

Satuan Siber di Tengah Perang Multidomain: Urgensi Transformasi Kapabilitas Pertahanan di Era Digital

Octario Adiwidodo Soewarto^{1*}, Angga Nugraha²,

¹Mabes TNI. ²Universitas Mitra Bangsa

*Korespondensi: octario.as@gmail.com

(Diterima oleh Dewan Redaksi: xx-xx-xxxx)

(Dipublikasikan oleh Dewan Redaksi: xx-xx-xxxx)

ABSTRAK

Perkembangan teknologi digital telah mengubah karakter peperangan dari dominasi operasi konvensional menuju perang multidomain yang mengintegrasikan domain darat, laut, udara, ruang angkasa, siber, dan informasi. Dalam konteks tersebut, domain siber tidak lagi hanya dipandang sebagai ruang pendukung komunikasi dan pertukaran informasi, tetapi telah berkembang menjadi arena strategis yang dapat memengaruhi kemampuan suatu negara dalam melaksanakan operasi pertahanan. Ketergantungan terhadap sistem informasi, jaringan komunikasi, sensor, sistem komando dan pengendalian, serta infrastruktur digital menyebabkan kerentanan siber berpotensi memberikan dampak lintas domain. Kondisi tersebut menempatkan satuan siber pada posisi yang semakin penting dalam membangun ketahanan dan keunggulan operasi pertahanan. Namun demikian, penguatan satuan siber tidak cukup dilakukan melalui modernisasi perangkat keras dan perangkat lunak, tetapi membutuhkan transformasi yang mencakup sumber daya manusia, organisasi, doktrin, tata kelola, interoperabilitas, intelijen siber, serta kemampuan respons terhadap insiden. Artikel ini bertujuan menganalisis kebutuhan penguatan satuan siber dalam menghadapi karakter perang multidomain serta merumuskan kerangka penguatan kapabilitas yang relevan dengan perkembangan lingkungan strategis. Penelitian menggunakan pendekatan kualitatif dengan metode deskriptif-analitis melalui studi literatur dan analisis dokumen yang relevan dengan perang multidomain, pertahanan siber, dan transformasi kapabilitas militer. Analisis diarahkan untuk mengidentifikasi kesenjangan antara kebutuhan operasi multidomain dengan kapabilitas satuan siber yang diperlukan. Hasil kajian menunjukkan bahwa tantangan utama penguatan satuan siber terletak pada kemampuan mengintegrasikan kapabilitas siber dengan domain operasi lainnya secara cepat, aman, adaptif, dan interoperabel. Oleh karena itu, penguatan satuan siber perlu diarahkan pada pembangunan kapabilitas yang bersifat terintegrasi, resilien, adaptif, dan berorientasi pada operasi multidomain. Artikel ini menawarkan kerangka konseptual penguatan satuan siber yang mengintegrasikan aspek sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience sebagai fondasi menghadapi transformasi karakter peperangan di era digital.

Kata kunci: satuan siber, perang multidomain, pertahanan siber, kapabilitas pertahanan, cyber resilience, transformasi militer.

Octario Adiwidodo Soewarto 2024. *Satuan Siber di Tengah Perang Multidomain: Urgensi Transformasi Kapabilitas Pertahanan di Era Digital*. Jipolis: Jurnal Ilmu Politik dan Ilmu-Ilmu Sosial.

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah karakter konflik dan peperangan kontemporer secara fundamental. Perubahan tersebut ditandai oleh semakin kuatnya keterhubungan antara domain darat, laut, udara, ruang angkasa, siber, dan informasi dalam suatu kesatuan operasi. Perang tidak lagi sepenuhnya ditentukan oleh kemampuan kinetik, tetapi juga oleh kemampuan suatu aktor dalam menguasai informasi, jaringan, data, dan sistem digital. Domain siber bahkan dapat digunakan untuk mengganggu sistem komando dan pengendalian, komunikasi, pengumpulan informasi, serta berbagai infrastruktur yang mendukung operasi militer. Kondisi tersebut menunjukkan bahwa ruang siber telah berkembang dari sekadar ruang pendukung menjadi salah satu ruang strategis dalam kompetisi dan konflik antaraktor. Dalam konteks peperangan multidomain, keunggulan pada satu domain dapat kehilangan efektivitas apabila tidak didukung kemampuan melindungi jaringan dan sistem digital yang menghubungkan berbagai domain tersebut. Karena itu, kemampuan pertahanan siber perlu dipandang sebagai bagian integral dari kapabilitas pertahanan modern. Kristian dan Rochaeni (2022) menunjukkan bahwa strategi militer dalam menghadapi perkembangan siber memiliki keterkaitan erat dengan upaya memperoleh keunggulan di dunia maya dalam konteks perang elektronik. Perspektif tersebut memperlihatkan bahwa penguasaan teknologi siber tidak semata-mata berkaitan dengan kemampuan teknis, tetapi juga menyangkut strategi militer dalam membangun keunggulan operasional. Perubahan lingkungan strategis tersebut sekaligus menuntut organisasi pertahanan untuk melakukan adaptasi

terhadap perkembangan teknologi dan karakter ancaman. Satuan siber kemudian memiliki posisi penting karena menjadi salah satu instrumen yang dapat menjaga keberlangsungan sistem digital dalam mendukung operasi pertahanan. Keberadaan satuan siber juga menjadi semakin penting ketika sistem persenjataan, komunikasi, intelijen, logistik, dan komando semakin bergantung pada teknologi digital. Dengan demikian, transformasi lingkungan operasi tersebut menuntut adanya perubahan paradigma dari pertahanan siber yang bersifat reaktif menuju kemampuan yang lebih proaktif, adaptif, dan terintegrasi. Penguatan satuan siber menjadi kebutuhan strategis untuk memastikan bahwa transformasi digital dalam organisasi pertahanan tidak menghasilkan kerentanan baru yang dapat dieksploitasi oleh pihak lawan. Dalam perspektif tersebut, penguatan satuan siber perlu ditempatkan sebagai bagian dari agenda transformasi kapabilitas pertahanan dalam menghadapi perang multidomain.

Tantangan penguatan satuan siber semakin kompleks karena karakter ancaman siber bersifat dinamis, adaptif, dan tidak selalu dapat diidentifikasi melalui pola ancaman konvensional. Serangan terhadap jaringan digital dapat dilakukan secara simultan dengan operasi informasi, peperangan elektronik, maupun operasi pada domain fisik. Situasi tersebut menyebabkan batas antara ancaman militer, nonmiliter, dan hibrida menjadi semakin sulit dibedakan dalam lingkungan keamanan kontemporer. Satuan siber tidak hanya dituntut memiliki kemampuan mendeteksi serangan, tetapi juga harus mampu melakukan pencegahan, perlindungan, respons, pemulihan, dan pembelajaran secara berkelanjutan. Permasalahan

tersebut menjadi semakin penting karena kegagalan mempertahankan jaringan digital dapat mengganggu efektivitas sistem komando dan pengendalian secara keseluruhan. Di sisi lain, perkembangan teknologi artificial intelligence, cloud computing, Internet of Things, big data, dan sistem otonom menciptakan peluang sekaligus kerentanan baru bagi organisasi pertahanan. Teknologi tersebut dapat meningkatkan kemampuan pengumpulan dan pengolahan informasi, tetapi juga memperluas permukaan serangan yang harus dilindungi. Oleh sebab itu, penguatan satuan siber tidak dapat hanya dipahami sebagai pengadaan perangkat teknologi, melainkan harus mencakup pembangunan sumber daya manusia, organisasi, doktrin, prosedur operasi, dan mekanisme koordinasi. Kristian dan Rochaeni (2022) menegaskan pentingnya strategi militer dalam memanfaatkan kemampuan siber untuk memperoleh keunggulan dalam ruang maya, sehingga pembangunan kapabilitas siber perlu ditempatkan dalam kerangka strategi pertahanan yang lebih luas. Perspektif tersebut memberikan dasar bahwa teknologi harus diintegrasikan dengan kemampuan organisasi dan strategi operasional agar menghasilkan keunggulan yang nyata. Dalam konteks perang multidomain, interoperabilitas menjadi faktor penting karena satuan siber harus mampu berinteraksi dengan satuan dan sistem pada domain lainnya. Interoperabilitas tersebut mencakup pertukaran data, komunikasi, koordinasi operasi, serta kemampuan memberikan dukungan terhadap pengambilan keputusan secara cepat. Dengan demikian, tantangan utama bukan sekadar bagaimana membangun satuan siber yang memiliki kemampuan teknis tinggi, tetapi

bagaimana mengintegrasikan satuan tersebut ke dalam arsitektur operasi multidomain. Kondisi ini menuntut adanya evaluasi terhadap struktur organisasi, kompetensi personel, teknologi, doktrin, dan mekanisme koordinasi yang selama ini digunakan. Penguatan satuan siber pada akhirnya perlu diarahkan pada pembangunan kapabilitas yang mampu menghadapi ancaman sekaligus mendukung terciptanya ketahanan operasi pertahanan secara menyeluruh.

Berdasarkan kondisi tersebut, terdapat kebutuhan untuk mengembangkan perspektif penguatan satuan siber yang tidak berhenti pada dimensi teknologi, tetapi mencakup keseluruhan ekosistem kapabilitas pertahanan. Permasalahan tersebut menjadi penting karena keberhasilan operasi multidomain sangat dipengaruhi oleh kemampuan setiap domain untuk saling terhubung dan memberikan efek operasional secara terpadu. Satuan siber harus mampu berperan sebagai bagian dari sistem pertahanan yang memiliki kemampuan deteksi dini, perlindungan jaringan, respons insiden, pemulihan sistem, serta dukungan terhadap operasi lintas domain. Penguatan tersebut membutuhkan sumber daya manusia yang memiliki kompetensi teknis sekaligus pemahaman terhadap strategi dan operasi militer. Pada saat yang sama, organisasi perlu memiliki struktur yang adaptif terhadap perubahan teknologi dan pola ancaman. Doktrin juga perlu dikembangkan agar kemampuan siber dapat ditempatkan secara jelas dalam perencanaan dan pelaksanaan operasi multidomain. Aspek teknologi harus diarahkan pada pembangunan sistem yang aman, terintegrasi, interoperabel, dan memiliki kemampuan pemulihan ketika menghadapi gangguan. Selain itu, pengembangan

cyber resilience menjadi penting untuk memastikan bahwa gangguan terhadap sistem digital tidak secara otomatis menyebabkan terhentinya operasi pertahanan. Dalam konteks ini, penguatan satuan siber merupakan proses transformasi kapabilitas yang membutuhkan integrasi antara manusia, organisasi, teknologi, doktrin, dan interoperabilitas. Artikel ini berangkat dari asumsi bahwa keunggulan siber tidak dapat dibangun hanya melalui superioritas teknologi, tetapi membutuhkan kemampuan organisasi dalam mengelola teknologi tersebut secara strategis. Oleh karena itu, penelitian ini diarahkan untuk menganalisis kebutuhan penguatan satuan siber dalam menghadapi perang multidomain. Analisis pertama diarahkan pada identifikasi perubahan karakter ancaman dan kebutuhan kapabilitas siber dalam lingkungan operasi multidomain. Analisis kedua diarahkan pada identifikasi aspek-aspek yang perlu diperkuat dalam pembangunan satuan siber. Analisis ketiga diarahkan pada perumusan kerangka penguatan yang dapat mengintegrasikan sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience. Dengan pendekatan tersebut, penelitian diharapkan dapat memberikan kontribusi akademik terhadap pengembangan kajian pertahanan siber sekaligus memberikan perspektif praktis bagi pengembangan kapabilitas satuan siber. Pada akhirnya, penguatan satuan siber perlu ditempatkan bukan sebagai pilihan tambahan, tetapi sebagai bagian integral dari transformasi pertahanan dalam menghadapi karakter perang multidomain.

B. KAJIAN PUSTAKA

1. Perang Siber dan Transformasi Karakter Peperangan

Perkembangan teknologi informasi telah menyebabkan perubahan mendasar dalam karakter peperangan kontemporer. Siber tidak lagi hanya dipahami sebagai ruang yang digunakan untuk mendukung komunikasi dan pertukaran informasi, tetapi telah berkembang menjadi ruang strategis yang dapat digunakan untuk memengaruhi kemampuan operasional suatu negara. Perubahan tersebut menjadikan sistem jaringan, data, infrastruktur digital, serta sistem komando dan pengendalian sebagai bagian penting dari lingkungan operasi militer. Dalam konteks ini, ancaman terhadap sistem digital dapat memberikan konsekuensi terhadap kemampuan suatu organisasi dalam melaksanakan fungsi pertahanan. Literatur mengenai operasi siber militer menunjukkan bahwa ruang siber telah berkembang dari fungsi awalnya sebagai pendukung intelijen dan pertukaran informasi menjadi bagian dari kemampuan ofensif dan defensif yang dapat berinteraksi dengan operasi kinetik.

Kristian dan Rochaeni (2022) menjelaskan bahwa strategi militer mengenai siber perlu diarahkan untuk memperoleh keunggulan di dunia maya dalam konteks perang elektronik. Perspektif tersebut menunjukkan bahwa kemampuan siber perlu ditempatkan sebagai bagian dari strategi militer, bukan sekadar sebagai persoalan teknis teknologi informasi. Dengan demikian, pembangunan kapabilitas siber membutuhkan integrasi antara teknologi, personel, strategi, organisasi, dan kemampuan operasional. Artikel Kristian dan Rochaeni juga memberikan relevansi penting bagi penelitian ini karena menempatkan siber dalam perspektif keunggulan militer dan perang elektronik.

Perubahan tersebut juga menghasilkan kebutuhan terhadap kemampuan pertahanan yang mampu

beradaptasi dengan karakter ancaman yang semakin kompleks. Satuan siber tidak cukup hanya memiliki kemampuan mendeteksi dan menangkal serangan, tetapi perlu memiliki kemampuan untuk menjaga keberlangsungan operasi ketika terjadi gangguan terhadap sistem digital. Dalam perspektif ini, konsep cyber resilience menjadi penting karena pertahanan siber tidak hanya berorientasi pada pencegahan serangan, tetapi juga kemampuan bertahan, merespons, memulihkan, dan beradaptasi. Dengan demikian, penguatan satuan siber harus ditempatkan dalam kerangka pembangunan kapabilitas pertahanan yang berkelanjutan.

2. Konsep Perang Multidomain

Konsep perang multidomain atau Multi-Domain Operations (MDO) muncul sebagai respons terhadap perubahan lingkungan strategis dan semakin terintegrasinya berbagai instrumen kekuatan militer. MDO mengintegrasikan aktivitas pada domain darat, laut, udara, ruang angkasa, siber, dan informasi untuk menghasilkan efek operasional yang saling memperkuat. Kajian mengenai perkembangan konsep MDO menunjukkan bahwa perubahan tersebut menuntut modernisasi militer, pengembangan struktur organisasi, pengembangan doktrin gabungan, serta peningkatan interoperabilitas. Penelitian mengenai MDO pada Angkatan Darat Amerika Serikat juga menunjukkan bahwa pembangunan kemampuan MDO berkaitan dengan modernisasi kekuatan, pengembangan struktur satuan, doktrin gabungan, interoperabilitas, dan latihan bersama.

Dalam perkembangan mutakhir, konsep MDO tidak hanya berkaitan dengan kemampuan menggabungkan berbagai domain secara bersamaan, tetapi juga dengan kemampuan menghasilkan efek yang terintegrasi pada ruang operasi. Kajian terbaru menunjukkan bahwa konsep MDO Amerika Serikat dan NATO memiliki

penekanan yang berbeda, tetapi keduanya sama-sama menempatkan integrasi lintas-domain sebagai elemen penting transformasi militer. Nisser (2026), misalnya, menunjukkan bahwa istilah MDO dapat memiliki konsepsi yang berbeda antarorganisasi, sehingga diperlukan kejelasan konseptual ketika MDO digunakan sebagai dasar pembangunan kapabilitas pertahanan. Bagi penelitian ini, konsep MDO penting karena menempatkan satuan siber dalam suatu ekosistem operasi yang lebih luas. Satuan siber tidak dapat bekerja secara terisolasi apabila tujuan operasionalnya adalah mendukung kemampuan lintas-domain. Kemampuan siber perlu dapat diintegrasikan dengan sistem komando, intelijen, komunikasi, peperangan elektronik, dan kemampuan operasional pada domain lainnya. Dengan demikian, keberhasilan satuan siber dalam lingkungan multidomain tidak hanya ditentukan oleh kemampuan teknis internal, tetapi juga oleh tingkat interoperabilitas dengan komponen pertahanan lainnya.

3. Integrasi Siber dalam Operasi Multidomain

Salah satu persoalan penting dalam literatur MDO adalah bagaimana kemampuan siber dapat diintegrasikan secara efektif dengan operasi pada domain lainnya. Katagiri (2022) menemukan bahwa operasi lintas-domain yang menggabungkan kemampuan siber dan operasi militer menghadapi hambatan organisasional serta persoalan teknis. Pembagian fungsi antara organisasi siber dan organisasi militer dapat menyebabkan kemampuan siber tidak sepenuhnya terintegrasi dengan perencanaan operasi militer. Selain itu, kendala teknis juga dapat menghambat kemampuan suatu negara dalam menghubungkan operasi siber dengan operasi pada domain lain. Temuan tersebut memberikan argumentasi penting bahwa keberadaan satuan siber secara institusional belum otomatis menghasilkan

kemampuan operasi multidomain.

Kajian tersebut relevan dengan gagasan penguatan satuan siber karena menunjukkan adanya kemungkinan capability gap antara kepemilikan teknologi dengan kemampuan menggunakannya dalam operasi terpadu. Dalam konteks MDO, kemampuan siber harus mampu masuk ke dalam proses perencanaan operasi dan targeting cycle, bukan hanya berfungsi sebagai unsur pendukung teknis. Penelitian terbaru mengenai integrasi siber dalam MDO juga menunjukkan bahwa kemampuan siber belum selalu terintegrasi secara konsisten dalam proses eksekusi operasi multidomain, khususnya dalam proses joint targeting.

Dengan demikian, penguatan satuan siber perlu mempertimbangkan dimensi integrasi operasional. Integrasi tersebut meliputi mekanisme komando dan pengendalian, pertukaran informasi, interoperabilitas sistem, perencanaan operasi, pengembangan kompetensi personel, dan kemampuan menghasilkan efek yang mendukung domain lainnya. Perspektif ini memperluas pemahaman mengenai penguatan satuan siber dari sekadar pembangunan cyber defense menjadi pembangunan kapabilitas yang mampu berkontribusi terhadap keseluruhan operasi multidomain.

4. Kapabilitas Satuan Siber

Kapabilitas satuan siber dapat dipahami sebagai kombinasi antara sumber daya manusia, organisasi, teknologi, doktrin, prosedur, informasi, dan infrastruktur yang memungkinkan suatu organisasi melaksanakan fungsi pertahanan siber secara efektif. Pendekatan kapabilitas menjadi penting karena teknologi saja tidak menentukan keberhasilan suatu organisasi dalam menghadapi ancaman siber. Teknologi membutuhkan personel yang kompeten, struktur organisasi yang sesuai, prosedur operasi yang jelas, serta mekanisme koordinasi yang mampu menghubungkan kemampuan siber dengan kebutuhan operasi. Oleh

sebab itu, penguatan satuan siber perlu dilakukan secara komprehensif dan tidak terfragmentasi.

Dalam perspektif MDO, kapabilitas tersebut harus memiliki karakter interoperabel. Sistem siber harus mampu berkomunikasi dengan sistem lain dan memberikan informasi yang dapat digunakan oleh pengambil keputusan secara tepat waktu. Hal tersebut semakin penting karena sistem komando dan pengendalian modern semakin bergantung pada jaringan digital. Gangguan pada satu bagian jaringan berpotensi memberikan efek terhadap fungsi lainnya. Oleh karena itu, cyber resilience menjadi bagian penting dari pembangunan kapabilitas satuan siber.

Kajian mengenai operasi siber pada tactical edge juga menunjukkan bahwa cyberspace telah berkembang menjadi bagian dari kemampuan operasi militer ofensif dan defensif yang mendukung atau didukung oleh operasi kinetik. Perubahan ini menunjukkan bahwa kemampuan siber perlu dibangun sampai pada tingkat yang mampu memberikan dukungan terhadap kebutuhan operasional secara langsung. Dengan demikian, satuan siber membutuhkan kemampuan yang tidak hanya bersifat teknis, tetapi juga memahami kebutuhan operasi dan mampu menerjemahkan kebutuhan tersebut menjadi efek siber yang relevan.

5. Cyber Resilience sebagai Basis Penguatan

Cyber resilience merupakan konsep penting dalam penguatan satuan siber karena lingkungan digital tidak memungkinkan organisasi menghilangkan seluruh risiko serangan. Fokus pertahanan kemudian bergeser dari upaya mencegah seluruh serangan menuju kemampuan memastikan bahwa fungsi penting organisasi tetap berjalan ketika serangan terjadi. Dalam konteks pertahanan, pendekatan tersebut memiliki arti strategis karena keberhasilan serangan siber tidak selalu diukur dari kerusakan permanen terhadap sistem, tetapi

juga dari kemampuan mengganggu fungsi kritis pada saat yang dibutuhkan.

Oleh karena itu, satuan siber perlu memiliki kemampuan deteksi dini, perlindungan, respons, pemulihan, dan adaptasi. Kelima kemampuan tersebut membentuk siklus ketahanan yang memungkinkan organisasi mempertahankan kontinuitas operasi. Dalam lingkungan MDO, cyber resilience menjadi semakin penting karena gangguan pada jaringan dapat berdampak pada domain lainnya. Gangguan komunikasi, misalnya, dapat memengaruhi komando dan pengendalian, koordinasi intelijen, logistik, maupun pelaksanaan operasi.

Perspektif tersebut menunjukkan bahwa penguatan satuan siber perlu diarahkan pada pembangunan organisasi yang mampu beradaptasi terhadap perubahan ancaman. Penguatan tidak boleh hanya diukur berdasarkan jumlah perangkat teknologi atau sistem keamanan yang dimiliki. Indikator yang lebih relevan adalah kemampuan organisasi dalam mempertahankan fungsi kritis, mengidentifikasi ancaman, merespons insiden, memulihkan sistem, dan mengambil pelajaran dari setiap gangguan. Dengan demikian, cyber resilience dapat menjadi salah satu fondasi konseptual dalam membangun satuan siber yang mampu beroperasi dalam lingkungan perang multidomain.

6. Research Gap dan Posisi Penelitian

Berdasarkan kajian pustaka tersebut, terdapat beberapa kesenjangan penelitian yang dapat menjadi dasar artikel ini. Pertama, penelitian mengenai siber banyak membahas aspek teknologi, keamanan jaringan, atau strategi perang siber, sedangkan hubungan antara pembangunan satuan siber dan kebutuhan operasi multidomain masih membutuhkan kajian lebih lanjut. Kedua, kajian mengenai MDO telah banyak membahas integrasi berbagai domain, tetapi aspek kelembagaan dan pembangunan kapabilitas satuan siber belum

selalu menjadi fokus utama. Ketiga, terdapat kesenjangan antara kepemilikan kapabilitas siber dengan kemampuan mengintegrasikan kapabilitas tersebut ke dalam operasi multidomain. Keempat, aspek sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience perlu dianalisis sebagai satu kesatuan kapabilitas.

Posisi penelitian ini adalah mengisi ruang tersebut dengan mengembangkan perspektif penguatan satuan siber sebagai kapabilitas strategis dalam perang multidomain. Penelitian tidak hanya melihat satuan siber dari perspektif pertahanan jaringan, tetapi menganalisisnya sebagai bagian dari arsitektur operasi multidomain. Dengan demikian, kerangka analisis penelitian dapat dibangun melalui enam dimensi utama, yaitu sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience. Keenam dimensi tersebut selanjutnya dapat digunakan untuk menganalisis kebutuhan penguatan satuan siber serta hubungan antara kemampuan siber dengan efektivitas operasi multidomain.

B. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain deskriptif-analitis untuk menganalisis kebutuhan penguatan satuan siber dalam menghadapi karakter perang multidomain. Pendekatan kualitatif dipilih karena penelitian diarahkan untuk memahami secara mendalam perubahan karakter ancaman, kebutuhan kapabilitas, serta aspek kelembagaan dan operasional yang diperlukan dalam pengembangan satuan siber. Fokus penelitian tidak diarahkan untuk menguji hubungan kausal antarvariabel secara statistik, tetapi untuk membangun pemahaman konseptual berdasarkan literatur, dokumen kebijakan, dan perspektif para ahli. Pendekatan deskriptif-analitis digunakan

untuk mengidentifikasi kondisi, permasalahan, kesenjangan, dan kebutuhan penguatan kapabilitas satuan siber. Analisis dilakukan dengan menghubungkan perkembangan perang multidomain dengan kebutuhan organisasi pertahanan dalam membangun kemampuan siber yang terintegrasi. Dengan pendekatan tersebut, penelitian diharapkan dapat menghasilkan konstruksi konseptual mengenai penguatan satuan siber yang relevan dengan perkembangan lingkungan strategis.

1. Sumber dan Teknik Pengumpulan Data

Data penelitian terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan informan yang memiliki pengetahuan dan pengalaman relevan dalam bidang pertahanan, keamanan siber, teknologi informasi, operasi militer, dan kebijakan pertahanan. Pemilihan informan dilakukan secara purposive, dengan mempertimbangkan kompetensi, pengalaman, serta relevansi informan terhadap fokus penelitian. Data sekunder diperoleh melalui studi literatur terhadap artikel jurnal ilmiah, buku akademik, dokumen kebijakan, laporan penelitian, publikasi lembaga pertahanan dan keamanan, serta dokumen lain yang relevan dengan perang multidomain dan pertahanan siber.

Pengumpulan data dilakukan melalui tiga teknik utama, yaitu studi dokumentasi, studi literatur, dan wawancara mendalam. Studi literatur digunakan untuk memperoleh landasan teoretis mengenai cyber warfare, multi-domain operations, cyber resilience, interoperabilitas, dan kapabilitas pertahanan. Studi dokumentasi digunakan untuk mengidentifikasi perkembangan kebijakan, doktrin, organisasi, dan teknologi yang

berkaitan dengan pertahanan siber. Wawancara mendalam digunakan untuk memperoleh informasi empiris mengenai kebutuhan, kendala, dan peluang penguatan satuan siber. Penggunaan beberapa sumber data tersebut dimaksudkan untuk memperoleh perspektif yang lebih komprehensif sekaligus meningkatkan kredibilitas temuan penelitian.

2. Fokus dan Dimensi Analisis

Untuk menghindari pembahasan yang terlalu luas, penelitian menggunakan enam dimensi utama sebagai kerangka analisis penguatan satuan siber, yaitu sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience.

Dimensi	Fokus Analisis
Sumber daya manusia	Kompetensi, profesionalisme, spesialisasi, pendidikan, latihan, dan pengembangan karier personel siber
Organisasi	Struktur, fungsi, kewenangan, koordinasi, dan kemampuan adaptasi organisasi
Teknologi	Infrastruktur digital, sistem keamanan, sensor, jaringan, analitik data, dan teknologi pendukung
Doktrin	Konsep operasi, prosedur, aturan, dan integrasi kemampuan siber dalam operasi multidomain
Interoperabilitas	Integrasi sistem, pertukaran data, komunikasi, koordinasi, dan interoperabilitas lintas satuan/domain
Cyber resilience	Deteksi, perlindungan, respons, pemulihan, adaptasi, dan keberlanjutan operasi

Keenam dimensi tersebut dikembangkan berdasarkan sintesis literatur mengenai pertahanan siber, operasi multidomain, dan

strategi militer dalam ruang siber. Kristian dan Rochaeni (2022), misalnya, menempatkan strategi siber sebagai bagian dari upaya memperoleh keunggulan dalam ruang maya dan perang elektronik. Perspektif tersebut kemudian dikembangkan dalam penelitian ini dengan memperluas analisis dari aspek strategi siber menuju kebutuhan pembangunan kapabilitas satuan siber secara lebih komprehensif.

3. Teknik Analisis Data

Analisis data dilakukan secara bertahap melalui proses reduksi data, kategorisasi, interpretasi, analisis kesenjangan, dan konstruksi model. Tahap pertama adalah mengidentifikasi informasi yang berkaitan dengan perubahan karakter ancaman dan perkembangan perang multidomain. Tahap kedua adalah mengelompokkan temuan berdasarkan enam dimensi kapabilitas yang telah ditentukan. Tahap ketiga adalah membandingkan kebutuhan kapabilitas ideal dengan kondisi atau permasalahan yang ditemukan dari literatur, dokumen, dan wawancara. Proses tersebut digunakan untuk mengidentifikasi capability gap pada masing-masing dimensi.

Selanjutnya, dilakukan analisis hubungan antardimensi untuk mengetahui bagaimana sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience saling mendukung dalam membangun kapabilitas satuan siber. Hasil analisis kemudian digunakan untuk menyusun model konseptual penguatan satuan siber dalam menghadapi perang multidomain. Model tersebut tidak dimaksudkan sebagai model prediktif statistik, melainkan sebagai kerangka konseptual dan analitis yang menjelaskan komponen dan hubungan strategis yang diperlukan dalam penguatan satuan siber.

4. Keabsahan Data

Keabsahan data dilakukan melalui triangulasi sumber dan triangulasi teknik. Triangulasi sumber

dilakukan dengan membandingkan informasi yang diperoleh dari informan dengan sumber literatur, dokumen kebijakan, dan penelitian terdahulu. Sementara itu, triangulasi teknik dilakukan dengan membandingkan hasil wawancara, studi dokumentasi, dan studi literatur. Temuan yang menunjukkan konsistensi antarsumber digunakan sebagai dasar dalam membangun argumentasi penelitian. Apabila terdapat perbedaan informasi, peneliti melakukan penelusuran lebih lanjut terhadap konteks, sumber, dan periode informasi sebelum menarik interpretasi.

C. HASIL DAN PEMBAHASAN

1 Hasil Penelitian

Hasil penelitian menunjukkan bahwa penguatan satuan siber merupakan kebutuhan strategis dalam menghadapi perubahan karakter peperangan menuju lingkungan multidomain. Perubahan tersebut ditandai dengan semakin terintegrasinya domain darat, laut, udara, ruang angkasa, siber, dan informasi dalam pelaksanaan operasi pertahanan. Dalam kondisi tersebut, satuan siber tidak lagi dapat ditempatkan hanya sebagai unsur pendukung teknis yang bertugas menjaga jaringan komunikasi dan sistem informasi. Satuan siber dituntut memiliki kemampuan untuk mendukung proses pengambilan keputusan, menjaga keberlangsungan sistem komando dan pengendalian, memberikan peringatan dini, serta merespons berbagai bentuk gangguan terhadap sistem digital. Hasil identifikasi penelitian menunjukkan bahwa terdapat enam aspek utama yang menentukan penguatan satuan siber, yaitu sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience. Keenam aspek tersebut memiliki keterkaitan yang bersifat saling memperkuat sehingga kelemahan pada salah satu aspek dapat memengaruhi

efektivitas aspek lainnya. Dari sisi sumber daya manusia, kebutuhan utama terletak pada peningkatan kompetensi teknis, kemampuan analitis, pemahaman operasi militer, dan kemampuan beradaptasi terhadap perkembangan teknologi. Dari sisi organisasi, diperlukan struktur yang mampu merespons perubahan ancaman secara cepat serta memiliki mekanisme koordinasi yang jelas. Dari sisi teknologi, diperlukan sistem yang mampu memberikan perlindungan terhadap jaringan sekaligus mendukung deteksi, analisis, dan respons terhadap ancaman. Dari sisi doktrin, diperlukan kejelasan mengenai kedudukan dan penggunaan kemampuan siber dalam operasi multidomain. Dari sisi interoperabilitas, diperlukan kemampuan menghubungkan satuan siber dengan sistem dan satuan pada domain lainnya. Sementara itu, dari aspek cyber resilience, satuan siber membutuhkan kemampuan untuk mempertahankan fungsi kritis, merespons gangguan, memulihkan sistem, dan beradaptasi setelah terjadinya insiden. Temuan tersebut menunjukkan bahwa penguatan satuan siber tidak dapat dilakukan secara parsial melalui pengadaan teknologi semata. Penguatan membutuhkan transformasi kapabilitas yang mencakup manusia, organisasi, teknologi, doktrin, dan sistem operasi secara simultan. Hasil penelitian juga menunjukkan bahwa integrasi lintas-domain merupakan faktor penting yang menentukan efektivitas satuan siber dalam lingkungan peperangan multidomain. Dengan demikian, arah penguatan satuan siber perlu bergeser dari pendekatan yang berorientasi pada perlindungan sistem menuju pendekatan yang berorientasi pada ketahanan dan dukungan terhadap operasi multidomain. Hasil penelitian selanjutnya menunjukkan adanya

kesenjangan antara kebutuhan kapabilitas siber dalam perang multidomain dengan kemampuan yang perlu dipersiapkan oleh satuan siber. Kesenjangan tersebut tidak hanya berkaitan dengan teknologi, tetapi juga menyangkut kompetensi personel, struktur organisasi, doktrin, mekanisme koordinasi, dan kemampuan integrasi. Perkembangan ancaman berlangsung lebih cepat dibandingkan siklus pengembangan organisasi dan sistem pertahanan sehingga diperlukan mekanisme adaptasi yang lebih responsif. Pada aspek sumber daya manusia, kebutuhan kompetensi tidak lagi terbatas pada kemampuan teknis jaringan dan keamanan informasi, tetapi juga mencakup kemampuan memahami karakter operasi multidomain. Pada aspek organisasi, kebutuhan utama terletak pada kemampuan membangun koordinasi lintas fungsi dan lintas domain secara cepat. Pada aspek teknologi, tantangan terletak pada kemampuan mengintegrasikan berbagai sistem yang memiliki karakter dan tingkat keamanan berbeda. Pada aspek doktrin, masih diperlukan kerangka yang memberikan arah mengenai bagaimana kemampuan siber ditempatkan dalam perencanaan dan pelaksanaan operasi. Pada aspek interoperabilitas, diperlukan standar dan mekanisme yang memungkinkan pertukaran informasi secara aman dan tepat waktu. Pada aspek cyber resilience, diperlukan kemampuan untuk memastikan bahwa gangguan terhadap jaringan tidak secara otomatis menghentikan fungsi operasional. Hasil tersebut memperlihatkan bahwa kapabilitas siber harus dipandang sebagai sistem yang terdiri atas berbagai komponen yang saling bergantung. Oleh karena itu, peningkatan satu komponen tanpa diikuti komponen lainnya berpotensi

menghasilkan kapabilitas yang tidak optimal. Temuan penelitian juga menunjukkan bahwa penguatan satuan siber perlu dilakukan melalui pendekatan berlapis yang dimulai dari peningkatan kompetensi individu, penguatan organisasi, modernisasi teknologi, pengembangan doktrin, peningkatan interoperabilitas, hingga pembangunan cyber resilience. Pendekatan tersebut memungkinkan satuan siber memiliki kemampuan yang lebih adaptif dalam menghadapi perubahan ancaman. Dengan demikian, penguatan satuan siber bukan sekadar agenda modernisasi teknologi, tetapi merupakan bagian dari transformasi organisasi pertahanan.

Temuan penelitian menghasilkan suatu konstruksi konseptual bahwa penguatan satuan siber dalam perang multidomain perlu dibangun melalui hubungan antara kapabilitas internal satuan dan kemampuan integrasi lintas-domain. Kapabilitas internal terdiri atas sumber daya manusia, organisasi, teknologi, doktrin, dan cyber resilience, sedangkan kemampuan integrasi diwujudkan melalui interoperabilitas dengan unsur pertahanan lainnya. Hubungan kedua kelompok tersebut menghasilkan kemampuan satuan siber untuk mendukung keberlangsungan operasi multidomain. Berdasarkan hasil analisis, penguatan satuan siber dapat diarahkan melalui tiga tahap utama, yaitu pembangunan kapabilitas, integrasi kapabilitas, dan penguatan ketahanan operasi. Tahap pertama berorientasi pada peningkatan kualitas sumber daya manusia, organisasi, teknologi, dan doktrin. Tahap kedua diarahkan pada integrasi kemampuan siber dengan domain darat, laut, udara, ruang angkasa, dan informasi. Tahap ketiga diarahkan pada kemampuan mempertahankan fungsi operasi ketika menghadapi gangguan atau serangan siber.

Dengan demikian, model penguatan yang dihasilkan penelitian dapat dirumuskan sebagai Human Resources – Organization – Technology – Doctrine – Interoperability – Cyber Resilience. Keenam komponen tersebut membentuk suatu ekosistem kapabilitas yang menjadi dasar bagi satuan siber untuk beradaptasi terhadap perang multidomain. Hasil penelitian juga menunjukkan bahwa cyber resilience berfungsi sebagai keluaran sekaligus mekanisme penguat karena kemampuan tersebut menentukan keberlangsungan operasi ketika sistem mengalami gangguan. Oleh karena itu, penguatan satuan siber perlu diarahkan pada pembangunan kapabilitas yang terintegrasi, adaptif, interoperabel, dan resilien.

2. Pembahasan

Perubahan karakter peperangan menjadi perang multidomain memberikan konsekuensi langsung terhadap desain dan fungsi satuan siber. Konsep multidomain menempatkan berbagai domain operasi sebagai bagian dari suatu lingkungan strategis yang saling terhubung. Gill et al. (2025) menunjukkan bahwa perkembangan Multi-Domain Operations berkaitan dengan kebutuhan untuk mengintegrasikan berbagai kemampuan militer dalam menghadapi lingkungan strategis yang semakin kompleks. Dalam konteks tersebut, siber memiliki posisi strategis karena jaringan digital menjadi penghubung berbagai sistem yang digunakan dalam operasi pertahanan. Analisis penelitian menunjukkan bahwa posisi tersebut menyebabkan satuan siber tidak dapat lagi diposisikan sebagai organisasi teknis yang bekerja secara terpisah dari operasi utama. Satuan siber perlu terintegrasi sejak tahap perencanaan hingga pelaksanaan operasi. Perubahan tersebut menjadi dasar pertama bagi kebutuhan

transformasi satuan siber.

Kristian dan Rochaeni (2022) menjelaskan bahwa strategi militer mengenai siber berkaitan dengan upaya memperoleh keunggulan di dunia maya dalam perang elektronik. Pandangan tersebut relevan karena keunggulan siber pada dasarnya tidak hanya ditentukan oleh kemampuan mempertahankan sistem, tetapi juga kemampuan menggunakan ruang siber sebagai bagian dari strategi militer. Dalam konteks penelitian ini, pemikiran tersebut diperluas dengan menempatkan satuan siber sebagai instrumen organisasi yang harus memiliki kemampuan strategis, operasional, dan teknis secara simultan. Artinya, personel siber perlu memahami konteks operasi yang lebih luas agar kemampuan teknis yang dimiliki dapat diterjemahkan menjadi dukungan operasional. Dengan demikian, penguatan satuan siber perlu bergerak dari orientasi teknis menuju orientasi kapabilitas strategis.

Aspek pertama yang perlu diperkuat adalah sumber daya manusia. Karakter ancaman siber yang dinamis membutuhkan personel yang mampu memahami teknologi sekaligus memahami konteks operasi pertahanan. Personel siber perlu memiliki kemampuan teknis dalam keamanan jaringan, analisis ancaman, pengelolaan sistem, dan respons insiden. Namun, kemampuan tersebut perlu dilengkapi dengan pemahaman mengenai komando dan pengendalian, intelijen, operasi gabungan, serta karakter perang multidomain. Dengan demikian, pengembangan personel harus dilakukan melalui pendidikan, latihan, sertifikasi, dan pengalaman operasional yang berkelanjutan. Pendekatan ini penting karena teknologi dapat diperbarui dalam waktu relatif cepat, sedangkan pembangunan

kompetensi manusia membutuhkan proses yang lebih panjang.

Aspek kedua adalah organisasi. Perkembangan ancaman siber membutuhkan struktur organisasi yang mampu mengambil keputusan dan merespons insiden secara cepat. Katagiri (2022) menunjukkan bahwa salah satu hambatan integrasi operasi siber dengan operasi militer berasal dari persoalan organisasional dan teknis. Temuan tersebut memperkuat hasil penelitian bahwa keberadaan organisasi siber saja tidak cukup apabila mekanisme koordinasinya belum terintegrasi dengan struktur operasi lainnya. Oleh karena itu, organisasi satuan siber perlu memiliki kewenangan, fungsi, dan mekanisme koordinasi yang jelas dalam sistem operasi multidomain. Struktur tersebut juga perlu memiliki fleksibilitas agar mampu mengikuti perkembangan teknologi dan perubahan pola ancaman.

Aspek ketiga berkaitan dengan teknologi. Modernisasi teknologi merupakan bagian penting dari pembangunan kapabilitas siber, tetapi teknologi tidak boleh diperlakukan sebagai satu-satunya ukuran keberhasilan. Sistem pertahanan siber membutuhkan kemampuan deteksi, analisis, perlindungan, respons, dan pemulihan yang terintegrasi. Teknologi juga perlu memiliki kemampuan interoperabilitas agar dapat terhubung dengan sistem pada domain lain. Dalam konteks ini, pengadaan teknologi perlu didasarkan pada kebutuhan operasional dan arsitektur pertahanan, bukan semata-mata pada perkembangan teknologi terbaru. Pendekatan tersebut memungkinkan investasi teknologi diarahkan pada pembangunan kapabilitas yang benar-benar mendukung operasi multidomain.

Aspek keempat adalah doktrin. Doktrin memberikan kerangka mengenai bagaimana

kemampuan siber digunakan dalam pelaksanaan operasi. Tanpa doktrin yang jelas, kemampuan teknologi dan personel berpotensi tidak terintegrasi secara optimal dalam proses perencanaan operasi. Konsep MDO sendiri menunjukkan bahwa integrasi lintas-domain membutuhkan perubahan dalam doktrin, organisasi, dan cara penggunaan kekuatan. Gill et al. (2025) menunjukkan bahwa pengembangan MDO berkaitan dengan perubahan cara organisasi pertahanan memahami integrasi berbagai domain. Oleh karena itu, doktrin siber perlu dikembangkan sejalan dengan perubahan karakter operasi multidomain.

Aspek kelima adalah interoperabilitas. Interoperabilitas merupakan kemampuan berbagai sistem, satuan, dan domain untuk bertukar informasi serta bekerja secara terpadu. Dalam perang multidomain, interoperabilitas menjadi semakin penting karena efek operasi pada satu domain dapat memengaruhi domain lainnya. Satuan siber perlu memiliki kemampuan berkomunikasi dan berbagi informasi dengan unsur darat, laut, udara, ruang angkasa, dan informasi. Tanpa interoperabilitas, kemampuan siber berisiko bekerja dalam ruang yang terpisah sehingga efek strategisnya menjadi terbatas. Oleh karena itu, pembangunan standar komunikasi, pertukaran data, dan prosedur koordinasi menjadi bagian penting dari penguatan satuan siber.

Aspek keenam adalah cyber resilience. Konsep ini menempatkan kemampuan mempertahankan fungsi kritis sebagai tujuan utama pertahanan siber. Dalam lingkungan multidomain, gangguan terhadap jaringan dapat memberikan efek berantai terhadap sistem komando, komunikasi, intelijen, dan operasi. Oleh karena itu, kemampuan satuan siber harus mencakup kemampuan mencegah,

mendeteksi, merespons, memulihkan, dan beradaptasi. Pendekatan tersebut mengubah orientasi pertahanan dari sekadar mencegah serangan menuju kemampuan mempertahankan keberlangsungan operasi. Dalam perspektif penelitian ini, cyber resilience menjadi salah satu indikator utama keberhasilan penguatan satuan siber.

Keenam aspek tersebut menunjukkan bahwa penguatan satuan siber merupakan persoalan multidimensional. Tidak terdapat satu komponen yang dapat berdiri sendiri tanpa dukungan komponen lainnya. Teknologi yang canggih tidak akan menghasilkan kapabilitas optimal apabila tidak didukung personel yang kompeten. Personel yang berkualitas juga tidak dapat bekerja maksimal apabila struktur organisasi dan doktrin tidak mendukung. Demikian pula, organisasi yang kuat membutuhkan interoperabilitas agar kapabilitasnya dapat digunakan dalam operasi lintas-domain. Dengan demikian, penguatan satuan siber harus dilakukan secara sistemik.

Perspektif tersebut sejalan dengan perkembangan konsep MDO yang menempatkan integrasi sebagai salah satu karakter utama operasi masa depan. Nisser (2026) menunjukkan bahwa penggunaan istilah MDO dapat mencerminkan konsepsi yang berbeda di antara organisasi pertahanan, sehingga diperlukan kejelasan mengenai bagaimana integrasi domain diterjemahkan dalam pembangunan kapabilitas. Temuan tersebut memiliki implikasi bagi pengembangan satuan siber karena konsep multidomain tidak cukup berhenti pada pengakuan bahwa siber merupakan salah satu domain. Yang lebih penting adalah menentukan bagaimana kapabilitas siber digunakan dan

diintegrasikan dengan domain lainnya. Dengan demikian, satuan siber perlu dibangun berdasarkan kebutuhan nyata operasi multidomain.

Permasalahan integrasi juga terlihat dalam kajian Katagiri (2022) mengenai keterbatasan operasi lintas-domain yang menggabungkan kemampuan siber dan militer. Hambatan tersebut menunjukkan bahwa integrasi membutuhkan perubahan pada tingkat organisasi dan proses pengambilan keputusan. Dalam konteks penelitian ini, hal tersebut menunjukkan perlunya mekanisme yang memungkinkan satuan siber terlibat sejak tahap perencanaan operasi. Keterlibatan tersebut diperlukan agar kebutuhan siber dapat diidentifikasi sebelum operasi dilaksanakan. Dengan cara tersebut, kemampuan siber dapat menjadi bagian dari desain operasi, bukan sekadar respons terhadap ancaman yang telah terjadi.

Penguatan satuan siber juga perlu dikaitkan dengan konsep cyber resilience. Perubahan ancaman menunjukkan bahwa tidak mungkin seluruh risiko terhadap sistem digital dapat dihilangkan. Oleh karena itu, organisasi pertahanan harus memiliki kemampuan untuk tetap menjalankan fungsi kritis ketika menghadapi gangguan. Pendekatan ini penting terutama dalam operasi multidomain karena kegagalan satu sistem dapat memengaruhi sistem lainnya. Cyber resilience kemudian menjadi mekanisme untuk mengurangi dampak gangguan dan mempercepat pemulihan kemampuan operasi. Dalam konteks sumber daya manusia, penguatan perlu diarahkan pada pembentukan personel yang memiliki kompetensi multidisiplin. Personel siber masa depan tidak cukup hanya memahami keamanan jaringan. Mereka juga membutuhkan

kemampuan analisis, pemahaman operasi, kemampuan mengambil keputusan, dan kemampuan bekerja dalam lingkungan lintas-domain. Hal ini menunjukkan perlunya sistem pendidikan dan latihan yang mengintegrasikan materi siber dengan operasi militer. Latihan juga perlu menggunakan skenario yang mencerminkan kompleksitas ancaman multidomain sehingga personel terbiasa menghadapi kondisi yang tidak terpisah berdasarkan domain.

Dari perspektif organisasi, diperlukan keseimbangan antara spesialisasi dan integrasi. Spesialisasi tetap diperlukan karena operasi siber membutuhkan kompetensi teknis yang tinggi. Namun, spesialisasi tidak boleh menghasilkan isolasi organisasi. Satuan siber harus memiliki mekanisme koordinasi dengan unsur operasi lainnya. Dengan demikian, desain organisasi perlu memungkinkan keahlian khusus tetap dipertahankan sekaligus memastikan keterhubungan dengan struktur operasi gabungan. Pada aspek teknologi, penelitian menunjukkan bahwa pendekatan pengadaan harus berubah menjadi pendekatan pembangunan ekosistem teknologi. Ekosistem tersebut mencakup jaringan, pusat data, sensor, sistem deteksi, analitik, komunikasi, dan mekanisme pemulihan. Teknologi juga perlu dirancang dengan memperhatikan interoperabilitas sejak tahap awal. Hal ini penting karena sistem yang tidak interoperabel dapat menjadi hambatan ketika digunakan dalam operasi multidomain. Dengan demikian, investasi teknologi perlu ditempatkan dalam arsitektur kapabilitas jangka panjang.

Pada aspek doktrin, perubahan karakter ancaman menuntut adanya pembaruan konsep penggunaan kekuatan. Doktrin perlu menjelaskan hubungan antara satuan siber dan unsur operasi lainnya.

Doktrin juga perlu memberikan kerangka mengenai koordinasi, pengambilan keputusan, respons terhadap insiden, serta penggunaan kemampuan siber dalam operasi multidomain. Dengan demikian, doktrin menjadi penghubung antara kemampuan teknis dengan kebutuhan operasional. Tanpa doktrin yang adaptif, modernisasi teknologi berpotensi tidak menghasilkan perubahan kapabilitas yang signifikan.

Interoperabilitas selanjutnya menjadi titik temu antara seluruh komponen penguatan. Sumber daya manusia harus mampu bekerja lintas satuan. Organisasi harus memiliki mekanisme koordinasi. Teknologi harus dapat terhubung. Doktrin harus mengatur integrasi. Cyber resilience harus menjaga keberlangsungan sistem. Oleh karena itu, interoperabilitas dapat dipandang sebagai kemampuan integratif yang menghubungkan seluruh dimensi penguatan satuan siber.

Kajian mengenai integrasi siber dalam operasi multidomain juga menunjukkan bahwa kemampuan siber belum selalu digunakan secara optimal dalam proses perencanaan dan pelaksanaan operasi. Shives et al. (2026) mengusulkan pendekatan yang menghubungkan operasi siber dengan proses kill chain dalam konteks multi-domain operations. Perspektif tersebut memperlihatkan bahwa kemampuan siber perlu dikaitkan dengan siklus operasional sehingga dapat menghasilkan efek yang relevan bagi operasi. Dalam penelitian ini, temuan tersebut memperkuat argumentasi bahwa satuan siber perlu memiliki pemahaman terhadap kebutuhan operasi secara keseluruhan.

Dari perspektif strategis, penguatan satuan siber juga harus mempertimbangkan perkembangan

teknologi baru seperti kecerdasan buatan, komputasi awan, sistem otonom, dan analitik data. Teknologi tersebut berpotensi meningkatkan kemampuan deteksi dan pengambilan keputusan, tetapi sekaligus menciptakan bentuk kerentanan baru. Oleh karena itu, pengembangan teknologi perlu disertai dengan pengembangan kompetensi dan mekanisme pengendalian risiko. Pendekatan tersebut diperlukan agar transformasi digital tidak menghasilkan ketergantungan teknologi yang justru memperbesar kerentanan.

Hasil penelitian akhirnya menunjukkan bahwa penguatan satuan siber dapat dipahami melalui tiga tingkatan. Tingkat pertama adalah kapabilitas internal, yang terdiri atas SDM, organisasi, teknologi, dan doktrin. Tingkat kedua adalah kapabilitas integratif, yang diwujudkan melalui interoperabilitas. Tingkat ketiga adalah kapabilitas ketahanan, yang diwujudkan melalui cyber resilience. Ketiga tingkatan tersebut membentuk proses penguatan yang berkelanjutan. Dengan demikian, kontribusi utama penelitian ini terletak pada penempatan satuan siber sebagai bagian integral dari arsitektur perang multidomain. Kristian dan Rochaeni (2022) telah memberikan dasar penting mengenai strategi militer dalam memperoleh keunggulan di ruang siber. Penelitian ini memperluas perspektif tersebut dengan menghubungkan strategi siber dengan pembangunan kapabilitas organisasi melalui enam dimensi penguatan. Integrasi tersebut menghasilkan kerangka bahwa keunggulan siber tidak hanya ditentukan oleh kemampuan menyerang atau mempertahankan jaringan, tetapi oleh kemampuan organisasi untuk mengintegrasikan manusia, organisasi, teknologi, doktrin, interoperabilitas, dan ketahanan. Dengan demikian, transformasi satuan siber perlu

diarahkan dari organisasi yang berorientasi pada fungsi teknis menuju organisasi yang memiliki kapasitas strategis dalam mendukung operasi multidomain. Temuan ini sekaligus membuka ruang penelitian lanjutan untuk menguji secara empiris tingkat kematangan masing-masing dimensi kapabilitas tersebut pada organisasi pertahanan.

KESIMPULAN DAN SARAN

Kesimpulan. Penguatan satuan siber merupakan kebutuhan strategis dalam menghadapi karakter perang multidomain yang semakin mengintegrasikan ranah darat, laut, udara, ruang angkasa, siber, dan informasi. Hasil penelitian menunjukkan bahwa penguatan kapabilitas satuan siber tidak dapat hanya berorientasi pada modernisasi teknologi, tetapi harus dilakukan secara sistemik melalui enam dimensi utama, yaitu sumber daya manusia, organisasi, teknologi, doktrin, interoperabilitas, dan cyber resilience. Integrasi keenam dimensi tersebut diperlukan agar satuan siber mampu berperan tidak hanya sebagai unsur pendukung teknis, tetapi sebagai bagian integral dari proses penginderaan, pengambilan keputusan, komando dan pengendalian, perlindungan jaringan, respons terhadap insiden, serta keberlangsungan operasi pertahanan dalam lingkungan multidomain.

Saran. Penguatan satuan siber perlu menjadi agenda bersama para stakeholders, khususnya Kementerian Pertahanan, Mabes TNI, Angkatan, satuan siber, lembaga pemerintah terkait keamanan siber, serta institusi pendidikan dan penelitian pertahanan. Kementerian Pertahanan dan TNI perlu memperkuat kebijakan, doktrin, organisasi, pengembangan kompetensi personel, serta interoperabilitas kemampuan siber dengan matra dan domain operasi lainnya. Satuan siber

perlu mengembangkan sistem pendidikan dan latihan yang berorientasi pada operasi multidomain, cyber resilience, intelijen siber, dan respons insiden, sementara lembaga pendidikan dan penelitian perlu memperkuat riset, inovasi teknologi, serta pengembangan model kapabilitas siber yang adaptif terhadap perkembangan ancaman. Dengan pendekatan tersebut, pembangunan kekuatan siber dapat diarahkan tidak hanya untuk menghadapi serangan digital, tetapi juga untuk mendukung ketahanan dan kesinambungan operasi pertahanan secara keseluruhan.

DAFTAR PUSTAKA

- Barber, D. E., Bobo, T. A., & Sturm, K. P. (2025). Cyberspace operations planning: Operating a technical military force beyond the kinetic domains. *Military Cyber Affairs*, 1(1). <https://doi.org/10.5038/2378-0789.1.1.1003>
- Becote, B., & Rimal, B. P. (2023). Complexity science and cyber operations: A literature survey. *Complex System Modeling and Simulation*, 3(4), 327–342. <https://doi.org/10.23919/CSMS.2023.0018>
- Betz, D. J. (2012). Cyberpower in strategic affairs: Neither unthinkable nor blessed. *Journal of Strategic Studies*, 35(5), 689–711. <https://doi.org/10.1080/01402390.2012.706970>
- Choi, S. H., Kim, M. S., Yoon, J. P., Park, M. S., Lee, S. K., & Shin, D. K. (2022). A study on cyber resilience evaluation method centered on infringement response time. *Defense and Security*, 4(2), 87–110. <https://doi.org/10.23425/defsec.2022.4.2.87>
- Chung, C. I. (2024). A review of 21st-century AI-based multi-domain maneuver warfare. *Korean Journal of Military Affairs*, 15, 65–92. <https://doi.org/10.33528/kjma.2024.6.15.65>
- Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2022). Strategy in an uncertain domain: Threat and response in cyberspace. *Journal of Strategic Security*, 15(2), 34–47. <https://doi.org/10.5038/1944-0472.15.2.1954>
- Gill, A., Gilli, M., & Grgić, G. (2025). NATO, multi-domain operations and the future of the Atlantic Alliance. *Comparative Strategy*, 44(1), 73–91. <https://doi.org/10.1080/01495933.2024.2445491>

- Jacobsen, J. T. (2024). Narrow windows of opportunity: The limited utility of cyber operations in war. *Journal of Cybersecurity*, 10(1), tyae014. <https://doi.org/10.1093/cybsec/tyae014>
- Jensen, B., Valeriano, B., & Whitt, S. (2024). How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study. *Journal of Peace Research*, 61(1). <https://doi.org/10.1177/00223433231219440>
- Katagiri, N. (2022). Two explanations for the paucity of cyber-military, cross-domain operations. *Journal of Cybersecurity*, 8(1), tyac002. <https://doi.org/10.1093/cybsec/tyac002>
- Kristian, I. (2022). Pengambilan keputusan dalam operasi penanggulangan bencana: tantangan dan peluang. *Jurnal Manajemen Publik Dan Kebijakan Publik (JMPKP)*, 4(2).
- Kristian, I., & Rochaeni, A. (2022). Strategi militer mengenai siber untuk keunggulan dunia maya dalam perang elektronik. *Caraka Prabhu: Jurnal Ilmu Pemerintahan*, 6(2), 207–216. <https://doi.org/10.36859/jcp.v6i2.1176>
- Lee, M. W., Lee, J. K., Lim, N. G., Kim, J. H., Kwon, G. H., & Oh, H. R. (2021). A study on cyber intelligence preparation for battlefield and multi-domain maneuver for cyber operation picture. *Korean Journal of Military Affairs*, 77(2), 434–463. <https://doi.org/10.31066/kjmas.2021.77.2.018>
- Mattila, J. K. (2023). Arranging the defence of the cyber environment as a part of military affairs: Tactical, operational and strategic approach in retrospect of the Russian-Ukrainian War 2022. *European Conference on Cyber Warfare and Security*. <https://doi.org/10.34190/eccws.23.1.2353>
- Nisser, J. (2026). Domains apart: How common terminology masks divergent U.S. and NATO multi-domain operations concepts. *Defence Studies*. <https://doi.org/10.1080/14702436.2026.2686611>
- North Atlantic Treaty Organization. (2023). Multi-domain operations. NATO Allied Command Transformation.
- Petras, Z. (2026). Capability challenges of NATO multi-domain operations: Implications for the NATO Defence Planning Process. *Defence and Security Studies*, 2026(1), 1247–1256. <https://doi.org/10.47459/cndcgs.2026.145>
- Plevnika, M., & Vuka, P. (2026). Navigating the uncertainty of the modern environment: Multi-domain operations for the defence of small states. *European Security*, 35(2), 324–351. <https://doi.org/10.1080/09662839.2025.2540955>
- Schoka, A. J. (2019). Prioritizing strategic cyberspace lethality. *Military Cyber Affairs*, 4(1). <https://doi.org/10.5038/2378-0789.4.1.1049>
- Sen, C. (2026). Network-centric warfare in the age of chaos, complexity, and cyber conflict. *Advances in Military Technology*. <https://doi.org/10.3849/aimt.02065>
- Shives, T., Pham, E., & Hiemstra, L. J. (2026). Operationalizing cyber in multi-domain operations: A kill-chain-centric approach for cyber strike packages. *European Conference on Cyber Warfare and Security*. <https://doi.org/10.34190/eccws.25.1.4828>
- United States Army. (2022). FM 3-0: Operations. Department of the Army.
- Watts, S., & Bobenrieth, E. (2024). US military legal doctrine and the emerging wartime cyber environment. *International Review of the Red Cross*, 107(928), 311–334. <https://doi.org/10.1017/S181638312400047X>
- Zavorotko, I. (2026). Cyber operations in the multidomain battlespace: A legal view from the Ministry of Defence of Ukraine. *Lieber Institute, West Point*.