Radar dan SIGINT di Asia-Pasifik: Implikasi Strategis bagi Pertahanan dan Kedaulatan Indonesia

Description

Abstrak Eksekutif

Studi ini menyajikan analisis mendalam mengenai hubungan interdependensi antara sistem radar dan Signal Intelligence (SIGINT) di kawasan Asia-Pasifik, menguraikan dampaknya terhadap lanskap keamanan regional, dan mengeksplorasi implikasi krusialnya bagi Indonesia. Temuan utama menunjukkan bahwa emisi radar, yang secara fundamental dirancang untuk mendeteksi ancaman, kini menjadi sumber intelijen vital bagi pihak lawan. Hal ini mendorong perlombaan teknologi yang intens dalam ranah peperangan elektronik (EW). Aktor utama seperti Tiongkok, Amerika Serikat, dan aliansi Five Eyes, khususnya Australia, telah mengembangkan kapabilitas SIGINT yang sangat canggih—mulai dari jaringan stasiun darat dan satelit hingga platform udara khusus—untuk mencapai keunggulan informasi. Bagi Indonesia, persaingan ini menghadirkan tantangan signifikan terhadap kedaulatan maritim dan udara, menyoroti kesenjangan kritis dalam modernisasi pertahanan, pengembangan sumber daya manusia, dan kerangka regulasi. Laporan ini merekomendasikan sebuah strategi holistik yang tidak hanya berfokus pada pengadaan alutsista, tetapi juga pada penguatan kapabilitas intelijen sinyal dan pertahanan siber domestik, didukung oleh kerangka hukum yang solid dan kebijakan luar negeri yang seimbang.

Pendahuluan

Lanskap keamanan di Asia-Pasifik ditandai dengan peningkatan ketegangan geopolitik, modernisasi militer yang cepat, dan persaingan strategis antara kekuatan besar. Di tengah dinamika ini, pertarungan untuk menguasai domain informasi, khususnya melalui interaksi antara sistem radar dan Signal Intelligence (SIGINT), telah menjadi elemen sentral dalam strategi pertahanan modern. Laporan ini akan mengupas interaksi tersebut secara mendalam dan merinci implikasinya bagi Indonesia. Analisis ini akan berfokus pada domain teknologi dan geopolitik yang relevan, sementara materi yang secara eksklusif membahas isu internal kepolisian (Polri) di luar konteks ini akan diabaikan.

Laporan ini berlandaskan pada pemahaman konseptual yang kokoh mengenai istilah-istilah kunci. Kata “radar” sendiri berasal dari akronim *Radio Detection and Ranging*. Fungsinya adalah menggunakan gelombang radio untuk menentukan jarak dan kecepatan suatu target. Secara umum, sebuah sistem radar terdiri dari pemancar yang mengirimkan sinyal radio dan penerima yang menangkap energi yang dipantulkan dari target. Radar cuaca modern, misalnya, menggunakan prinsip Doppler untuk mendeteksi pergeseran fase gelombang yang kembali, yang digunakan untuk menghitung kecepatan target.[1]

Di sisi lain, *Signal Intelligence* (SIGINT) merupakan kategori pengumpulan intelijen yang dilakukan dengan menyadap sinyal. SIGINT memiliki dua sub-disiplin utama: *Communications Intelligence* (COMINT) yang menargetkan komunikasi antarmanusia seperti percakapan radio atau pesan, dan *Electronic Intelligence* (ELINT) yang menargetkan sinyal elektronik yang tidak digunakan untuk komunikasi, seperti emisi dari radar dan sistem senjata.[3] Hubungan antara radar dan SIGINT menciptakan sebuah paradoks strategis. Radar dirancang untuk bertindak proaktif dengan memancarkan sinyal guna mendapatkan informasi, tetapi tindakan pemancaran ini secara inheren menjadi sumber intelijen bagi sistem SIGINT lawan yang beroperasi secara pasif. Semakin sering dan kuat suatu radar memancarkan sinyal, semakin mudah ia dideteksi dan dianalisis oleh musuh.

Bagian I: Fondasi Teknis dan Strategis: Kemampuan Radar dan Peperangan Elektronik

1.1 Kemampuan Deteksi Radar dan Perannya dalam Kekuatan Udara

Radar adalah “mata” yang vital dalam peperangan modern, terutama di domain udara. Laporan ini secara rinci menjelaskan bagaimana sistem radar beroperasi, terutama dalam konteks deteksi dan pelacakan target. Radar pulsa Doppler, contohnya WSR-88D, bekerja dengan mengirimkan gelombang radio dalam pulsa yang sangat singkat dan kemudian mendengarkan pantulannya.[2] Dengan mengukur waktu antara pengiriman dan penerimaan pulsa, sistem dapat menghitung jarak target. Kemampuan Doppler memungkinkan radar untuk melangkah lebih jauh dengan menganalisis pergeseran fase (frekuensi) dari sinyal yang dipantulkan, yang mengindikasikan kecepatan target relatif terhadap radar.

Fungsi radar sangat esensial untuk pertahanan udara, navigasi, dan pelacakan target. Namun, di tengah kecanggihan ini, terdapat kerentanan mendasar. Sinyal yang dipancarkan oleh radar, yang dirancang untuk deteksi, secara instan menjadi sumber informasi penting bagi lawan yang memiliki kapabilitas SIGINT. Ini mengubah peran radar dari sekadar alat deteksi menjadi aset strategis yang juga harus dilindungi. Kehadiran suatu radar di perbatasan atau di wilayah tertentu tidak hanya memberikan kapabilitas defensif, tetapi juga secara langsung mengungkapkan keberadaannya kepada musuh.

1.2 Hubungan Simbiotik: Bagaimana Radar Menjadi Sumber Utama Intelijen Sinyal

Emisi radar yang dirancang untuk deteksi justru menjadi target utama bagi sistem ELINT. Sistem ELINT, yang bersifat pasif, mengumpulkan dan menganalisis sinyal Frekuensi Radio (RF) dari radar musuh untuk mengidentifikasi karakteristik teknisnya seperti frekuensi, pola pulsa, dan jenis modulasi.[7] Analisis ini memungkinkan operator intelijen untuk mengidentifikasi jenis dan tujuan sistem radar, misalnya apakah itu radar pencari udara atau sistem pelacak tembakan untuk rudal permukaan-ke-

udara (SAM).[7]

Dalam domain ELINT, terdapat dua cabang utama yang berfokus pada analisis ini:

- **Technical ELINT (TechELINT):** Berfokus pada pendeskripsian struktur sinyal, karakteristik emisi, dan fungsi sistem. Informasi yang dihasilkan digunakan untuk mengembangkan peralatan deteksi radar lawan atau *countermeasure*.[8]
- **Operational ELINT (OpELINT):** Berfokus pada melokalisasi target ELINT dan menentukan pola operasional dari sistem tersebut. Informasi ini krusial untuk perencanaan misi taktis.[8]

Operasi SIGINT, termasuk ELINT, tidak bergantung pada satu sensor, melainkan pada jaringan penerima yang terkoordinasi secara global. Jaringan ini dapat terdiri dari stasiun darat, kapal intelijen, pesawat pengintai, dan satelit.[4] Dengan proliferasi teknologi modern seperti kecerdasan buatan (*AI*) dan pembelajaran mesin (*machine learning*), data dari berbagai sumber dapat diproses secara *real-time*.[10] Hal ini menekankan bahwa perlombaan senjata modern tidak lagi hanya tentang platform fisik, tetapi juga tentang kecepatan dan kecanggihan dalam mengumpulkan, menganalisis, dan memanfaatkan data sinyal untuk mendapatkan keunggulan informasi. Pihak yang paling rinci dalam SIGINT adalah pihak yang paling cepat dalam siklus ini.

1.3 Konsep “Transparent Battlefield” dan Peran Peperangan Elektronik (EW)

Proses pengumpulan intelijen yang masif melalui berbagai sensor telah menciptakan apa yang disebut sebagai “medan perang transparan”.[11] Dalam lingkungan ini, pasukan menjadi lebih rentan terhadap deteksi dan serangan presisi. Peperangan Elektronik (EW) muncul sebagai respons strategis terhadap tantangan ini. EW didefinisikan sebagai penggunaan spektrum elektromagnetik untuk menyerang musuh atau mencegah mereka menggunakan spektrum tersebut secara efektif.[13]

EW terbagi menjadi tiga sub-divisi utama:

- **Electronic Attack (EA):** Tindakan ofensif seperti *jamming* (mengacaukan) radar atau komunikasi untuk menetralkan kemampuan musuh.
- **Electronic Protection (EP):** Tindakan defensif untuk melindungi aset sendiri dari efek serangan elektronik musuh.
- **Electronic Warfare Support (ES):** Tindakan untuk mendeteksi, mencegat, dan melokalisasi emisi musuh untuk pengenalan ancaman secara *real-time*.[13]

Dalam konteks ini, peperangan modern telah bergeser dari dominasi konvensional menjadi dominasi informasi. Kemampuan untuk mengendalikan, mengaburkan, atau menipu spektrum elektromagnetik telah menjadi prasyarat untuk keberhasilan operasi militer.[14] Negara-negara maju seperti Tiongkok dan Australia, dengan pesawat EW seperti EA-18G Growler, menunjukkan pergeseran fokus dari platform fisik ke penguasaan spektrum elektromagnetik. Keunggulan informasi yang didapat dari SIGINT kini dapat menghasilkan efek strategis yang sama atau bahkan lebih besar dari keunggulan senjata konvensional.

Bagian II: Profil Kapabilitas SIGINT dan Kekuatan Udara Regional

2.1 Tiongkok: Jaringan yang Mendalam dan Strategi Penyangkalan (A2/AD)

Tiongkok, melalui departemen teknisnya, memiliki kapabilitas SIGINT paling ekstensif di kawasan Asia-Pasifik.[15] Tiongkok mengoperasikan puluhan stasiun SIGINT darat yang tersebar di seluruh negeri untuk memantau sinyal dari negara-negara tetangga, termasuk Rusia, Taiwan, Jepang, Korea Selatan, India, dan Asia Tenggara.[15] Fasilitas SIGINT besar di Pulau Hainan secara khusus memantau aktivitas angkatan laut Amerika Serikat di Laut Cina Selatan.[15] Selain itu, Tiongkok telah mengembangkan kapal-kapal pengumpul intelijen sinyal (

AGI-type vessels) untuk memantau operasi militer di kawasan.[15] Jaringan pengawasan ini juga diperkuat oleh jaringan sensor dan sistem komunikasi tanpa awak yang dipasang di antara Kepulauan Hainan dan Paracel, dilengkapi dengan radar kecil untuk deteksi dini.[18]

Kapabilitas SIGINT Tiongkok ini terintegrasi erat dengan strategi pertahanan utamanya, yaitu *Anti-Access/Area Denial* (A2/AD). Strategi ini dirancang untuk mencegah kekuatan lawan memasuki atau beroperasi secara bebas di area tertentu.[19] SIGINT dan EW menjadi komponen krusial dalam strategi A2/AD ini, yang bertujuan untuk melumpuhkan sistem Komando, Kontrol, Komunikasi, Komputer, Intelijen, Pengawasan, dan Pengintaian (

C4ISR) musuh.[21] Pendekatan Tiongkok menunjukkan bahwa alih-alih mencoba meniru keunggulan konvensional AS, Tiongkok mengembangkan doktrin asimetris yang berfokus pada menargetkan sistem saraf lawan. Dengan demikian, pengumpulan intelijen pasif (SIGINT) secara langsung mendukung operasi ofensif (A2/AD dan EW), menjadikannya bukan hanya perlombaan teknologi, tetapi juga perlombaan doktrin militer.

2.2 Amerika Serikat dan Aliansi Five Eyes: Jangkauan Global dan Interoperabilitas

Amerika Serikat, bersama Australia, Kanada, Inggris, dan Selandia Baru, membentuk aliansi berbagi intelijen sinyal yang dikenal sebagai Five Eyes.[23] Aliansi ini memungkinkan Australia untuk mendapatkan keuntungan teknologi, inovasi, keahlian, dan jangkauan intelijen yang akan sulit dicapai secara mandiri.[23] Australia berperan sebagai pusat SIGINT di kawasan, dengan beberapa fasilitas kunci:

- **Pine Gap:** Fasilitas gabungan AS-Australia di dekat Alice Springs, berfungsi sebagai stasiun kontrol untuk satelit SIGINT. Peran utamanya adalah mendeteksi peluncuran rudal, melacak sinyal elektronik, dan mengumpulkan data komunikasi di seluruh Hemisfer Timur.[25]
- **Stasiun Kojarena:** Stasiun komunikasi satelit yang mencegat komunikasi dari satelit regional, termasuk yang digunakan oleh Rusia, Tiongkok, Jepang, India, dan Pakistan.[27]
- **Stasiun Shoal Bay:** Terletak di dekat Darwin, stasiun ini secara spesifik memantau komunikasi satelit Palapa dan komunikasi radio Indonesia. Selama krisis Timor Timur, stasiun ini bahkan mencegat transmisi radio antara unit militer Indonesia dan markas di Bali.[28]

Kapabilitas udara dalam aliansi ini juga sangat canggih. Angkatan Udara Australia (*RAAF*) mengoperasikan jet tempur F-35A Lightning II, yang merupakan pesawat tempur generasi kelima dengan sensor canggih dan kemampuan fusi data untuk memberikan kesadaran situasional.[30] RAAF juga memiliki pesawat peperangan elektronik EA-18G Growler, yang dirancang untuk mengganggu, menipu, dan menolak sistem elektronik militer lawan, serta menyediakan data ELINT.[32]

Inisiatif keamanan trilateral **AUKUS** (Australia, Inggris, AS) semakin memperkuat kapabilitas ini.[34] Pilar I AUKUS berfokus pada akuisisi kapal selam bertenaga nuklir (

SSN) oleh Australia. Ini akan secara signifikan meningkatkan kemampuan pengawasan bawah air, jangkauan, dan kemampuan siluman yang diperlukan untuk operasi SIGINT yang efektif.[34] Namun, terungkapnya peran Stasiun Shoal Bay dalam memantau komunikasi Indonesia menimbulkan ketegangan antara diplomasi persahabatan dan realitas pengumpulan intelijen yang pragmatis. Hal ini menunjukkan bahwa Indonesia tidak dapat menganggap hubungan dengan mitra terdekat sekalipun sebagai jaminan penuh dari pengawasan. Kedaulatan kini tidak hanya soal teritori fisik, tetapi juga tentang keamanan di domain digital dan elektromagnetik.

2.3 Jepang dan Aktor Lainnya di Kawasan

Jepang adalah aktor penting lainnya dalam persaingan teknologi ini. Sebagai respon terhadap ancaman regional, Jepang telah berinvestasi pada sistem radar canggih. Salah satunya adalah radar SPY-7 buatan Lockheed Martin, yang dirancang untuk mendeteksi, melacak, dan menanggulangi rudal balistik serta ancaman udara canggih lainnya.[36] Selain itu, Jepang juga mengoperasikan sistem radar buatan Thales, seperti GM200, yang menawarkan deteksi target kecil, cepat, dan lincah pada jarak yang lebih jauh.[37]

Aktivitas militer Tiongkok di sekitar Jepang menunjukkan adanya “permainan kucing-kucingan” yang konstan. Sebuah insiden dilaporkan di mana sebuah pesawat pengintai elektronik Tiongkok (Y-9) memasuki wilayah udara Jepang.[39] Respons cepat Jepang dengan mengirimkan jet tempur F-15 menunjukkan kesiapsiagaan mereka. Peristiwa ini mencerminkan taktik yang sering digunakan: pelanggaran wilayah udara yang singkat dapat menjadi cara untuk menguji waktu respons lawan dan mengumpulkan data sinyal dari sistem pertahanan yang diaktifkan.[39]

Tabel Perbandingan Kapabilitas SIGINT dan Radar Regional

Aktor	Aset Utama SIGINT/ELINT	Fokus Geografis dan Strategis	Kapabilitas Tam
Tiongkok	Stasiun Darat (Hainan), Kapal Spionase (Type 815), Jaringan Sensor Nirawak (Laut Cina Selatan) [15]	Asia Tenggara, Taiwan, Pasifik Barat. Strategi A2/AD [15]	Peperangan Sib C4ISR yang ku
AS & Australia	Pine Gap, Stasiun Kojarena, Stasiun Shoal Bay [25]	Indo-Pasifik, Hemisfer Timur. Pengawasan Rudal Balistik dan Komunikasi Satelit [26]	Pesawat RAAF Growler, Jet Te kapal selam SS [34]
Jepang	Radar canggih seperti SPY-7 [36]	Kawasan sekitarnya (terutama Laut Cina Timur dan Selat Taiwan) [39]	Aliansi dengan pertahanan uda terintegrasi.

Bagian III: Implikasi bagi Keamanan Regional dan Peran Indonesia

3.1 Dampak Geopolitik: Perlombaan Senjata di Era Informasi

Perlombaan SIGINT yang intensif ini memiliki dampak signifikan terhadap geopolitik Asia-Pasifik. Persaingan teknologi ini meningkatkan ketidakstabilan regional dan mempercepat perlombaan senjata.[40] Upaya suatu negara untuk meningkatkan kapabilitas pertahanannya, misalnya dengan menginstal radar canggih, dapat dipersepsikan sebagai ancaman oleh negara lain. Fenomena ini menciptakan dilema keamanan klasik di mana tindakan defensif dapat memicu reaksi ofensif dari pihak lawan.

Inisiatif seperti AUKUS, yang dirancang untuk memperkuat deterensi, bisa saja disalahartikan dan malah memicu ketidakpercayaan serta respons dari negara-negara lain di kawasan.[42] Hal ini menggeser fokus peperangan modern dari sekadar kekuatan militer konvensional menjadi dominasi informasi. Kapabilitas untuk mengendalikan spektrum elektromagnetik, atau bahkan menipu sensor musuh, kini menjadi aset strategis yang sangat dihargai. Keunggulan informasi yang didapat dari SIGINT dapat menghasilkan efek strategis yang sama atau lebih besar dari keunggulan senjata konvensional.

3.2 Tantangan Krusial bagi Kedaulatan Udara dan Maritim Indonesia

Sebagai negara kepulauan yang strategis, Indonesia sangat rentan terhadap pengawasan SIGINT dari kekuatan eksternal. Fakta yang terekam dalam laporan menunjukkan bahwa Stasiun Shoal Bay di Australia secara spesifik memantau komunikasi satelit Palapa dan komunikasi radio Indonesia.[28] Hal ini merupakan fakta penting yang menunjukkan bahwa Indonesia telah menjadi target SIGINT bahkan dari negara yang dianggap sebagai mitra.

Di domain maritim, keberadaan jaringan pengawasan tanpa awak Tiongkok di Laut Cina Selatan [18] secara langsung memengaruhi kedaulatan maritim Indonesia, terutama di Zona Ekonomi Eksklusif (

ZEE) yang berbatasan. Fakta-fakta ini menunjukkan bahwa kedaulatan tidak lagi hanya soal teritori fisik, tetapi juga tentang penguasaan dan keamanan di domain siber dan elektromagnetik. Indonesia tidak dapat lagi menganggap “bebas aktif” sebagai perisai yang memadai di era di mana pengawasan intelijen menjadi bagian tak terpisahkan dari hubungan antarnegara. Kebijakan luar negeri harus mencakup dimensi kedaulatan digital dan elektromagnetik untuk secara proaktif melindungi diri dari pengawasan asing.

3.3 Kesenjangan Kapabilitas Pertahanan dan Intelijen Indonesia

Analisis mendalam terhadap kapabilitas Indonesia menunjukkan adanya kesenjangan yang signifikan dalam menghadapi ancaman SIGINT dan EW modern.

- **Kesenjangan Regulasi:** Terdapat “absennya regulasi komprehensif” yang dapat menjadi payung hukum bagi lembaga keamanan dan pertahanan, seperti Badan Intelijen Negara (BIN) dan Badan Intelijen Strategis (BAIS) TNI, untuk menghadapi ancaman siber dan intelijen.[43] Ketiadaan kerangka hukum yang jelas membatasi peran dan fungsi kedua lembaga ini.
- **Kesenjangan Sumber Daya Manusia dan Infrastruktur:** BIN dan BAIS menghadapi tantangan besar dalam hal kesiapan sumber daya manusia, infrastruktur, dan dukungan finansial untuk melakukan operasi intelijen siber yang efektif.[43] Kecepatan arus informasi di dunia maya menuntut sumber daya manusia yang terampil untuk menganalisis data secara akurat dan tepat

waktu.

- **Ketergantungan Teknologi:** Modernisasi pertahanan Indonesia saat ini masih sangat bergantung pada vendor asing. Thales, misalnya, menyediakan radar GM200 dan sistem EW, serta sistem manajemen tempur angkatan laut.[45] Perusahaan Denmark, Terma, juga memasok sistem peperangan elektronik angkatan laut.[46] Ketergantungan ini menciptakan kerentanan strategis jika vendor tersebut tidak lagi dapat atau bersedia memberikan dukungan teknis atau pasokan di masa depan.

Kesenjangan-kesenjangan ini menimbulkan kekhawatiran bahwa Indonesia berisiko membangun kekuatan yang kuat secara fisik tetapi rentan secara digital dan informasi. Strategi modernisasi pertahanan yang sesungguhnya harus dimulai dari dalam: membangun doktrin, regulasi, dan sumber daya manusia yang kuat, bukan hanya mengandalkan pengadaan alutsista dari luar negeri.

Bagian IV: Rekomendasi Strategis untuk Indonesia

4.1 Modernisasi Pertahanan yang Terintegrasi dan Mandiri

Diperlukan pergeseran paradigma dalam modernisasi pertahanan Indonesia. Strategi harus bersifat holistik, tidak hanya berfokus pada pengadaan platform keras, tetapi juga pada integrasi sistem radar dengan kemampuan peperangan elektronik (EW) dan *Counter-SIGINT*.[14] Indonesia harus memanfaatkan program-program seperti DEFEND ID untuk mendorong transfer pengetahuan dan lokalisasi produksi, sebagaimana yang telah dilakukan dengan Thales untuk perbaikan radar.[45] Prioritas harus diberikan pada pengembangan kapabilitas yang spesifik untuk lingkungan maritim Indonesia, termasuk pengawasan perairan yang luas dan *chokepoint* strategis seperti Selat Lombok.[42]

4.2 Penguatan Kapasitas Sumber Daya Manusia dan Doktrin Intelijen

Indonesia harus berinvestasi secara masif dalam pelatihan personel yang ahli di bidang SIGINT dan peperangan siber untuk mengatasi kesenjangan sumber daya manusia yang ada.[43] Kolaborasi yang kuat antara lembaga pendidikan, sektor swasta, dan institusi pertahanan perlu dibangun untuk menciptakan dan mempertahankan talenta domestik. Selain itu, pengembangan doktrin pertahanan dan intelijen yang spesifik untuk Indonesia, yang menggabungkan metode konvensional dengan metode peperangan modern yang berfokus pada spektrum elektromagnetik, sangat krusial.[47]

4.3 Penyusunan Kerangka Regulasi yang Komprehensif

Pemerintah harus mengambil langkah untuk menyusun payung hukum yang jelas dan terpadu yang dapat mengoordinasikan semua pemangku kepentingan keamanan dan pertahanan dalam menghadapi ancaman intelijen dan siber.[43] Regulasi ini harus secara eksplisit mengatur tanggung jawab, wewenang, dan mekanisme pengawasan untuk memastikan efektivitas, akuntabilitas, dan independensi lembaga-lembaga ini.

4.4 Diplomasi Pertahanan yang Fleksibel dan Realistis

Dalam menjalankan kebijakan luar negeri, Indonesia harus mempertahankan pendekatan yang berimbang, namun dengan kesadaran penuh bahwa pengawasan intelijen adalah bagian dari realitas

hubungan antarnegara, bahkan dengan mitra terdekat sekalipun.[28] Penting untuk meningkatkan dialog strategis dengan semua pihak guna membangun mekanisme saling percaya dan mengurangi risiko salah perhitungan, sembari terus berupaya memperkuat kapasitas pertahanan mandiri.

Kesimpulan

Analisis ini menyimpulkan bahwa persaingan strategis di Asia-Pasifik, yang didorong oleh interaksi antara radar dan Signal Intelligence, adalah ancaman nyata yang menuntut respons terkoordinasi dan terukur dari Indonesia. Meskipun Indonesia telah menunjukkan ambisi untuk memodernisasi kekuatan militernya, terdapat kesenjangan kritis dalam doktrin, sumber daya manusia, dan kerangka regulasi yang dapat mengekspos kedaulatan nasional. Perlombaan intelijen sinyal dan peperangan elektronik ini adalah pertarungan untuk dominasi informasi, di mana pihak yang paling terampil dalam mengumpulkan, menganalisis, dan memanfaatkan data akan mendapatkan keuntungan strategis. Untuk menjaga kedaulatan di domain udara, maritim, dan digital, Indonesia harus mengadopsi strategi yang holistik. Strategi ini harus berfokus pada pembangunan kapabilitas intelijen domestik dan mandiri, didukung oleh regulasi yang kuat, sambil tetap menjaga keseimbangan dalam kebijakan luar negeri. Tanpa langkah-langkah ini, Indonesia berisiko menjadi subjek pasif dari permainan intelijen regional, yang pada akhirnya dapat mengkompromikan keamanan nasional.

Works cited

1. noaa.gov, accessed on August 27, 2025, https://www.noaa.gov/jetstream/doppler/how-radar-works#:~:text=The%20word%20radar%20comes%20from,any%20reflected%20energy%20from%20
2. How radar works | National Oceanic and Atmospheric Administration, accessed on August 27, 2025, https://www.noaa.gov/jetstream/doppler/how-radar-works
3. What is Signals Intelligence? – BAE Systems, accessed on August 27, 2025, https://www.baesystems.com/en-us/definition/what-is-signals-intelligence
4. Signals intelligence – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/Signals_intelligence
5. Signals Intelligence, accessed on August 27, 2025, https://irp.fas.org/program/collect/vpu-001.htm
6. What Is Signals Intelligence? Understanding SIGINT | American Military University (AMU), accessed on August 27, 2025, https://www.amu.apus.edu/area-of-study/intelligence/resources/what-is-signals-intelligence/
7. Gaining ELINT by intercepting and analyzing RF radar signals – CRFS, accessed on August 27, 2025, https://www.crfs.com/blog/gaining-electronic-intelligence-by-intercepting-and-analyzing-rf-radar-signals
8. ELECTRONIC INTELLIGENCE (ELINT) AT NSA – National Security Agency, accessed on August 27, 2025, https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/misc/elint.pdf
9. US signals intelligence in the Cold War – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/US_signals_intelligence_in_the_Cold_War
10. AI Impact Analysis on Defense Electronics Industry – MarketsandMarkets, accessed on August 27, 2025, https://www.marketsandmarkets.com/ResearchInsight/ai-impact-analysis-on-defense-electronics-industry.asp
11. The Transparent Battlefield w/TRADOC G2 (E38) – Apple Podcasts, accessed on August 27, 2025, https://podcasts.apple.com/us/podcast/the-transparent-battlefield-w-tradoc-g2-

e38/id1660058003?i=1000692458127
12. Hider-Finder Competition, Deception, and Ground Manoeuvre on the “Transparent Battlefield” – TDHJ.org, accessed on August 27, 2025, https://tdhj.org/blog/post/deception-transparent-battlefield/
13. Electronic warfare – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/Electronic_warfare
14. Harnessing SIGINT and EW for Tactical Dominance: A Guide for Combat Arms Leaders, accessed on August 27, 2025, https://www.army.mil/article/286341/harnessing_sigint_and_ew_for_tactical_dominance_a_guide_fo
15. SIGINT – Signals Intelligence Programs and Activities – Chinese Intelligence Agencies, accessed on August 27, 2025, https://irp.fas.org/world/china/program/sigint.htm
16. Asia Pacific Signals Intelligence (SIGINT) Market Size, 2028 – KBV Research, accessed on August 27, 2025, https://www.kbvresearch.com/asia-pacific-signals-intelligence-market/
17. Signals intelligence operational platforms by nation – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/Signals_intelligence_operational_platforms_by_nation
18. CHINA’S UNMANNED OCEAN NETWORK IN SOUTH CHINA SEA – CENJOWS, accessed on August 27, 2025, https://cenjows.in/wp-content/uploads/2022/05/Chinas-Unmanned-Ocean-Network-in-South-China-Sea-08-Jul-2020.pdf
19. Development of the Chinese A2/AD System in the Context of US–China Relations, accessed on August 27, 2025, https://www.researchgate.net/publication/364022503_Development_of_the_Chinese_A2AD_System China_Relations
20. Anti-access/area denial – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/Anti-access/area_denial
21. China’s Cyber Playbook for the Indo-Pacific – Indian Strategic Studies, accessed on August 27, 2025, https://www.strategicstudyindia.com/2025/08/chinas-cyber-playbook-for-indo-pacific.html
22. Chapter 8 – China’s Evolving Counter-Intervention Capabilities and the Role of Indo-Pacific Allies, accessed on August 27, 2025, https://www.uscc.gov/sites/default/files/2024-11/Chapter_8–Chinas_Evolving_Counter-Intervention_Capabilities.pdf
23. Intelligence partnerships | Australian Signals Directorate, accessed on August 27, 2025, https://www.asd.gov.au/about/history/asd-stories/2022-03-16-intelligence-partnerships
24. National Intelligence Community partners, accessed on August 27, 2025, https://www.oni.gov.au/national-intelligence-community/about-the-NIC/partners
25. Pine Gap – an introduction | Nautilus Institute for Security and Sustainability, accessed on August 27, 2025, https://nautilus.org/publications/books/australian-forces-abroad/defence-facilities/pine-gap/pine-gap-intro/
26. Pine Gap – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/Pine_Gap
27. Australian Defence Satellite Communications Station – Wikipedia, accessed on August 27, 2025, https://en.wikipedia.org/wiki/Australian_Defence_Satellite_Communications_Station
28. Shoal Bay Receiving Station | Nautilus Institute for Security and Sustainability, accessed on August 27, 2025, https://nautilus.org/publications/books/australian-forces-abroad/defence-facilities/shoal-bay-receiving-station/
29. Shoal Bay Receiving Station (Building) – Mapy.com, accessed on August 27, 2025, https://mapy.com/en/?source=osm&id=1073019378
30. F-35A Lightning II | Air Force, accessed on August 23, 2025, https://www.airforce.gov.au/aircraft/f-35a-lightning-ii

31. Australia Has the Most Technologically Advanced Fighter Jet In the World | The F35-A Lightning II – YouTube, accessed on August 23, 2025, https://m.youtube.com/watch?v=Q4Rf2z9b00c&t=50s
32. EA-18G Growler – Boeing Australia, accessed on August 27, 2025, https://www.boeing.com.au/products-services/defence-space-security/growler
33. EA-18G Growler – Royal Australian Air Force, accessed on August 27, 2025, https://www.airforce.gov.au/aircraft/ea-18g-growler
34. AUKUS Explained: How Will the Trilateral Pact Shape Indo-Pacific Security?, accessed on August 23, 2025, https://www.cfr.org/in-brief/aukus-explained-how-will-trilateral-pact-shape-indo-pacific-security
35. AUKUS – Wikipedia, accessed on August 23, 2025, https://en.wikipedia.org/wiki/AUKUS
36. SPY-7 | Lockheed Martin, accessed on August 27, 2025, https://www.lockheedmartin.com/en-us/products/spy-7.html
37. Ground Master 200 MM/C | Thales Group, accessed on August 27, 2025, https://www.thalesgroup.com/en/markets/defence-and-security/air-forces/ground-master-200-mmc
38. Ground Master 200 | Thales Group, accessed on August 27, 2025, https://www.thalesgroup.com/en/markets/defence-and-security/air-forces/airspace-protection/mid-range-radars/ground-master-200
39. Chinese Electronic Intelligence Plane Makes Unprecedented Incursion Into Japanese Airspace – The War Zone, accessed on August 27, 2025, https://www.twz.com/air/chinese-electronic-intelligence-plane-makes-unprecedented-incursion-into-japanese-airspace
40. Indo-Pacific Security Dynamics & Taiwan Conflict Readiness 2025, accessed on August 27, 2025, https://behorizon.org/emerging-security-dynamics-in-the-indo-pacific/
41. asia-pacific regional security assessment 2024 – The International Institute for Strategic Studies, accessed on August 27, 2025, https://www.iiss.org/globalassets/media-library—content–migration/files/publications—free-files/aprsa-2024/asia-pacific-regional-security-assessment-2024.pdf
42. Indonesia and Australia: Defence cooperation under Prabowo – Lowy Institute, accessed on August 23, 2025, https://www.lowyinstitute.org/the-interpreter/indonesia-australia-defence-cooperation-under-prabowo
43. Identify Cyber Intelligence Threats in Indonesia INTRODUCTION War is essentially a situation where two or more countries are inv, accessed on August 27, 2025, https://ijhess.com/index.php/ijhess/article/download/426/515
44. (PDF) Identify Cyber Intelligence Threats in Indonesia – ResearchGate, accessed on August 27, 2025, https://www.researchgate.net/publication/373604751_Identify_Cyber_Intelligence_Threats_in_Indon
45. Thales in Indonesia | Thales Group, accessed on August 27, 2025, https://www.thalesgroup.com/en/countries/asia-pacific/thales-indonesia
46. Terma signs 2 new naval electronic warfare contracts in Indonesia …, accessed on August 27, 2025, https://www.navalnews.com/naval-news/2021/10/terma-signs-2-new-naval-electronic-warfare-contracts-in-indonesia/
47. Examining the sociotechnical determinants of revolution in military affairs on electronic warfare capability development – Malque Publishing, accessed on August 27, 2025, https://malque.pub/ojs/index.php/mr/article/download/6484/3431/45363