Jurnal Stategi Pertahanan Laut
Volume 12 Nomor 1 2025 E-ISSN : 2830-2338

# *WARNING LATENCY* DAN KERENTANAN PANGKALAN UDARA: KERANGKA KONTRAINTELIJEN ANTISIPATIF BAGI ANCAMAN HIBRIDA

*WARNING LATENCY AND AIR BASE VULNERABILITY: AN ANTICIPATORY COUNTERINTELLIGENCE FRAMEWORK FOR HYBRID THREATS*

Joshua Insetyadi B[1]*, Mhd. Halkis[2], Agus H. Sulistiyono Reksoprodjo[1]

[1]Prodi Pepeperangan Asimetris FSP Unhan
[2]Unsurya
*Penulis korespondensi: Joshuainsetyadi@gmail.com

**Abstract.** Technically sophisticated air bases may remain vulnerable to strategic surprise when adversaries combine civilian logistics, low-cost unmanned systems, insider access, and cyber-information activities. Existing studies predominantly attribute such vulnerability to deficiencies in sensors or interceptors, while hybrid warfare scholarship rarely explains why base-defense organizations fail to act despite observable pre-attack indicators. This article addresses this gap through a structured-focused comparison of six purposively selected cases: Ukraine's Operation Spiderweb (2025), Tower 22 in Jordan (2024), Ain al-Asad in Iraq (2024), armed disruptions at Aminggaru/Ilaga Airport, Indonesia (2021–2025), laser disruptions at Sultan Hasanuddin Airport, Indonesia (2016–2017), and the disrupted ISIS plot against a TACOM facility in Michigan (2025). Findings suggest that vulnerability stems less from sensor failure than from warning latency: the cumulative organizational interval between the emergence of potentially recognizable indicators and relevant protective action. The article conceptualizes warning latency through six components—detection, correlation, assessment, dissemination, authority, and response—and integrates intelligence-failure, normal-accident, and high-reliability organization theories. It further develops anticipatory counterintelligence and proposes an Early Hybrid Threat Detection Framework (EHTDF) for shifting defense from weapon interception toward disruption of the adversary's preparation chain, with particular relevance to airpower resilience in archipelagic states such as Indonesia.

**Keywords:** Warning latency · Anticipatory counterintelligence · Hybrid threats · Intelligence failure · Air base defense · High-performance organization · Indonesia

**ABSTRAK**. Pangkalan udara dengan pertahanan teknis yang canggih tetap rentan terhadap *strategic surprise* ketika adversari mengombinasikan logistik sipil, sistem nirawak berbiaya rendah, akses orang dalam, serta aktivitas siber-informasi. Literatur umumnya mengaitkan kerentanan tersebut dengan keterbatasan sensor atau interseptor, sementara studi *hybrid warfare* belum memadai dalam menjelaskan

kegagalan organisasi pertahanan pangkalan bertindak meskipun indikator pra-serangan tersedia. Artikel ini mengisi kesenjangan tersebut melalui *structured-focused comparison* terhadap enam kasus yang dipilih secara purposif: Operation Spiderweb Ukraina (2025), Tower 22 di Yordania (2024), Ain al-Asad di Irak (2024), gangguan bersenjata di Bandar Udara Aminggaru/Ilaga (2021–2025), gangguan laser di Bandar Udara Sultan Hasanuddin (2016–2017), dan plot ISIS terhadap fasilitas TACOM di Michigan (2025). Temuan menunjukkan bahwa kerentanan terutama bersumber dari warning latency, yakni interval organisasional kumulatif antara munculnya indikator yang dapat dikenali dan pelaksanaan tindakan protektif. Konsep ini diuraikan ke dalam enam komponen: deteksi, korelasi, asesmen, diseminasi, kewenangan, dan respons. Artikel selanjutnya mengembangkan anticipatory counterintelligence dan Early Hybrid Threat Detection Framework (EHTDF) untuk menggeser orientasi pertahanan dari intersepsi senjata menuju deteksi dan disrupsi rantai persiapan adversari, khususnya guna memperkuat resiliensi kekuatan udara negara kepulauan seperti Indonesia.

**Kata kunci** Warning latency · Kontraintelijen antisipatif · Ancaman hibrida · Kegagalan intelijen · Pertahanan pangkalan udara · Organisasi berkinerja tinggi · Indonesia

## 1 PENDAHULUAN

Kompetisi kekuatan udara kontemporer menghadirkan sebuah teka-teki empiris yang belum terjelaskan secara memuaskan oleh literatur yang ada. Angkatan udara menginvestasikan sumber daya besar pada pesawat tempur, sensor generasi terbaru, senjata presisi, jaringan komando-kendali, dan sistem pertahanan udara berlapis. Namun demikian, sejumlah pangkalan dengan tingkat investasi pertahanan yang tinggi tetap mengalami strategic surprise ketika diserang melalui kombinasi logistik sipil, sistem nirawak komersial berbiaya rendah, akses orang dalam, dan aktivitas siber-informasi—sebuah pola yang berulang pada kasus-kasus yang dianalisis dalam artikel ini. Teka-teki ini bukan mengenai ketersediaan teknologi pertahanan, sebab pada hampir seluruh kasus yang dikaji, pihak yang bertahan pada dasarnya memiliki kapasitas sensor dan intersepsi yang jauh melampaui kapasitas pihak yang menyerang. Teka-teki ini justru mengenai mengapa kapasitas teknis tersebut tidak selalu diterjemahkan menjadi tindakan protektif yang tepat waktu.

Teka-teki empiris tersebut berimpitan dengan sebuah teka-teki literatur. Literatur hybrid warfare yang berkembang pesat pasca-2014 cenderung berfokus pada level strategis-negara—grand strategy, information warfare, proxy warfare—sementara literatur force protection dan pertahanan pangkalan cenderung bersifat

teknis-taktis dan berorientasi pada sistem senjata seperti counter-unmanned aerial system. Di antara keduanya terdapat kesenjangan konseptual: belum tersedia kerangka yang secara eksplisit menjelaskan kegagalan pertahanan pangkalan sebagai fenomena organisasional-temporal yang dapat didekomposisi dan diukur secara konseptual, alih-alih sekadar dideskripsikan sebagai "kegagalan intelijen" secara umum. Kajian yang menjembatani teori kontraintelijen, teori kegagalan intelijen, dan teori organisasi pada level pertahanan pangkalan udara, khususnya dalam konteks negara berkembang dengan geografi kepulauan seperti Indonesia, masih relatif jarang ditemukan.

Pertanyaan penelitian artikel ini adalah: mengapa pangkalan dengan pertahanan teknis yang kuat tetap dapat mengalami strategic surprise, dan bagaimana kontraintelijen dapat direposisi untuk mengatasi persoalan tersebut tanpa memasukkan seluruh bentuk ketidakamanan penerbangan ke dalam kategori hybrid warfare yang inflasioner?

Argumen utama artikel ini dapat dinyatakan sebagai satu proposisi teoretis sentral: **kerentanan pangkalan udara terhadap ancaman hibrida terutama merupakan persoalan organizational-temporal vulnerability, bukan semata-mata physical vulnerability.** Kerentanan tersebut muncul melalui mekanisme kausal yang berulang pada seluruh kasus yang dianalisis: indikator lemah yang terfragmentasi lintas domain (fragmented weak signals) menyebabkan kegagalan korelasi (failure of correlation), yang menyebabkan peringatan tertunda (delayed warning), yang berinteraksi dengan keterlambatan otoritas (authority latency), sehingga menghasilkan ruang waktu keputusan yang terkompresi (compressed decision time), yang pada akhirnya bermuara pada kerentanan operasional (operational vulnerability). EHTDF yang diusulkan pada bagian akhir artikel ini bukan merupakan "produk" yang berdiri sendiri, melainkan operasionalisasi dari mekanisme kausal tersebut: setiap tahap dalam EHTDF secara langsung menyasar satu komponen dari interval kumulatif yang, pada bagian 3, kami definisikan sebagai warning latency.

Artikel ini memberikan tiga kontribusi yang saling terkait erat, dipadatkan dari kontribusi yang lebih luas pada draf sebelumnya agar central claim tetap tajam. Pertama, kontribusi teoretis: mengembangkan warning latency sebagai construct analitis yang mendekomposisi interval antara indikator dan tindakan menjadi enam komponen terukur secara konseptual, serta menurunkan empat proposisi yang secara

eksplisit membagi labour analitis antara teori kegagalan intelijen (Betts 1978), teori kecelakaan normal (Perrow 1984), dan teori organisasi berkinerja tinggi (Weick and Sutcliffe 2001). Kedua, kontribusi metodologis: menerapkan structured-focused comparison dengan codebook eksplisit dan hierarki evidensi yang membedakan fakta, klaim, dan inferensi analitis pada enam kasus, termasuk satu kasus batas negatif dan satu kasus kontras keberhasilan antisipasi—desain yang jarang digunakan dalam kajian force protection yang cenderung hanya mempelajari kegagalan. Ketiga, kontribusi operasional: merumuskan EHTDF sebagai seperangkat ekspektasi yang dapat difalsifikasi mengenai bagaimana fusi indikator lintas domain memperpendek warning latency, dengan implikasi yang diturunkan secara teoretis—bukan ditempelkan sebagai kewajiban topikal—bagi konteks geografis dan institusional Indonesia.

## 2 ANCAMAN HIBRIDA, KONTRAINTELIJEN, DAN KEGAGALAN PERINGATAN

Literatur hybrid warfare menekankan penggunaan terpadu antara cara konvensional dan nonkonvensional, aktor negara dan nonnegara, operasi informasi, tekanan ekonomi-politik, aktivitas proksi, sarana siber, serta kekerasan terbatas yang beroperasi di bawah atau di sekitar ambang perang terbuka (Hoffman 2007). Konsep ini memiliki daya tarik analitis karena menangkap fenomena yang tidak sepenuhnya tercakup kategori perang konvensional maupun kategori damai. Namun, ekspansi penggunaan istilah "hibrida" yang semakin longgar dapat menghapus nilai analitisnya. Bartoszewicz (2025) menunjukkan bahwa inflasi konseptual pada istilah hibrida dapat menghasilkan bahasa krisis permanen yang melemahkan kesiapan yang spesifik terhadap aktor dan mekanisme ancaman tertentu; ketika hampir setiap insiden keamanan dilabeli hibrida, organisasi kehilangan kemampuan membedakan mekanisme kausal yang berbeda.

Artikel ini karena itu menggunakan "ancaman hibrida" dalam pengertian operasional yang dipersempit: kombinasi yang terkoordinasi atau secara strategis koheren antara instrumen terbuka dan terselubung yang melintasi lebih dari satu domain, atau penggunaan mekanisme sipil-komersial untuk menghasilkan efek yang setara dengan efek militer sambil memperumit atribusi, peringatan, atau respons. Kategori hibrida diperlakukan sebagai klaim analitis yang membutuhkan bukti, bukan label otomatis. Perspektif asymmetric conflict menjelaskan logika strategis di balik pilihan taktik hibrida: aktor yang lebih lemah cenderung menghindari

konfrontasi langsung dan menyerang titik yang menghasilkan efek tidak proporsional (Arreguín-Toft 2005). Dalam konteks kekuatan udara, apabila lawan tidak mampu mengalahkan angkatan udara di ruang udara, ia dapat berupaya menurunkan sortie generation rate, kontinuitas komando, ketersediaan logistik, atau kapasitas pemeliharaan ketika aset masih berada di darat.

Betts (1978), dalam salah satu artikel paling berpengaruh dalam studi intelijen strategis, mengajukan argumen bahwa kegagalan intelijen strategis pada tingkat tertentu bersifat inheren, bukan semata patologi organisasional yang dapat "disembuhkan" melalui reformasi struktural. Ambiguitas bukti, ambivalensi penilaian, dan atrofi reformasi kelembagaan yang dirancang untuk mencegah kegagalan merupakan sumber kesalahan yang sebagian bersifat paradoks yang tidak dapat sepenuhnya dipecahkan. Argumen ini sejalan dengan analisis klasik Wohlstetter (1962) mengenai Pearl Harbor, yang menunjukkan bahwa kegagalan peringatan pada dasarnya bukan kegagalan mengumpulkan sinyal, melainkan kegagalan memisahkan sinyal yang relevan dari derau (noise) informasi yang sangat besar jumlahnya. Dalam kerangka artikel ini, Betts menjelaskan mengapa **detection latency** dan **assessment latency**—dua komponen warning latency yang dirumuskan pada bagian 3—tidak dapat direduksi menjadi nol betapa pun canggihnya sistem analisis yang dibangun.

Pangkalan udara bukan sekadar runway dan perimeter fisik. Ia merupakan sistem sosio-teknis yang menggabungkan pesawat, bahan bakar, senjata, pemeliharaan, komunikasi, jaringan digital, spektrum elektromagnetik, personel, kontraktor, logistik, pengendalian lalu lintas udara, infrastruktur lokal, dan masyarakat sekitar. Kerentanan struktural muncul dari interaksi antarkomponen tersebut. Teori kecelakaan normal dari Perrow (1984) menjelaskan mengapa sistem yang secara simultan bersifat kompleks secara interaktif (interactively complex) dan terpaut erat (tightly coupled) cenderung menghasilkan kegagalan yang, meskipun jarang terjadi, pada dasarnya "normal" sebagai konsekuensi struktural dari desain sistem itu sendiri. Pangkalan udara modern menunjukkan kedua karakteristik tersebut: kompleksitas interaktif tampak pada keterkaitan antara sistem logistik, siber, komunikasi, dan keamanan fisik yang jarang sepenuhnya dipahami oleh satu unit organisasi tunggal; keterpautan erat tampak pada kecepatan sistem nirawak komersial dan cyber probing yang tidak menyediakan banyak ruang waktu (slack) bagi organisasi untuk melakukan koreksi. Dalam kerangka artikel ini, Perrow

menjelaskan mengapa **correlation latency** dan **authority latency** cenderung memburuk, bukan membaik, seiring bertambahnya jumlah subsistem yang harus dihubungkan sebelum tindakan dapat diambil.

Artikel ini juga secara sengaja tidak otomatis menyebut setiap pangkalan udara sebagai center of gravity. Formulasi yang lebih defensibel adalah memperlakukan pangkalan udara sebagai critical operational node yang degradasinya dapat memengaruhi pembangkitan dan kontinuitas kekuatan udara, tanpa mengklaim status center of gravity tanpa bukti analitis memadai.

Berbeda dengan Perrow yang cenderung pesimistis mengenai kemungkinan mencegah kegagalan sistem kompleks-terpaut-erat, Weick and Sutcliffe (2001) menunjukkan bahwa sejumlah organisasi yang beroperasi dalam kondisi risiko dan kompleksitas serupa—dek penerbangan kapal induk, unit gawat darurat, unit pemadam kebakaran—mampu mempertahankan kinerja yang jauh lebih andal dibandingkan yang diprediksikan oleh tingkat risiko struktural mereka. Kunci kemampuan tersebut terletak pada lima prinsip kewaspadaan kolektif (mindful organizing): preokupasi terhadap kegagalan kecil sebagai sinyal potensi masalah yang lebih besar; keengganan menyederhanakan interpretasi; kepekaan terhadap operasi garis depan; komitmen terhadap resiliensi organisasional; dan penghormatan terhadap keahlian teknis, bukan semata hierarki formal, saat krisis berkembang cepat. Dalam kerangka artikel ini, Weick and Sutcliffe menjelaskan bagaimana **dissemination latency** dan **response latency** dapat dipersingkat melalui budaya organisasional yang secara aktif mendorong pelaporan anomali dan mendistribusikan otoritas keputusan kepada personel yang paling dekat dengan sumber informasi—bukan menghilangkan kegagalan struktural yang dijelaskan Perrow, melainkan mengurangi probabilitas dan konsekuensinya.

Nilsson, Weissmann, and Palmertz (2026) menunjukkan bahwa ancaman hibrida menantang komunitas intelijen konvensional karena indikator yang relevan tersebar di antara lembaga pemerintah, entitas swasta, masyarakat sipil, dan sistem teknis yang masing-masing memiliki logika kelembagaan dan budaya berbagi informasi yang berbeda. Weissmann and Nilsson (2024) menunjukkan ketegangan struktural antara kualitas informasi dan kecepatan penyampaian dalam current intelligence. Proctor (2025) membedakan persoalan konseptual "early warning" dari sekadar pelaporan cepat: semakin dini peringatan dihasilkan, semakin tinggi ketidakpastiannya; semakin terlambat, semakin sedikit pilihan preventif yang

tersedia. Gentry and Gordon (2019) menunjukkan bahwa persoalan warning intelligence secara historis tidak hanya terletak pada informasi, tetapi pada kesulitan mengubah informasi menjadi respons tepat waktu. Kontraintelijen, dalam pengertian Prunckun (2019), berkaitan dengan identifikasi dan netralisasi spionase, sabotase, dan aktivitas intelijen lawan sekaligus perlindungan informasi dan kemampuan organisasi sendiri—sebuah fungsi yang, sebagaimana ditegaskan doktrin AFDP 3-10 (Department of the Air Force 2023) dan AFDP 2-0 (Department of the Air Force 2026), seharusnya dilembagakan sebagai fungsi pendukung force protection yang antisipatif, bukan sekadar kegiatan investigatif pascainsiden.

## 3 TEORI TERINTEGRASI WARNING LATENCY

### 3.1 Konstruk

Bagian ini merumuskan kontribusi teoretis utama artikel: sebuah construct analitis bernama **warning latency**, yang mengikat argumen konseptual pada bagian 2 menjadi satu kerangka yang dapat diuji.

Warning latency didefinisikan sebagai interval organisasional antara munculnya indikator ancaman yang secara potensial dapat dikenali (detectable indicator) dan dilaksanakannya tindakan protektif yang relevan (protective action). Secara notasional:

**WL = T(action) − T(detectable indicator)**

Warning latency bukan model kuantitatif yang menuntut pengukuran presisi dalam artikel ini; ia digunakan sebagai construct analitis untuk menstrukturkan narasi kasus dan perbandingan lintas kasus. Warning latency didekomposisi menjadi enam komponen yang berurutan namun dapat tumpang tindih:

**WL = L(d) + L(c) + L(a) + L(w) + L(auth) + L(r)**

di mana L(d) adalah detection latency (waktu antara indikator dapat diamati dan benar-benar diamati oleh suatu elemen organisasi); L(c) adalah correlation latency (waktu antara indikator diamati secara terisolasi dan dikorelasikan dengan indikator lain lintas domain); L(a) adalah assessment latency (waktu untuk mengubah pola yang terkorelasi menjadi penilaian ancaman dengan confidence level tertentu); L(w) adalah dissemination/warning latency (waktu untuk menyalurkan assessment kepada otoritas yang relevan); L(auth) adalah authority latency (waktu untuk

memperoleh kewenangan bertindak); dan L(r) adalah response latency (waktu antara kewenangan diberikan dan tindakan protektif benar-benar dilaksanakan).

### 3.2 Mekanisme kausal

Proposisi sentral pada bagian 1.3 dioperasionalkan melalui rantai kausal berikut: **fragmented weak signals → failure of correlation → delayed warning → authority latency → compressed decision time → operational vulnerability.** Setiap tautan dalam rantai ini berkontribusi pada satu atau lebih komponen warning latency. Fragmentasi indikator memperbesar L(d) dan L(c); kegagalan korelasi memperbesar L(a); keterlambatan otoritas memperbesar L(auth); dan akumulasi keempatnya mengompresi ruang waktu yang tersedia bagi L(r), memaksa tindakan protektif dilakukan secara tergesa dan proporsionalitasnya sulit dijamin, atau tidak dilakukan sama sekali sebelum dampak terjadi.

### 3.3 Pembagian labour analitis antarteori

Tabel 1 memperlihatkan secara eksplisit division of analytical labour antara tiga tradisi teoretis yang digunakan artikel ini, sehingga integrasi ketiganya tidak bersifat aditif semata, melainkan menghasilkan penjelasan yang saling melengkapi atas komponen warning latency yang berbeda-beda.

**Tabel 1 Pembagian labour analitis antarteori**

| Teori | Apa yang dijelaskan | Komponen warning latency yang relevan |
|---|---|---|
| Betts (1978) — teori kegagalan intelijen | Mengapa warning failure tidak dapat dihilangkan sepenuhnya; ambiguitas bukti bersifat inheren | Detection latency, assessment latency |
| Perrow (1984) — teori kecelakaan normal | Mengapa kompleksitas interaktif dan keterpautan erat memperbesar kegagalan korelasi dan otoritas | Correlation latency, authority latency |
| Weick and Sutcliffe (2001) — organisasi berkinerja tinggi | Bagaimana organisasi dapat mengurangi probabilitas dan konsekuensi kegagalan melalui kewaspadaan kolektif | Dissemination latency, response latency |
| Sintesis artikel | Mengapa kontraintelijen antisipatif harus memperbesar decision space sebelum hostile action, dengan menyasar keenam komponen warning latency secara simultan | Seluruh komponen WL |

3.4 Proposisi teoretis

Dari sintesis pada Tabel 1, artikel ini menurunkan empat proposisi yang dapat diuji pada penelitian lanjutan dan yang menjadi rujukan eksplisit bagi analisis lintas kasus pada bagian 5.

**P1 — Indicator Fragmentation Proposition.** Semakin tersebar indikator persiapan ancaman di antara domain dan unit organisasi yang berbeda, semakin tinggi probabilitas kegagalan peringatan, meskipun setiap unit organisasi secara individual memiliki sensor yang memadai.

**P2 — Temporal Compression Proposition.** Semakin dekat kemampuan serang dapat diposisikan terhadap target melalui jaringan sipil atau logistik yang sah, semakin kecil hubungan antara strategic depth geografis dan warning time yang tersedia bagi pihak yang bertahan.

**P3 — Organizational Latency Proposition.** Efektivitas sistem peringatan ditentukan bukan hanya oleh kecepatan deteksi awal, melainkan oleh waktu kumulatif di sepanjang keenam komponen warning latency—detection, correlation, assessment, dissemination, authority, dan response.

**P4 — Anticipatory Counterintelligence Proposition.** Kontraintelijen meningkatkan resiliensi pangkalan bukan terutama melalui intersepsi ancaman pada fase terminal, melainkan melalui peningkatan jumlah observable points di sepanjang adversary preparation chain, yang secara langsung memperpendek detection latency dan correlation latency.

Keempat proposisi ini bersifat plausible causal mechanisms yang diturunkan dari perbandingan kasus berbasis dokumen terbuka (lihat bagian 4), bukan hukum kausal yang telah diverifikasi secara eksperimental. Status epistemik ini dipertahankan secara konsisten sepanjang artikel.

## 4 DESAIN PENELITIAN

### 4.1 Desain: structured-focused comparison

Penelitian ini menggunakan desain kualitatif-komparatif yang secara spesifik mengikuti logika structured-focused comparison: pertanyaan yang sama diajukan secara sistematis pada setiap kasus (apa indikator yang tersedia, kapan indikator tersebut dapat dikenali, bagaimana indikator dikorelasikan atau gagal dikorelasikan,

dan berapa lama interval hingga tindakan protektif dilaksanakan), dipadukan dengan rekonstruksi dalam-kasus (within-case reconstruction) dan pencocokan pola lintas kasus (cross-case pattern matching). Artikel ini secara sengaja tidak mengklaim melakukan causal process tracing dalam pengertian yang ketat—yang menuntut hoop tests, smoking-gun tests, pengurutan bukti yang presisi, dan bukti kausal dalam-kasus yang mendalam (Gentry and Gordon 2019; Betts 1978)—mengingat desain penelitian sepenuhnya berbasis dokumen terbuka tanpa akses terhadap catatan operasional internal. Klaim metodologis artikel karena itu dirumuskan secara lebih defensibel sebagai upaya mengidentifikasi dan membandingkan **plausible causal mechanisms** melalui structured-focused comparison dan pattern matching, bukan menelusuri mekanisme kausal secara definitif. Kata "plausible" dipertahankan secara konsisten karena sumber data adalah OSINT dan dokumen publik.

Artikel ini secara sengaja diposisikan sebagai studi konseptual dan berbasis dokumen (document-based conceptual study), bukan laporan empiris hasil wawancara langsung pada institusi militer Indonesia. Outline riset yang menjadi titik tolak artikel ini semula merencanakan penelitian lapangan pada unsur intelijen dan pengamanan TNI Angkatan Udara, tetapi transkrip wawancara dan hasil observasi lapangan tersebut belum tersedia sebagai data pada tahap penulisan ini, sehingga artikel tidak membuat klaim mengenai praktik internal yang tidak tersedia dalam sumber terbuka.

4.2 Pemilihan kasus: desain enam-kasus

Pemilihan kasus dalam penelitian ini bersifat theory-building dan purposive. Untuk menghindari kritik selecting on the dependent variable—yaitu risiko bahwa artikel hanya mempelajari kegagalan peringatan tanpa pernah mengamati keberhasilan—desain penelitian secara sengaja disusun sebagai **desain enam-kasus** yang terdiri atas tiga tipe kasus yang berbeda fungsi analitisnya, dan jumlah ini digunakan secara konsisten di seluruh artikel, termasuk abstrak.

Tipe pertama adalah empat kasus vulnerability-exposing yang menunjukkan bagaimana warning latency menghasilkan kerentanan operasional: Operation Spiderweb (Rusia, 2025), Tower 22 (Yordania, 2024), Ain al-Asad (Irak, 2024), dan Aminggaru/Ilaga (Indonesia, 2021–2025). Tipe kedua adalah satu kasus batas negatif (negative/boundary case) yaitu Sultan Hasanuddin (Indonesia, 2016–2017), yang secara sengaja dipilih karena menunjukkan kondisi ketika kerentanan operasional

nyata ada tetapi bukti hybridity tidak ada—berguna untuk menguji batas konseptual "ancaman hibrida" yang dirumuskan pada bagian 2.1. Tipe ketiga adalah satu kasus kontras keberhasilan antisipasi (successful-anticipation case), yaitu plot serangan ISIS yang berhasil digagalkan terhadap fasilitas Tank-Automotive & Armaments Command (TACOM) Angkatan Darat Amerika Serikat di Warren, Michigan, pada Mei 2025 (U.S. Attorney's Office, Eastern District of Michigan 2025). Kasus ini secara eksplisit bukan sebuah pangkalan udara, melainkan fasilitas materiil darat, sehingga generalisasi lintas domain penerbangan tetap memerlukan kehati-hatian dan dinyatakan secara terbuka sebagai batasan pada bagian 8. Kasus ini dipilih bukan karena kesamaan domain, melainkan karena secara tepat mengilustrasikan mekanisme yang menjadi inti argumen artikel—disrupsi adversary preparation chain melalui kontraintelijen dan liaison penegak hukum, bukan intersepsi senjata pada fase terminal—sehingga berfungsi sebagai kontras metodologis yang menjawab pertanyaan: mengapa indikator persiapan menghasilkan tindakan tepat waktu pada satu kasus, sementara pada kasus lain tidak?

Empat kriteria digunakan dalam pemilihan seluruh kasus: ketersediaan dokumentasi publik yang memadai untuk triangulasi; relevansi terhadap domain ancaman yang menjadi fokus artikel; variasi tingkat kompleksitas dan skala dampak; dan relevansi geografis-institusional bagi konteks Indonesia, khususnya bagi dua kasus domestik.

### 4.3 Hierarki sumber dan triangulasi

Sumber dibedakan secara eksplisit berdasarkan fungsi evidensialnya. Literatur peer-reviewed digunakan untuk teori dan temuan akademik; sumber resmi negara dan doktrin militer digunakan untuk posisi institusional dan fakta terkonfirmasi; media massa bereputasi digunakan untuk merekonstruksi kronologi dan membandingkan penilaian; klaim pihak berkonflik selalu diberi atribusi eksplisit. Hierarki ini mencegah pencampuran yang tidak disengaja antara fakta, klaim, dan inferensi—sebuah persoalan yang, sebagaimana ditunjukkan perbedaan angka kerusakan pada kasus Spiderweb, sangat rentan terjadi dalam kajian mengenai konflik yang sedang berlangsung.

**Tabel 2 Hierarki evidensi dalam penelitian**

| Kategori sumber | Fungsi utama | Contoh | Perlakuan analitis |
|---|---|---|---|
| Literatur peer-reviewed | Teori, konsep, temuan terdahulu | Intelligence and National Security; International Journal of Intelligence and CounterIntelligence; European Journal for Security Research; World Politics; Frontiers in Big Data | Bobot utama bagi klaim teoretis dan analitis |
| Sumber resmi negara/ militer/ penegak hukum | Fakta terkonfirmasi, doktrin, definisi institusional | U.S. Department of Defense; USAF doctrine; U.S. Department of Justice; Kementerian Perhubungan RI | Otoritatif mengenai apa yang secara resmi dinyatakan institusi; tidak otomatis netral untuk klaim kausal yang diperdebatkan |
| Media massa bereputasi | Rekonstruksi peristiwa dan cross-check assessment | Reuters; Associated Press; ANTARA | Triangulasi tanggal, metode, kerusakan, dan pernyataan pejabat |
| Klaim pihak berkonflik | Niat aktor dan efek yang diklaim | SBU/Ukraina; pernyataan Rusia | Tetap diberi label sebagai klaim jika tidak terverifikasi independen |
| Inferensi analitis | Identifikasi mekanisme dan theory-building | Pattern matching lintas kasus | Dibedakan eksplisit dari fakta observasional dan diperlakukan sebagai interpretasi yang dapat diuji |

### 4.4 Prosedur coding dan codebook

Untuk menjadikan analisis lebih transparan dan replicable—salah satu pembeda utama antara artikel konseptual biasa dan artikel metodologis yang kuat—setiap insiden dikodekan secara manual oleh peneliti mengikuti codebook eksplisit pada Tabel 3. Unit coding adalah episode insiden (satu kasus dapat memiliki lebih dari satu episode, sebagaimana Ain al-Asad). Pendekatan coding bersifat deduktif: kategori construct diturunkan dari kerangka warning latency pada bagian 3, kemudian diterapkan pada bukti yang tersedia untuk setiap kasus. Ambiguous evidence—yaitu kondisi ketika sumber terbuka tidak cukup rinci untuk menentukan nilai suatu construct secara pasti—dikodekan sebagai "uncertain" dan dinyatakan secara eksplisit dalam narasi kasus pada bagian 5, bukan dipaksakan menjadi 0 atau 1. Rival interpretation diperiksa dengan cara membandingkan klaim resmi, klaim pihak

berkonflik, dan penilaian media secara berdampingan sebagaimana ditunjukkan pada Tabel 4.

**Tabel 3 Codebook construct warning latency**

| Construct | Definisi operasional | Bukti yang dapat diamati | Aturan coding |
|---|---|---|---|
| Detection failure | Indikator persiapan tersedia dalam catatan publik tetapi tidak dikenali oleh elemen organisasi mana pun sebelum insiden | Laporan investigasi, catatan sensor, access log yang diungkap pascainsiden | 1 = terkonfirmasi terjadi; 0 = terkonfirmasi tidak terjadi; uncertain = bukti publik tidak cukup |
| Correlation failure | Indikator individual teramati tetapi tidak dihubungkan dengan indikator lain lintas domain sebelum insiden | Kesaksian investigasi, laporan after-action, pernyataan pejabat mengenai celah koordinasi | 1/0/uncertain, sama seperti di atas |
| Warning/ assessment failure | Assessment ancaman tidak dihasilkan, atau dihasilkan tetapi tidak mencapai confidence level yang memicu tindakan | Dokumen resmi mengenai investigasi kegagalan pertahanan | 1/0/uncertain |
| Authority latency | Tindakan protektif tertunda karena ketidakjelasan atau keterlambatan kewenangan bertindak | Kronologi resmi, laporan investigasi kelembagaan | 1/0/uncertain |
| Response failure/success | Tindakan protektif yang dilaksanakan tidak sesuai skala ancaman, atau sebaliknya berhasil mencegah dampak | Bukti hasil (outcome evidence): kerusakan aktual dibandingkan potensi kerusakan | 1 (gagal) / 0 (berhasil) / uncertain |

4.5 Prosedur analisis

Analisis dilakukan melalui empat tahap. Pertama, informasi setiap insiden dikodekan ke dalam lima domain ancaman (fisik/kinetik, manusia dan akses, informasi/kognitif, siber-elektromagnetik, nirawak/logistik) sekaligus ke dalam construct warning latency pada Tabel 3. Kedua, setiap kasus direkonstruksi sebagai preparation chain—reconnaissance, akses, logistik, positioning, command-and-control, launch, exploitation—untuk mengidentifikasi aktivitas yang harus terjadi sebelum insiden terminal. Ketiga, pattern matching digunakan untuk menemukan titik kegagalan atau keberhasilan yang berulang lintas kasus pada keenam komponen

warning latency. Keempat, mekanisme yang teridentifikasi disintesiskan menjadi EHTDF pada bagian 6.

Threat assessment menggunakan empat variabel klasik—threat, vulnerability, adversary capability, consequence—sebagai struktur judgement kualitatif, bukan skor numerik yang semu presisinya. Kerangka Ends-Ways-Means (Lykke 1989) digunakan sebagai alat bantu tambahan untuk menghubungkan outcome strategis, proses organisasi, dan sumber daya.

### 4.6 Trustworthiness dan refleksivitas

Mengingat sifat kualitatif penelitian ini, artikel mengadopsi kriteria trustworthiness dari tradisi penelitian naturalistik (Lincoln and Guba 1985). Credibility diupayakan melalui triangulasi sumber sistematis (subbagian 4.3) dan pembandingan silang klaim Ukraina, penilaian pejabat Amerika Serikat, dan pengakuan Rusia pada kasus Spiderweb. Dependability diupayakan melalui dokumentasi eksplisit codebook dan prosedur coding (subbagian 4.4–4.5). Confirmability diupayakan melalui pemisahan tegas data observasional, klaim aktor, dan inferensi analitis. Transferability tidak diklaim secara statistik; artikel menyediakan deskripsi kasus yang cukup rinci (thick description) agar pembaca pada konteks lain dapat menilai relevansi mekanisme yang teridentifikasi.

Penelitian ini mengakui posisi refleksif penulis: analisis dilakukan sepenuhnya dari sumber terbuka tanpa akses informasi terklasifikasi, sehingga interpretasi mengenai efektivitas atau kegagalan sistem pertahanan tertentu bersifat inferensial dan tidak dapat diverifikasi terhadap catatan operasional internal.

## 5 TEMUAN LINTAS KASUS

### 5.1 Operation Spiderweb sebagai kasus theory-generating, bukan pusat artikel

Operation Spiderweb pada 1 Juni 2025 digunakan dalam artikel ini sebagai theory-generating critical case, bukan sebagai pusat argumen. Klaim terbaik yang dapat diajukan berdasarkan bukti publik bukanlah bahwa Rusia "gagal" secara definitif, melainkan bahwa kasus ini mengekspos kerentanan yang lebih umum: mobilitas sipil, logistik terselubung, dan sistem otonom berbiaya rendah, apabila dikombinasikan, mengompresi warning time pihak yang bertahan.

Otoritas Ukraina menyatakan bahwa 117 drone first-person-view digunakan, dipersiapkan lebih dari delapan belas bulan. Reuters merekonstruksi metode penyembunyian drone di bawah atap struktur kayu portabel yang diangkut menggunakan truk sipil menuju lokasi peluncuran dekat sejumlah pangkalan udara strategis Rusia. Penilaian pejabat Amerika Serikat yang diberitakan Reuters memperkirakan sekitar sepuluh pesawat dihancurkan dan hingga dua puluh terkena, jauh lebih rendah dibandingkan klaim awal Ukraina mengenai empat puluh satu pesawat dan estimasi tiga puluh empat persen armada pembawa rudal jelajah strategis terdampak. Perbedaan angka ini bukan kelemahan data, melainkan justru alasan metodologis untuk triangulasi sumber dan menahan diri dari memperlakukan klaim pihak berkonflik sebagai fakta final.

Ditinjau melalui construct warning latency: detection failure dan correlation failure pada kasus ini dikodekan sebagai 1 (terkonfirmasi terjadi), mengingat operasi berlangsung lebih dari delapan belas bulan tanpa terdeteksi oleh sistem kontraintelijen Rusia sebagaimana dilaporkan secara luas. Operasi ini membutuhkan pengadaan atau perakitan platform, pembangunan cover logistik sipil, pergerakan peralatan, penyimpanan dan concealment jangka panjang, reconnaissance sasaran, perencanaan rute, komunikasi terselubung, pemilihan launch site, dan command-and-control—rangkaian aktivitas yang secara individual tampak benign, tetapi yang nilai intelijennya baru muncul ketika dikorelasikan (sejalan dengan P1). Kasus ini juga mengonfirmasi P2: strategic depth tidak lagi berbanding lurus dengan warning time ketika kapasitas peluncuran dapat diinfiltrasikan melalui infrastruktur sipil yang sah—mobilitas sipil pada dasarnya dikonversi menjadi strike range.

### 5.2 Tower 22 dan Ain al-Asad: warning adalah rantai komponen, bukan sensor tunggal

Tower 22 menunjukkan mengapa penjelasan sensor-sentris tidak memadai. Departemen Pertahanan Amerika Serikat mengonfirmasi bahwa serangan one-way unmanned aerial system pada 28 Januari 2024 menewaskan tiga personel Amerika Serikat dan melukai lebih dari empat puluh orang, dengan investigasi CENTCOM mengenai penetrasi pertahanan. Artikel ini tidak mengubah hipotesis media mengenai kegagalan identifikasi menjadi fakta yang terbukti, mengingat keterbatasan sumber terbuka. Ditinjau melalui codebook pada Tabel 3, kasus ini paling defensibel dikodekan sebagai warning/assessment failure dan authority latency, konsisten dengan enam komponen warning latency: setiap transisi antara detection,

classification, threat assessment, dissemination, authority allocation, dan response membutuhkan waktu dan sering melintasi batas organisasi, sehingga sensor yang berfungsi secara teknis tetap dapat berujung pada kegagalan operasional (P3).

Ain al-Asad menambahkan dimensi persistensi: ancaman berulang menciptakan dua risiko yang saling bertentangan—overreaction yang menguras sumber daya, dan underreaction yang menghasilkan normalization of deviance. Reuters melaporkan beberapa serangan drone/roket pada 2024, dengan salah satu drone dilaporkan ditembak jatuh dekat perimeter dan serangan berikutnya menyebabkan personel Amerika Serikat terluka. Kontraintelijen dan current intelligence pada konteks ini perlu secara aktif membaca pola adaptasi lawan lintas insiden, bukan memperlakukan setiap kejadian sebagai episode terisolasi.

### 5.3 Indonesia: Aminggaru/Ilaga sebagai kasus vulnerability, Sultan Hasanuddin sebagai kasus batas negatif

Aminggaru/Ilaga memperlihatkan arti penting infrastruktur udara di wilayah dengan akses darat yang secara struktural sulit. Data resmi Kementerian Perhubungan menempatkan bandar udara tersebut sebagai bandar udara domestik Kelas III di Kabupaten Puncak, Papua Tengah. ANTARA mendokumentasikan pembakaran fasilitas pada Juni 2021 dan gangguan bersenjata pada Februari 2022 yang menyebabkan operasi ditutup sementara dan seorang personel pengamanan TNI Angkatan Udara cedera; gangguan bersenjata kembali terjadi pada 2025. Rangkaian ini mendukung proposisi bahwa aktor bersenjata dengan kemampuan relatif kecil dapat menghasilkan biaya operasional tidak proporsional dengan menyerang critical access node. Namun, berdasarkan bukti publik yang tersedia, klasifikasi "ancaman bersenjata asimetris" jauh lebih defensibel daripada "hybrid warfare", mengingat tidak terdapat bukti publik mengenai koordinasi strategis lintas domain.

Sultan Hasanuddin secara sengaja digunakan sebagai negative/boundary case, bukan ilustrasi tambahan semata. Fungsinya adalah menunjukkan kondisi ketika kerentanan operasional nyata ada—data Kementerian Perhubungan menunjukkan 39.892 pergerakan pesawat, lebih dari 6,44 juta penumpang, dan sekitar 41 juta kilogram kargo pada 2025, menegaskan posisinya sebagai simpul penerbangan penting—tetapi bukti hybridity tidak ada. ANTARA dan media nasional melaporkan gangguan laser terhadap pesawat pada fase take-off atau landing, termasuk laporan AirNav Makassar mengenai tujuh kejadian dalam satu episode pada 2017. Data ini

membuktikan aviation-safety vulnerability yang berasal dari luar perimeter, tetapi sama sekali tidak membuktikan hostile intelligence intent. Dengan menempatkan kasus ini secara eksplisit sebagai kasus batas, artikel menguji sendiri batas konseptual definisi hibrida pada bagian 2.1: apabila artikel gagal menahan diri untuk tidak melabeli kasus ini sebagai hibrida, konsistensi metodologis seluruh artikel akan runtuh.

5.4 TACOM, Michigan: kasus kontras keberhasilan antisipasi

Berbeda dari kelima kasus di atas, kasus ini menunjukkan warning latency yang berhasil dipersingkat sebelum dampak terjadi. Menurut siaran pers resmi U.S. Attorney's Office, Eastern District of Michigan (2025) yang didukung Divisi Keamanan Nasional Departemen Kehakiman Amerika Serikat, Biro Investigasi Federal (FBI), dan Army Counterintelligence Command, seorang mantan anggota Garda Nasional Angkatan Darat Michigan berusia sembilan belas tahun ditangkap pada 13 Mei 2025—hari yang direncanakan sebagai hari serangan—setelah melakukan reconnaissance udara menggunakan drone komersial terhadap fasilitas Tank-Automotive & Armaments Command (TACOM) di Detroit Arsenal, Warren, Michigan, sebagai bagian dari rencana penembakan massal atas nama ISIS. Ia sebelumnya memberikan amunisi penembus lapis baja, memberikan pelatihan senjata dan pembuatan bom molotov kepada dua petugas penegak hukum yang menyamar, serta merencanakan rincian titik masuk dan gedung sasaran sejak komunikasi awal pada Juni 2024.

Ditinjau melalui construct warning latency, kasus ini dikodekan sebagai response success (0 pada Tabel 3): detection dan correlation berhasil dilakukan pada tahap reconnaissance dan fasilitasi logistik—jauh sebelum peluncuran drone pada hari serangan—melalui liaison aktif antara FBI Joint Terrorism Task Force dan Army Counterintelligence Command. Assessment, dissemination, dan authority berjalan cukup cepat sehingga response dapat dilaksanakan sebelum weapon employment terjadi, bukan sesudahnya. Kasus ini secara langsung mengilustrasikan P4: anticipatory counterintelligence meningkatkan resiliensi bukan melalui intersepsi drone secara teknis pada saat drone mengudara, melainkan melalui disrupsi preparation chain pada tahap reconnaissance dan fasilitasi jauh sebelum peluncuran. Perlu ditegaskan secara eksplisit bahwa TACOM adalah fasilitas materiil darat, bukan pangkalan udara, sehingga kasus ini digunakan sebagai kontras mekanisme, bukan

sebagai bukti langsung mengenai domain penerbangan; batasan ini dibahas lebih lanjut pada bagian 9.

5.5 Sintesis lintas kasus

Tabel 4 merekonsiliasi klaim faktual utama dan hasil coding warning latency untuk keenam kasus, mempertahankan ketidakpastian secara eksplisit tanpa "menyelesaikannya" dengan memilih angka yang paling dramatis.

**Tabel 4 Rekonsiliasi data faktual dan status analitis enam kasus**

| Kasus | Tipe kasus | Tanggal | Fakta terverifikasi/resmi | Klaim terbatas/diperdebatkan | Hasil coding warning latency |
|---|---|---|---|---|---|
| Operation Spiderweb, Rusia | Vulnerability-exposing | 1 Juni 2025 | Ukraina menyatakan 117 FPV drone digunakan; Reuters merekonstruksi penyembunyian dalam struktur kayu dan peluncuran dekat pangkalan; Rusia mengakui serangan dan kerusakan | Ukraina awalnya mengklaim 41 pesawat terkena dan 34% pembawa rudal jelajah terdampak; AS memperkirakan sekitar 20 terkena dan 10 hancur | Detection failure = 1; correlation failure = 1 |
| Tower 22, Yordania | Vulnerability-exposing | 28 Januari 2024 | DoD AS mengonfirmasi serangan one-way UAS menewaskan 3 dan melukai lebih dari 40; investigasi CENTCOM diumumkan | Rantai kausal lengkap kegagalan pertahanan tidak ditetapkan sumber publik | Warning/assessment failure = 1; authority latency = 1 |
| Ain al-Asad, Irak | Vulnerability-exposing | 2024 | Reuters melaporkan beberapa serangan drone/roket; satu drone ditembak jatuh dekat perimeter; serangan berikutnya melukai personel | Atribusi dan dampak setiap serangan berbeda antarlaporan | Detection failure = uncertain; response failure (persisten) = 1 |
| Aminggaru /Ilaga, Indonesia | Vulnerability-exposing | 2021–2025 | Pembakaran fasilitas 2021; penutupan sementara dan cedera personel 2022; gangguan bersenjata 2025 | Ancaman bersenjata asimetris terkonfirmasi; hybrid warfare tidak terbukti | Response failure (berulang) = 1; hybridity = tidak terbukti |

| Kasus | Tipe kasus | Tanggal | Fakta terverifikasi/resmi | Klaim terbatas/diperdebatkan | Hasil coding warning latency |
|---|---|---|---|---|---|
| Sultan Hasanuddin, Indonesia (negative case) | Boundary case | 2016–2017; data 2025 | Gangguan laser terhadap pesawat; 7 laporan AirNav dalam satu episode 2017; 39.892 pergerakan pesawat 2025 | Tidak ada bukti operasi negara atau hybrid warfare | Vulnerability = ada; hybridity = tidak ada |
| TACOM, Michigan, AS (successful-anticipation case) | Positive/contrast case | 13 Mei 2025 | DOJ, FBI, dan Army CI mengonfirmasi plot digagalkan; pelaku ditangkap saat meluncurkan drone reconnaissance pada hari serangan | Detail lengkap kronologi internal investigasi tidak dipublikasikan | Detection/correlation success = 0; response success = 0 |

5.6 Lima mekanisme lintas kasus

Analisis komparatif mengidentifikasi lima mekanisme yang berulang, yang secara langsung memetakan ke enam komponen warning latency dan menjadi dasar EHTDF pada bagian 6.

**Paradoks perimeter.** Pertahanan yang dioptimalkan untuk ancaman dari luar instalasi secara langsung dapat dilewati apabila peluncuran, akses, atau gangguan berasal dari lingkungan sipil sekitar atau jalur logistik yang sah—memperbesar detection latency.

**Fragmentasi indikator.** Tanda peringatan tersebar pada keamanan fisik, siber, logistik, personel, penegakan hukum, lalu lintas udara, pemantauan spektrum, dan sumber terbuka—memperbesar correlation latency, sejalan dengan P1.

**Kompresi temporal.** Drone komersial, remote control, akses siber, dan sistem yang telah diposisikan sebelumnya memperpendek interval antara tindakan bermusuhan yang mulai teramati dan dampak yang ditimbulkan—mempersempit ruang waktu bagi response latency, sejalan dengan P2.

**Ambiguitas ambang.** Indikator dini secara inheren mengandung ketidakpastian (Proctor 2025; Betts 1978). Tanpa warning level dan decision trigger yang ditetapkan

sebelumnya, organisasi terjebak antara menunggu kepastian berlebihan atau bereaksi berlebihan—memperbesar assessment latency.

**Celah organisasi.** Kesenjangan paling menentukan pada kelima kasus vulnerability-exposing konsisten berada di antara detection dan action, sejalan dengan Perrow (1984): siapa memiliki informasi, siapa berwenang melakukan fusion, siapa berwenang menaikkan postur, dan siapa berwenang melakukan intervensi—memperbesar authority latency. Kasus TACOM menunjukkan bahwa celah ini dapat dipersempit ketika liaison lintas lembaga (FBI–Army Counterintelligence Command) berfungsi sebagai jembatan otoritas eksplisit.

## 6 DARI TEMUAN MENUJU EHTDF

Early Hybrid Threat Detection Framework (EHTDF) merupakan operasionalisasi dari mekanisme kausal pada bagian 3, bukan produk yang berdiri sendiri. Setiap tahap EHTDF secara langsung menyasar satu atau lebih komponen warning latency yang telah diidentifikasi memburuk pada kelima kasus vulnerability-exposing dan berhasil dipersingkat pada kasus TACOM. Framework ini secara sengaja bukan blueprint surveillance teknis dan tidak menganjurkan pengumpulan data tanpa batas. Fokus utamanya adalah tata kelola analitis: indikator apa yang relevan, bagaimana data difusikan, bagaimana ketidakpastian dinyatakan, dan bagaimana warning diterjemahkan menjadi tindakan protektif proporsional.

Konsisten dengan status epistemik proposisi pada bagian 3.4, EHTDF dinyatakan sebagai kerangka yang **secara teoretis diperkirakan dapat** memperpendek warning latency, bukan sebagai kerangka yang telah terbukti meningkatkan efektivitas deteksi. Setiap tahap disertai satu falsifiable expectation yang dapat diuji pada penelitian lanjutan (bagian 9).

**Tabel 5 Early Hybrid Threat Detection Framework (EHTDF) dan komponen warning latency yang disasar**

| Tahap | Pertanyaan inti | Komponen WL yang disasar | Produk utama | Falsifiable expectation |
|---|---|---|---|---|
| 1. Threat baseline | Apa yang normal bagi pangkalan dan lingkungannya? | Detection latency | Baseline ancaman spesifik pangkalan | Pangkalan dengan baseline yang lebih mutakhir seharusnya menunjukkan detection latency yang lebih pendek dibandingkan |

| Tahap | Pertanyaan inti | Komponen WL yang disasar | Produk utama | Falsifiable expectation |
|---|---|---|---|---|
| | | | | pangkalan tanpa baseline terstruktur |
| 2. Indicator mapping | Aktivitas apa yang dapat mendahului tindakan bermusuhan? | Detection latency, correlation latency | Indicator library dengan confidence dan relevance rating | Semakin lengkap indicator library, semakin tinggi proporsi indikator pra-serangan yang terekam sebelum insiden, bukan hanya pascainsiden |
| 3. Multi-source fusion | Apakah weak signals berkorelasi lintas domain? | Correlation latency | Common threat picture | Organisasi dengan mekanisme fusi lintas domain yang berfungsi seharusnya menunjukkan interval indicator-to-warning yang lebih pendek dibandingkan organisasi dengan struktur silo |
| 4. Dynamic threat assessment | Kombinasi intent, capability, vulnerability, consequence apa yang muncul? | Assessment latency | Threat assessment dengan confidence level | Assessment yang secara eksplisit menyatakan confidence level dan alternative hypotheses seharusnya menghasilkan lebih sedikit overreaction dan underreaction dibandingkan assessment biner |
| 5. Indications and warning | Apakah pola telah melewati decision threshold? | Dissemination latency, authority latency | Warning level dan decision trigger | Decision trigger yang telah diprautorisasi seharusnya mempersingkat authority latency dibandingkan keputusan ad hoc di bawah tekanan waktu |
| 6. Protective response & feedback | Tindakan proporsional apa yang menurunkan risiko sekaligus menghasilkan informasi baru? | Response latency | Actionable protection plan dan reassessment loop | Organisasi dengan graduated response yang telah diprautorisasi seharusnya menunjukkan response latency yang lebih pendek dibandingkan organisasi yang bergantung pada eskalasi manual penuh |

6.1 Indikator bersifat relasional, bukan sekadar daftar

Daftar indikator yang panjang dapat menghasilkan false confidence apabila diperlakukan sebagai checklist mekanistik. Nilai analitis indikator bergantung pada konteks, relasi, dan urutan kemunculan. Pembelian drone komersial di sekitar pangkalan pada umumnya benign; namun observasi drone berulang yang

dikombinasikan dengan fotografi berorientasi sasaran, aktivitas RF tidak lazim, probing kredensial, dan anomali logistik dapat menghasilkan assessment yang berbeda. EHTDF karena itu memprioritaskan correlated patterns dibandingkan observasi tunggal, sekaligus mengurangi false positive: analis mempertahankan alternative explanations, menyatakan confidence level, dan menentukan informasi tambahan yang secara diskriminatif membedakan hipotesis benign dari hostile—sejalan dengan prinsip kewaspadaan kolektif Weick and Sutcliffe (2001).

### 6.2 Tingkat peringatan dan pemicu keputusan

**Tabel 6 Model peringatan dan respons bertingkat**

| Tingkat | Kondisi analitis | Tindakan ilustratif | Logika keputusan |
|---|---|---|---|
| Hijau — Baseline | Tidak ada deviasi bermakna dari baseline | Monitoring rutin, latihan, pengembangan sumber, review OPSEC | Menjaga kesiapan tanpa pembatasan yang tidak perlu |
| Kuning — Anomali | Satu atau lebih indikator tidak biasa tetapi corroboration lemah | Focused collection, liaison check, validasi, peningkatan awareness sementara | Mencari informasi diskriminatif; menghindari overreaction |
| Oranye — Persiapan berkorelasi | Beberapa indikator lintas domain menunjukkan persiapan hostile yang plausible | Menaikkan posture, membatasi akses sensitif, meningkatkan C-UAS/cyber readiness, mempertimbangkan dispersal/deception | Bertindak sebelum kepastian penuh bila consequence dan plausibility membenarkan tindakan proporsional |
| Merah — Imminent/hostile action | Indikator high-confidence menunjukkan serangan, penetrasi, atau peluncuran dalam waktu dekat | Melaksanakan protective/defensive response sesuai kewenangan dan rules yang berlaku | Memprioritaskan keselamatan, mission continuity, dan rapid reassessment |

## 7 PEMBAHASAN

### 7.1 Persoalan utama adalah arsitektur keputusan, bukan kelangkaan sensor

Kasus-kasus yang dianalisis secara konsisten menunjukkan bahwa variabel penentu keberhasilan atau kegagalan pertahanan pangkalan udara lebih sering berupa organizational latency dibandingkan kekurangan kapabilitas sensor teknis. Organisasi militer cenderung merespons ancaman baru terutama melalui pengadaan

sensor atau interceptor tambahan. Kapabilitas semacam itu diperlukan, tetapi hanya menyelesaikan sebagian persoalan. Apabila informasi tetap terkurung dalam silo, anomali akses tidak dihubungkan dengan kejadian siber, laporan masyarakat tidak sampai kepada analis, atau warning tidak memiliki kewenangan memicu tindakan tertentu, penambahan sensor hanya menghasilkan lebih banyak data yang tidak terkorelasi—konsisten dengan P1 dan P3, serta dengan argumen Betts (1978) bahwa kegagalan intelijen strategis lebih sering merupakan persoalan interaksi antara analisis dan keputusan dibandingkan sekadar kegagalan mengumpulkan data.

7.2 Penjelasan alternatif dan kondisi batas

Bagian ini secara sengaja diberi ruang tersendiri karena argumentasi menuju EHTDF pada bagian 6 dapat tampak terlalu lancar tanpa mempertimbangkan penjelasan saingan. EHTDF tidak mengasumsikan bahwa seluruh kegagalan pertahanan pangkalan merupakan intelligence failure dalam pengertian yang dirumuskan artikel ini. Pada sebagian kasus, indikator pra-serangan mungkin memang tidak tersedia secara memadai dalam sumber terbuka, sehingga peristiwa lebih tepat digambarkan sebagai true surprise daripada correlation failure—kondisi yang tidak dapat dibedakan dari detection failure hanya berdasarkan bukti pascainsiden, sebuah keterbatasan yang diakui secara eksplisit dalam codebook pada Tabel 3 melalui kategori "uncertain". Pada kasus lain, informasi mengenai ancaman mungkin memang tersedia tepat waktu, tetapi kapasitas teknis untuk merespons—jumlah interceptor, jangkauan sensor, kecepatan reaksi sistem senjata—tidak memadai, sehingga persoalannya lebih dekat pada technological insufficiency dibandingkan organizational latency. Pada kasus lain lagi, keputusan untuk tidak segera bertindak terhadap indikator ambigu mungkin merupakan pilihan rasional, bukan kegagalan, karena biaya false-positive—mengganggu operasi normal, merusak hubungan sipil-militer, atau memicu eskalasi yang tidak diinginkan—dinilai terlalu tinggi dibandingkan probabilitas ancaman yang belum terkonfirmasi; penjelasan ini bersinggungan dengan literatur bureaucratic politics dan command risk aversion yang tidak dieksplorasi secara mendalam dalam artikel ini. Deception effectiveness pihak penyerang—sebagaimana ditunjukkan secara eksplisit oleh kasus Spiderweb melalui penyamaran drone sebagai muatan sipil biasa—juga merupakan penjelasan yang bersaing dengan penjelasan organizational latency murni, meskipun keduanya tidak saling eksklusif: efektivitas deception justru bekerja dengan memanfaatkan celah korelasi yang sama yang dijelaskan P1.

Artikel ini tidak mengklaim mampu memisahkan secara definitif kontribusi relatif masing-masing penjelasan alternatif tersebut terhadap setiap kasus, mengingat keterbatasan sumber terbuka yang dinyatakan pada bagian 9. Namun, pola berulang pada kelima kasus vulnerability-exposing—di mana celah paling konsisten berada di antara detection dan action, bukan pada ketiadaan sensor—memberikan dukungan yang cukup kuat bagi proposisi organizational-temporal vulnerability sebagai mekanisme dominan, tanpa mengeklaim bahwa mekanisme tersebut satu-satunya yang beroperasi.

### 7.3 Kontraintelijen memperluas pertahanan ke sisi kiri peluncuran

Pertahanan pangkalan udara secara tradisional bekerja paling kuat ketika ancaman telah dapat diamati secara fisik, pada sisi kanan garis waktu serangan. Kontraintelijen menciptakan nilai tambah lebih dini dengan mempertanyakan apa yang harus diketahui, diakses, dipindahkan, dikomunikasikan, atau disembunyikan lawan sebelum serangan dapat dilaksanakan—prinsip yang secara konkret ditunjukkan kasus TACOM, ketika disrupsi terjadi pada tahap reconnaissance dan fasilitasi logistik, bukan pada saat drone benar-benar mengudara untuk menyerang. Tidak seluruh preparation activity dapat dideteksi secara realistis, tetapi preparation chain secara keseluruhan menyediakan jauh lebih banyak observation points dibandingkan weapon terminal semata (P4). Implikasinya, investasi pada counter-unmanned aerial system perlu dilengkapi logistics awareness, insider-risk programme, cyber threat intelligence, information protection, liaison aktif dengan penegak hukum dan otoritas penerbangan sipil, serta intelligence fusion yang benar-benar berfungsi lintas domain.

### 7.4 Disiplin konseptual meningkatkan, bukan mengurangi, relevansi operasional

Jika setiap ancaman nonkonvensional otomatis diberi label hibrida, istilah tersebut kehilangan kemampuan membedakan mekanisme kausal yang berbeda (Bartoszewicz 2025). Sultan Hasanuddin, yang secara sengaja diperlakukan sebagai negative/boundary case pada bagian 5.3, menunjukkan konkretnya pentingnya restraint tersebut: kerentanan penerbangan terhadap gangguan eksternal berbiaya rendah nyata ada, tetapi bukti hybridity tidak ada. Aminggaru/Ilaga memberikan bukti kuat mengenai asymmetric disruption, tetapi juga tidak membuktikan kampanye hibrida yang terkoordinasi secara strategis. Justru klasifikasi yang lebih sempit dan disiplin inilah yang memperkuat kontribusi artikel, karena EHTDF dapat

digunakan baik ketika mekanisme hibrida terbukti secara meyakinkan, maupun tetap berguna bagi ancaman asimetris dan kompleks yang lebih luas.

### 7.5 Kerentanan struktural, kewaspadaan kolektif, dan batas kemampuan organisasi

Integrasi antara Perrow (1984) dan Weick and Sutcliffe (2001) menghasilkan pemahaman realistis mengenai apa yang dapat dan tidak dapat dicapai EHTDF. Mengikuti Perrow, artikel ini tidak mengklaim bahwa pangkalan udara sebagai sistem sosio-teknis kompleks-terpaut-erat dapat sepenuhnya dibebaskan dari risiko kegagalan struktural; sejumlah kegagalan, sebagaimana ditunjukkan kasus Tower 22, kemungkinan besar tetap terjadi meskipun sistem peringatan dini dirancang dengan baik. Namun mengikuti Weick and Sutcliffe—dan dikonfirmasi secara konkret oleh kasus TACOM—probabilitas dan dampak kegagalan tersebut dapat dikurangi signifikan melalui budaya organisasional yang mempraktikkan kewaspadaan kolektif. EHTDF pada dasarnya menerjemahkan prinsip HRO yang abstrak menjadi arsitektur operasional yang konkret bagi konteks pertahanan pangkalan udara.

### 7.6 Pengamanan hukum dan etika sebagai persyaratan operasional

Model kontraintelijen antisipatif membawa risiko governance yang nyata. Pengumpulan data mengenai personel, kontraktor, masyarakat sekitar, aktivitas digital, atau logistik komersial dapat menjadi terlalu luas apabila indikator ancaman tidak didefinisikan secara ketat. EHTDF karena itu memasukkan necessity, proportionality, role-based access, auditability, source protection, dan periodic review sebagai design requirements sejak awal. Indikator harus berbasis perilaku dan ancaman aktual, bukan identitas kelompok. Safeguards ini bukan penghambat efektivitas, melainkan prasyarat kualitas sinyal dan legitimasi institusional jangka panjang.

## 8 IMPLIKASI BAGI RESILIENSI KEKUATAN UDARA INDONESIA

Berbeda dari pendekatan yang menempelkan konteks Indonesia sebagai kewajiban topikal, bagian ini menurunkan relevansi Indonesia secara eksplisit dari teori warning latency pada bagian 3, melalui rantai logika berikut: geografi kepulauan → ketergantungan tinggi pada simpul udara sebagai penghubung antarwilayah →

tumpang tindih infrastruktur sipil-militer pada banyak bandar udara → rantai logistik yang terdistribusi dan sulit diawasi penuh → lingkungan ancaman yang heterogen antarwilayah → kebutuhan koordinasi lintas domain yang jauh lebih tinggi dibandingkan negara dengan geografi kontinental. Setiap tautan dalam rantai ini secara langsung memperbesar risiko fragmentasi indikator (P1) dan memperpanjang correlation latency serta authority latency yang menjadi inti argumen artikel—menjadikan Indonesia sebuah theoretically relevant setting, bukan sekadar lokasi aplikasi tambahan.

Pertama, fungsi kontraintelijen, pengamanan pangkalan, pertahanan siber, operasi, keselamatan penerbangan, dan liaison eksternal memerlukan mekanisme formal untuk menghasilkan shared threat picture yang dapat diakses tepat waktu, dengan kejelasan jalur informasi, ownership data, dan decision authority pada setiap tahap EHTDF—bukan semata pembentukan organisasi baru.

Kedua, setiap pangkalan strategis idealnya memiliki living threat baseline dan indicator library yang dikaitkan dengan misi, geografi, infrastruktur sipil sekitar, model akses, rantai logistik, lingkungan spektrum, dan eksposur informasi publik. Pangkalan di wilayah perkotaan padat, pangkalan yang berbagi fasilitas dengan penerbangan sipil sebagaimana lazim di Indonesia, dan pangkalan pada wilayah terpencil seperti diilustrasikan kasus Aminggaru/Ilaga akan memiliki pola normal dan anomali yang berbeda, sehingga baseline generik seragam berisiko tidak sensitif terhadap kondisi lokal.

Ketiga, desain latihan kesiapan perlu bergerak ke sisi kiri dari titik serangan terminal. Latihan counter-UAS yang baru dimulai ketika drone melewati perimeter hanya menguji lapisan terminal dan mengabaikan preparation chain. Skenario yang lebih menantang harus dimulai dari weak precursor signals: reconnaissance mencurigakan, akun terkompromikan, akses vendor anomali, irregularity logistik, atau klaster laporan sipil—model yang secara konkret dicontohkan kasus TACOM. Ukuran keberhasilan bukan sekadar kecepatan intersepsi teknis, melainkan apakah organisasi mampu mengorelasikan sinyal, menyatakan ketidakpastian secara jujur, menaikkan warning level secara proporsional, dan bertindak sebelum hostile launch.

Keempat, resiliensi kekuatan udara perlu dinilai berdasarkan mission continuity, bukan semata perimeter integrity. Dispersal, redundansi, deception, alternative communications, continuity planning, dan rapid recovery mengurangi strategic payoff bagi lawan bahkan apabila penetrasi awal berhasil. Kontraintelijen

dan resiliensi bersifat komplementer: yang pertama mengenali dan mengganggu persiapan lawan sedini mungkin (memperpendek warning latency), sedangkan yang kedua membatasi consequence apabila pencegahan gagal.

Kelima, liaison sipil-militer sangat penting dalam konteks geografis dan institusional Indonesia. Otoritas penerbangan komersial, AirNav Indonesia, kepolisian, pemerintah daerah, operator telekomunikasi dan infrastruktur kritis, serta masyarakat sekitar fasilitas udara dapat memiliki akses terhadap indikator awal yang tidak tersedia bagi sistem intelijen militer yang bekerja terisolasi—sebagaimana ditunjukkan kasus TACOM melalui liaison FBI–Army Counterintelligence Command. Integrasi tersebut harus rule-governed dan purpose-limited; tujuannya bukan agregasi data tanpa batas, melainkan memastikan informasi ancaman relevan mencapai otoritas yang mampu menilai dan bertindak tepat waktu.

## 9 KETERBATASAN DAN AGENDA PENELITIAN LANJUTAN

Artikel ini memiliki lima keterbatasan yang dinyatakan secara eksplisit. Pertama, analisis sepenuhnya menggunakan sumber terbuka, sehingga tidak dapat menilai prosedur kontraintelijen terklasifikasi, cakupan sensor sesungguhnya, atau rules of engagement internal. Kedua, keenam kasus berbeda signifikan dalam aktor, geografi, jenis sasaran, dan konteks politik; perbandingan karena itu mengidentifikasi plausible causal mechanisms, bukan regularitas kausal universal, sejalan dengan pembatasan klaim metodologis pada subbagian 4.1. Ketiga, pemberitaan konflik yang sedang berlangsung, khususnya Spiderweb, mengandung strategic communication dan battle-damage assessment yang tidak lengkap; mitigasi dilakukan dengan mempertahankan perbedaan eksplisit antara klaim Ukraina, assessment Amerika Serikat, pengakuan Rusia, dan pelaporan independen. Keempat, kasus TACOM bukan pangkalan udara, sehingga generalisasi lintas domain penerbangan tetap memerlukan kehati-hatian, sebagaimana dinyatakan pada subbagian 4.2; kasus ini berfungsi sebagai kontras mekanisme, bukan bukti domain-spesifik. Kelima, dan yang paling mendasar, EHTDF merupakan framework konseptual yang belum diuji secara empiris melalui field research. **Framework ini karena itu sebaiknya diinterpretasikan sebagai proposisi yang diturunkan secara analitis dan diinformasikan secara empiris, bukan sebagai doktrin operasional yang telah tervalidasi.**

Penelitian lanjutan perlu menempuh lima langkah metodologis untuk menguji falsifiable expectations pada Tabel 5 dan proposisi P1–P4 pada bagian 3.4. Pertama, wawancara semi-terstruktur dengan unsur intelijen dan pengamanan pada pangkalan udara terpilih di Indonesia, sebagaimana semula direncanakan dalam outline riset yang menjadi titik tolak artikel ini. Kedua, tabletop exercise berbasis skenario dari keenam kasus untuk menguji sejauh mana personel pada berbagai level organisasi mampu mengoperasionalkan EHTDF secara praktis di bawah tekanan waktu, sekaligus mengukur secara empiris komponen warning latency pada simulasi. Ketiga, process tracing yang lebih mendalam terhadap satu atau dua kasus tunggal, dengan hoop tests dan smoking-gun tests yang lebih ketat apabila akses dokumen internal memungkinkan, untuk menguji proposisi P1–P4 secara lebih presisi daripada yang dimungkinkan structured-focused comparison berbasis dokumen terbuka. Keempat, Delphi study yang melibatkan pakar kontraintelijen, force protection, dan keamanan penerbangan untuk memvalidasi indicator library dan ambang warning level pada Tabel 5 dan Tabel 6. Kelima, red-team exercise pada pangkalan terpilih untuk menguji trade-off antara false-positive dan false-negative dalam penerapan EHTDF, serta menguji desain kewenangan berbagi informasi lintas fungsi organisasi pada bagian 8.

## 10 KESIMPULAN

Kerentanan pangkalan udara dalam konflik kontemporer dibentuk oleh interaksi antara infrastruktur tetap bernilai tinggi dan sistem serang yang terdistribusi, berbiaya rendah, terselubung, dan dimungkinkan teknologi komersial. Namun demikian, keenam kasus yang dianalisis—termasuk satu kasus batas negatif dan satu kasus kontras keberhasilan antisipasi—secara konsisten menunjukkan bahwa persoalan penentu bukanlah ketersediaan teknologi pertahanan, melainkan warning latency: interval organisasional kumulatif antara indikator yang secara potensial dapat dikenali dan tindakan protektif yang relevan. Operation Spiderweb menunjukkan bagaimana strategic depth dapat ditembus ketika kapasitas peluncuran diinfiltrasikan melalui logistik sipil. Tower 22 dan Ain al-Asad menunjukkan bahwa efektivitas warning bergantung pada keseluruhan rantai komponen, bukan satu titik tunggal. Aminggaru/Ilaga dan Sultan Hasanuddin menunjukkan, dengan karakter

yang secara analitis berbeda—satu kasus vulnerability-exposing, satu kasus batas negatif—bagaimana disiplin konseptual mengenai istilah "hibrida" tetap harus dipertahankan bahkan pada kasus domestik. TACOM menunjukkan bahwa warning latency dapat dipersingkat secara nyata ketika liaison kontraintelijen-penegak hukum berfungsi pada tahap preparation chain, bukan pada fase terminal.

Argumen utama artikel ini, dipadatkan menjadi satu proposisi sentral, adalah bahwa kerentanan pangkalan udara terhadap ancaman hibrida terutama merupakan persoalan organizational-temporal vulnerability, bukan semata physical vulnerability. Kontraintelijen antisipatif meningkatkan resiliensi dengan memperluas decision space melalui pemindahan fokus pertahanan dari weapon interception menuju adversary preparation chain—mekanisme yang dioperasionalkan EHTDF melalui enam tahap yang masing-masing menyasar komponen warning latency tertentu, dan yang dinyatakan sebagai serangkaian falsifiable expectations, bukan doktrin yang telah tervalidasi.

Kontribusi teoretis artikel ini terletak pada pembagian labour analitis yang eksplisit antara teori kegagalan intelijen strategis (Betts 1978), teori kecelakaan normal pada sistem kompleks (Perrow 1984), dan teori organisasi berkinerja tinggi (Weick and Sutcliffe 2001), yang bersama-sama menjelaskan komponen warning latency yang berbeda-beda dan menghasilkan empat proposisi yang dapat diuji pada penelitian lanjutan. Disiplin epistemik dipertahankan secara konsisten: fakta observasional, klaim resmi, assessment pihak ketiga, dan inferensi analitis penulis tetap dapat dibedakan pembaca sepanjang artikel, sebab ambiguitas bukan hanya metode yang digunakan lawan untuk mengaburkan atribusi, tetapi juga bahaya metodologis bagi peneliti yang mengkaji fenomena tersebut. Pendekatan yang lebih presisi secara konseptual tidak menghilangkan ketidakpastian yang inheren dalam setiap sistem peringatan, sebagaimana ditegaskan Betts (1978), tetapi menghasilkan warning yang jauh lebih dapat dipertanggungjawabkan secara akademik dan lebih berguna secara praktis, termasuk bagi penguatan resiliensi kekuatan udara Indonesia.

## DEKLARASI

**Ketersediaan data** Penelitian ini menggunakan publikasi ilmiah, dokumen resmi, dan pemberitaan media bereputasi yang tersedia untuk publik. Tidak ada data operasional terklasifikasi atau terbatas yang direproduksi dalam artikel ini.

**Persetujuan etik** Tidak berlaku karena penelitian ini bersifat berbasis dokumen dan tidak menggunakan partisipan manusia atau data pribadi.

**Kontribusi penulis** Seluruh tahap konseptualisasi, analisis, dan penulisan dilakukan oleh penulis yang tercantum pada halaman judul.

DAFTAR PUSTAKA

Arreguín-Toft I (2005) How the Weak Win Wars: A Theory of Asymmetric Conflict. Cambridge University Press, Cambridge.

Bartoszewicz MG (2025) Hybrid everything, operational nothing: conceptual drift, perpetual crisis, and the failure to prepare for proxy terrorism. European Journal for Security Research. https://doi.org/10.1007/s41125-025-00107-2

Betts RK (1978) Analysis, war, and decision: why intelligence failures are inevitable. World Politics 31(1):61–89. https://doi.org/10.2307/2009967

Deppe C, Schaal GS (2024) Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data 7:1452129. https://doi.org/10.3389/fdata.2024.1452129

Department of the Air Force (2023) Air Force Doctrine Publication 3-10: Force Protection. LeMay Center for Doctrine Development and Education, Maxwell AFB.

Department of the Air Force (2025) Air Force Doctrine Publication 3-0: Operations. LeMay Center for Doctrine Development and Education, Maxwell AFB.

Department of the Air Force (2026) Air Force Doctrine Publication 2-0: Intelligence. LeMay Center for Doctrine Development and Education, Maxwell AFB.

Gentry JA, Gordon JS (2019) Strategic Warning Intelligence: History, Challenges, and Prospects. Georgetown University Press, Washington, DC.

Hoffman FG (2007) Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington.

Kementerian Perhubungan Republik Indonesia, Direktorat Jenderal Perhubungan Udara (2026) Profil Bandar Udara Sultan Hasanuddin dan data lalu lintas udara 2025.

Kementerian Perhubungan Republik Indonesia, Direktorat Jenderal Perhubungan Udara (2026) Data Bandar Udara Ilaga/Aminggaru.

Lincoln YS, Guba EG (1985) Naturalistic Inquiry. Sage Publications, Beverly Hills.

Lykke AF Jr (1989) Military Strategy: Theory and Application. U.S. Army War College, Carlisle.

Nilsson N, Weissmann M, Palmertz B (2026) Hybrid threats and the intelligence community: priming for a volatile age. International Journal of Intelligence and CounterIntelligence. https://doi.org/10.1080/08850607.2024.2435265

Perrow C (1984) Normal Accidents: Living with High-Risk Technologies. Basic Books, New York.

Proctor JP (2025) Exploring the meaning and challenges of early warning. Intelligence and National Security 40(5):817–837. https://doi.org/10.1080/02684527.2025.2526930

Prunckun H (2019) Counterintelligence Theory and Practice, 2nd edn. Rowman & Littlefield, Lanham.

Reuters (2024) Reporting on drone and rocket attacks against Ain al-Asad Air Base, Iraq, 2024.

Reuters (2025a) To attack Russian air bases, Ukrainian spies hid drones in wooden sheds. 1 June 2025.

Reuters (2025b) How Ukraine pulled off an audacious attack deep inside Russia. Reuters Graphics, 4 June 2025.

Reuters (2025c) Ukraine hit fewer Russian planes than it estimated, U.S. officials say. 4 June 2025.

U.S. Attorney's Office, Eastern District of Michigan (2025) Melvindale man arrested and charged with attempting to attack a military base on behalf of ISIS. Press release, U.S. Department of Justice, 14 May 2025.

U.S. Department of Defense (2024) Three U.S. service members killed, others injured in Jordan following drone attack. DoD News, 29 January 2024.

Weick KE, Sutcliffe KM (2001) Managing the Unexpected: Assuring High Performance in an Age of Complexity. Jossey-Bass, San Francisco.

Weissmann M, Nilsson N (2024) Current intelligence and assessments: information flows and the tension between quality and speed. International Journal of Intelligence and CounterIntelligence. https://doi.org/10.1080/08850607.2023.2296886

Wohlstetter R (1962) Pearl Harbor: Warning and Decision. Stanford University Press, Stanford.

ANTARA (2016) Masyarakat jangan ganggu pesawat terbang dengan laser. 10 Juli 2016.

ANTARA (2021) Pemberitaan mengenai pembakaran fasilitas Bandara Ilaga/Aminggaru, Juni 2021.

ANTARA (2022) Bandara Aminggaru ditutup sementara akibat gangguan kelompok bersenjata. 19 Februari 2022.

ANTARA (2025) Pemberitaan mengenai gangguan bersenjata dan pengamanan Bandara Aminggaru/Ilaga, Juni 2025.