IMPLEMENTASI *BIG DATA* DALAM PERUMUSAN STRATEGI KEAMANAN SIBER MILITER

Eka Indri Widarti[1*]
[1]Prodi Teknik Elektronika Pertahanan Akademi Militer
ekaindriwidarti1995@gmail.com [1*]

Adi Murtopo[2]
[2]Prodi Teknik Elektronika Pertahanan Akademi Militer
adimurtopo@nikelektronikahan.akmil.ac.id[2]

Frangky Silitonga[3]
[3]Politeknik Pariwisata Batam, Indonesia
frangky@btp.ac.id[3]

ABSTRAK

Kemajuan teknologi informasi telah menghadirkan tantangan baru bagi pertahanan nasional, khususnya di domain siber. *Big Data* menjadi instrumen strategis yang memungkinkan militer memproses data dalam jumlah besar secara *real-time* untuk mendukung deteksi dini ancaman, perumusan strategi, serta pengambilan keputusan berbasis bukti. Penelitian ini bertujuan untuk menganalisis implementasi *Big Data* dalam perumusan strategi keamanan siber militer di Indonesia. Metode penelitian yang digunakan adalah deskriptif kualitatif melalui tinjauan pustaka dari jurnal akademik, laporan kebijakan, dan doktrin pertahanan. Hasil penelitian menunjukkan bahwa *Big Data* berkontribusi pada lima aspek utama: deteksi dini ancaman siber, optimalisasi strategi pertahanan, penguatan intelijen siber, efisiensi manajemen sumber daya, dan peningkatan daya tangkal. Selain itu, implementasi *Big Data* selaras dengan doktrin pertahanan Indonesia, khususnya Asta Gatra dan Sistem Pertahanan Semesta, yang menekankan penguasaan teknologi informasi dalam menjaga kedaulatan negara. Namun, tantangan masih muncul terkait keterbatasan personel terampil, infrastruktur teknologi, serta risiko keamanan data. Studi ini merekomendasikan penguatan regulasi, pembangunan pusat data militer, peningkatan kompetensi personel, serta promosi integrasi lintas domain untuk memperkuat kemandirian pertahanan digital Indonesia. Dengan demikian, *Big Data* tidak hanya dipandang sebagai alat teknis, tetapi juga sebagai pilar utama strategi keamanan siber dalam mewujudkan Indonesia Emas 2045.

Kata kunci: *Big Data, keamanan siber, militer, strategi pertahanan, Asta Gatra*

A THEORETICAL STUDY OF BIG DATA AS A BASIS FOR FORMULATION OF MILITARY CYBERSECURITY

ABSTRACT

The advancement of information technology has introduced new challenges to national defense, particularly in the cyber domain. Big Data serves as a strategic instrument that enables the military to process massive amounts of real-time data to support early threat detection, strategy formulation, and evidence-based decision-making. This study aims to analyze the implementation of Big Data in formulating military cybersecurity strategies in Indonesia. The research employed a descriptive qualitative method using literature reviews from academic journals, policy reports, and defense doctrines. The findings reveal that Big Data contributes to five key aspects: early cyber threat detection, optimization of defense strategies, strengthening of cyber intelligence, efficient

resource management, and enhanced deterrence. Moreover, the implementation of Big Data aligns with Indonesia's defense doctrine, particularly Asta Gatra and the Total Defense System, which emphasize the mastery of information technology in safeguarding national sovereignty. Nevertheless, challenges remain in terms of limited skilled personnel, technological infrastructure, and data security risks. The study recommends strengthening regulations, developing military data centers, enhancing personnel competencies, and promoting cross-domain integration to reinforce Indonesia's digital defense autonomy. Thus, Big Data should not only be regarded as a technical tool but also as a central pillar of cybersecurity strategy in realizing Indonesia Emas 2045.

Keywords: *Big Data, cybersecurity, military, defense strategy, Asta Gatra*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam dinamika pertahanan negara. Salah satu bentuk ancaman baru yang muncul adalah serangan siber, yang dapat melumpuhkan infrastruktur kritis, merusak sistem komando dan kendali militer, serta mengancam kedaulatan negara (Clarke & Knake, 2010). Dalam konteks perang modern, serangan siber bahkan dianggap sebagai salah satu dimensi peperangan non-konvensional yang mampu memberikan efek strategis tanpa harus mengerahkan kekuatan fisik secara langsung (Rid, 2013).

Militer sebagai garda terdepan pertahanan negara perlu memiliki strategi keamanan siber yang tangguh, adaptif, dan berbasis data. Pemanfaatan *Big Data* menjadi salah satu instrumen penting dalam mewujudkan hal ini. Dengan karakteristiknya yang mencakup *Volume, Velocity, Variety, Veracity,* dan *Value, Big Data* mampu mengolah serta menganalisis data dalam jumlah besar secara cepat untuk mendukung pengambilan keputusan strategis (Gandomi & Haider, 2015). Dalam konteks pertahanan, *Big Data* dapat digunakan untuk deteksi dini ancaman, penguatan intelijen, hingga perumusan strategi pertahanan siber yang efektif (Chen, Mao, & Liu, 2014).

Penelitian terdahulu telah menunjukkan potensi *Big Data* dalam berbagai konteks pertahanan dan keamanan. Studi internasional oleh Almulla (2019) menekankan peran analisis data besar dalam memperkuat intelijen militer, namun lebih fokus pada perencanaan operasi dan manajemen risiko secara umum, tanpa membahas secara spesifik konteks pertahanan siber di Indonesia. Rid (2013) menyoroti dimensi peperangan siber modern, tetapi belum mengeksplorasi integrasi *Big Data* sebagai instrumen strategi pertahanan. Penelitian lokal oleh Kementerian Pertahanan RI (2020) menekankan pentingnya pertahanan siber nasional, namun masih bersifat konseptual, belum ada kajian empiris yang menunjukkan implementasi *Big Data* dalam sistem pertahanan siber TNI.

Berdasarkan tinjauan penelitian terdahulu, terdapat beberapa kekosongan pengetahuan yang menjadi dasar penelitian ini, konteks lokal Indonesia yaitu penelitian internasional menunjukkan efektivitas *Big Data* dalam intelijen militer, namun studi empiris terkait penerapan *Big Data* dalam pertahanan siber Indonesia masih terbatas. Integrasi *Big Data* dengan strategi pertahanan siber, sebagian besar penelitian terdahulu masih memisahkan konsep *Big Data* dan pertahanan siber; penelitian ini mencoba menghubungkan kedua aspek secara langsung. Pendekatan empiris dan strategis, penelitian sebelumnya bersifat konseptual atau deskriptif, sehingga penelitian ini mengisi gap dengan pendekatan analitis yang menilai peran *Big Data* dalam deteksi dini, intelijen, dan strategi keamanan siber TNI secara sistematis.

Indonesia sendiri telah menyadari pentingnya pertahanan siber dalam kerangka pertahanan negara. Kementerian Pertahanan Republik Indonesia (2020) menegaskan bahwa pertahanan siber merupakan salah satu pilar utama dalam sistem pertahanan negara modern. Namun demikian,

implementasi *Big Data* dalam merumuskan strategi keamanan siber militer masih menghadapi sejumlah tantangan, seperti keterbatasan sumber daya manusia, infrastruktur teknologi, serta integrasi kebijakan. Oleh karena itu, kajian ilmiah mengenai implementasi *Big Data* dalam strategi pertahanan siber militer menjadi relevan dan mendesak untuk dikembangkan.

1.1 Rumusan Masalah

Berdasarkan gap yang ditemukan pada penelitian terdahulu, rumusan masalah penelitian ini adalah:

1. Bagaimana peran *Big Data* dalam mendukung deteksi dini dan respon terhadap ancaman siber di lingkungan militer Indonesia?
2. Bagaimana implementasi *Big Data* dapat memperkuat intelijen siber untuk mendukung pengambilan keputusan strategis TNI?
3. Bagaimana *Big Data* dapat diintegrasikan ke dalam strategi keamanan siber militer yang adaptif dan efektif, sesuai konteks pertahanan Indonesia?

1.2 Tujuan Penelitian

Penelitian ini bertujuan untuk menjawab gap penelitian terdahulu dengan fokus pada konteks Indonesia, yaitu:

1. Menganalisis peran *Big Data* dalam mendukung deteksi dini dan respons terhadap ancaman siber militer di Indonesia.
2. Mengkaji implementasi *Big Data* dalam memperkuat intelijen siber sebagai basis pengambilan keputusan strategis TNI.
3. Merumuskan strategi keamanan siber militer berbasis *Big Data* yang adaptif, efektif, dan sesuai dengan kebutuhan pertahanan nasional.

1.3 Manfaat Penelitian

1. Manfaat Teoritis.
   Memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang pertahanan siber dan pemanfaatan *Big Data*. Memperkaya literatur tentang integrasi *Big Data* dengan strategi keamanan siber, khususnya dalam konteks Indonesia. Menyediakan kerangka konseptual baru yang dapat dijadikan referensi untuk penelitian lanjutan di bidang pertahanan, teknologi, dan kebijakan publik.

2. Manfaat Praktis.
   Bagi Institusi Militer (TNI), memberikan rekomendasi strategis untuk memperkuat sistem deteksi dini, intelijen siber, dan respons terhadap ancaman siber. Membantu TNI mengintegrasikan *Big Data* dalam perencanaan dan pelaksanaan strategi pertahanan siber secara efektif.

Bagi Pemerintah dan Pembuat Kebijakan, menjadi dasar ilmiah untuk pengembangan kebijakan nasional terkait pertahanan siber berbasis *Big Data*. Mendukung pencapaian visi pertahanan nasional, termasuk target Indonesia Emas 2045, melalui integrasi teknologi dan strategi siber.

Bagi Akademisi, menjadi referensi bagi pengembangan kurikulum, kajian akademik dan penelitian lanjutan terkait pertahanan siber dan teknologi *Big Data*.

Bagi Industri Pertahanan dan Teknologi, membuka peluang kolaborasi antara militer, pemerintah, dan industri teknologi untuk membangun ekosistem keamanan siber yang tangguh. Memberikan dasar empiris untuk pengembangan solusi teknologi *Big Data* yang sesuai kebutuhan pertahanan nasional.

METODE PENELITIAN

2.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis. Pendekatan ini dipilih karena penelitian berfokus pada analisis mendalam mengenai implementasi *Big Data* dalam strategi keamanan siber militer. Penelitian tidak hanya meninjau literatur secara deskriptif, tetapi juga menganalisis dokumen kebijakan, laporan penelitian terdahulu, serta studi kasus untuk merumuskan kesimpulan strategis (Creswell, 2018).

2.2 Lokasi Penelitian

Penelitian dilakukan pada lingkup kebijakan, doktrin dan praktik pertahanan siber Indonesia, dengan fokus pada lingkungan militer dan lembaga pertahanan terkait seperti TNI**,** Kementerian Pertahanan serta lembaga penelitian pertahanan yang relevan. Analisis juga mencakup perbandingan dengan praktik pertahanan siber di beberapa negara lain untuk memperkuat konteks strategis.

2.3 Objek Penelitian

Objek penelitian adalah pemanfaatan *Big Data* dalam merumuskan strategi keamanan siber militer, yang mencakup:

1. Deteksi dini ancaman siber.
2. Respon pertahanan siber.
3. Pengelolaan intelijen dan analisis informasi strategis.
4. Implikasi kebijakan pertahanan berbasis data.

2.4 Sumber Data

Literatur akademik (jurnal ilmiah, buku, tesis) dan publikasi internasional tentang *Big Data*, keamanan siber, dan strategi pertahanan.

Dokumen resmi, kebijakan, dan laporan dari Kementerian Pertahanan RI, TNI, serta lembaga penelitian pertahanan.

Kriteria pemilihan literatur yang relevan dengan fokus penelitian, diterbitkan dalam periode 2010–2025, dan memiliki metode atau temuan yang dapat mendukung analisis strategis.

2.5 Teknik Pengumpulan Data

1. Studi Literatur: menganalisis jurnal, buku, laporan penelitian terdahulu, dan publikasi internasional terkait *Big Data* dan keamanan siber militer.
2. Dokumentasi: menelaah dokumen resmi, kebijakan, dan peraturan pertahanan siber di Indonesia dan perbandingan internasional.

2.6 Teknik Analisis Data

Analisis dilakukan menggunakan model Miles & Huberman (1994) yang terdiri dari:

1. Reduksi Data: memilah dan menyeleksi data yang relevan dengan fokus penelitian, yaitu implementasi *Big Data* dalam strategi keamanan siber militer.
2. Penyajian Data (*Data Display*): menyusun data dalam bentuk matriks, tabel, diagram, dan narasi deskriptif untuk memudahkan identifikasi pola dan hubungan antarvariabel.
3. Penarikan Kesimpulan (*Verification*): menghasilkan temuan konseptual dan praktis mengenai peran *Big Data* dalam mendukung strategi pertahanan siber militer.

Selain itu, dilakukan analisis isi (*content analysis*) pada dokumen kebijakan dan publikasi ilmiah untuk mengidentifikasi tema, strategi dan best practice yang relevan dengan konteks pertahanan Indonesia.

2.7 Validitas Data

Validitas data dalam penelitian ini dilakukan melalui penilaian kredibilitas dan relevansi sumber literatur. Proses validasi mencakup evaluasi kualitas publikasi, reputasi penulis, serta kesesuaian isi dengan variabel penelitian. Selain itu, peneliti melakukan triangulasi teori dengan membandingkan berbagai referensi dari jurnal nasional maupun internasional untuk memastikan konsistensi konsep. Validitas metodologis diperkuat melalui penggunaan kriteria inklusi eksklusi dan penelusuran sistematis pada database ilmiah. Seluruh temuan kemudian diverifikasi melalui telaah sejawat (*peer review*) guna memastikan akurasi dan ketepatan analisis.

Dengan tambahan kriteria pemilihan literatur, periode sumber, dan analisis isi, metode penelitian ini lebih jelas, sistematis, dan dapat memberikan landasan yang kuat untuk merumuskan strategi keamanan siber berbasis *Big Data* bagi militer Indonesia.

HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Berdasarkan studi literatur, dokumentasi, dan analisis kebijakan, penelitian ini menemukan bahwa implementasi *Big Data* dalam pertahanan siber militer memberikan kontribusi signifikan pada empat aspek utama:

3.2 Deteksi Dini Ancaman Siber

Deteksi dini ancaman siber merupakan salah satu aspek krusial dalam strategi pertahanan militer modern. Implementasi *Big Data* memungkinkan militer untuk mengumpulkan, menyimpan, dan menganalisis data dalam jumlah besar secara real-time, yang mencakup *network traffic*, *log system*, serta aktivitas mencurigakan pada infrastruktur pertahanan strategis. Volume data yang sangat besar dan beragam ini, apabila dianalisis secara manual, sulit untuk diolah dalam waktu singkat. Namun, dengan pendekatan analitik *Big Data*, proses tersebut dapat dilakukan secara cepat dan efisien sehingga memperkuat *situational awareness* di ranah siber (Chen, Mao, & Liu, 2014).

Selain itu, integrasi algoritma *machine learning* dan *artificial intelligence* memungkinkan sistem pertahanan siber untuk mengenali pola serangan dan mendeteksi anomali yang tidak biasa. Misalnya, lonjakan akses jaringan yang tidak wajar, pola komunikasi yang menyerupai serangan *Distributed Denial of Service (DDoS)*, atau manipulasi data pada sistem komando dan kontrol militer dapat segera teridentifikasi. Proses deteksi ini berbasis *pattern recognition* dan *predictive analytics*, sehingga serangan dapat dicegah sebelum menimbulkan kerusakan yang lebih besar (Zikopoulos et al., 2012).

Lebih jauh, kemampuan deteksi dini dengan *Big Data* tidak hanya terbatas pada identifikasi serangan yang sedang berlangsung, tetapi juga mampu mengantisipasi potensi serangan di masa depan. Hal ini dilakukan melalui analisis historis terhadap data serangan, pemetaan kecenderungan aktivitas siber musuh, serta pengenalan tanda-tanda awal yang sering muncul sebelum serangan dilancarkan. Dengan demikian, sistem pertahanan tidak hanya bersifat reaktif, tetapi juga proaktif dan prediktif dalam menjaga keamanan siber militer (Gandomi & Haider, 2015).

Dalam konteks pertahanan negara, kemampuan deteksi dini berbasis *Big Data* memiliki implikasi strategis. Pertama, ia memperkuat fungsi intelijen siber dengan menyediakan informasi yang lebih akurat dan terkini tentang pola ancaman. Kedua, ia mendukung *command and control system* dengan memberikan peringatan cepat kepada pengambil keputusan strategis, sehingga respons dapat dilakukan dalam waktu yang singkat. Ketiga, ia meningkatkan *resilience* pertahanan siber karena sistem selalu belajar dari setiap anomali yang terdeteksi, memperbaiki algoritma, dan memperkuat lapisan keamanan berikutnya. Dengan demikian, deteksi dini ancaman siber berbasis *Big Data* dapat dipandang sebagai salah satu fondasi utama dalam merumuskan strategi keamanan siber militer yang tangguh dan adaptif di era perang modern.

3.3 Optimalisasi Strategi Pertahanan Siber

Optimalisasi strategi pertahanan siber merupakan langkah penting bagi militer dalam menghadapi kompleksitas ancaman di era digital. Pemanfaatan *Big Data* memungkinkan strategi yang dibangun tidak lagi hanya berdasarkan asumsi atau pengalaman masa lalu, melainkan berbasis data aktual yang terus diperbarui secara real-time. Melalui analisis *Big Data*, militer dapat mengidentifikasi pola serangan yang berulang, mengkaji kelemahan pada infrastruktur pertahanan, serta memetakan kerentanan sistem yang paling rentan diserang. Dengan demikian, strategi pertahanan yang dirumuskan menjadi lebih terarah,

efektif, dan adaptif terhadap dinamika ancaman siber yang terus berkembang (Gandomi & Haider, 2015).

Selain itu, *Big Data* mendukung proses pengambilan keputusan strategis dengan menyediakan *evidence-based strategy*. Misalnya, data mengenai frekuensi serangan, sumber serangan, serta dampaknya terhadap sistem militer dapat digunakan untuk menentukan prioritas perlindungan pada aset-aset kritis, seperti pusat komando, jaringan komunikasi, dan sistem persenjataan cerdas. Dengan pendekatan ini, sumber daya pertahanan, baik personel maupun anggaran, dapat dialokasikan secara lebih efisien pada area yang memiliki tingkat risiko tertinggi. Hal ini memperkuat prinsip *resource optimization* dalam manajemen pertahanan siber (Kavanagh & Rich, 2019).

Selanjutnya, *Big Data* juga membuka peluang integrasi antara strategi pertahanan siber dengan operasi militer lainnya. Analisis data yang diperoleh dari berbagai domain baik darat, laut, udara dan siber sehingga dapat dipadukan untuk membentuk sistem pertahanan terpadu. Integrasi ini akan meningkatkan efektivitas operasi militer karena informasi yang dihasilkan lebih komprehensif, akurat, dan mendukung kecepatan dalam pengambilan keputusan. Dengan kata lain, *Big Data* membantu mewujudkan konsep *multi-domain operations* dalam pertahanan modern (Minkov, 2019).

Di sisi lain, optimalisasi strategi pertahanan siber melalui *Big Data* juga memiliki dimensi kebijakan. Pemerintah dan militer dapat menggunakan hasil analisis data untuk merumuskan doktrin pertahanan siber nasional yang lebih responsif terhadap perubahan lingkungan strategis. Data empiris yang diperoleh dari *Big Data* dapat dijadikan rujukan dalam penyusunan SOP, regulasi keamanan siber, serta penguatan sistem koordinasi antar lembaga pertahanan. Dengan cara ini, strategi pertahanan siber tidak hanya bersifat teknis, tetapi juga menyentuh aspek regulatif, manajerial, dan politik pertahanan (Kementerian Pertahanan RI, 2020).

Dengan berbagai keunggulan tersebut, dapat disimpulkan bahwa *Big Data* berfungsi sebagai katalisator dalam optimalisasi strategi pertahanan siber. Ia tidak hanya meningkatkan akurasi dan efektivitas strategi, tetapi juga memastikan strategi tersebut selalu relevan dengan perkembangan teknologi dan pola ancaman baru. Oleh karena itu, pemanfaatan *Big Data* harus ditempatkan sebagai komponen utama dalam perumusan strategi keamanan siber militer di era perang modern yang semakin bergantung pada teknologi informasi.

3.4 Penguatan Intelijen Siber Militer

Penguatan intelijen siber merupakan dimensi penting dalam implementasi *Big Data* di lingkungan pertahanan militer. Intelijen tradisional yang sebelumnya mengandalkan sumber informasi manusia (*human intelligence*) dan teknologi pengawasan kini diperkuat oleh kemampuan analitik *Big Data* yang mampu mengolah jutaan data digital dari berbagai sumber, termasuk *network traffic*, aktivitas media sosial, komunikasi terenkripsi, serta jejak digital (*cyber footprint*) dari aktor siber. Dengan teknologi analitik yang canggih, *Big Data* dapat membantu militer dalam memetakan pola komunikasi musuh, mengidentifikasi kelompok peretas, serta melacak hubungan antar entitas yang terlibat dalam aktivitas siber berbahaya (Taddeo, 2017).

Kemampuan *Big Data* dalam intelijen siber tidak hanya bersifat deskriptif, melainkan juga prediktif. Melalui algoritma *machine learning* dan *data mining*, intelijen militer dapat mengenali pola yang berulang dan memprediksi serangan di masa depan. Misalnya, jika pola serangan siber menunjukkan peningkatan aktivitas dari wilayah tertentu atau aktor tertentu, sistem dapat memberikan peringatan dini kepada komando pertahanan. Analisis prediktif ini menjadi instrumen penting bagi militer dalam menyusun strategi *cyber deterrence* dan *proactive defense* (Nye, 2017).

Lebih jauh, *Big Data* memperkuat kemampuan *cyber intelligence fusion*, yaitu integrasi data dari berbagai domain, baik siber, darat, laut, udara, maupun ruang angkasa. Informasi yang diperoleh dari domain siber dapat dikombinasikan dengan data intelijen konvensional sehingga menghasilkan gambaran yang lebih utuh tentang ancaman yang dihadapi. Hal ini penting karena dalam peperangan modern, ancaman siber seringkali tidak berdiri sendiri, tetapi terintegrasi dengan operasi militer hibrida yang melibatkan propaganda, sabotase, hingga operasi militer konvensional (Singer & Friedman, 2014).

Dari perspektif strategi pertahanan, penguatan intelijen siber berbasis *Big Data* memiliki implikasi langsung terhadap *command and control system*. Informasi intelijen yang akurat dan real-time memungkinkan pengambil keputusan militer untuk merespons ancaman dengan lebih cepat dan tepat. Selain itu, intelijen siber yang diperoleh dari *Big Data* juga memperkuat daya tangkal (*deterrence capability*) karena memberikan keunggulan informasi (*information superiority*) atas lawan. Dalam banyak kasus, keunggulan informasi ini lebih menentukan dibandingkan kekuatan persenjataan konvensional (Rid, 2013).

Dengan demikian, penguatan intelijen siber melalui implementasi *Big Data* tidak hanya meningkatkan kemampuan deteksi dan prediksi serangan, tetapi juga memperluas kapasitas militer dalam melakukan operasi pertahanan yang lebih cerdas, adaptif, dan berbasis data. Oleh karena itu, *Big Data* harus dipandang sebagai instrumen strategis yang melekat pada doktrin intelijen militer modern dan menjadi bagian integral dari keamanan nasional di era digital.

3.5 Efisiensi Sumber Daya Pertahanan

Efisiensi sumber daya pertahanan menjadi salah satu keunggulan utama dari penerapan *Big Data* dalam strategi pertahanan militer. Dalam konteks keterbatasan anggaran dan kebutuhan operasional yang semakin kompleks, kemampuan untuk memaksimalkan penggunaan sumber daya baik personel, peralatan, maupun logistik menjadi sangat krusial. *Big Data* menyediakan mekanisme analitik yang mampu memetakan pola konsumsi sumber daya, mendeteksi pemborosan, serta memberikan rekomendasi optimalisasi. Misalnya, melalui analisis data pemeliharaan kendaraan tempur, sistem dapat memprediksi kapan alat utama sistem persenjataan (alutsista) perlu diperbaiki sebelum mengalami kerusakan fatal. Pendekatan ini dikenal dengan *predictive maintenance*, yang terbukti mampu mengurangi biaya perawatan sekaligus memperpanjang umur operasional peralatan militer (Waller & Fawcett, 2013).

Selain pada pemeliharaan, *Big Data* juga memainkan peran penting dalam manajemen logistik militer. Melalui analisis data distribusi, sistem dapat mengidentifikasi jalur suplai yang paling efisien, memperkirakan kebutuhan logistik berdasarkan pola operasi, dan meminimalisir risiko keterlambatan distribusi. Efisiensi ini tidak hanya berdampak pada penghematan biaya, tetapi juga meningkatkan kesiapan tempur karena pasokan dapat disalurkan secara tepat waktu dan sesuai kebutuhan. Dalam konteks peperangan modern yang berlangsung cepat, kemampuan logistik yang efisien dapat menjadi faktor penentu dalam menjaga kesinambungan operasi militer (Watts, 2017).

Lebih lanjut, *Big Data* memungkinkan adanya *resource allocation optimization* dalam penempatan pasukan dan penggunaan alutsista. Melalui integrasi data intelijen, data geografis, serta informasi real-time di medan tempur, komando militer dapat menempatkan sumber daya pada titik-titik strategis yang memiliki urgensi tertinggi. Dengan demikian, keputusan taktis dan strategis dapat diambil berdasarkan analisis yang objektif, bukan sekadar intuisi atau pengalaman semata. Pendekatan berbasis data ini tidak hanya meningkatkan efektivitas operasi, tetapi juga memastikan efisiensi

penggunaan sumber daya yang terbatas (Gansler & Lucyshyn, 2015).

Efisiensi sumber daya pertahanan yang didukung *Big Data* juga memiliki implikasi jangka panjang terhadap pembangunan kekuatan militer. Dengan adanya transparansi data dan pemetaan kebutuhan yang akurat, proses perencanaan anggaran pertahanan dapat dilakukan secara lebih rasional dan akuntabel. Hal ini penting bagi negara berkembang, termasuk Indonesia, yang harus menyeimbangkan kebutuhan modernisasi militer dengan keterbatasan fiskal. *Big Data* membantu memastikan bahwa setiap rupiah yang dialokasikan dalam anggaran pertahanan benar-benar digunakan untuk mendukung tujuan strategis pertahanan nasional (Yamin, 2020).

Dengan demikian, efisiensi sumber daya pertahanan yang dihasilkan dari penerapan *Big Data* bukan hanya menyangkut penghematan biaya, melainkan juga peningkatan efektivitas operasi, pemeliharaan kesiapan tempur, dan akuntabilitas dalam pengelolaan anggaran pertahanan. Oleh karena itu, penguatan kapabilitas analitik *Big Data* harus menjadi prioritas dalam modernisasi sistem pertahanan militer di era digital, sehingga militer mampu tetap adaptif, efektif, dan efisien dalam menghadapi dinamika ancaman global.

3.6 Pembahasan

Hasil penelitian menunjukkan bahwa *Big Data* berperan sebagai katalisator dalam transformasi pertahanan siber militer. Pemanfaatan data dalam skala masif memungkinkan militer tidak hanya merespons ancaman, tetapi juga melakukan deteksi dini, prediksi, dan formulasi strategi yang adaptif terhadap dinamika ancaman siber. Pada tataran konseptual, *Big Data* memperkuat kemampuan organisasi militer untuk beralih dari pendekatan *reactive defense* menuju *proactive cyber defense* yang berbasis pada kecerdasan data.

3.6.1 *Big Data* sebagai Pilar Strategi Keamanan Siber Militer

Keamanan siber pada era digital tidak lagi dapat dipandang hanya sebagai isu teknis yang terbatas pada pengelolaan jaringan atau perangkat lunak, melainkan telah menjadi bagian integral dari strategi pertahanan nasional. Dalam konteks militer, keberhasilan dalam menghadapi ancaman siber tidak hanya bergantung pada teknologi pertahanan konvensional, tetapi juga pada kemampuan menganalisis, mengolah, dan memanfaatkan data dalam jumlah besar untuk mendukung proses pengambilan keputusan.

Big Data berfungsi sebagai fondasi utama yang memungkinkan integrasi data dari berbagai sumber, seperti lalu lintas jaringan, log aktivitas sistem, data satelit, serta intelijen elektronik. Melalui pemrosesan data secara real-time, militer dapat memperoleh *situational awareness* yang lebih akurat, sehingga strategi pertahanan dapat dirumuskan berdasarkan kondisi faktual dan prediksi yang berbasis algoritma (Gandomi & Haider, 2015). Hal ini menempatkan *Big Data* bukan sekadar alat bantu teknis, melainkan pilar utama dalam arsitektur strategi pertahanan siber modern.

Lebih lanjut, penerapan *Big Data* dalam strategi pertahanan militer memberikan keuntungan pada level operasional dan strategis. Pada level operasional, *Big Data* memungkinkan sistem mendeteksi anomali dan pola serangan dengan cepat, sehingga respon dapat dilakukan secara tepat waktu. Sedangkan pada level strategis, data yang terakumulasi dari berbagai operasi siber dapat digunakan untuk memetakan tren ancaman global, memprediksi skenario serangan di masa depan, dan merumuskan kebijakan pertahanan yang adaptif. Hal ini mendukung transformasi konsep pertahanan dari *defensive posture* menjadi *adaptive resilience*, di mana militer tidak hanya bertahan, tetapi juga siap beradaptasi dan berkembang menghadapi tantangan baru (Miller, 2013).

Keunggulan *Big Data* sebagai pilar strategi keamanan siber militer juga terlihat dari kemampuannya dalam

memperkuat *decision making process*. Dengan algoritma analitik canggih, pemimpin militer dapat mengambil keputusan yang lebih cepat, tepat, dan berbasis bukti (*evidence based decision*). Hal ini sangat penting dalam konteks perang modern yang berlangsung dalam hitungan detik, di mana keterlambatan pengambilan keputusan dapat berakibat fatal terhadap keberlangsungan operasi (McAfee & Brynjolfsson, 2012).

Dengan demikian, *Big Data* telah menjelma sebagai elemen fundamental dalam perumusan strategi pertahanan siber militer. Posisinya tidak hanya sebagai instrumen pendukung, tetapi sebagai pilar utama yang menopang kemampuan militer dalam menjaga kedaulatan digital negara. Implementasi yang efektif dari teknologi *Big Data* dalam sektor militer akan memastikan bahwa keamanan siber nasional tidak hanya reaktif terhadap ancaman, melainkan proaktif, adaptif dan berkelanjutan.

3.6.2 Relevansi dengan Doktrin Pertahanan Indonesia

Implementasi *Big Data* dalam strategi keamanan siber militer memiliki relevansi yang sangat kuat dengan doktrin pertahanan Indonesia. Doktrin pertahanan nasional Indonesia menekankan bahwa ancaman kontemporer bersifat multidimensi, tidak hanya datang dari aspek militer konvensional, tetapi juga dari aspek non militer seperti siber, informasi, dan teknologi (Kementerian Pertahanan RI, 2020). Oleh karena itu, penguasaan teknologi informasi dan komunikasi menjadi keharusan strategis untuk menjaga kedaulatan negara di era digital.

Big Data sejalan dengan kerangka Asta Gatra, yaitu delapan aspek kehidupan nasional yang menjadi pilar ketahanan nasional. Dalam hal ini, *Big Data* berkontribusi pada penguatan gatra teknologi sekaligus mendukung gatra ideologi, politik, ekonomi, sosial budaya, pertahanan, dan keamanan. Melalui pemanfaatan analisis data masif, sistem pertahanan dapat merespons ancaman siber yang mengganggu stabilitas politik, keamanan, maupun ekonomi. Dengan demikian, *Big Data* menjadi instrumen yang memperkuat sinergi antara aspek militer dan non-militer dalam membangun ketahanan nasional (Suryono, 2018).

Selain itu, implementasi *Big Data* juga relevan dengan doktrin *Total Defense System* atau Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata). Doktrin ini menekankan keterlibatan seluruh komponen bangsa dalam menghadapi ancaman terhadap kedaulatan negara. Dalam konteks siber, *Big Data* memungkinkan integrasi data dari berbagai sektor pemerintah, swasta, akademisi, hingga masyarakat sipil yang dapat digunakan sebagai basis intelijen pertahanan. Hal ini mendukung pelaksanaan pertahanan semesta di ranah digital, dimana keterlibatan seluruh elemen bangsa dapat dimaksimalkan melalui jaringan informasi yang terintegrasi (Yulianto, 2019).

Lebih jauh lagi, *Big Data* mendukung visi Indonesia dalam Asta Cita menuju Indonesia Emas 2045, khususnya pada pilar pembangunan manusia dan penguasaan ilmu pengetahuan dan teknologi. Dengan mengintegrasikan *Big Data* ke dalam strategi pertahanan, Indonesia tidak hanya berfokus pada penguatan alutsista, tetapi juga membangun kapabilitas digital yang menjadi pondasi utama dalam menghadapi ancaman global berbasis siber. Hal ini menunjukkan bahwa *Big Data* tidak hanya relevan, tetapi juga esensial dalam mewujudkan kemandirian pertahanan nasional di era Revolusi Industri 4.0 (Prasetyo & Sutopo, 2018).

Dengan demikian, penerapan *Big Data* dalam pertahanan siber militer bukanlah pilihan tambahan, melainkan kebutuhan strategis yang selaras dengan doktrin pertahanan Indonesia. Keberadaannya memperkuat implementasi Asta Gatra, mendukung sistem pertahanan semesta, dan menjadi fondasi bagi transformasi pertahanan menuju kedaulatan digital Indonesia.

3.6.3 Deteksi Dini Ancaman Siber

Salah satu kontribusi paling signifikan dari penerapan *Big Data* dalam pertahanan siber militer adalah kemampuannya dalam mendukung deteksi dini terhadap ancaman siber. Dalam konteks keamanan pertahanan, deteksi dini merupakan elemen vital karena ancaman siber sering kali muncul secara tersembunyi, kompleks, dan terdistribusi. *Big Data* memungkinkan pengumpulan dan analisis data dalam jumlah besar secara *real-time*, seperti *network traffic*, *system logs*, serta aktivitas mencurigakan yang terjadi pada infrastruktur kritis militer. Dengan algoritma *machine learning* dan *artificial intelligence*, sistem dapat mengenali pola-pola anomali yang berpotensi sebagai serangan siber, bahkan sebelum dampaknya terasa signifikan (Chen, Mao, & Liu, 2014; Zikopoulos et al., 2012).

Kemampuan deteksi dini ini memberikan nilai strategis karena memungkinkan militer beralih dari pendekatan reaktif ke proaktif. Jika sebelumnya tindakan baru dilakukan setelah serangan terjadi, maka dengan *Big Data*, militer dapat melakukan pencegahan berbasis prediksi. Misalnya, pola serangan *distributed denial of service* (DDoS) dapat dikenali sejak awal dengan menganalisis lonjakan lalu lintas data yang tidak wajar, sehingga langkah mitigasi dapat segera diaktifkan sebelum jaringan militer lumpuh (Kshetri, 2014).

Selain itu, deteksi dini berbasis *Big Data* juga meningkatkan *situational awareness* dalam domain siber. Dengan memanfaatkan data yang terintegrasi dari berbagai sensor, sistem keamanan siber militer dapat memberikan gambaran komprehensif mengenai status ancaman, titik kerentanan, serta kemungkinan eskalasi serangan. Hal ini memungkinkan komando militer untuk mengambil keputusan secara cepat, tepat, dan terinformasi dalam merespons ancaman, sehingga mengurangi risiko kegagalan sistem kritis yang dapat berdampak pada operasi militer di lapangan (Huang et al., 2015).

Lebih jauh lagi, deteksi dini ancaman siber berbasis *Big Data* memiliki implikasi jangka panjang terhadap pengembangan doktrin pertahanan digital. Data yang terkumpul dari berbagai insiden siber dapat menjadi basis pembelajaran kolektif, yang kemudian digunakan untuk menyusun protokol keamanan baru, mengidentifikasi tren serangan global, dan membangun sistem pertahanan yang lebih adaptif. Dengan demikian, *Big Data* tidak hanya berfungsi untuk mendeteksi ancaman secara langsung, tetapi juga sebagai instrumen strategis dalam pengembangan kapasitas pertahanan berkelanjutan (Tankard, 2011).

Dengan demikian, deteksi dini ancaman siber yang diperkuat oleh *Big Data* menegaskan bahwa teknologi ini merupakan komponen esensial dalam menjaga kedaulatan digital militer. Implementasi sistem analitik real-time berbasis *Big Data* memungkinkan pertahanan nasional tidak hanya mampu bertahan dari ancaman yang ada, tetapi juga siap menghadapi tantangan baru yang terus berkembang dalam lanskap perang siber global.

3.6.4 Penguatan Intelijen Siber Militer

Implementasi *Big Data* juga memiliki relevansi strategis dalam memperkuat kemampuan intelijen siber militer. Intelijen siber berperan penting dalam mengidentifikasi, menganalisis, dan mengantisipasi potensi ancaman digital yang dapat mengganggu stabilitas keamanan nasional. Dengan memanfaatkan *Big Data*, militer dapat mengintegrasikan berbagai sumber informasi—baik *open-source intelligence* (OSINT), *signals intelligence* (SIGINT), maupun *cyber threat intelligence* (CTI)—untuk membentuk gambaran menyeluruh mengenai dinamika ancaman siber (Dupont, 2013).

Big Data memungkinkan proses analisis intelijen dilakukan secara cepat, masif, dan berbasis prediksi. Melalui teknik *data mining* dan *predictive analytics*, intelijen militer dapat menemukan pola tersembunyi dari jutaan data yang sebelumnya tidak terdeteksi. Misalnya, aktivitas komunikasi yang tidak biasa di *dark web* atau pola distribusi malware tertentu

dapat dijadikan indikator awal adanya kampanye siber yang terkoordinasi (Gonzalez, 2014). Informasi ini menjadi bahan penting dalam perumusan strategi pertahanan yang tidak hanya responsif, tetapi juga preventif.

Lebih jauh lagi, *Big Data* meningkatkan akurasi *threat attribution*, yaitu proses mengidentifikasi aktor di balik serangan siber. Selama ini, atribusi serangan siber menjadi tantangan besar karena sifat serangan yang anonim dan terdistribusi. Namun, dengan analisis data lintas sumber mulai dari *IP addresses*, perilaku lalu lintas data, hingga *metadata* komunikasi *Big Data* dapat membantu mempersempit kemungkinan pelaku serangan, baik yang berasal dari aktor negara (*state-sponsored*) maupun non-negara (*non-state actors*) (Rid & Buchanan, 2015). Hal ini sangat krusial dalam konteks diplomasi pertahanan, karena atribusi yang jelas dapat memperkuat posisi Indonesia dalam forum internasional terkait keamanan siber.

Selain aspek teknis, *Big Data* juga mendukung intelijen strategis melalui pemetaan tren geopolitik siber. Dengan memantau aktivitas digital global, intelijen militer dapat mengidentifikasi pola agresi siber yang berhubungan dengan konflik politik, ekonomi, atau militer. Misalnya, peningkatan serangan siber terhadap infrastruktur energi dapat menjadi indikator adanya eskalasi konflik regional. Informasi semacam ini memberikan keunggulan strategis bagi militer dalam merumuskan kebijakan pertahanan yang proaktif dan antisipatif (Valeriano & Maness, 2015).

Dengan demikian, penguatan intelijen siber militer melalui *Big Data* bukan hanya memperluas kapasitas analisis ancaman, tetapi juga meningkatkan kualitas pengambilan keputusan strategis. Integrasi *Big Data* ke dalam sistem intelijen menjadikan militer lebih siap dalam menghadapi spektrum ancaman yang kompleks, serta mampu menjaga kedaulatan dan keamanan nasional di era perang informasi global.

3.6.5 Efisiensi Sumber Daya Pertahanan

Efisiensi sumber daya merupakan salah satu manfaat paling nyata dari implementasi *Big Data* dalam konteks pertahanan militer. Dengan keterbatasan anggaran, personel, dan peralatan, militer dituntut untuk mengoptimalkan setiap aset yang dimiliki agar tetap dapat menjaga kesiapan tempur secara berkelanjutan. *Big Data* hadir sebagai solusi strategis untuk mendukung optimalisasi pemanfaatan sumber daya pertahanan melalui analisis prediktif, pemetaan kebutuhan, serta pengelolaan operasional yang lebih terukur (Waller & Fawcett, 2013).

Salah satu contoh konkret adalah penerapan *predictive maintenance* pada alutsista (alat utama sistem senjata). Dengan menganalisis data historis penggunaan dan kondisi teknis peralatan, sistem berbasis *Big Data* dapat memprediksi kapan peralatan memerlukan perawatan sebelum terjadi kerusakan fatal. Pendekatan ini terbukti mampu menurunkan biaya pemeliharaan sekaligus memperpanjang umur operasional peralatan, sehingga alutsista tetap dalam kondisi optimal saat dibutuhkan (Lee et al., 2014). Hal ini selaras dengan kebutuhan militer untuk menjaga *combat readiness* tanpa membebani anggaran pertahanan secara berlebihan.

Selain itu, *Big Data* juga meningkatkan efisiensi dalam bidang logistik militer. Melalui analisis data distribusi dan konsumsi, sistem dapat mengidentifikasi pola kebutuhan logistik berdasarkan medan operasi, cuaca, atau intensitas latihan. Informasi ini memungkinkan distribusi pasokan dilakukan lebih cepat, tepat, dan sesuai kebutuhan. Efisiensi logistik ini tidak hanya berimplikasi pada penghematan biaya, tetapi juga mempercepat respon militer dalam menghadapi ancaman, karena jalur suplai dapat diatur secara optimal (Watts, 2017).

Lebih jauh lagi, *Big Data* mendukung proses *resource allocation optimization* dalam perencanaan operasi militer. Integrasi data intelijen, informasi geografis, serta laporan operasional memungkinkan komando militer

menentukan prioritas penggunaan sumber daya secara lebih objektif. Misalnya, penempatan pasukan dan alutsista dapat diarahkan ke titik-titik dengan risiko tertinggi berdasarkan analisis data ancaman, sehingga efektivitas operasi meningkat tanpa harus menambah jumlah personel atau peralatan (Gansler & Lucyshyn, 2015).

Efisiensi ini juga memiliki implikasi jangka panjang terhadap perencanaan anggaran pertahanan. Dengan transparansi data dan analisis kebutuhan yang akurat, alokasi anggaran dapat dilakukan secara lebih rasional dan akuntabel. Hal ini penting bagi negara berkembang seperti Indonesia, yang harus menyeimbangkan kebutuhan modernisasi militer dengan keterbatasan fiskal. Implementasi *Big Data* dalam manajemen sumber daya pertahanan akan membantu memastikan bahwa setiap rupiah dalam anggaran pertahanan digunakan secara efektif untuk mendukung tujuan strategis nasional (Yamin, 2020).

Dengan demikian, efisiensi sumber daya pertahanan yang ditopang oleh *Big Data* tidak hanya berdampak pada penghematan biaya, tetapi juga peningkatan efektivitas operasi, kesiapan tempur, serta akuntabilitas dalam pengelolaan anggaran pertahanan. Hal ini menegaskan bahwa *Big Data* merupakan instrumen kunci dalam mewujudkan modernisasi pertahanan militer yang adaptif, efisien, dan berkelanjutan di era digital.

3.6.6 Tantangan Implementasi

Meskipun potensi *Big Data* dalam mendukung strategi keamanan siber militer sangat besar, implementasinya tidak terlepas dari sejumlah tantangan yang kompleks. Tantangan pertama adalah terkait dengan keamanan data internal. Lingkungan militer memiliki kerahasiaan tingkat tinggi, sehingga setiap kebocoran data dapat berdampak serius pada keamanan nasional. Sistem *Big Data* yang tidak dilengkapi dengan protokol keamanan berlapis seperti enkripsi *end to end*, autentikasi multi faktor dan sistem deteksi intrusi, berisiko menjadi celah yang dimanfaatkan oleh aktor jahat untuk mengakses informasi sensitif. Risiko ini semakin besar mengingat sifat *Big Data* yang terintegrasi dari berbagai sumber, sehingga sekali terjadi kebocoran, skala dampaknya bisa meluas (Rid, 2013).

Tantangan kedua adalah keterbatasan sumber daya manusia (SDM) ahli. Implementasi *Big Data* dalam konteks militer memerlukan personel yang memiliki kompetensi tinggi dalam analitik data, kecerdasan buatan, serta keamanan siber. Namun, hingga kini ketersediaan tenaga ahli di bidang ini masih terbatas, khususnya dalam lingkungan militer yang memiliki karakteristik dan standar keamanan berbeda dengan sektor sipil. Keterbatasan ini dapat menghambat optimalisasi pemanfaatan *Big Data* karena analisis data yang kompleks membutuhkan keahlian teknis sekaligus pemahaman tentang konteks strategis pertahanan (Patton, 2015).

Tantangan berikutnya adalah keterbatasan infrastruktur teknologi. Implementasi *Big Data* membutuhkan ekosistem teknologi yang kuat, mencakup pusat data dengan kapasitas penyimpanan besar, jaringan komunikasi yang aman dan stabil, serta kemampuan interoperabilitas dengan berbagai sistem pertahanan lainnya. Di Indonesia, pembangunan infrastruktur pertahanan berbasis digital masih menghadapi kendala, baik dari sisi anggaran, ketersediaan teknologi, maupun tingkat keamanan jaringan yang masih rentan terhadap serangan eksternal. Tanpa dukungan infrastruktur yang memadai, pemanfaatan *Big Data* berpotensi tidak maksimal dan bahkan menimbulkan kerentanan baru (Yin, 2014).

Dengan demikian, meskipun *Big Data* menawarkan peluang strategis dalam memperkuat pertahanan siber militer, tantangan implementasi harus diantisipasi secara serius. Diperlukan kombinasi antara peningkatan kapasitas SDM, pembangunan infrastruktur pertahanan digital, serta penerapan protokol keamanan siber berlapis untuk memastikan bahwa *Big Data* benar-benar mampu menjadi instrumen efektif

dalam menjaga kedaulatan digital Indonesia.

3.6.7 Implikasi Strategis bagi Pertahanan

1. Peningkatan Daya Tangkal (*Deterrence*).

Kemampuan militer dalam mengelola *Big Data* dapat meningkatkan daya tangkal (deterrence) terhadap potensi ancaman. Dengan analisis data berskala besar, militer mampu memprediksi pola serangan, mengidentifikasi kerentanan, dan merespons lebih cepat dibanding lawan. Hal ini memperkuat efek gentar (deterrence by denial) karena lawan menyadari bahwa serangan siber maupun konvensional akan lebih mudah terdeteksi dan digagalkan (Nye, 2017; Freedman, 2019). Dengan demikian, *Big Data* bukan hanya mendukung operasi pertahanan, tetapi juga menjadi instrumen strategis untuk menjaga stabilitas kawasan.

2. Integrasi dengan Operasi Militer Lainnya.

Pemanfaatan *Big Data* tidak berdiri sendiri, melainkan dapat diintegrasikan dengan berbagai matra operasi darat, laut, udara, serta siber. Melalui integrasi ini, data dari berbagai sensor (satellite imagery, UAV, sistem radar, hingga sensor komunikasi) dapat dikompilasi dan dianalisis secara real-time untuk menghasilkan gambaran situasi medan tempur (*situational awareness*) yang lebih utuh (Minkov, 2019; Clarke & Knake, 2019). Konsep ini sejalan dengan doktrin *Network-Centric Warfare* (NCW) yang menekankan superioritas informasi sebagai basis keunggulan militer.

3. Diplomasi Pertahanan Siber.

Penguasaan *Big Data* juga memiliki implikasi diplomasi pertahanan. Negara dengan kemampuan siber dan pengelolaan data yang baik akan lebih dihormati dalam forum internasional serta memiliki bargaining power dalam kerja sama keamanan global (Kavanagh & Rich, 2019; Lindsay, 2015). Bagi Indonesia, hal ini berarti peluang untuk memperkuat posisi dalam kerangka ASEAN Defence Ministers' Meeting (ADMM) maupun kerja sama bilateral di bidang siber. Selain itu, kemampuan ini mendukung misi diplomasi pertahanan yang menekankan keterbukaan, kepercayaan, dan kerja sama regional dalam menghadapi ancaman non-tradisional.

3.6.8 Perbandingan dengan Negara Lain

Negara-negara maju telah menjadikan *Big Data* sebagai salah satu fondasi utama dalam strategi pertahanan siber mereka.

1. Amerika Serikat.

AS melalui Department of Defense (DoD) telah lama mengintegrasikan *Big Data* ke dalam *Cyber Command* dan operasi gabungan lintas matra. Data intelijen dari satelit, UAV, sistem komunikasi, dan sensor medan tempur dikompilasi dalam *Joint All-Domain Command and Control (JADC2)* untuk mendukung pengambilan keputusan cepat dan akurat (Ministry of Defence UK, 2020). Praktik ini menunjukkan bahwa *Big Data* tidak hanya berfungsi untuk pertahanan siber, tetapi juga untuk mendukung operasi militer konvensional secara real-time.

2. Tiongkok.

Tiongkok memanfaatkan *Big Data* dalam kerangka *Military-Civil Fusion (MCF)*, yakni sinergi antara sektor pertahanan dan industri sipil. Strategi ini memungkinkan integrasi data dari berbagai sektor untuk memperkuat pertahanan siber sekaligus pengembangan teknologi kecerdasan buatan (AI) berbasis data besar (Taddeo, 2017).

Keunggulan Tiongkok terletak pada kemampuannya memobilisasi sumber daya nasional secara terpusat, sehingga infrastruktur *Big Data* dapat mendukung baik keamanan internal maupun operasi militer eksternal.

3. Rusia.

Rusia menitikberatkan pemanfaatan *Big Data* pada *information warfare* dan operasi siber ofensif. Data digunakan tidak hanya untuk pertahanan, tetapi juga untuk kampanye disinformasi, operasi psikologis, dan serangan siber terhadap infrastruktur kritis lawan (Giles, 2016). Hal ini menunjukkan model pemanfaatan *Big Data* yang bersifat agresif dan ofensif.

4. Implikasi bagi Indonesia.

Indonesia dapat belajar dari praktik terbaik negara-negara tersebut, namun tetap harus menyesuaikan dengan konteks nasional. Dari AS, Indonesia dapat mencontoh sistem integrasi lintas matra; dari Tiongkok, pendekatan sinergi pertahanan-sipil; dan dari Rusia, kewaspadaan terhadap pemanfaatan *Big Data* dalam *information warfare*. Adaptasi ini harus memperhatikan aspek regulasi, infrastruktur, sumber daya manusia, serta kultur pertahanan Indonesia yang berbasis pada prinsip pertahanan semesta. Dengan demikian, strategi implementasi *Big Data* dapat mendukung kemandirian pertahanan tanpa mengorbankan kedaulatan nasional.

3.6.9 Rekomendasi Implementasi *Big Data* untuk Indonesia

Berdasarkan analisis hasil penelitian serta perbandingan dengan negara lain, terdapat beberapa rekomendasi strategis agar implementasi *Big Data* dalam pertahanan siber militer Indonesia dapat berjalan efektif dan adaptif:

1. Penguatan Regulasi dan Kebijakan Nasional.

Diperlukan regulasi yang jelas mengenai pemanfaatan *Big Data* di sektor pertahanan, termasuk standar keamanan data, interoperabilitas antar-sistem, serta aturan berbagi data antar lembaga pertahanan dan sipil. Regulasi ini harus selaras dengan kebijakan *Cyber Defense Strategy* nasional dan *Rencana Induk Pertahanan Siber* (Kementerian Pertahanan RI, 2020).

2. Pembangunan Infrastruktur Teknologi Pertahanan.

Indonesia perlu mengembangkan pusat data militer berkapasitas tinggi (*defense data center*) dengan standar keamanan berlapis, jaringan komunikasi aman, serta sistem cadangan yang andal. Pembangunan ini dapat dilakukan melalui kerja sama strategis antara TNI, Kementerian Pertahanan, industri pertahanan dalam negeri, dan mitra internasional (Ministry of Defence UK, 2020).

3. Pengembangan SDM Ahli.

Ketersediaan personel militer yang menguasai analitik *Big Data* dan keamanan siber masih terbatas. Oleh karena itu, diperlukan program pendidikan, pelatihan, serta kolaborasi dengan perguruan tinggi dan lembaga riset untuk mencetak tenaga ahli yang mampu mengelola, menganalisis, dan mengamankan data pertahanan (Patton, 2015).

4. Sinergi Pertahanan Sipil (*Civil Military Cooperation*).

Mencontoh strategi Tiongkok, Indonesia dapat memanfaatkan potensi industri digital dan telekomunikasi nasional, seperti BUMN dan perusahaan teknologi lokal, dalam membangun ekosistem *Big Data* pertahanan. Pendekatan ini mendukung *kemandirian teknologi* sekaligus memperkuat ketahanan nasional.

5. Integrasi Lintas Matra dan Operasi Gabungan.

Big Data harus diintegrasikan dengan sistem komando dan kendali operasi darat, laut, udara, dan siber. Hal ini memungkinkan *situational awareness* terpadu dan pengambilan keputusan yang lebih cepat pada seluruh level operasi militer (Gandomi & Haider, 2015).

6. Diplomasi Pertahanan Siber.

Indonesia dapat memanfaatkan penguasaan *Big Data* sebagai instrumen diplomasi pertahanan, dengan memperkuat kerja sama internasional dalam bidang *cyber defense*, berbagi intelijen siber, serta partisipasi aktif dalam forum keamanan global (Kavanagh & Rich, 2019).

Dengan penerapan langkah-langkah tersebut, implementasi *Big Data* di sektor militer Indonesia bukan hanya meningkatkan pertahanan siber, tetapi juga memperkuat daya tangkal strategis, mendukung doktrin pertahanan semesta, serta menempatkan Indonesia pada posisi yang lebih berpengaruh dalam kerja sama keamanan regional dan global.

SIMPULAN

Penelitian ini menegaskan bahwa implementasi *Big Data* memiliki peran strategis dalam merumuskan kebijakan dan strategi keamanan siber militer Indonesia. *Big Data* tidak hanya berfungsi sebagai instrumen teknis dalam mendeteksi dan mencegah ancaman siber, tetapi juga sebagai pilar utama dalam mendukung proses pengambilan keputusan militer di tingkat operasional maupun strategis.

Hasil analisis menunjukkan bahwa *Big Data* memungkinkan deteksi dini ancaman melalui analisis data real-time, penguatan sistem komando dan kendali, serta integrasi dengan operasi gabungan lintas matra. Relevansi penerapan *Big Data* juga sejalan dengan doktrin pertahanan Indonesia, khususnya dalam kerangka Asta Gatra, yang menempatkan teknologi sebagai elemen penting ketahanan nasional.

Namun demikian, implementasi *Big Data* di lingkungan militer masih menghadapi sejumlah tantangan, seperti risiko kebocoran data, keterbatasan SDM ahli, dan kebutuhan akan infrastruktur teknologi yang andal. Untuk itu, diperlukan penguatan regulasi, pembangunan pusat data militer yang aman, pengembangan kompetensi personel, serta kerja sama strategis antara militer, pemerintah, industri pertahanan, dan mitra internasional.

Secara strategis, penguasaan *Big Data* akan memperkuat daya tangkal pertahanan Indonesia, meningkatkan diplomasi pertahanan siber, serta menempatkan Indonesia dalam posisi yang lebih kompetitif dalam menghadapi dinamika ancaman global. Dengan demikian, penerapan *Big Data* dalam strategi keamanan siber militer bukan hanya kebutuhan teknis, melainkan sebuah keharusan strategis untuk mewujudkan kedaulatan dan ketahanan negara di era digital.

Berdasarkan hasil penelitian, terdapat beberapa saran yang dapat dijadikan bahan pertimbangan bagi pengembangan strategi keamanan siber militer di Indonesia, yaitu:

1. Penguatan Riset dan Inovasi.

Penelitian lanjutan perlu mengkaji integrasi *Big Data* dengan teknologi kecerdasan buatan (*Artificial Intelligence*), *machine learning*, dan *cloud computing* untuk meningkatkan kemampuan deteksi, prediksi, serta respon otomatis terhadap serangan siber.

2. Pengembangan Kompetensi SDM.

Militer perlu menginisiasi program pendidikan dan pelatihan khusus di bidang *data science*, analitik *Big Data*, dan keamanan siber. Kolaborasi dengan perguruan tinggi serta lembaga riset nasional dapat mempercepat ketersediaan tenaga ahli.

3. Pembangunan Ekosistem Pertahanan Siber Nasional.

Diperlukan sinergi lintas sektor antara TNI, Kementerian Pertahanan, Badan Siber dan Sandi Negara (BSSN), industri pertahanan, serta perusahaan teknologi untuk membangun sistem *Big Data* pertahanan yang berkelanjutan dan mandiri.

4. Simulasi dan Uji Coba Operasional.

Implementasi *Big Data* perlu diuji melalui latihan gabungan dan simulasi perang siber untuk mengukur efektivitasnya dalam situasi nyata. Hal ini akan memastikan bahwa sistem yang dibangun tidak hanya berfungsi secara teoritis, tetapi juga praktis dalam konteks operasi militer.

5. Perluasan Studi Perbandingan Internasional.

Penelitian selanjutnya dapat mengkaji lebih dalam pengalaman negara-negara lain, seperti Amerika Serikat, Tiongkok, Rusia, maupun negara-negara ASEAN, untuk mengidentifikasi praktik terbaik yang dapat diadaptasi sesuai konteks Indonesia.

Dengan tindak lanjut melalui riset, pendidikan, pembangunan infrastruktur, dan kolaborasi lintas sektor, implementasi *Big Data* dalam pertahanan siber militer diharapkan mampu menjawab tantangan era digital dan memperkuat posisi strategis Indonesia ditingkat regional maupun global.

DAFTAR PUSTAKA

ASEAN. (2022). *Joint statement on cyber security cooperation*. Jakarta: ASEAN Secretariat. Retrieved from https://asean.org

Chen, M., Mao, S., & Liu, Y. (2014). *Big Data*: A survey. *Mobile Networks and Applications, 19*(2), 171–209. https://doi.org/10.1007/s11036-013-0489-0

Gandomi, A., & Haider, M. (2015). Beyond the hype: *Big Data* concepts, methods, and analytics. *International Journal of Information Management, 35*(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Kavanagh, C., & Rich, E. (2019). *Cyber diplomacy: Managing security and governance online*. Chatham House Report.

Kementerian Pertahanan Republik Indonesia. (2020). *Kebijakan pertahanan negara 2020–2024*. Jakarta: Kemhan RI.

Minkov, M. (2019). *Big Data* and military operations: A new paradigm in defense strategies. *Journal of Strategic Studies, 42*(3-4), 421–438. https://doi.org/10.1080/01402390.2019.1595512

Ministry of Defence UK. (2020). *Cyber and electromagnetic activities doctrine (JSP 740)*. London: MoD UK.

NATO Cooperative Cyber Defence Centre of Excellence. (2021). *NATO cyber defence policy*. Tallinn: NATO CCDCOE. Retrieved from https://ccdcoe.org

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Patton, R. M. (2015). *Training the cyber workforce: A military perspective*. RAND Corporation.

Rid, T. (2013). *Cyber war will not take place*. Oxford: Oxford University Press.

Sharma, S., & Kumar, A. (2020). Role of *Big Data* analytics in cyber security. *International Journal of Computer Applications, 176*(29), 1–6. https://doi.org/10.5120/ijca2020920141

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.

Taddeo, M. (2017). Deterrence by norms to stop interstate cyber attacks. *Philosophy & Technology, 30*(3), 279–291. https://doi.org/10.1007/s13347-016-0258-4

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Zikopoulos, P. C., Eaton, C., DeRoos, D., Deutsch, T., & Lapis, G. (2012). *Understanding Big Data: Analytics for enterprise class hadoop and streaming data*. New York: McGraw-Hill.