

Pendampingan Penguatan Interoperabilitas Siber Militer melalui Forum Kolaboratif dalam Mendukung Pertahanan Negara

Immer HP Butarbutar^{1*}, Rudy Agus Gemilang Gultom², R. Djoko Andreas Navalino³, Susilo Adi Purwanto⁴

¹ Program Studi Ilmu Pertahanan, Pascasarjana, Universitas Pertahanan Republik Indonesia

^{2,3,4} Universitas Pertahanan Republik Indonesia

Email Author: immerbutarbutar2@gmail.com*

Kata Kunci:

Interoperabilitas; Siber
Militer; Pendampingan;
Pertahanan Siber;
Pertahanan Negara

Abstrak

Ruang siber telah berkembang menjadi domain strategis pertahanan yang menuntut respons cepat, koordinasi lintas satuan, dan pertukaran informasi yang selaras. Di lingkungan pertahanan Indonesia, kemampuan siber berkembang pada Kementerian Pertahanan, Markas Besar TNI, dan Angkatan, namun masih terdapat kesenjangan pada aspek organisasi, sumber daya manusia, sarana-prasarana, standarisasi, serta mekanisme koordinasi. Kegiatan pengabdian kepada masyarakat ini diarahkan kepada komunitas profesional pertahanan siber melalui pendampingan partisipatif dan forum diskusi kolaboratif untuk memperkuat kesamaan pemahaman serta merumuskan agenda penguatan interoperabilitas siber militer. Tahapan kegiatan meliputi pemetaan kebutuhan, penyamaan persepsi mengenai interoperabilitas, identifikasi kesenjangan operasional, penyusunan matriks prioritas, dan perumusan tindak lanjut. Hasil pendampingan mengerucut pada lima kebutuhan: tata kelola dan organisasi yang terhubung, mekanisme komando-kendali dan pertukaran informasi yang disepakati, penguatan kompetensi serta sertifikasi personel, modernisasi dan standarisasi sarana-prasarana, dan pengembangan mekanisme evaluasi berkelanjutan. Forum kolaboratif menegaskan bahwa interoperabilitas tidak identik dengan integrasi penuh, tetapi bertumpu pada prosedur bersama, pemahaman informasi yang sama, sumber daya yang kompatibel, dan kemampuan subsistem untuk bekerja bersama sesuai kebutuhan operasi. Kegiatan menghasilkan peta masalah, matriks kebutuhan, dan agenda tindak lanjut yang dapat digunakan sebagai bahan pembahasan kelembagaan untuk memperkuat pertahanan negara.

Key Word:

Interoperability; Military
Cyber; Mentoring; Cyber
Defense; National
Defense

Abstract

Cyberspace has evolved into a strategic defense domain requiring rapid response, cross-unit coordination, and aligned information exchange. Within Indonesia's defense sector, cyber capabilities have developed across the Ministry of Defense, the Indonesian National Armed Forces Headquarters, and the Services, yet gaps remain in organizational arrangements, human resources, infrastructure, standardization, and coordination mechanisms. This community engagement program targeted the professional military cyber community through participatory mentoring and collaborative discussion forums to strengthen shared understanding and formulate an agenda for improving military cyber interoperability. The activities included needs mapping, conceptual alignment on interoperability, identification of operational gaps, preparation of a priority matrix, and formulation of follow-up actions. The engagement identified five key needs: connected governance and organization, agreed command-and-control and information-sharing mechanisms, stronger personnel competencies and certification, modernization and standardization of supporting infrastructure, and continuous evaluation mechanisms. The forum emphasized that interoperability is not equivalent to full integration; rather, it relies on common procedures, shared understanding of information, compatible resources, and the ability of subsystems to operate together when required. The activity produced a problem map, a needs matrix, and a follow-up agenda that can support institutional deliberation to strengthen national defense.

Copyright © 2026 Immer HP Butarbutar

This work is licensed under a **Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)**

PENDAHULUAN

Pertahanan negara merupakan fungsi fundamental yang diarahkan untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari setiap ancaman dan gangguan. Undang-Undang Nomor 3 Tahun 2002 menegaskan bahwa Indonesia menyelenggarakan pertahanan yang bersifat semesta dengan melibatkan warga negara, wilayah, serta sumber daya nasional yang dipersiapkan secara dini dan dikelola secara total, terpadu, terarah, dan berkelanjutan. Dalam kerangka tersebut, ilmu pengetahuan dan teknologi merupakan bagian dari sumber daya buatan yang memiliki posisi semakin strategis. Ketergantungan sistem pemerintahan,

ekonomi, komunikasi, layanan publik, dan pertahanan terhadap teknologi digital menjadikan ruang siber bukan lagi sekadar media pendukung, tetapi telah berkembang menjadi lingkungan operasi yang berpengaruh langsung terhadap ketahanan dan pertahanan negara.

Perkembangan ruang siber berlangsung bersamaan dengan meningkatnya konektivitas jaringan, komputasi, artificial intelligence, big data, dan otomatisasi. Perubahan tersebut memperluas spektrum ancaman karena gangguan tidak lagi harus dilakukan melalui kontak fisik atau kehadiran kekuatan militer di wilayah lawan. Serangan terhadap jaringan, sistem informasi, perangkat, atau aliran data dapat digunakan untuk mengganggu komunikasi, memengaruhi pengambilan keputusan, menurunkan kesiapan operasi, bahkan menimbulkan efek terhadap infrastruktur strategis. Sharma et al. (2022) menempatkan ancaman siber sebagai bagian dari perubahan karakter konflik kontemporer, sedangkan Perwej et al. (2021) menunjukkan bahwa peningkatan interkoneksi sistem juga memperluas permukaan serangan dan kebutuhan terhadap tata kelola keamanan yang lebih komprehensif.

Dalam praktiknya, ancaman siber dapat muncul dalam berbagai bentuk, termasuk phishing, malware, ransomware, denial of service, rekayasa sosial, pencurian data, pengambilalihan sesi, serta serangan terdistribusi. Sadiku et al. (2020) menjelaskan bahwa perkembangan teknik serangan berlangsung seiring perubahan teknologi, sehingga pertahanan siber tidak dapat bergantung pada perangkat atau prosedur yang statis. Pemanfaatan artificial intelligence pada keamanan siber juga menambah dimensi baru. Teknologi ini dapat membantu mendeteksi pola anomali dan mendukung respons yang lebih cepat, tetapi pada saat yang sama dapat dimanfaatkan oleh aktor ancaman untuk meningkatkan skala dan kompleksitas serangan. Wibisono et al. (2024) menekankan pentingnya peningkatan kapabilitas satuan siber melalui pemanfaatan teknologi dan kerangka keamanan yang terstruktur.

Bagi Indonesia, isu tersebut berkaitan langsung dengan kebutuhan menjaga kedaulatan, integritas wilayah, dan keselamatan bangsa. Pemerintah telah melakukan berbagai langkah kebijakan, termasuk pembentukan Tim Kerja Pertahanan Dunia Maya dan penerbitan Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. Di lingkungan TNI, kesadaran bahwa ruang siber merupakan bagian dari medan operasi modern juga mendorong pengembangan kemampuan cyber army dan satuan-satuan siber pada berbagai tingkat organisasi. Meskipun demikian, perkembangan kemampuan pada masing-masing organisasi belum secara otomatis menghasilkan interoperabilitas. Naskah yang menjadi basis kegiatan ini menunjukkan adanya tantangan koordinasi antara Kementerian Pertahanan, Markas Besar TNI, dan Angkatan, baik pada aspek organisasi, sumber daya manusia, peralatan, maupun prosedur operasional.

Interoperabilitas menjadi isu penting karena operasi pertahanan siber membutuhkan kecepatan pertukaran informasi, kesamaan pemahaman terhadap situasi, serta koordinasi tindakan lintas satuan. Federal Research Division sebagaimana dikutip Kom dan McDaniel (2020) menjelaskan interoperabilitas sebagai kapasitas untuk bertukar informasi antarpelaku dan proses dengan pemahaman yang sama terhadap informasi yang dipertukarkan. Kapasitas tersebut bergantung pada ketersediaan sumber daya yang kompatibel, prosedur yang disepakati dan terdokumentasi, serta penyelarasan aspek organisasi, budaya, bahasa, motivasi, dan kebijakan. Dengan demikian, interoperabilitas tidak sekadar persoalan koneksi teknis antarsistem, melainkan mencakup dimensi organisasi, manusia, proses, dan tata kelola.

Dua karakter konsep interoperabilitas perlu dipahami secara tepat. Pertama, interoperabilitas tidak identik dengan integrasi penuh. Sistem yang berbeda dapat tetap memiliki karakter, fungsi, dan pengelolaan masing-masing, tetapi harus mampu bertukar informasi dan bekerja bersama ketika diperlukan. Kedua, interoperabilitas tidak menuntut homogenitas perangkat atau aplikasi. Perbedaan platform dapat dipertahankan selama tersedia standar, prosedur, protokol, dan mekanisme komunikasi yang memungkinkan kerja lintas sistem. Mansyur et al. (2019) menekankan bahwa sistem yang interoperabel dapat tetap terhubung secara longgar dan diaktifkan sesuai kebutuhan operasi. Pemahaman ini penting untuk mencegah kecenderungan bahwa solusi terhadap setiap masalah koordinasi selalu berupa penyatuan organisasi atau perangkat.

Pemetaan awal yang terdapat dalam naskah sumber memperlihatkan beberapa persoalan nyata. Pada aspek organisasi, Pusat Pertahanan Siber (Pushansiber) Baintarahan Kementerian Pertahanan memiliki keterbatasan jangkauan koordinasi terhadap satuan siber di Markas Besar TNI dan Angkatan. Pada

aspek sumber daya manusia, kebutuhan personel belum sepenuhnya sesuai dengan Daftar Susunan Personel dan kepemilikan sertifikasi profesional seperti Offensive Security Certified Professional maupun Certified Ethical Hacker masih terbatas. Pada aspek sarana-prasarana, sebagian tools belum berlisensi sehingga pemutakhiran dan pemeliharaan belum optimal; kondisi ini berdampak pada kemampuan deteksi traffic, analisis serangan, identifikasi, proteksi, respons, dan pemulihan. Temuan tersebut sejalan dengan Krisnata et al. (2022), yang menyoroti keterbatasan aset, kemampuan, dan proses persiapan pada pengembangan kapabilitas siber pertahanan.

Masalah tersebut menunjukkan bahwa kebutuhan penguatan tidak cukup dijawab melalui investasi teknologi. Komunitas profesional pertahanan siber juga memerlukan ruang untuk menyamakan pemahaman, memetakan hubungan antarmasalah, mengidentifikasi prioritas, dan menyusun rekomendasi yang dapat diterjemahkan ke dalam agenda kelembagaan. Di sinilah pendekatan pengabdian kepada masyarakat menjadi relevan. Pengabdian tidak diarahkan pada simulasi serangan, penetrasi sistem, atau aktivitas teknis yang berisiko, tetapi pada pendampingan konseptual dan penguatan tata kelola bagi komunitas praktisi pertahanan siber. Forum kolaboratif ditempatkan sebagai media untuk menghubungkan perspektif organisasi, sumber daya manusia, teknologi, dan operasi.

Kegiatan ini bertujuan: (1) memetakan kebutuhan utama komunitas profesional pertahanan siber terkait interoperabilitas; (2) memperkuat kesamaan pemahaman mengenai makna dan prinsip interoperabilitas; (3) menyusun prioritas penguatan pada dimensi organisasi, sumber daya manusia, sarana-prasarana, mekanisme komando-kendali, dan pertukaran informasi; (4) merumuskan agenda tindak lanjut yang dapat digunakan sebagai bahan pembahasan oleh pemangku kepentingan; dan (5) memperkuat orientasi kolaboratif dalam pengembangan pertahanan siber militer. Secara akademik, kegiatan ini menghubungkan ilmu pertahanan dengan pendekatan pendampingan komunitas profesional; secara praktis, kegiatan menghasilkan kerangka masalah dan rekomendasi yang dapat membantu proses penataan interoperabilitas siber militer.

METODE

Kegiatan pengabdian menggunakan pendekatan partisipatif berbasis pendampingan konseptual dan Focus Group Discussion (FGD). Pendekatan ini disusun dari metode yang terdapat pada naskah awal, yaitu analisis data sekunder dan forum diskusi dengan sumber serta pakar. Dalam konteks pengabdian, metode tersebut diarahkan untuk memfasilitasi komunitas profesional pertahanan siber dalam membaca masalah secara bersama, menguji konsistensi pemahaman, dan menyusun prioritas tindak lanjut. Fokus kegiatan bukan pada pengujian kerentanan teknis jaringan dan bukan pula pada praktik ofensif siber, melainkan pada dimensi tata kelola, interoperabilitas, kompetensi, standarisasi, dan koordinasi kelembagaan.

Sasaran kegiatan adalah komunitas profesional yang berkaitan dengan penyelenggaraan pertahanan siber militer, terutama lingkungan Kementerian Pertahanan, TNI, dan Angkatan sebagaimana menjadi locus pada naskah sumber. Artikel ini tidak menetapkan jumlah peserta tertentu karena data tersebut tidak tersedia pada dokumen sumber. Oleh sebab itu, keberhasilan kegiatan dievaluasi berdasarkan kualitas keluaran konseptual dan keterhubungan rumusan masalah dengan kebutuhan yang teridentifikasi, bukan berdasarkan klaim kuantitatif mengenai jumlah peserta atau peningkatan skor pengetahuan.

Bahan pendampingan disusun dari data sekunder, literatur ilmiah, regulasi, dan hasil pemetaan kondisi organisasi yang telah tersedia. Literatur digunakan untuk memberikan kerangka mengenai pertahanan siber, interoperabilitas, ancaman siber, dan penguatan kapasitas. Regulasi digunakan untuk menempatkan rekomendasi dalam konteks pertahanan negara. Temuan lapangan pada naskah sumber diposisikan sebagai bahan pemicu diskusi, terutama terkait keterbatasan organisasi, personel, standarisasi peralatan, mekanisme laporan, serta hubungan koordinasi antara Pushansiber, Markas Besar TNI, dan Angkatan.

Pelaksanaan pendampingan dibagi menjadi beberapa tahapan yang saling berurutan. Tahap pertama adalah orientasi masalah untuk menyepakati ruang lingkup dan batas kegiatan. Tahap kedua adalah pemetaan kebutuhan dengan mengelompokkan persoalan ke dalam dimensi organisasi, sumber daya manusia, sarana-prasarana, informasi, dan operasi. Tahap ketiga adalah penyamaan persepsi mengenai interoperabilitas agar peserta tidak menyamakan interoperabilitas dengan integrasi penuh. Tahap

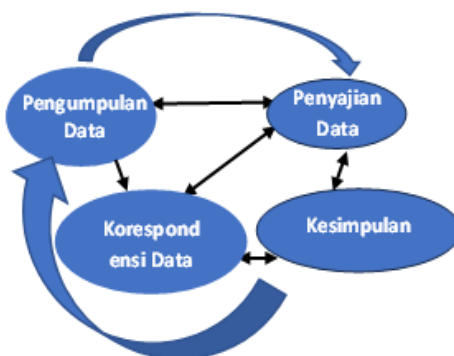
keempat adalah analisis kesenjangan antara kondisi yang dihadapi dengan karakter sistem yang diharapkan. Tahap kelima adalah penyusunan matriks prioritas, dilanjutkan dengan perumusan rekomendasi dan mekanisme tindak lanjut. Tahap terakhir adalah refleksi untuk menilai kelayakan rumusan dan mengidentifikasi aspek yang masih memerlukan keputusan pada tingkat kelembagaan.

Tabel 1. Tahapan Kegiatan Pendampingan Penguatan Interoperabilitas Siber Militer

No.	Tahap	Aktivitas Utama	Keluaran
1	Orientasi dan pembatasan ruang lingkup	Menjelaskan tujuan, batas kegiatan, dan fokus pada tata kelola serta interoperabilitas; tidak melakukan pengujian ofensif atau penetrasi sistem.	Kesamaan ruang lingkup kegiatan.
2	Pemetaan kebutuhan	Mengidentifikasi kondisi organisasi, SDM, sarana-prasarana, standardisasi, mekanisme pelaporan, dan koordinasi.	Peta masalah dan kebutuhan prioritas.
3	FGD dan penyamaan persepsi	Membahas definisi interoperabilitas, perbedaan interoperabilitas dan integrasi, kebutuhan pertukaran informasi, dan prosedur bersama.	Kesamaan pemahaman prinsip interoperabilitas.
4	Analisis kesenjangan	Membandingkan kondisi teridentifikasi dengan kebutuhan sistem yang mampu bekerja lintas organisasi dan subsistem.	Daftar kesenjangan organisasi, SDM, teknologi, dan proses.
5	Penyusunan prioritas	Mengelompokkan kebutuhan menurut urgensi, keterkaitan, dan prasyarat implementasi.	Matriks prioritas penguatan.
6	Perumusan tindak lanjut	Menyusun rekomendasi mengenai tata kelola, kompetensi, standardisasi, komando-kendali, serta evaluasi.	Agenda tindak lanjut kelembagaan.
7	Refleksi	Menilai konsistensi hasil pendampingan dengan kebutuhan pertahanan siber dan mengidentifikasi batas kegiatan.	Catatan evaluasi dan kebutuhan pembahasan lanjutan.

Teknik pendampingan menggabungkan pemaparan singkat, diskusi terarah, pemetaan masalah, dan refleksi. Pemaparan digunakan untuk memberikan landasan konsep. Diskusi terarah digunakan untuk menguji keterkaitan antara masalah organisasi dan kebutuhan operasi. Pemetaan masalah membantu menghindari pembahasan yang terlalu sektoral karena satu persoalan dapat memengaruhi persoalan lain. Sebagai contoh, keterbatasan tools yang tidak berlisensi tidak hanya berkaitan dengan pengadaan, tetapi berpengaruh pada maintenance, kemampuan update, keandalan deteksi, dan pada akhirnya kecepatan respons. Demikian pula keterbatasan personel bersertifikat bukan hanya persoalan pelatihan, tetapi juga berkaitan dengan desain organisasi dan pembagian peran.

Analisis hasil pendampingan menggunakan pola deskriptif-kualitatif. Data dan pernyataan dikelompokkan, disajikan menurut tema, dibandingkan untuk melihat konsistensi, kemudian ditarik kesimpulan berupa arah penguatan. Alur ini mengacu pada logika analisis data kualitatif yang menempatkan pengumpulan data, penyajian, pengujian konsistensi, dan penarikan kesimpulan sebagai proses yang saling berulang. Creswell (2015) menekankan bahwa penelitian dan analisis kualitatif menuntut kedalaman pemaknaan terhadap data; dalam kegiatan pengabdian, prinsip tersebut diterapkan untuk memastikan bahwa rekomendasi tidak hanya merespons gejala teknis, tetapi juga akar masalah tata kelola.



Gambar 1. Alur Analisis Kualitatif untuk Evaluasi Hasil Pendampingan

Evaluasi kegiatan tidak menggunakan indikator keberhasilan kuantitatif yang tidak tersedia dalam dokumen sumber. Sebagai gantinya, evaluasi menggunakan indikator keluaran: tersusunnya peta masalah yang dapat ditelusuri ke temuan awal, adanya kesamaan definisi terhadap interoperabilitas, terbentuknya matriks kebutuhan lintas dimensi, terumuskannya prioritas yang logis, dan tersedianya agenda tindak lanjut. Pendekatan ini menjaga agar artikel pengabdian tidak mengklaim perubahan kemampuan operasional yang belum diukur. Keterbatasan tersebut sekaligus menjadi dasar untuk menyarankan evaluasi lanjutan apabila program pendampingan diterapkan kembali dengan instrumen pre-test/post-test, survei kepuasan, atau audit kesiapan organisasi yang formal.

HASIL DAN PEMBAHASAN

1. Pemetaan Permasalahan dan Kebutuhan Sasaran

Hasil pemetaan menunjukkan bahwa kebutuhan interoperabilitas siber militer bersifat multidimensional. Persoalan tidak berada pada satu unit atau satu jenis sumber daya, tetapi muncul dari hubungan antara organisasi, personel, sarana-prasarana, standardisasi, aliran informasi, dan mekanisme koordinasi. Kondisi tersebut penting disampaikan sejak awal pendampingan karena solusi yang hanya berorientasi pada pembelian teknologi berisiko tidak menyelesaikan hambatan proses. Interoperabilitas justru membutuhkan penyelarasan antara perangkat yang digunakan, kompetensi manusia yang mengoperasikan, aturan pertukaran informasi, kewenangan, serta prosedur komando-kendali.

Pada dimensi organisasi, Pushansiber Bainsrahan Kementerian Pertahanan berperan dalam penanganan pertahanan siber di lingkungan Kementerian Pertahanan, tetapi jangkauan koordinasinya belum sepenuhnya mencakup satuan siber pada Markas Besar TNI dan Angkatan. Konsekuensinya, kegiatan pemantauan, analisis, dan pelaporan berpotensi berjalan dalam jalur kelembagaan masing-masing. Dalam situasi ancaman yang membutuhkan respons lintas satuan, kondisi tersebut dapat mengurangi kecepatan pembentukan situational awareness bersama. Pendampingan karena itu mengarahkan diskusi pada kebutuhan desain tata kelola yang memungkinkan setiap organisasi mempertahankan mandatnya namun memiliki mekanisme untuk bertukar informasi dan mengoordinasikan respons.

Pada dimensi sumber daya manusia, naskah awal mengidentifikasi kesenjangan antara kebutuhan personel dan Daftar Susunan Personel, disertai keterbatasan kepemilikan sertifikasi teknis. Isu kompetensi dalam pertahanan siber bersifat sangat dinamis karena teknologi, pola serangan, dan alat analisis terus berubah. Oleh sebab itu, pendampingan tidak berhenti pada usulan penambahan personel, tetapi menempatkan kompetensi sebagai siklus: pemetaan kebutuhan jabatan, pelatihan, sertifikasi, penempatan, latihan bersama, evaluasi, dan pembaruan kompetensi. Orientasi ini sejalan dengan kebutuhan membangun kapasitas organisasi yang berkelanjutan, bukan sekadar memenuhi jumlah personel.

Pada dimensi sarana-prasarana, pemetaan menunjukkan bahwa keberadaan tools yang tidak berlisensi dapat menghambat pemutakhiran dan maintenance. Dampaknya tidak hanya administratif, tetapi dapat memengaruhi kemampuan deteksi, analisis, identifikasi, proteksi, respons, dan recovery. Standardisasi keamanan informasi seperti ISO 27001 juga disebut belum berjalan optimal pada kondisi yang dipetakan. Forum pendampingan menempatkan isu ini dalam kerangka lifecycle management:

perencanaan kebutuhan, pengadaan, lisensi, pembaruan, pemeliharaan, interoperabilitas antarsistem, keamanan supply chain, serta evaluasi kinerja peralatan.

Pada dimensi proses, mekanisme penyusunan laporan harian bergantung pada data tangkapan sensor di beberapa satuan kerja Kementerian Pertahanan, yang kemudian dianalisis melalui fungsi monitoring, malware, dan forensik. Model kerja tersebut memperlihatkan adanya kapasitas analitis, namun kebutuhan interoperabilitas muncul ketika informasi harus diteruskan dan digunakan oleh organisasi di luar jalur internal. Oleh sebab itu, proses pertukaran informasi perlu disertai definisi klasifikasi data, siapa yang berwenang mengakses, format laporan, waktu respons, mekanisme eskalasi, dan prosedur pengambilan keputusan bersama.

Tabel 2. Pemetaan Masalah Utama dan Arah Pendampingan

Dimensi	Kondisi yang Teridentifikasi	Arah Penguatan melalui Pendampingan
Organisasi dan koordinasi	Koordinasi belum sepenuhnya menjangkau satuan siber Mabes TNI dan Angkatan; hubungan lintas organisasi masih perlu diperjelas.	Menyusun prinsip tata kelola interoperabel, hubungan komando-kendali, titik koordinasi, dan prosedur lintas organisasi.
Sumber daya manusia	Kebutuhan personel belum sepenuhnya terpenuhi; sertifikasi teknis profesional masih terbatas.	Pemetaan kompetensi jabatan, pelatihan dan sertifikasi, latihan bersama, serta pengembangan kompetensi berkelanjutan.
Sarana-prasarana	Sebagian tools tidak berlisensi; update dan maintenance belum optimal; standardisasi keamanan belum sepenuhnya berjalan.	Modernisasi berbasis kebutuhan, lisensi, maintenance, standardisasi, dan uji kompatibilitas antarsistem.
Informasi dan pelaporan	Data dapat terkumpul dalam jalur internal, tetapi pertukaran lintas organisasi memerlukan prosedur dan otorisasi yang jelas.	Standar format, klasifikasi, jalur distribusi, waktu respons, mekanisme eskalasi, dan keamanan pertukaran informasi.
Operasi dan respons	Kecepatan, inisiatif, serta kolaborasi belum didukung secara merata oleh mekanisme yang interoperabel.	SOP lintas satuan, latihan koordinasi, skenario respons, dan evaluasi bersama.

2. Penguatan Kesamaan Pemahaman tentang Interoperabilitas

Tahap penyamaan persepsi menghasilkan pemahaman bahwa interoperabilitas merupakan kemampuan sistem, organisasi, dan personel untuk bekerja bersama dengan tetap mempertahankan fungsi masing-masing. Pemahaman ini penting karena diskusi tentang pertahanan siber sering kali cenderung diarahkan pada integrasi total seluruh jaringan atau penyatuan organisasi. Padahal, konsep interoperabilitas memungkinkan sistem terhubung secara terkontrol, berbasis kebutuhan, dan sesuai kewenangan. Prinsip ini membantu komunitas praktisi melihat bahwa desain masa depan tidak harus menghapus batas organisasi, tetapi harus memastikan bahwa batas tersebut tidak menghalangi pertukaran informasi dan koordinasi ketika ancaman muncul.

Forum kolaboratif juga memperlihatkan bahwa interoperabilitas memiliki beberapa lapisan. Lapisan teknis berkaitan dengan kompatibilitas perangkat, protokol, format data, dan keamanan koneksi. Lapisan prosedural berkaitan dengan SOP, alur kerja, pelaporan, eskalasi, dan waktu respons. Lapisan manusia berkaitan dengan kompetensi, bahasa teknis yang sama, dan kemampuan memahami informasi yang diterima. Lapisan organisasi berkaitan dengan kewenangan, komando-kendali, akuntabilitas, serta mekanisme kerja sama. Lapisan strategis berkaitan dengan keselarasan tujuan pertahanan dan prioritas nasional. Jika salah satu lapisan lemah, interoperabilitas keseluruhan juga berpotensi terganggu.

Dalam kerangka pertahanan negara, penyamaan pemahaman tersebut memperkuat orientasi bahwa kerja sama antarsubsistem bukan pilihan tambahan, melainkan prasyarat menghadapi ancaman yang bergerak cepat. Ancaman siber dapat melintasi jaringan, sektor, dan batas organisasi dalam waktu

singkat. Oleh karena itu, kemampuan satu unit yang sangat baik tetapi berdiri sendiri tidak cukup untuk menciptakan ketahanan sistem secara keseluruhan. Rahmawati (2017) dan Rizki (2022) sama-sama menekankan bahwa ancaman siber memerlukan pendekatan sistemik dan peningkatan kapasitas nasional; forum pendampingan menerjemahkan kebutuhan tersebut ke dalam konteks hubungan antara Kementerian Pertahanan, TNI, dan Angkatan.

3. Tata Kelola Organisasi dan Mekanisme Kolaborasi

Prioritas pertama yang dirumuskan adalah penataan tata kelola organisasi. Penataan tidak dimaknai sebagai peleburan seluruh satuan siber, tetapi pembentukan arsitektur hubungan yang jelas. Arsitektur tersebut perlu menjawab siapa yang memimpin koordinasi dalam situasi tertentu, siapa yang menyediakan data, siapa yang melakukan analisis, siapa yang berwenang mengeluarkan rekomendasi, dan bagaimana keputusan diteruskan kepada satuan pelaksana. Pertanyaan-pertanyaan tersebut merupakan inti komando-kendali dan menentukan apakah informasi dapat diubah menjadi tindakan secara cepat.

Naskah awal merekomendasikan organisasi pertahanan siber militer yang terintegrasi dan interoperabel antara Kementerian Pertahanan, Markas Besar TNI, dan Angkatan, bahkan menempatkan pembentukan Angkatan Siber sebagai salah satu arah transformasi. Dalam kegiatan pendampingan, rekomendasi tersebut diperlakukan sebagai agenda strategis yang memerlukan pembahasan lebih lanjut, bukan sebagai hasil keputusan final. Forum lebih menekankan prasyarat yang dapat dibangun terlebih dahulu: focal point lintas organisasi, protokol koordinasi, daftar kewenangan, standar pelaporan, mekanisme berbagi informasi, serta latihan koordinasi. Langkah-langkah tersebut dapat meningkatkan interoperabilitas bahkan sebelum perubahan struktur formal dilakukan.

Aspek tata kelola juga berkaitan dengan akuntabilitas. Pertahanan siber melibatkan informasi sensitif dan keputusan yang dapat berdampak pada operasi pertahanan. Karena itu, mekanisme kolaborasi harus menghindari kondisi di mana pertukaran informasi berlangsung tanpa otorisasi atau tanpa jejak keputusan. Setiap prosedur perlu mendefinisikan klasifikasi, hak akses, pencatatan, pengamanan, dan evaluasi. Dengan demikian, peningkatan kecepatan tidak boleh mengorbankan keamanan dan akuntabilitas.

4. Penguatan Sumber Daya Manusia dan Kompetensi

Prioritas kedua adalah penguatan sumber daya manusia. Sistem pertahanan siber yang memiliki teknologi modern tetap memerlukan personel yang mampu mengoperasikan, menganalisis, dan mengambil keputusan. Kesenjangan personel yang ditemukan pada naskah awal menunjukkan kebutuhan pendekatan berbasis kompetensi. Pemetaan harus dimulai dari fungsi yang dibutuhkan: monitoring, threat analysis, malware analysis, digital forensics, incident response, architecture, governance, risk management, dan koordinasi operasi. Masing-masing fungsi dapat diterjemahkan menjadi kompetensi inti, jenjang kemahiran, serta kebutuhan pelatihan.

Sertifikasi seperti OSCP dan CEH yang disebut dalam naskah sumber dapat digunakan sebagai salah satu indikator kompetensi teknis, tetapi forum pendampingan menempatkan sertifikasi sebagai bagian dari sistem pengembangan, bukan tujuan akhir. Kompetensi juga dibangun melalui pengalaman operasi, latihan bersama, pembelajaran dari insiden, dan evaluasi kinerja. Karena interoperabilitas menuntut kerja lintas satuan, latihan bersama memiliki peran khusus: personel perlu terbiasa menggunakan terminologi yang sama, memahami format informasi yang dipertukarkan, dan mengetahui mekanisme eskalasi ketika kejadian melibatkan lebih dari satu organisasi.

Pengembangan SDM juga perlu menjaga kesinambungan. Rotasi personel, perubahan jabatan, dan perkembangan teknologi dapat menyebabkan pengetahuan yang telah dibangun hilang atau cepat usang. Oleh sebab itu, dibutuhkan knowledge management berupa dokumentasi prosedur, lesson learned, repositori pengetahuan, program mentoring internal, dan pembaruan kurikulum pelatihan. Pendekatan ini menjadikan kompetensi sebagai aset organisasi, bukan hanya kemampuan individual.

5. Modernisasi, Standardisasi, dan Tata Kelola Sarana-Prasarana

Prioritas ketiga adalah modernisasi dan standardisasi peralatan. Temuan mengenai tools yang tidak berlisensi menunjukkan bahwa pengadaan harus dilihat sebagai siklus penuh. Peralatan yang digunakan untuk fungsi kritis membutuhkan dukungan pembaruan, pemeliharaan, dokumentasi, keamanan, dan

kompatibilitas. Jika salah satu komponen tersebut tidak tersedia, kemampuan teknologi dapat menurun seiring waktu meskipun alat pada awalnya dapat berfungsi. Dalam konteks keamanan siber, keterlambatan update dapat meningkatkan risiko karena ancaman dan kerentanan berkembang cepat.

Standardisasi memiliki dua tujuan. Pertama, menjaga tingkat keamanan dan keandalan minimum. Kedua, memudahkan interaksi antarsistem. Standardisasi tidak berarti seluruh satuan harus menggunakan produk yang sama, tetapi perlu ada spesifikasi antarmuka, format data, protokol, dan persyaratan keamanan yang dapat dipenuhi oleh berbagai platform. Konsep ini konsisten dengan interoperabilitas yang tidak menuntut homogenitas. Karena itu, proses modernisasi sebaiknya memasukkan requirement interoperabilitas sejak tahap perencanaan dan pengadaan, bukan baru dibahas setelah sistem terpasang.

Pendampingan juga menempatkan tata kelola aset sebagai bagian penting. Inventaris sistem, status lisensi, jadwal maintenance, versi perangkat lunak, dukungan vendor, criticality, dan hubungan antarsistem perlu diketahui secara akurat. Informasi tersebut membantu menentukan prioritas investasi dan mengurangi ketergantungan pada keputusan ad hoc. Untuk sistem pertahanan, tata kelola supply chain juga perlu diperhatikan agar modernisasi tidak menciptakan ketergantungan baru yang sulit dikendalikan.

6. Mekanisme Komando-Kendali dan Pertukaran Informasi

Interoperabilitas pada akhirnya diuji ketika terjadi insiden dan organisasi harus mengubah informasi menjadi keputusan. Oleh sebab itu, forum pendampingan memberi perhatian pada mekanisme komando-kendali. Kecepatan respons tidak hanya ditentukan oleh kemampuan sensor mendeteksi anomali, tetapi juga seberapa cepat informasi dapat diverifikasi, diklasifikasikan, diteruskan, dan ditindaklanjuti. Setiap keterlambatan pada rantai tersebut dapat memperbesar dampak insiden.

Mekanisme pertukaran informasi perlu mendefinisikan paket informasi minimum yang harus dibagikan. Informasi dapat mencakup indikator kompromi, waktu kejadian, sistem terdampak, tingkat keyakinan analisis, tindakan sementara, kebutuhan dukungan, dan rekomendasi eskalasi. Format yang konsisten akan membantu unit penerima memahami informasi tanpa interpretasi ulang yang panjang. Di sisi lain, informasi sensitif harus tetap dibatasi sesuai kewenangan. Karena itu, prinsip need-to-know dan need-to-share perlu diseimbangkan melalui aturan klasifikasi dan otorisasi.

Latihan koordinasi menjadi sarana yang relevan untuk menguji mekanisme tersebut. Kegiatan pengabdian ini tidak melakukan simulasi teknis serangan, tetapi hasil pendampingan menunjukkan perlunya latihan meja (table-top exercise) dan latihan prosedural pada tahap lanjutan untuk menguji alur komunikasi, kejelasan peran, dan waktu pengambilan keputusan. Fokus latihan dapat diarahkan pada proses, bukan pada eksploitasi teknis, sehingga tetap aman dan sesuai tujuan penguatan tata kelola.

Tabel 3. Kerangka Interoperabilitas yang Dihasilkan dari Pendampingan

Lapisan	Pertanyaan Kunci	Keluaran yang Dibutuhkan
Strategis	Apakah seluruh organisasi memahami tujuan pertahanan siber dan prioritas nasional yang sama?	Tujuan bersama, prioritas ancaman, dan prinsip koordinasi.
Organisasi	Siapa berwenang memimpin, mengoordinasikan, menganalisis, dan mengambil keputusan?	Matriks kewenangan, focal point, mekanisme komando-kendali.
Prosedural	Bagaimana informasi dilaporkan, diverifikasi, diekskalasi, dan ditindaklanjuti?	SOP lintas satuan, format laporan, target waktu respons.
Manusia	Apakah personel memiliki kompetensi, terminologi, dan pengalaman kerja bersama yang memadai?	Peta kompetensi, pelatihan, sertifikasi, latihan kolaboratif.
Teknis	Apakah sistem dapat bertukar data secara aman dan kompatibel?	Standar antarmuka, protokol, requirement keamanan, uji kompatibilitas.

7. Penyusunan Agenda Implementasi Bertahap

Hasil pendampingan menunjukkan bahwa penguatan interoperabilitas perlu dilakukan secara bertahap. Perubahan struktur organisasi formal membutuhkan proses kebijakan, sedangkan beberapa tindakan dapat dimulai melalui standardisasi prosedur dan koordinasi. Karena itu, agenda implementasi dibagi menjadi horizon jangka pendek, menengah, dan panjang. Horizon jangka pendek diarahkan pada kesamaan terminologi, focal point, pemetaan aset, pemetaan kompetensi, dan format pelaporan. Horizon menengah diarahkan pada latihan koordinasi, standardisasi sistem, peningkatan kompetensi, dan penguatan mekanisme komando-kendali. Horizon panjang berkaitan dengan penataan struktur strategis, modernisasi berkelanjutan, serta evaluasi kelembagaan.

Pendekatan bertahap membantu mengurangi risiko bahwa interoperabilitas diperlakukan sebagai proyek sekali selesai. Ancaman siber dan teknologi berubah, sehingga desain sistem harus adaptif. Setiap tahap perlu disertai indikator kinerja yang sesuai, seperti kejelasan prosedur, waktu pertukaran informasi, tingkat pemenuhan kompetensi, status standardisasi peralatan, dan hasil latihan koordinasi. Indikator tersebut dapat dikembangkan pada kegiatan lanjutan dan disesuaikan dengan tingkat kerahasiaan serta kebutuhan masing-masing organisasi.

Tabel 4. Agenda Tindak Lanjut Bertahap

Horizon	Prioritas	Contoh Keluaran
Jangka pendek	Penyamaan terminologi, focal point, pemetaan aset dan kompetensi, penataan format laporan, serta inventarisasi SOP yang ada.	Daftar focal point; peta aset; peta kompetensi; format laporan bersama; daftar kesenjangan SOP.
Jangka menengah	Penyusunan SOP lintas satuan, pelatihan dan sertifikasi, latihan prosedural, standardisasi requirement peralatan, serta mekanisme evaluasi.	SOP interoperabilitas; program latihan; target kompetensi; standard requirement; laporan evaluasi berkala.
Jangka panjang	Penataan arsitektur organisasi strategis, modernisasi berkelanjutan, penguatan komando-kendali, dan evaluasi kebijakan.	Arsitektur tata kelola; roadmap modernisasi; mekanisme C2; keputusan kebijakan dan evaluasi kelembagaan.

8. Nilai Tambah Kegiatan bagi Komunitas Profesional Pertahanan Siber

Nilai tambah utama pendampingan terletak pada perubahan cara membaca masalah. Sebelum dipetakan secara bersama, persoalan personel, peralatan, dan koordinasi dapat tampak sebagai isu terpisah. Forum kolaboratif menunjukkan bahwa masalah tersebut saling memengaruhi. Keterbatasan peralatan dapat memperlambat analisis; keterlambatan analisis memengaruhi kualitas informasi; kualitas informasi memengaruhi keputusan; dan keputusan yang terlambat dapat menurunkan efektivitas respons. Sebaliknya, prosedur yang jelas dapat meningkatkan pemanfaatan kemampuan yang sudah ada meskipun modernisasi belum selesai.

Kegiatan juga memberi kerangka bahasa bersama yang penting bagi kolaborasi. Istilah interoperabilitas, integrasi, standardisasi, kompetensi, komando-kendali, dan pertukaran informasi diposisikan sebagai bagian dari satu sistem. Kesamaan bahasa mengurangi risiko bahwa unit yang berbeda memahami tujuan secara berbeda. Dalam organisasi pertahanan yang memiliki karakter komando dan prosedur formal, kesamaan pemahaman menjadi prasyarat penting sebelum penyusunan kebijakan atau investasi.

Dari sisi ilmu pertahanan, kegiatan memperlihatkan bahwa penguatan pertahanan siber merupakan bagian dari pengelolaan sumber daya pertahanan. Teknologi tidak berdiri sendiri, tetapi harus dirancang, diorganisasi, dikelola, dilaksanakan, dan dikendalikan untuk mendukung tujuan pertahanan. Perspektif ini sesuai dengan pemikiran Tippe (2016) mengenai ilmu pertahanan sebagai landasan untuk merumuskan strategi dan mengelola sistem pertahanan. Dalam konteks ancaman digital, pengelolaan

tersebut semakin membutuhkan kolaborasi lintas fungsi dan kesiapan untuk menyesuaikan struktur dengan perubahan teknologi.

Dari perspektif lingkungan strategis, kebutuhan interoperabilitas juga dapat dipahami melalui logika self-help dan security dilemma. Negara perlu membangun kemampuan untuk melindungi kepentingannya di tengah ketidakpastian dan potensi ancaman dari aktor negara maupun non-negara. Namun pembangunan kemampuan tidak hanya berarti meningkatkan kekuatan teknis, tetapi juga memperkuat kapasitas koordinasi agar sumber daya yang tersebar dapat digunakan secara efektif. Karena itu, interoperabilitas menjadi penghubung antara kepemilikan kemampuan dan kemampuan nyata untuk mengoperasikannya sebagai sistem pertahanan.

9. Evaluasi Keluaran dan Keterbatasan Kegiatan

Evaluasi menunjukkan bahwa keluaran utama kegiatan dapat ditelusuri ke masalah yang telah diidentifikasi: peta masalah menghubungkan dimensi organisasi, SDM, teknologi, dan proses; penyamaan persepsi memperjelas konsep interoperabilitas; matriks prioritas menunjukkan urutan kebutuhan; dan agenda tindak lanjut memberi kerangka implementasi bertahap. Keluaran tersebut bersifat konseptual dan manajerial. Artikel ini tidak menyatakan bahwa pendampingan telah meningkatkan kemampuan operasional secara terukur karena tidak tersedia data pre-test/post-test, data performa jaringan, atau hasil latihan teknis dalam dokumen sumber.

Keterbatasan tersebut penting untuk dipertahankan agar artikel pengabdian tetap dapat dipertanggungjawabkan. Kegiatan lanjutan sebaiknya mengembangkan instrumen evaluasi yang lebih kuat, misalnya survei pemahaman sebelum dan sesudah pendampingan, rubrik kematangan interoperabilitas, pengukuran waktu proses pelaporan, audit pemenuhan kompetensi, serta evaluasi SOP melalui table-top exercise. Instrumen dapat dirancang tanpa membuka informasi sensitif dengan menggunakan indikator agregat atau data yang telah diklasifikasikan sesuai ketentuan.

Keterbatasan lainnya adalah bahwa rekomendasi mengenai perubahan organisasi strategis, termasuk kemungkinan pembentukan Angkatan Siber, berada pada tingkat kebijakan yang memerlukan kajian, keputusan, dan legitimasi kelembagaan tersendiri. Oleh sebab itu, hasil pendampingan lebih tepat diposisikan sebagai bahan masukan dan agenda diskusi, bukan keputusan final. Pendekatan ini menjaga peran pengabdian sebagai fasilitator pembelajaran dan kolaborasi komunitas profesional.

Tabel 5. Indikator Evaluasi untuk Program Pendampingan Lanjutan

Aspek	Indikator yang Dapat Digunakan	Catatan
Pemahaman	Perubahan skor pemahaman konsep interoperabilitas dan perbedaan dengan integrasi.	Dapat menggunakan pre-test/post-test konseptual non-sensitif.
Prosedur	Ketersediaan SOP lintas satuan, kejelasan alur eskalasi, dan konsistensi format laporan.	Dievaluasi melalui review dokumen dan table-top exercise.
SDM	Persentase pemenuhan kompetensi jabatan, sertifikasi, dan partisipasi latihan bersama.	Disesuaikan dengan kebijakan personel dan kerahasiaan.
Teknologi	Status lisensi, maintenance, standardisasi, kompatibilitas, dan kesiapan peralatan pendukung.	Dapat dinilai melalui audit internal tanpa mempublikasikan detail sensitif.
Kolaborasi	Kecepatan pertukaran informasi, ketepatan eskalasi, dan kejelasan peran saat latihan.	Gunakan indikator agregat untuk menjaga keamanan informasi.

10. Implikasi Pengembangan Program Pengabdian Berkelanjutan

Pengembangan kegiatan pengabdian berikutnya dapat diarahkan dari pendampingan konseptual menuju penguatan kapasitas yang lebih terstruktur. Tahap awal tetap diperlukan untuk memastikan kesamaan istilah dan pemetaan kebutuhan, kemudian dilanjutkan dengan penyusunan modul penguatan

interoperabilitas yang berisi tata kelola, manajemen insiden, pertukaran informasi, pengembangan kompetensi, dan pengelolaan sarana-prasarana. Modul tersebut dapat digunakan dalam workshop lintas satuan sehingga proses pembelajaran tidak bergantung pada satu forum, tetapi dapat direplikasi dan diperbarui sesuai perkembangan ancaman. Kegiatan pengabdian juga dapat mengembangkan lembar kerja pemetaan interoperabilitas yang membantu setiap unit menilai kondisi organisasinya sendiri tanpa harus mempublikasikan data sensitif.

Program berkelanjutan sebaiknya menerapkan prinsip train-the-trainer. Personel yang memiliki pengalaman dan kompetensi dapat disiapkan sebagai fasilitator internal untuk menyebarkan pemahaman interoperabilitas pada satuan masing-masing. Pendekatan ini relevan karena perubahan personel dan perkembangan teknologi menuntut proses pembelajaran yang terus berlangsung. Fasilitator internal dapat menggunakan studi kasus yang telah dianonimkan, latihan meja, serta evaluasi prosedural untuk memperkuat keterampilan koordinasi. Dengan demikian, pengabdian tidak berhenti pada penyampaian rekomendasi, tetapi membantu komunitas membangun mekanisme pembelajaran mandiri dan berbagi pengetahuan.

Selain itu, kemitraan antara perguruan tinggi pertahanan dan komunitas praktisi dapat diarahkan pada penyusunan indeks kematangan interoperabilitas yang bersifat non-operasional. Indeks dapat memuat dimensi kebijakan, organisasi, SDM, prosedur, teknologi, dan evaluasi. Penggunaan indikator agregat memungkinkan proses pendampingan dan evaluasi dilakukan tanpa membuka konfigurasi teknis atau informasi yang bersifat rahasia. Hasil penilaian dapat digunakan untuk menentukan prioritas program pelatihan, standardisasi, dan penguatan tata kelola. Kolaborasi seperti ini menempatkan perguruan tinggi sebagai mitra pengembangan kapasitas dan pengetahuan, sedangkan keputusan operasional serta kebijakan tetap menjadi kewenangan institusi pertahanan.

Dalam jangka lebih panjang, program pengabdian dapat membangun siklus pendampingan tahunan yang menggabungkan pemetaan kebutuhan, workshop, table-top exercise prosedural, evaluasi, dan penyusunan lesson learned. Siklus tersebut memungkinkan rekomendasi diperbarui berdasarkan perubahan organisasi, regulasi, dan teknologi. Dengan mekanisme yang berulang, manfaat pengabdian menjadi lebih terukur dan dapat mendukung pembentukan budaya kolaborasi. Arah ini konsisten dengan kebutuhan pertahanan siber yang bersifat dinamis: kesiapan tidak dapat dibentuk melalui satu kegiatan, tetapi melalui proses pembelajaran, evaluasi, dan penyesuaian yang berkesinambungan.

11. Rencana Replikasi dan Diseminasi

Agar manfaat pendampingan tidak berhenti pada komunitas yang terlibat dalam forum awal, hasil kegiatan dapat direplikasi melalui paket materi yang bersifat aman untuk diseminasi. Paket tersebut dapat memuat pengantar interoperabilitas, lembar pemetaan organisasi, matriks kompetensi generik, contoh alur eskalasi non-sensitif, dan panduan refleksi. Materi tidak perlu mencantumkan konfigurasi sistem, alamat jaringan, jenis perangkat spesifik, atau data insiden yang bersifat rahasia. Dengan pendekatan tersebut, prinsip-prinsip tata kelola dapat dibagikan kepada satuan lain tanpa meningkatkan risiko keamanan informasi.

Diseminasi juga dapat dilaksanakan melalui seminar internal, workshop lintas fungsi, dan forum akademik-praktisi. Perguruan tinggi dapat berperan menyiapkan metodologi evaluasi, dokumentasi lesson learned, serta kajian perbandingan konsep interoperabilitas, sedangkan institusi pertahanan menentukan batas informasi dan kebutuhan operasional. Pembagian peran ini penting agar kegiatan pengabdian tetap berada pada wilayah penguatan kapasitas dan tidak mengambil alih kewenangan teknis atau kebijakan. Setiap kegiatan replikasi perlu diakhiri dengan catatan kebutuhan lokal karena kondisi organisasi, sumber daya, dan sarana-prasarana pada setiap satuan dapat berbeda.

Keberlanjutan diseminasi dapat diperkuat dengan membentuk komunitas pembelajaran yang bertemu secara berkala untuk membahas perubahan regulasi, kebutuhan kompetensi, standardisasi, dan hasil evaluasi prosedural. Komunitas tersebut tidak harus membahas detail operasi; fokusnya dapat diarahkan pada tata kelola, terminologi, metode evaluasi, dan pengembangan kapasitas. Melalui pola ini, pengabdian kepada masyarakat berfungsi sebagai jembatan antara pengetahuan akademik dan kebutuhan praktis, sekaligus membantu menjaga agar rekomendasi interoperabilitas selalu diperbarui sesuai perubahan lingkungan strategis dan teknologi.

KESIMPULAN

Pendampingan penguatan interoperabilitas siber militer melalui forum kolaboratif memberikan kerangka yang relevan bagi komunitas profesional pertahanan siber untuk memetakan persoalan secara lebih menyeluruh. Permasalahan utama tidak hanya berkaitan dengan teknologi, tetapi juga tata kelola organisasi, sumber daya manusia, standardisasi, pertukaran informasi, serta mekanisme komando-kendali. Kesamaan pemahaman menjadi keluaran penting karena interoperabilitas tidak identik dengan integrasi penuh dan tidak menuntut homogenitas sistem. Interoperabilitas menuntut kemampuan subsistem yang berbeda untuk bertukar informasi dan bekerja bersama berdasarkan prosedur, kewenangan, sumber daya, dan standar yang disepakati. Hasil pendampingan menghasilkan lima arah penguatan: penataan tata kelola dan hubungan organisasi; penguatan komando-kendali dan prosedur pertukaran informasi; pengembangan kompetensi dan sertifikasi personel; modernisasi, lisensi, maintenance, serta standardisasi sarana-prasarana; dan pembentukan mekanisme evaluasi berkelanjutan. Agenda tersebut perlu dilakukan secara bertahap mulai dari penyamaan terminologi dan focal point, penyusunan SOP dan latihan koordinasi, hingga penataan arsitektur organisasi dan kebijakan jangka panjang. Kegiatan ini menghasilkan keluaran konseptual berupa peta masalah, matriks kebutuhan, kerangka interoperabilitas, dan agenda tindak lanjut. Karena dokumen sumber tidak menyediakan pengukuran kuantitatif dampak program, artikel tidak mengklaim peningkatan kemampuan operasional secara terukur. Program berikutnya disarankan memasukkan instrumen evaluasi sebelum-sesudah, rubrik kematangan interoperabilitas, dan latihan prosedural sehingga manfaat pendampingan dapat dinilai secara lebih sistematis tanpa mengungkap informasi sensitif pertahanan.

DAFTAR REFERENSI

- Babys, S. A. M. (2021). Ancaman perang siber di era digital dan solusi keamanan nasional Indonesia. *Oratio Directa (Prodi Ilmu Komunikasi)*, 3(1).
- Creswell, J. W. (2015). *Penelitian kualitatif dan desain riset: Memilih di antara lima pendekatan*. Pustaka Pelajar.
- Frankel, J., & Waltz, K. N. (2010). *Theory of international politics*. Waveland Press.
- Glaser, C. L., & Kaufmann, C. (1998). What is the offense-defense balance and can we measure it? *International Security*.
- Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, 30(2), 167-214. <https://doi.org/10.2307/2009958>
- Kementerian Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia*.
- Kom, J., & McDaniel, N. (2020). *Military interoperability: Definitions, models, actors, and guidelines*. Library of Congress/CGHE, Uniformed Services University.
- Krisnata, R., Reksoprodjo, A. H. S., & Waluyo, S. D. (2022). Strategi pengembangan kapabilitas siber pertahanan untuk menghadapi peperangan siber (Studi kasus pada PUSHANSIBER KEMHAN RI 2020-2021). *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 9(6), 2094-2103.
- Macri, G. (2016). NSA chief says without artificial intelligence, cyber 'is a losing strategy.' *InsideSources*.
- Mansyur, M. R., Prakoso, L. Y., & Damayanti, R. (2019). The implementation of policies to protect national vital objects in the Indonesian Navy's second fleet base Surabaya. *The 3rd Indonesia International Defense Science Seminar*, 506-512.
- Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. (2014).
- Perwej, D. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D. N., & Kumar Jaiswal, A. (2021). A systematic literature review on cyber security. *International Journal of Scientific Research and Management*, 9(12), 669-710. <https://doi.org/10.18535/ijstrm/v9i12.ec04>
- Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber (cyber crime) dalam peningkatan cyber defense. *Jurnal Pertahanan dan Bela Negara*, 7(2), 35-50.

- Rizki, M. (2022). Perkembangan sistem pertahanan/keamanan siber Indonesia dalam menghadapi tantangan perkembangan teknologi dan informasi. *Politeia: Jurnal Ilmu Politik*, 14(1), 54-62.
- Sadiku, M. N. O., Fagbohunbe, O. I., & Musa, S. M. (2020). Artificial intelligence in cyber security. *International Journal of Engineering Research and Advanced Technology*, 6(5), 1-7. <https://doi.org/10.31695/IJERAT.2020.3612>
- Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques: A review of cyber defense mechanisms. *International Journal of Advanced Research in Computer and Communication Engineering*.
- Sugiyono. (2012). *Metode penelitian kuantitatif, kualitatif dan R&D*. Alfabeta.
- Syafi'i, M. H., Supriyadi, A. A., Prihanto, Y., & Gultom, R. A. G. (2023). Kajian ilmu pertahanan dalam strategi pertahanan negara guna menghadapi ancaman teknologi digital di Indonesia. *Journal on Education*, 5(2), 4063-4076. <https://doi.org/10.31004/joe.v5i2.1100>
- Tippe, S. (2016). *Ilmu pertahanan: Sejarah, konsep, teori dan implementasi*. Salemba Humanika.
- Toft, P. (2005). John J. Mearsheimer: An offensive realist between geopolitics and power. *Journal of International Relations and Development*, 8(4), 381-408. <https://doi.org/10.1057/palgrave.jird.1800065>
- Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara. (2002).
- Vashisht, P., & Gupta, V. (2015). Big data analytics techniques: A survey. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 264-269.
- Wibisono, G., Gultom, R. A. G., & Mantoro, T. (2024). Strategi peningkatan kapabilitas Satuan Siber Dispansanau melalui pemanfaatan artificial intelligence pada keamanan siber berdasarkan National Institute of Standards and Technology Cybersecurity Framework Version 1.1. *Jurnal Review Pendidikan dan Pengajaran*, 7(1), 968-975. <https://doi.org/10.31004/jrpp.v7i1.24878>
- Yani, Y., Montratama, I., & Mahyudin, E. (2017). *Pengantar studi keamanan*. Intrans Publishing.