JURNAL DWIJA KUSUMA VOL.13.NO.2. September 2025 P-ISSN 2355-5793
doi.org/10.63824/administrasipertahanan E-ISSN 2986-8084

MODEL MANAJEMEN RISIKO DALAM ADMINISTRASI PERTAHANAN: Kajian Literatur Sistematis Terhadap Ancaman Hibrida Dan Non-Militer

Khairul Muslim[1], Ahmad Taufik[2]
Prodi Administrasi Pertahanan Akademi Militer[1,2]
* serdaduintelek@gmail.com[1], ahmadtaufik96@gmail.com[2]

ABSTRAK

Administrasi pertahanan menghadapi tantangan kompleks akibat ancaman hibrida dan non-militer yang mampu melemahkan efektivitas pertahanan negara. Penelitian ini bertujuan merumuskan model manajemen risiko adaptif berbasis kajian literatur sistematis terhadap 35 artikel akademik, laporan kebijakan, dan standar internasional. Metode analisis menggunakan content analysis dan thematic coding dengan kerangka ISO 31000:2018 serta doktrin NATO AJP-3.15. Hasil penelitian menunjukkan lima tahapan utama manajemen risiko—identifikasi, analisis, evaluasi, mitigasi, serta monitoring—yang diperkaya dengan prinsip whole-of-government dan whole-of-society. Kebaruan penelitian ini terletak pada sintesis kerangka internasional dengan adaptasi konteks Indonesia, menghasilkan model konseptual administrasi pertahanan yang sistematis, partisipatif, dan responsif. Temuan ini berimplikasi pada penguatan kebijakan Kementerian Pertahanan dan TNI dalam membangun resiliensi pertahanan nasional di era ancaman multidimensi.

Kata kunci: administrasi pertahanan; manajemen risiko; ancaman hibrida; ancaman non-militer; ketahanan nasional

ABSTRACT

Defense administration faces complex challenges from hybrid and non-military threats that undermine national defense effectiveness. This study aims to formulate an adaptive risk management model through a systematic literature review of 35 academic articles, policy reports, and international standards. Data were analyzed using content analysis and thematic coding, adopting the ISO 31000:2018 framework and NATO AJP-3.15 doctrine. The findings highlight five key stages of risk management—identification, analysis, evaluation, mitigation, and monitoring—enriched with whole-of-government and whole-of-society principles. The novelty of this research lies in synthesizing international frameworks with Indonesia's local context, producing a conceptual model of defense administration that is systematic, participatory, and responsive. These findings imply significant contributions for the Ministry of Defense and the Armed Forces in strengthening national defense resilience against multidimensional threats.

Keywords: *defense administration; risk management; hybrid threats; non-military threats; national resilience*

PENDAHULUAN

Administrasi pertahanan merupakan pilar penting dalam penyelenggaraan sistem pertahanan negara karena mencakup pengelolaan sumber daya manusia, logistik, kelembagaan, serta kebijakan strategis. Dalam era geopolitik multipolar, karakter ancaman mengalami pergeseran dari bentuk konvensional ke ancaman multidimensi, khususnya ancaman hibrida dan non-militer. Ancaman hibrida seringkali memanfaatkan ranah siber, informasi, ekonomi, serta politik untuk melemahkan negara tanpa konfrontasi militer langsung (Bachmann & Gunneriusson, 2022; Chivvis, 2021). Di sisi lain, ancaman non-militer seperti bencana alam, pandemi, perubahan iklim, dan kriminalitas transnasional menimbulkan risiko serius terhadap stabilitas keamanan dan efektivitas administrasi pertahanan (Snyder, 2021; Suryadinata, 2020).

Fenomena aktual memperlihatkan bahwa risiko tersebut bukan sekadar ancaman potensial, tetapi nyata dan terus meningkat. Data Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 361 juta upaya serangan siber terjadi di Indonesia sepanjang 2021–2022, yang berpotensi mengganggu sektor vital termasuk pertahanan. Di sisi lain, Badan Nasional Penanggulangan Bencana (BNPB) melaporkan lebih dari 3.500 kejadian bencana alam pada tahun 2023, sebagian besar berdampak langsung pada infrastruktur logistik dan komunikasi nasional. Fakta ini menunjukkan bahwa administrasi pertahanan Indonesia menghadapi tekanan ganda: dari ancaman berbasis teknologi modern dan dari ancaman tradisional berbasis kerentanan geografis.

Sejumlah studi terdahulu telah membahas manajemen risiko dalam konteks pertahanan. Namun, sebagian besar penelitian berfokus pada aspek teknis operasional militer atau pada sektor umum, sehingga kurang memperhatikan spesifikasi administrasi pertahanan Indonesia. ISO 31000:2018 memang memberikan kerangka manajemen risiko yang sistematis, tetapi terlalu generik bila langsung diterapkan pada pertahanan (ISO, 2018). Sementara itu, doktrin NATO AJP-3.15 menawarkan integrasi risiko sipil-militer, namun relevansinya terbatas pada negara-negara anggota NATO dengan kapasitas koordinasi multinasional yang tinggi (NATO, 2020). Kritik utama terhadap literatur terdahulu adalah belum adanya kerangka yang menghubungkan standar internasional dengan kebutuhan lokal Indonesia, yang ditandai oleh birokrasi parsial, keterbatasan SDM, dan lemahnya integrasi digital pertahanan (Aditya & Kusuma, 2022).

Di Indonesia sendiri, arah kebijakan pertahanan telah diatur dalam UU No. 3 Tahun 2002 tentang Pertahanan Negara dan diperkuat oleh Perpres No. 8 Tahun 2021 tentang Kebijakan Umum Pertahanan Negara, yang menekankan pentingnya kesiapan menghadapi ancaman non-militer. Namun, implementasi di lapangan masih menghadapi tantangan serius. Belum adanya model adaptif yang mengintegrasikan kerangka internasional dengan kebutuhan lokal menjadi celah kebijakan yang harus segera diisi.

Berdasarkan kesenjangan tersebut, penelitian ini diarahkan untuk merumuskan model manajemen risiko yang tidak hanya sistematis tetapi juga kontekstual dengan kondisi Indonesia. Kebaruan penelitian ini adalah menyintesis kerangka manajemen risiko internasional (ISO 31000 dan NATO AJP-3.15) dengan prinsip *whole-of-government* dan *whole-of-society*, sehingga menghasilkan model konseptual administrasi pertahanan yang adaptif terhadap ancaman hibrida dan non-militer.

Tujuan penelitian ini adalah: (1) mengidentifikasi risiko yang berpotensi mengganggu efektivitas administrasi pertahanan, (2) menganalisis kerentanan sistem pertahanan terhadap ancaman hibrida dan non-militer, serta (3) merumuskan model manajemen risiko adaptif yang dapat menjadi rujukan dalam penyusunan kebijakan pertahanan nasional. Hasil penelitian diharapkan memberikan kontribusi teoritis terhadap literatur administrasi pertahanan, manfaat praktis bagi Kementerian Pertahanan dan TNI dalam memperkuat kapasitas kelembagaan, serta implikasi kebijakan bagi pembangunan sistem pertahanan nasional yang tangguh di era ancaman multidimensi.

METODE PENELITIAN

Penelitian ini menggunakan desain kajian literatur sistematis (systematic literature review/SLR) untuk menghimpun, menilai, dan menyintesis penelitian-penelitian terdahulu terkait manajemen risiko dalam administrasi pertahanan. Desain ini dipilih karena isu yang dikaji bersifat multidimensi, mencakup aspek kebijakan, kelembagaan, logistik, dan keamanan non-militer, sehingga membutuhkan pendekatan integratif. Kajian literatur sistematis juga memungkinkan identifikasi pola, tren, serta *research gap* yang menjadi dasar pengembangan model konseptual (Kitchenham & Charters, 2007; Snyder, 2019).

Prosedur penelitian dilakukan dengan mengacu pada kerangka PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Page et al., 2021), yang memastikan transparansi dan akuntabilitas dalam proses penelusuran, seleksi, dan analisis literatur. Empat tahap utama yang dilakukan adalah: Tahap pertama adalah identifikasi literatur, yang dilaksanakan dengan melakukan penelusuran artikel melalui basis data internasional seperti Scopus, Web of Science, SpringerLink, Taylor & Francis, ScienceDirect, RAND Corporation reports, serta dokumen NATO Standardization Office. Penelusuran juga mencakup basis data nasional seperti Garuda, Neliti, dan SINTA. Kata kunci yang digunakan meliputi *"administrasi pertahanan"*, *"defense administration"*, *"risk management"*, *"ISO 31000"*, *"hybrid threats"*, *"non-military threats"*, dan *"national resilience"*.

Tahap kedua adalah seleksi literatur, yang dilakukan menggunakan kriteria inklusi dan eksklusi. Kriteria inklusi mencakup artikel jurnal bereputasi (Q1–Q4 Scopus atau Sinta 1–2), prosiding konferensi, buku akademik, laporan resmi lembaga internasional (misalnya RAND, NATO, UN), serta dokumen kebijakan nasional (misalnya Perpres No. 8 Tahun 2021 tentang Kebijakan Umum Pertahanan Negara) dengan rentang publikasi 2014–2024. Adapun kriteria eksklusi meliputi artikel populer non-akademik, publikasi tanpa *peer review*, dan berita media yang tidak memiliki dasar metodologis. Seleksi dilakukan bertahap melalui skrining judul, abstrak, hingga telaah isi penuh artikel agar diperoleh literatur yang benar-benar relevan.

Tahap ketiga adalah analisis dan sintesis literatur. Artikel yang lolos seleksi dianalisis menggunakan analisis isi (*content analysis*) untuk mengekstrak data mengenai jenis risiko, strategi mitigasi, dan praktik terbaik. Selanjutnya, dilakukan pengkodean tematik (*thematic coding*) sehingga artikel dikelompokkan ke dalam lima tema utama, yaitu: (1) risiko dalam administrasi pertahanan, (2) ancaman hibrida, (3) ancaman non-militer, (4) model manajemen risiko internasional (ISO 31000 dan NATO framework), serta (5) adaptasi model pada konteks Indonesia.

Tahap keempat adalah validasi temuan. Validasi dilakukan melalui triangulasi sumber dengan cara membandingkan literatur akademik, laporan kebijakan resmi, serta regulasi pemerintah. Selain itu, untuk meningkatkan transparansi, penelitian ini mengadaptasi diagram alur PRISMA yang memperlihatkan proses seleksi mulai dari identifikasi hingga inklusi akhir.

Instrumen penelitian berupa lembar coding literatur yang digunakan untuk mencatat informasi penting dari setiap sumber. Lembar ini memuat nama penulis, tahun terbit, fokus kajian, metode penelitian, temuan utama, serta relevansi dengan administrasi pertahanan.

Tabel 1. Contoh Lembar Coding Literatur

Penulis & Tahun	Fokus Kajian	Metode	Temuan Utama	Relevansi
Bachmann & Gunneriusson (2022)	Hybrid warfare & governance	Konseptual	Hybrid threats memerlukan adaptasi manajemen risiko	Tinggi
Chivvis (2021, RAND)	Strategic aspects of hybrid warfare	Studi kasus	Administrasi lemah membuka peluang lawan	Tinggi
ISO (2018)	Risk management guideline	Standar	Lima tahap risk management berbasis ISO 31000	Sangat Tinggi
Suryadinata (2020)	Indonesia's security during COVID-19	Analitis	Administrasi pertahanan belum responsif menghadapi pandemi	Sedang
Aditya & Kusuma (2022)	Administrasi pertahanan di era disrupsi	Kualitatif	Birokrasi pertahanan Indonesia masih parsial	Tinggi
Snyder (2021)	Non-military threats (iklim, pandemi)	Kajian teoritis	Ancaman non-militer kian dominan di era globalisasi	Tinggi
Page et al. (2021, PRISMA)	Systematic review guideline (PRISMA 2020)	Standar	Peningkatan transparansi & akuntabilitas review sistematis	Metodologis

Tabel 1 menyajikan hasil pengkodean literatur yang dipilih dalam kajian ini. Dari tujuh referensi yang terpilih, terlihat bahwa fokus penelitian terkait administrasi pertahanan dan manajemen risiko telah berkembang dalam dua dekade terakhir dengan penekanan yang berbeda-beda.

Kajian Bachmann dan Gunneriusson (2022) menekankan bahwa hybrid warfare mengharuskan negara mengadaptasi manajemen risiko agar dapat menghadapi ancaman non-linear yang sulit diprediksi. Temuan ini diperkuat oleh laporan RAND yang ditulis oleh Chivvis (2021), yang menunjukkan bahwa kelemahan administrasi pertahanan sering kali menjadi celah strategis bagi lawan untuk melancarkan operasi hibrida.

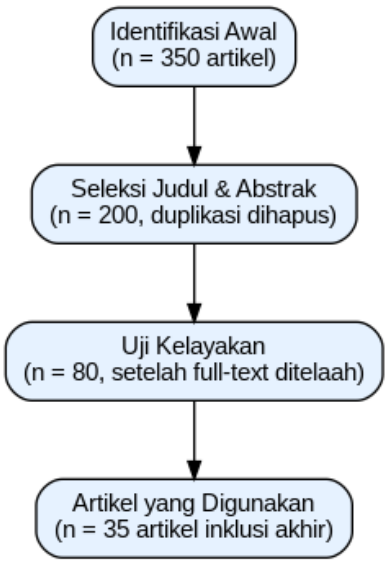
Dari sisi standar internasional, ISO (2018) memberikan kerangka prosedural manajemen risiko dalam lima tahap, yaitu identifikasi, analisis, evaluasi, mitigasi, serta monitoring. Meskipun sifatnya generik lintas sektor, standar ini menjadi rujukan dasar dalam tata kelola risiko. Sementara itu, penelitian Suryadinata (2020) memperlihatkan bagaimana pandemi COVID-19 mengekspos kerentanan sistem pertahanan Indonesia, khususnya pada kesiapan logistik darurat.

Penelitian nasional oleh Aditya dan Kusuma (2022) menyoroti bahwa birokrasi pertahanan Indonesia masih bersifat parsial dan belum memiliki mekanisme integrasi manajemen risiko yang komprehensif. Hal ini sejalan dengan temuan Snyder (2021), yang menggarisbawahi bahwa ancaman non-militer seperti iklim, pandemi, dan kriminalitas

transnasional semakin dominan dan menuntut adaptasi administrasi pertahanan. Terakhir, Page et al. (2021) melalui PRISMA 2020 memberikan kerangka metodologis terbaru yang memastikan transparansi dan akuntabilitas dalam kajian literatur sistematis. Referensi ini penting karena memperkuat validitas penelitian ini dari sisi metodologi.

Secara keseluruhan, Tabel 1 menunjukkan bahwa penelitian terdahulu telah memberikan fondasi konseptual dan empiris yang kuat, namun belum ada sintesis komprehensif yang menggabungkan kerangka manajemen risiko internasional (ISO 31000 dan NATO AJP-3.15) dengan kebutuhan spesifik administrasi pertahanan Indonesia. Dari sinilah penelitian ini menemukan research gap dan mengajukan kebaruan berupa model manajemen risiko adaptif untuk konteks nasional.

Untuk menunjukkan proses seleksi artikel secara sistematis, penelitian ini menyajikan diagram PRISMA. Diagram ini menggambarkan bahwa dari 350 artikel yang teridentifikasi, dilakukan skrining awal sehingga diperoleh 200 artikel setelah duplikasi dihapus. Dari jumlah tersebut, 80 artikel ditelaah secara penuh untuk menilai kelayakan. Pada tahap akhir, sebanyak 35 artikel dipilih sebagai inklusi yang dianalisis lebih lanjut dalam kajian ini.



Gambar 1. Diagram PRISMA

Analisis data dilakukan dalam tiga pendekatan. Pertama, analisis kualitatif untuk mengidentifikasi pola risiko dan strategi mitigasi yang muncul dalam literatur. Kedua, analisis komparatif untuk membandingkan model manajemen risiko internasional seperti ISO 31000:2018 dan NATO AJP-3.15 dengan kondisi administrasi pertahanan Indonesia. Ketiga, analisis integratif yang menyintesis hasil-hasil kajian sehingga menghasilkan sebuah model konseptual manajemen risiko administrasi pertahanan yang sistematis, adaptif, dan aplikatif.

Dengan prosedur penelitian ini, kajian literatur yang dilakukan bersifat sistematis, transparan, dan berbasis bukti ilmiah. Hal ini memastikan bahwa model manajemen risiko yang dihasilkan tidak hanya relevan secara teoretis, tetapi juga dapat diterapkan dalam konteks administrasi pertahanan Indonesia.

HASIL DAN PEMBAHASAN

Hasil kajian literatur sistematis mengungkapkan bahwa administrasi pertahanan Indonesia menghadapi risiko multidimensi yang bersumber dari ancaman hibrida maupun non-militer. Kedua kategori ancaman tersebut memiliki karakteristik berbeda, namun saling berkaitan dalam melemahkan efektivitas pertahanan negara.

Dari sisi ancaman hibrida, literatur internasional menekankan bahwa strategi lawan sering kali memanfaatkan celah kelembagaan dan kerentanan digital untuk melumpuhkan sistem pertahanan (Bachmann & Gunneriusson, 2022; Chivvis, 2021). Serangan siber, propaganda digital, dan infiltrasi ekonomi bukan hanya mengganggu aspek teknis, tetapi juga melemahkan kepercayaan publik terhadap institusi negara. Sementara itu, ancaman non-militer seperti pandemi global, bencana alam, serta kriminalitas transnasional menunjukkan bahwa administrasi pertahanan juga dituntut mampu mendukung operasi selain perang (*Military Operations Other Than War*).

Analisis mendalam terhadap literatur menunjukkan bahwa kelemahan administrasi pertahanan Indonesia bukan hanya terletak pada keterbatasan teknologi, melainkan juga fragmentasi kelembagaan. Hal ini menyebabkan koordinasi antarinstansi kurang optimal, padahal ancaman multidimensi membutuhkan respons terintegrasi.

1. Pemetaan Risiko Administrasi Pertahanan

Tabel 2. Pemetaan Risiko Administrasi Pertahanan Berdasarkan Literatur

Kategori Ancaman	Bentuk Risiko	Mekanisme Serangan / Gangguan	Dampak terhadap Administrasi Pertahanan	Literatur Rujukan
Hibrida	Serangan siber	Malware, ransomware, sabotase infrastruktur	Gangguan sistem logistik, komunikasi, & komando	Bachmann & Gunneriusson (2022); NATO (2020)
	Propaganda digital	Disinformasi, *psy-ops*, operasi media sosial	Disrupsi komando, pelemahan moral prajurit, erosi legitimasi	Chivvis (2021); RAND (2023)
	Infiltrasi ekonomi	Investasi strategis, penguasaan sumber daya	Ketergantungan ekonomi, kebocoran anggaran pertahanan	Mumford (2020)
Non-Militer	Bencana alam	Gempa, tsunami, banjir	Kerusakan infrastruktur militer,	Snyder (2021)

		disrupsi rantai pasok logistik	
Pandemi global	Gangguan kesehatan massal	Disrupsi mobilisasi pasukan & logistik darurat	Suryadinata (2020)
Kriminalitas transnasional	Penyelundupan senjata/narkoba	Kerentanan perbatasan & degradasi kewibawaan negara	Aditya & Kusuma (2022)

Tabel 2 menunjukkan klasifikasi risiko yang dihadapi administrasi pertahanan Indonesia, yang terbagi dalam dua kategori besar: ancaman hibrida dan ancaman non-militer. Ancaman hibrida mencakup serangan siber, disinformasi, dan infiltrasi ekonomi, sedangkan ancaman non-militer meliputi bencana alam, pandemi, serta kriminalitas transnasional. Keduanya memiliki karakteristik berbeda, namun secara simultan dapat melemahkan sistem pertahanan nasional.

Secara empiris, serangan siber merupakan salah satu bentuk ancaman hibrida yang paling dominan. BSSN (2022) mencatat lebih dari 360 juta upaya serangan siber di Indonesia sepanjang tahun 2021–2022, dengan mayoritas menyerang sistem pemerintahan dan sektor vital. Hal ini membuktikan bahwa risiko digital menjadi isu mendesak dalam administrasi pertahanan. Disinformasi melalui media sosial juga meningkat, terbukti dari penyebaran hoaks politik dan keamanan yang dapat memicu ketidakstabilan sosial.

Sementara itu, ancaman non-militer juga memberikan dampak signifikan. BNPB (2023) melaporkan lebih dari 3.500 kejadian bencana alam dalam satu tahun, yang tidak hanya mengakibatkan kerugian ekonomi tetapi juga menguji efektivitas logistik dan koordinasi administrasi pertahanan. Pandemi COVID-19 menambah bukti kelemahan sistem, terutama pada aspek respons cepat dan integrasi antarinstansi. Selain itu, aktivitas kriminal lintas negara, seperti penyelundupan senjata dan perdagangan ilegal, memperlihatkan kerentanan batas negara yang berdampak langsung pada pertahanan nasional.

Dari perspektif regulasi, UU No. 3 Tahun 2002 tentang Pertahanan Negara serta Perpres No. 8 Tahun 2021 tentang Kebijakan Umum Pertahanan menegaskan bahwa ancaman non-militer memiliki bobot strategis yang sama dengan ancaman militer. Hal ini memperkuat urgensi penerapan manajemen risiko administrasi pertahanan yang tidak hanya berorientasi pada peperangan konvensional, tetapi juga pada mitigasi ancaman multidimensi.

Dengan demikian, Tabel 2 tidak hanya berfungsi sebagai klasifikasi akademik, tetapi juga sebagai peta risiko strategis yang menegaskan perlunya model manajemen risiko adaptif. Model ini harus mampu menangkap kompleksitas ancaman kontemporer sekaligus mengakomodasi kebutuhan lokal Indonesia melalui koordinasi lintas kementerian, lembaga, dan masyarakat.

2. Perbandingan Model Manajemen Risiko

Hasil kajian memperlihatkan adanya dua kerangka manajemen risiko yang banyak diacu: ISO 31000:2018 dan NATO AJP-3.15. ISO memberikan kerangka generik, sedangkan NATO lebih spesifik pada konteks pertahanan.

Tabel 3. Perbandingan Model Manajemen Risiko Internasional dan Adaptasi Indonesia

Aspek	ISO 31000:2018	NATO AJP-3.15	Adaptasi untuk Indonesia
Tahapan Utama	Identifikasi – Analisis – Evaluasi – Mitigasi – Monitoring	Integrasi risiko ke dalam operasi sipil-militer	Kombinasi 5 tahap ISO dengan konteks TNI/Kemenhan
Ruang Lingkup	Generik lintas sektor	Spesifik pertahanan & keamanan	Fokus pada pertahanan & ketahanan nasional
Aktor yang Terlibat	Internal organisasi	Multiaktor (militer, sipil, internasional)	Whole-of-government & whole-of-society
Pendekatan	Sistematis & preventif	Kolaboratif & operasional	Sistematis, adaptif, partisipatif
Tantangan Implementasi	Terlalu umum jika tanpa adaptasi	Membutuhkan koordinasi lintas negara	Birokrasi parsial, SDM terbatas, infrastruktur digital lemah

Tabel 3 menampilkan perbandingan antara kerangka ISO 31000:2018, doktrin NATO AJP-3.15, serta kemungkinan adaptasinya dalam konteks administrasi pertahanan Indonesia. Hasil analisis memperlihatkan bahwa kedua model internasional memiliki keunggulan, tetapi juga keterbatasan yang perlu dipertimbangkan ketika diterapkan di Indonesia.

ISO 31000 menekankan lima tahapan utama, yaitu identifikasi, analisis, evaluasi, mitigasi, serta monitoring dan review. Kelebihan model ini adalah sifatnya yang generik dan dapat diaplikasikan lintas sektor. Namun, kelemahannya justru terletak pada sifat generik tersebut, sehingga jika tidak diadaptasi secara spesifik untuk bidang pertahanan, penerapannya dapat menjadi terlalu abstrak dan prosedural. Meskipun demikian, ISO 31000 tetap relevan sebagai fondasi prosedural bagi administrasi pertahanan Indonesia dalam membangun tata kelola risiko yang sistematis dan terdokumentasi dengan baik (ISO, 2018).

Sementara itu, doktrin NATO AJP-3.15 lebih menekankan pada konteks pertahanan dengan integrasi risiko ke dalam operasi sipil-militer. Model ini memberikan kelebihan berupa keterlibatan multiaktor, baik militer, sipil, maupun mitra internasional, yang memungkinkan respons lebih komprehensif terhadap ancaman hibrida. Namun, implementasi model NATO menghadapi tantangan serius karena membutuhkan kapasitas koordinasi lintas negara dan kesiapan diplomatik yang tinggi. Hal ini membuat model NATO lebih tepat dijadikan referensi

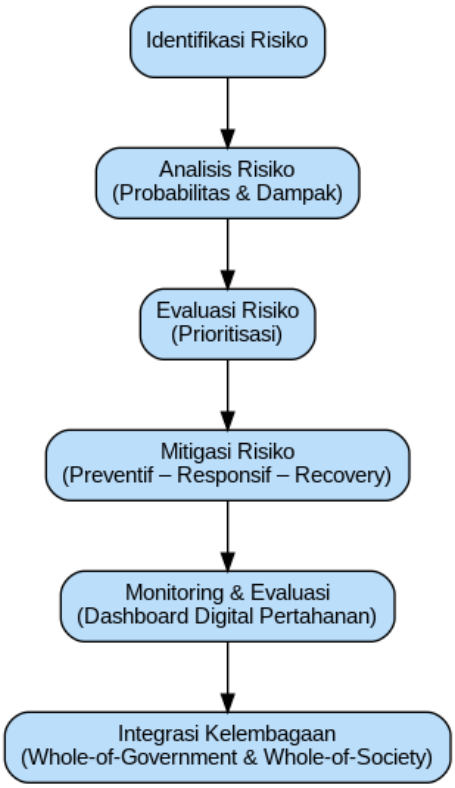
praktik terbaik (best practice), bukan adopsi langsung, terutama mengingat karakteristik politik dan birokrasi Indonesia yang berbeda dengan negara-negara anggota NATO (NATO, 2020).

Dalam konteks Indonesia, model manajemen risiko yang ideal adalah model adaptif yang menggabungkan kekuatan ISO 31000 sebagai kerangka dasar prosedural dengan prinsip-prinsip NATO yang menekankan kolaborasi multiaktor. Adaptasi ini diwujudkan melalui pendekatan whole-of-government dan whole-of-society, yang tidak hanya melibatkan Kementerian Pertahanan dan TNI, tetapi juga kementerian terkait, lembaga sipil, sektor swasta, akademisi, dan masyarakat. Dengan cara ini, administrasi pertahanan Indonesia dapat menghadapi kompleksitas ancaman hibrida dan non-militer secara lebih efektif.

Analisis dari tabel ini menunjukkan bahwa keberhasilan penerapan manajemen risiko pertahanan di Indonesia sangat bergantung pada dua faktor kunci, yaitu: (1) kemampuan birokrasi pertahanan mengadopsi kerangka sistematis berbasis ISO, dan (2) kesediaan institusi nasional untuk membuka ruang partisipasi luas lintas aktor sebagaimana prinsip NATO. Dengan mengintegrasikan keduanya, Indonesia dapat membangun sistem administrasi pertahanan yang tidak hanya efisien secara prosedural, tetapi juga tangguh secara kolaboratif.

3. Sintesis Model Konseptual

Hasil kajian literatur sistematis menghasilkan sebuah model konseptual manajemen risiko dalam administrasi pertahanan yang bersifat sistematis, adaptif, dan kontekstual dengan kebutuhan Indonesia. Model ini merupakan integrasi antara kerangka ISO 31000:2018 yang menekankan pada prosedur manajemen risiko dengan doktrin NATO AJP-3.15 yang menekankan pada kolaborasi multiaktor. Adaptasi lokal diwujudkan melalui prinsip whole-of-government dan whole-of-society untuk memastikan keterlibatan seluruh komponen bangsa dalam menghadapi ancaman multidimensi.



Gambar 2. Model Konseptual Manajemen Risiko Administrasi Pertahanan

Gambar 2 model konseptual ini menjelaskan enam tahapan utama manajemen risiko dalam administrasi pertahanan yang dirumuskan melalui kajian literatur sistematis dan adaptasi terhadap konteks Indonesia. Tahap pertama adalah identifikasi risiko, yang mencakup pemetaan ancaman hibrida seperti serangan siber, disinformasi, dan infiltrasi ekonomi, serta ancaman non-militer berupa bencana alam, pandemi, dan kriminalitas transnasional. Tahap kedua adalah analisis risiko, yang menilai probabilitas dan dampak dari setiap ancaman dengan memperhatikan kondisi geografis dan sosial Indonesia yang rentan terhadap bencana dan instabilitas informasi. Tahap ketiga adalah evaluasi risiko, yaitu proses prioritisasi berdasarkan tingkat ancaman, tidak hanya dilihat dari kerugian ekonomi, tetapi juga dari potensi gangguan sosial-politik dan kohesi nasional. Selanjutnya, tahap keempat adalah mitigasi risiko, yang mencakup langkah preventif, responsif, dan pemulihan pasca-krisis dengan menekankan pendekatan kolaboratif. Tahap kelima adalah monitoring dan evaluasi berkelanjutan, yang memanfaatkan instrumen digital berupa *dashboard risiko pertahanan nasional* untuk memberikan peringatan dini dan mengukur efektivitas kebijakan. Tahap terakhir adalah integrasi kelembagaan, yang menjadi kebaruan utama model ini. Integrasi dilakukan melalui prinsip *whole-of-government* dan *whole-of-society*, dengan melibatkan kementerian/lembaga, TNI, aparat sipil, sektor swasta, akademisi, media, serta masyarakat sipil.

Dengan demikian, gambar model konseptual ini tidak hanya menekankan alur prosedural sebagaimana terdapat dalam ISO 31000 maupun doktrin NATO, tetapi juga menambahkan dimensi partisipasi dan integrasi nasional sesuai amanat UU No. 3 Tahun 2002 tentang Pertahanan Negara dan Perpres No. 8 Tahun 2021 tentang Kebijakan Umum Pertahanan Negara. Kebaruan inilah yang menjadikan model ini lebih relevan untuk Indonesia, karena memperkuat administrasi pertahanan agar lebih sistematis, adaptif, dan responsif dalam menghadapi ancaman multidimensi yang bersifat hibrida maupun non-militer.

4. Diskusi

Diskusi penelitian ini memperlihatkan adanya kesenjangan yang cukup signifikan antara kerangka manajemen risiko internasional dengan kebutuhan administrasi pertahanan Indonesia. ISO 31000:2018 menawarkan pendekatan yang sistematis dan prosedural, namun sifatnya generik sehingga tidak secara langsung dapat menjawab kompleksitas pertahanan nasional yang sarat dengan dimensi militer, non-militer, dan sosial-politik. Sementara itu, NATO AJP-3.15 menekankan pada integrasi multiaktor sipil-militer, tetapi relevansi penerapannya di Indonesia terbatas karena mekanisme koordinasi nasional belum sekuat negara-negara NATO, baik dari sisi kapasitas kelembagaan maupun digitalisasi pertahanan.

Hasil kajian juga menunjukkan bahwa ancaman yang dihadapi Indonesia memiliki karakteristik unik. Data BSSN (2022) mencatat lebih dari 360 juta serangan siber dalam kurun waktu satu tahun, menandakan ancaman digital sebagai salah satu risiko terbesar yang berimplikasi langsung terhadap administrasi pertahanan. Di sisi lain, BNPB (2023) melaporkan lebih dari 3.500 kejadian bencana alam, yang menegaskan pentingnya kesiapan administrasi pertahanan dalam mendukung logistik, mobilisasi, dan koordinasi lintas sektor. Pandemi COVID-19 menjadi bukti konkret lemahnya integrasi antarinstansi, karena koordinasi awal respons nasional berjalan lambat dan tidak sinkron. Temuan-temuan ini memperlihatkan bahwa

kerangka manajemen risiko yang ada belum sepenuhnya dapat dioperasionalkan secara efektif dalam konteks Indonesia.

Dari perspektif kebijakan, Indonesia sebenarnya telah memiliki dasar hukum yang kuat. UU No. 3 Tahun 2002 tentang Pertahanan Negara mengamanatkan sistem pertahanan semesta yang melibatkan seluruh komponen bangsa, sedangkan Perpres No. 8 Tahun 2021 tentang Kebijakan Umum Pertahanan Negara menekankan urgensi menghadapi ancaman non-militer secara setara dengan ancaman militer. Namun, implementasi kebijakan ini sering terhambat oleh fragmentasi birokrasi, keterbatasan sumber daya manusia yang menguasai manajemen risiko, serta lemahnya infrastruktur digital pertahanan.

Kebaruan penelitian ini terletak pada upaya menyintesis dua kerangka internasional—ISO 31000 yang bersifat prosedural dan NATO AJP-3.15 yang bersifat kolaboratif—dengan adaptasi konteks Indonesia. Hasil sintesis menghasilkan model konseptual manajemen risiko administrasi pertahanan yang menambahkan tahap integrasi kelembagaan dan menekankan prinsip *whole-of-government* serta *whole-of-society*. Inilah pembeda utama dengan model internasional, karena menempatkan partisipasi masyarakat sebagai bagian integral dari sistem resiliensi pertahanan.

Implikasi kebijakan dari temuan ini adalah pentingnya Kementerian Pertahanan dan TNI untuk: (1) membangun dashboard risiko pertahanan nasional sebagai sistem peringatan dini berbasis digital, (2) melakukan reformasi birokrasi pertahanan untuk memperkuat koordinasi lintas instansi, (3) meningkatkan kapasitas SDM melalui pelatihan berbasis standar ISO dan praktik terbaik internasional, serta (4) memperluas kolaborasi sipil-militer agar administrasi pertahanan tidak hanya bertumpu pada kekuatan militer, melainkan juga partisipasi seluruh elemen bangsa.

Dengan demikian, diskusi ini menegaskan bahwa penelitian tidak hanya memberikan kontribusi konseptual terhadap literatur administrasi pertahanan, tetapi juga nilai guna praktis dalam membangun sistem pertahanan nasional yang adaptif, partisipatif, dan tangguh menghadapi ancaman multidimensi.

KESIMPULAN

Penelitian ini menunjukkan bahwa administrasi pertahanan Indonesia menghadapi risiko ganda dari ancaman hibrida seperti serangan siber, disinformasi, dan infiltrasi ekonomi, serta ancaman non-militer seperti bencana alam, pandemi, dan kriminalitas transnasional. Kajian literatur sistematis memperlihatkan bahwa kerangka manajemen risiko internasional, yaitu ISO 31000:2018 dan NATO AJP-3.15, memiliki relevansi terbatas bila diterapkan langsung dalam konteks Indonesia. ISO dinilai terlalu generik, sedangkan NATO membutuhkan kapasitas koordinasi yang belum sepenuhnya tersedia di Indonesia.

Kebaruan penelitian ini adalah pengembangan model konseptual manajemen risiko administrasi pertahanan yang menyintesis keunggulan kerangka internasional dengan kebutuhan lokal Indonesia. Model ini menambahkan tahap *integrasi kelembagaan* dan menekankan prinsip *whole-of-government* serta *whole-of-society*, sehingga menjadikan administrasi pertahanan lebih sistematis, adaptif, dan partisipatif.

Implikasi kebijakan dari penelitian ini menegaskan perlunya: (1) penguatan kapasitas digital melalui *dashboard risiko pertahanan nasional*, (2) reformasi birokrasi pertahanan untuk memperkuat koordinasi lintas instansi, (3) peningkatan kapasitas SDM melalui pelatihan berbasis standar internasional, serta (4) penguatan kolaborasi sipil-militer untuk membangun resiliensi nasional. Dengan demikian, penelitian ini tidak hanya memberikan kontribusi konseptual pada literatur akademik, tetapi juga memberikan nilai praktis bagi Kementerian Pertahanan dan TNI dalam membangun sistem pertahanan yang tangguh menghadapi ancaman multidimensi.

Penelitian lanjutan dapat diarahkan pada uji empiris model melalui studi kasus sektor pertahanan Indonesia atau perbandingan dengan negara-negara non-NATO yang menghadapi tantangan serupa.

DAFTAR PUSTAKA

Aditya, R., & Kusuma, D. (2022). Administrasi pertahanan Indonesia di era disrupsi: Tantangan dan peluang. *Jurnal Pertahanan dan Bela Negara, 12*(2), 145–162. https://doi.org/10.22146/jpbn.2022

Bachmann, S. D., & Gunneriusson, H. (2022). Hybrid wars in the 21st century: New threats, new approaches. *Defence Studies, 22*(1), 1–19. https://doi.org/10.1080/14702436.2022.2034159

Badan Nasional Penanggulangan Bencana. (2023). *Laporan tahunan bencana Indonesia 2023*. BNPB. https://bnpb.go.id

Badan Siber dan Sandi Negara. (2022). *Laporan tahunan keamanan siber Indonesia 2022*. BSSN. https://bssn.go.id

Chivvis, C. S. (2021). *Understanding Russian "hybrid warfare" and what can be done about it*. RAND Corporation. https://www.rand.org/pubs/perspectives/PE301.html

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO. https://www.iso.org/standard/65694.html

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Keele University.

Mumford, A. (2020). *Strategy in the contemporary world: Hybrid threats and strategic adaptation*. Oxford University Press.

NATO Standardization Office. (2020). *AJP-3.15 Allied joint doctrine for countering hybrid threats*. NATO. https://nso.nato.int/nso/nsdd/listpromulg.html

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

RAND Corporation. (2023). *Countering disinformation and hybrid threats: NATO's evolving strategies*. RAND. https://www.rand.org/pubs/research_reports/RRA1234-1.html

Republik Indonesia. (2002). *Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara*. Lembaran Negara Republik Indonesia.

Republik Indonesia. (2021). *Peraturan Presiden Nomor 8 Tahun 2021 tentang Kebijakan Umum Pertahanan Negara*. Sekretariat Negara Republik Indonesia.

Snyder, J. (2021). Non-military threats in the age of globalization: Climate, pandemics, and resilience. *Journal of Strategic Security, 14*(3), 25–40. https://doi.org/10.5038/1944-0472.14.3.1889

Suryadinata, L. (2020). Indonesia's defense administration during the COVID-19 pandemic: Challenges and adaptations. *Contemporary Southeast Asia, 42*(2), 219–240. https://doi.org/10.1355/cs42-2e