-2024-05-29/>

Reuters. (2024, July 18). *Ukraine rushes to create AI-enabled war drones.*
<https://www.reuters.com/technology/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/>

Reuters. (2024, December 20). *Ukraine collects vast war data trove to train AI models.*
<https://www.reuters.com/technology/ukraine-collects-vast-war-data-trove-train-ai-models-2024-12-20/>

Reuters. (2025, July 17). *Ukraine offers its front line as test bed for foreign weapons.*
<https://www.reuters.com/business/aerospace-defense/ukraine-offers-its-front-line-test-bed-foreign-weapons-2025-07-17/>

Reuters. (2025, July 22). *Indonesia targets foreign investment with new AI roadmap, official says.*
<https://www.reuters.com/business/media-telecom/indonesia-targets-foreign-investment-with-new-ai-roadmap-official-says-2025-07-22/>

Reuters. (2025, August 4). *Ukraine bets big on interceptor drones as low-cost air shield.*
<https://www.reuters.com/business/aerospace-defense/ukraine-bets-big-interceptor-drones-low-cost-air-shield-2025-08-04/>

Reuters. (2026, January 29). *Iran's army receives batch of 1,000 drones, Tasnim reports.*
<https://www.reuters.com/business/aerospace-defense/irans-army-receives-batch-1000-drones-tasnim-reports-2026-01-29/>

Reuters. (2026, February 9). *Ukraine opens up arms exports, seeking to cash in on wartime technology.*
<https://www.reuters.com/business/aerospace-defense/ukraine-opens-up-arms-exports-seeking-cash-wartime-technology-2026-02-09/>

Reuters. (2026, February 12). *Ukrainian arms producers receive first wartime export licences, Kyiv says.*

<https://www.reuters.com/business/aerospace-defense/ukrainian-arms-producers-receive-first-war-time-export-licences-kyiv-says-2026-02-12/>

Reuters. (2026, March 3). *US debuts suicide drone to counter Iran after fast-tracked Pentagon procurement.*

<https://www.reuters.com/world/middle-east/us-debuts-suicide-drone-iran-after-fast-tracked-pentagon-procurement-2026-03-03/>

Reuters. (2026, March 4). *Iran could disrupt Strait of Hormuz with drones for months.*

<https://www.reuters.com/business/aerospace-defense/iran-could-disrupt-strait-hormuz-with-drones-months-2026-03-04/>

Reuters. (2026, March 4). *Iran's Revolutionary Guards take wartime lead, ensuring harder line, sources say.*

<https://www.reuters.com/world/middle-east/irans-revolutionary-guards-take-wartime-lead-ensuring-harder-line-sources-say-2026-03-04/>

Reuters. (2026, March 12). *Ukraine opens battlefield data access to allies for AI models.*

<https://www.reuters.com/business/aerospace-defense/ukraine-opens-battlefield-data-access-allies-ai-models-2026-03-12/>

Reuters. (2026, March 16). *Cheap drones are reshaping the war in the sky.*

<https://www.reuters.com/graphics/IRAN-CRISIS/DRONES/dwpkyamxqpm/>

Reuters. (2026, March 18). *Blackwater founder backs Ukrainian drone tech sales to U.S.*

<https://www.reuters.com/technology/blackwater-founder-backs-ukrainian-drone-tech-sales-us-2026-03-18/>

Reuters. (2026, March 20). *Pentagon to adopt Palantir AI as core U.S. military system, memo says.*

<https://www.reuters.com/technology/pentagon-adopt-palantir-ai-as-core-us-military-system-memo-says-2026-03-20/>

Reuters. (2026, March 25). *German army eyes AI tools to expedite wartime decision-making.*

<https://www.reuters.com/technology/german-army-eyes-ai-tools-expedite-wartime-decision-making-2026-03-25/>

Reuters. (2026, March 25). *White House pushes first big federal AI law this year.*

<https://www.reuters.com/technology/artificial-intelligence/artificial-intelligencer-white-house-pushes-first-big-federal-ai-law-this-year-2026-03-25/>

Reuters. (2026, April 1). *Italian bill offers incentives for fishing nets to shield Ukraine from drones.*

<https://www.reuters.com/world/italian-bill-offers-incentives-fishing-nets-shield-ukraine-drones-2026-04-01/>

Reuters. (2026, April 1). *Romania, Ukraine advance talks on EU-funded joint drone production.*

<https://www.reuters.com/world/romania-ukraine-advance-talks-eu-funded-joint-drone-production-2026-04-01/>

Reuters. (2026, April 3). *After Ukraine, Iran war further supercharges marine drone revolution.*

<https://www.reuters.com/default/after-ukraine-iran-war-further-supercharges-marine-drone-revolution-2026-04-03/>

Reuters. (2026, April 3). *Microsoft to invest \$10 billion in Japan AI, cyber defence expansion.*

<https://www.reuters.com/business/media-telecom/microsoft-invest-10-billion-japan-ai-cyber-defence-expansion-2026-04-03/>

Schraagen, J. M. C. (Ed.). (2024). *Responsible use of AI in military systems*. Routledge.

Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Press.

State Department of the United States. (2023). *Political declaration on responsible military use of artificial intelligence and autonomy.*

<https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy>

Tangredi, S. J., & Galdorisi, G. (Eds.). (2021). *AI at war: How big data, artificial intelligence, and machine learning are changing naval warfare*. Naval Institute Press.

United States Department of State. (2024). *2023 digest of United States practice in international law.*

<https://2021-2025.state.gov/wp-content/uploads/2024/12/2023-Digest-of-United-States-Practice-in-International-Law-Full.pdf>

Zaloga, S. J. (2008). *Unmanned aerial vehicles: Robotic air warfare 1917–2007*. Osprey Publishing.

Tentang Penulis



Onno W. Purbo, saat ini bertugas sebagai rektor di Institut Teknologi Tangerang Selatan (ITTS). Onno memperoleh gelar Ph.D bidang Electrical Engineering dari University of Waterloo, Canada, adalah seorang copyleft, educator dan ICT evangelist. Dia sudah mempublikasikan 50++ buku, termasuk free ICT ebook untuk sekolah tahun 2008. Beberapa buku terakhirnya adalah "Internet-TCP/IP: Konsep Dan Implementasi", 2018; "Sistem Operasi, Konsep Dan Membuat Linux OpenWRT Dan ROM Android", 2019; "IPv6 Untuk Mendukung Operasi Jaringan Dan Domain Name System", 2019; "Kubernetes untuk Pemula", 2024 dan "Membuat Operator Seluler 5G Sendiri", 2024.

Dia memimpin sambungan pertama Internet di Institut Teknologi Bandung, tahun 1993-2000, dan menggunakannya untuk membuat jaringan Internet pendidikan yang pertama di Indonesia. Dia membebaskan frekuensi WiFi, memperkenalkan RT/RW-net, antenna Wajanbolic dan jaringan selular OpenBTS dan private 5G sendiri. Dia memimpin jaringan telepon pertama di atas Internet, VoIP Merdeka, yang kemudian hari dikenal sebagai VoIP Rakyat berbasis SIP dan menggunakan kode area +62520 dan +62521. Dia saat ini aktif memperkenalkan e-Learning, dan menjalankan server e-Learning di <http://lms.onnocenter.or.id/moodle/> 66,000++ siswa / mahasiswa dan <https://opencourse.itts.ac.id> 39.000+ mahasiswa secara gratis. Email: onno@indo.net.id