Jurnal Strategi Pertahanan Udara,
Volume 11, Nomor 2, 2025 E-ISSN 2830-3490

Strategi Penguatan Satuan Siber Dinas Pengamanan dan Sandi TNI Angkatan Udara Dalam Menghadapi Ancaman Siber

(*Strategy for Strengthening the Cyber Unit of the Indonesian Air Force's Security and Cipher Service in Facing Cyber Threats*)

Oni Musmaedi, Bastari R, Yemia Hendrawoto

Fakultas Strategi Pertahanan, Unhan RI
Oni.musmaedi@sp.idu.ac.id, bastari.rajatihang@idu.ac.id, yere69.mia@gmail.com

Abstract. *The rapid development of information technology has had a significant impact on the national defense system, particularly with the emergence of cyber warfare threats. The Indonesian Air Force (TNI AU), as a crucial component of the national air defense, must possess cyber resilience capabilities to address the ever-evolving cyber threats. The Cyber Unit of Dispamsanau (Satsiberau) plays a strategic role in building cyber resilience, which encompasses both prevention and recovery aspects. However, to date, there has been no comprehensive study integrating these two aspects simultaneously and cohesively within the context of TNI AU. This research aims to formulate strategies for strengthening cyber resilience in Satsiberau, focusing on the prevention and recovery of cyber threats. The research method used is a qualitative approach with in-depth interviews, observations, and document analysis. Data is obtained from competent sources in the field of cyber defense within TNI AU, including the Head of Satsiber Dispamsanau. The findings indicate that, although significant prevention efforts are underway, personnel capabilities regarding cyber certification remain limited. On the other hand, recovery after a cyberattack also requires an improvement in technical capacity and better coordination in incident response. Recommendations from this study include the need to develop technical competencies through international certifications, the formulation of clear cyber competency policies, and the enhancement of education and training quality to strengthen the cyber resilience of TNI AU.*

Keywords: *Cyber Resilience, Threat Prevention, Recovery*

Abstrak. Perkembangan teknologi informasi yang pesat telah membawa dampak besar terhadap sistem pertahanan negara, terutama dengan munculnya ancaman *cyber warfare*. TNI Angkatan Udara (TNI AU) sebagai komponen penting dalam pertahanan udara nasional harus memiliki kemampuan *cyber resilience* untuk menghadapi ancaman siber yang terus berkembang. Satuan Siber Dispamsanau (Satsiberau) memiliki peran strategis dalam membangun ketahanan siber, yang meliputi aspek pencegahan dan pemulihan. Namun, hingga saat ini, belum ada kajian komprehensif yang mengintegrasikan kedua aspek tersebut secara simultan dan terpadu dalam konteks TNI AU. Penelitian ini bertujuan untuk merumuskan

strategi penguatan *cyber resilience* di Satsiberau, dengan fokus pada pencegahan dan pemulihan terhadap ancaman siber. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan wawancara mendalam, observasi, dan analisis dokumen. Data diperoleh dari narasumber yang berkompeten dalam bidang pertahanan siber di TNI AU, termasuk Kasatsiber Dispamsanau. Hasil penelitian ini menunjukkan bahwa meskipun terdapat upaya pencegahan yang signifikan, kapabilitas personel dalam hal sertifikasi siber masih terbatas. Di sisi lain, pemulihan pasca serangan siber juga memerlukan peningkatan kapasitas teknis dan koordinasi yang lebih baik dalam respons insiden. Rekomendasi dari penelitian ini adalah perlunya pengembangan kompetensi teknis personel melalui sertifikasi internasional, penyusunan kebijakan kompetensi siber yang jelas, serta peningkatan kualitas pendidikan dan pelatihan siber untuk memperkuat ketahanan siber TNI AU.

Kata Kunci: Ketahanan Siber, Pencegahan Siber, Pemulihan Siber

1. Pendahuluan

Pesatnya perkembangan teknologi turut memengaruhi modernisasi sistem persenjataan, terutama di negara-negara maju. Perubahan ini juga berdampak pada dinamika perang modern yang mengalami transformasi signifikan, menjadikan *cyber warfare* sebagai ancaman nyata yang tidak bisa diabaikan. Perkembangan teknologi informasi yang pesat telah mendorong peningkatan kompleksitas serta intensitas ancaman siber terhadap sistem pertahanan negara, termasuk terhadap institusi TNI Angkatan Udara (TNI AU). Kemampuan *cyber resilience* menjadi kebutuhan yang mendesak bagi TNI AU agar mampu bertahan, merespons, serta memulihkan diri dari berbagai bentuk gangguan maupun serangan siber (Dasgupta, S., & Kumar 2021) *Cyber resilience* tidak hanya menggambarkan kesiapan teknologi semata, tetapi juga mencerminkan ketangguhan organisasi dan sumber daya manusia dalam menjaga kesinambungan fungsi pertahanan negara (Nissenbaum, 2020).

Organisasi siber yang ideal harus memiliki kemampuan yang tangguh untuk menghadapi ancaman siber yang semakin kompleks dan dinamis. Satuan Siber Dispamsanau (Satsiberau) sebagai unsur pelaksana teknis pertahanan siber

di lingkungan TNI AU memiliki peran strategis dalam menghadapi spektrum ancaman siber yang semakin kompleks di era digitalisasi. Strategi penguatan *cyber resilience* menjadi prioritas utama, khususnya dalam aspek pencegahan dan pemulihan terhadap potensi gangguan siber. Pencegahan mencakup langkah-langkah sistematis untuk mendeteksi, mengidentifikasi, dan mengeliminasi potensi kerentanan sebelum dimanfaatkan oleh pihak lawan (Liu, D., & Wu, 2017). Sementara itu, pemulihan menekankan pada kemampuan institusi untuk kembali beroperasi secara optimal pasca insiden, melalui mekanisme respons yang terstruktur dan berkelanjutan (Dasgupta, S., & Kumar, 2021). Namun demikian, hingga saat ini belum terdapat kajian komprehensif yang secara khusus merumuskan strategi pembangunan *cyber resilience* di lingkungan TNI AU, terutama yang mengintegrasikan aspek pencegahan dan pemulihan secara simultan dan terpadu. Hal ini menjadi celah strategis yang perlu dikaji agar Satsiberau mampu menjadi organisasi yang adaptif dan resilien dalam menghadapi ancaman siber yang terus berkembang. Oleh karena itu, penelitian ini bertujuan untuk menganalisis dan merumuskan strategi penguatan *cyber resilience* TNI AU, dengan fokus pada pendekatan pencegahan dan pemulihan secara terintegrasi.

2. Tinjauan Pustaka

a. Teori Ketahanan Siber.

Teori Ketahanan Siber atau *Cyber resilience Theory* oleh Alexander Kott dalam buku yang berjudul *Cyber resilience of Systems and Networks*, diterbitkan oleh Springer pada tahun 2018. Ketahanan siber sebagai kemampuan suatu sistem untuk mempersiapkan diri, menyerap, memulihkan, dan beradaptasi terhadap gangguan, khususnya yang disebabkan oleh serangan siber (Kott, 2018). Berbeda dengan pendekatan keamanan siber tradisional yang berfokus pada pencegahan dan perlindungan, pendekatan ketahanan siber menekankan pada kemampuan sistem untuk tetap berfungsi dan cepat

pulih setelah mengalami gangguan.

b. Teori Profesionalisme.

Teori Profesionalisme menurut Linda Evans (2008) dalam karyanya *Professionalism, Professionality and the Development of Education Professionals*, membedakan antara dua konsep penting yaitu *professionalism* (ciri-ciri atau atribut profesional) dan *professionality* (tingkat kompetensi atau praktik aktual seseorang dalam menjalankan peran profesionalnya). Profesionalisme melibatkan aspek sikap (attitudinal), perilaku (behavioral), dan intelektual (Evans Linda, 2008). Profesionalisme berarti bahwa personel harus tidak hanya memiliki kompetensi teknis (hard skill) tetapi juga sikap yang bertanggung jawab, komitmen terhadap tugas, serta integritas dalam melindungi kepentingan negara dari ancaman, termasuk dalam domain siber.

c. Teori Kapasitas.

Kapasitas menurut Jason Healey (2012) dalam buku yang berjudul, "*Cybersecurity Policy Guidebook*" menguraikan bahwa ketahanan dan efektivitas sistem keamanan siber nasional tidak hanya ditentukan oleh teknologi semata, tetapi juga sangat bergantung pada kapasitas institusional para aktor utamanya (Jason Healey 2012). Kapasitas institusional yang dimaksud mencakup kemampuan organisasi dalam mengembangkan kebijakan siber, membangun struktur komando yang efisien, meningkatkan keterampilan sumber daya manusia, serta membentuk kerja sama lintas sektor. Healey menggarisbawahi pentingnya pendekatan menyeluruh (*whole of nation approach*), di mana kapasitas harus terintegrasi dan terkoordinasi untuk menghasilkan sistem pertahanan siber yang tangguh dan adaptif terhadap dinamika ancaman global.

3. Metodologi.

Metode penelitian ini merujuk pada pendekatan sistematis yang dirancang secara cermat untuk melaksanakan studi dan mencapai tujuan yang telah ditetapkan. Penelitian ini menggunakan metode kualitatif, yang menitikberatkan pada pengumpulan data non-numerik melalui wawancara mendalam, observasi partisipatif, serta analisis dokumen atau teks. Subyek penelitian dalam mendukung proses pengumpulan data yaitu pihak yang kompeten yang mengetahui secara mendalam tentang pertahanan siber di lingkungan TNI AU yaitu Kasatsiber Dispamsanau. Adapun obyek penelitian yaitu kemampuan pencegahan dan kemampuan pemulihan yang dimiliki Satsiber Dispamsanau. Analisis data menggunakan pendekatan induktif, yaitu temuan dari wawancara dan observasi akan dianalisis dengan menyeluruh untuk dapat mengidentifikasi berbagai pola, tema, dan tantangan yang muncul dalam mewujudkan peran Dispamsanau dalam rangka mencapai *cyber resilience* TNI AU.

4. Hasil dan Diskusi

a. Peran Pencegahan Ancaman Siber

Di tengah transformasi karakter perang modern yang semakin mengedepankan dimensi siber sebagai medan pertempuran baru, peran pencegahan terhadap ancaman siber menjadi sangat krusial dalam menjaga kedaulatan dan stabilitas sistem pertahanan negara. Operasional TNI AU yang semakin bergantung pada infrastruktur digital dalam pengoperasian alutsista dan sistem komandonya, menghadapi risiko serangan siber yang berpotensi melumpuhkan fungsi strategis pertahanan udara. Satsiber Dispamsanau berperan sebagai garda terdepan dalam membangun sistem pertahanan siber yang tangguh, dengan menitikberatkan pada aspek pencegahan sebagai garis pertahanan pertama. Pencegahan yang efektif tidak hanya bergantung pada kecanggihan teknologi deteksi dini, tetapi juga pada kesiapan personel, tingkat kesadaran keamanan informasi, dan

kebijakan perlindungan infrastruktur informasi vital yang terstruktur. Oleh karena itu, membangun sistem pencegahan siber yang adaptif, responsif, dan berkelanjutan merupakan fondasi utama dalam mewujudkan *cyber resilience* bagi TNI AU dalam menghadapi eskalasi ancaman siber yang semakin kompleks dan tidak terduga.

Berdasarkan data yang diperoleh penulis dari staf Satsiber Dispamsanau, personel yang mengawaki jabatan pada struktur organisasi Satsiber Dispamsanau sesuai dengan DSP (saat ini personel Satsiber sebanyak 47 orang (47.47 %) dari 101 orang (100 %). Personel yang telah memiliki sertifikasi internasional dibidang teknis pencegahan dan pemulihan siber sangat terbatas. Jumlah personel Satsiber Dispamsanau yang telah memiliki sertifikat baru sebanyak 19 personel dimana satu personel bisa memiliki lebih dari satu atau lebih sertifikasi. Adapun macam sertifikasi tersebut ditunjukkan oleh tabel dibawah.

Tabel Sertifikasi Siber Personel Dispamsanau

NO	SERTIFIKASI SIBER PERSONEL DISPAMSANAU	JUMLAH
1	***CEH (Certified Ethical Hacker)*** Kemampuan menguji sistem keamanan komputer dengan cara yang legal dan etis	7
2	***CND (Certified Network Defender)*** Kemampuan di bidang keamanan jaringan	3
3	***CPENT (Certified Penetration Testing Professional)*** Kemampuan melakukan uji penetrasi (*penetration testing*) secara menyeluruh terhadap sistem dan jaringan.	2
4	***CHFI (Computer Hacking Forensic Investigator)*** Kemampuan mengidentifikasi, mengumpulkan, menganalisis, dan memelihara bukti digital yang berkaitan dengan tindak kejahatan dunia maya atau insiden keamanan TI.	1

5	***JPT (Junior Penetration Tester)*** *Entry-level* dalam bidang keamanan siber *ofensif* (*offensive security*) yang bertugas membantu dalam mengidentifikasi, mengevaluasi, dan melaporkan kerentanan keamanan pada sistem, aplikasi, atau jaringan	12
6	***CSA (Certified SOC Analyst)*** Pengetahuan dan keterampilan dasar yang dibutuhkan untuk bekerja sebagai analisis keamanan di Security Operations Center (SOC).	1
7	***L1 SOC (Level 1 Security Operations Center Analyst)*** Kemampuan mendeteksi, memantau, dan merespons ancaman siber secara *real-time*.	8
8	***AAKI (Assintant Auditor Keamanan Informasi)*** *Entry-level* dalam bidang audit keamanan informasi, yang bertugas membantu auditor senior dalam melakukan penilaian sistem keamanan TI.	3
9	***CTIA (Certified Threat Intelligence Analyst)*** Kemampuan mengumpulkan, menganalisis, dan menghasilkan intelijen ancaman siber (*cyber threat intelligence*) yang dapat ditindaklanjuti oleh tim keamanan.	1

Sumber : DSP Satsiber Dispamsanau (April 2025)

Kemampuan pencegahan siber merupakan aspek vital dalam membangun *cyber resilience* yang di lingkungan TNI AU, mengingat tingginya risiko ancaman siberyang sangat kompleks saat ini. Berdasarkan kerangka *Cyber resilience Theory*, tahapan "*prepare*" dan "*absorb*" sangat bergantung pada kesiapan personel dalam mengenali, mencegah, dan menanggulangi potensi ancaman siber sebelum menjadi insiden nyata (Schneier, 2019). Tahapan *prepare* (persiapan) dan *absorb* (mitigasi dampak) menjadi fondasi utama yang harus diperkuat. Kemampuan personel dalam tahap pencegahan ini juga mendukung efektivitas organisasi dalam menyerap dampak awal serangan siber (*absorb phase*), yaitu dengan memastikan bahwa infrastruktur digital tidak langsung *down* atau lumpuh ketika terjadi gangguan. Tahapan ini sangat bergantung pada tingkat kesiapan personel dalam mengenali pola-pola serangan siber, menganalisis potensi celah keamanan, serta mengimplementasikan langkah- langkah preventif sebelum sebuah serangan berkembang menjadi insiden yang lebih besar. Hal ini berfungsi sebagai lapisan pertahanan awal yang memungkinkan organisasi siber mampu mengidentifikasi potensi risiko, memperkuat sistem, dan menyerap dampak awal sebelum eskalasi serangan terjadi. Namun, dengan kesiapan sebanyak 12 orang yang memiliki sertifikasi CEH, CND, dan CPENT maka dapat dikatakan bahwa kapabilitas pada tahap ini menjadi terbatas secara fungsional maupun struktural jika dibandingkan dengan potensi serangan siber yang semakin kompleks. Hal ini mengindikasikan adanya gap atau kesenjangan antara tuntutan operasional dan kapasitas teknis yang dimiliki personel saat ini.

Kesenjangan ini menjadi akar permasalahan atas belum optimalnya peran pencegahan siber, khususnya pemenuhan kebutuhan organisasi terhadap tenaga profesional bersertifikasi di bidang pertahanan siber. Sampai saat ini, belum

terdapat kebijakan struktural yang secara tegas mengatur kewajiban maupun fasilitasi bagi pengembangan kompetensi teknis personel melalui jalur sertikasi internasional. Artinya, meskipun kebutuhan akan tenaga profesional yang memiliki kompetensi teknis berskala global semakin mendesak, belum ada regulasi atau pedoman institusional yang mengatur secara terstruktur tentang pentingnya mengikuti pelatihan atau sertifikasi teknis yang diakui secara internasional. Hal ini berimplikasi terhadap pengembangan sumber daya manusia masih berjalan secara sporadis, dan bergantung pada inisiatif individu atau satuan, tanpa adanya standar baku yang dapat menjamin kesetaraan kualitas dan pengakuan kompetensi di tingkat global. Hal ini selaras dengan laporan dari *World Economic Forum* (2022), salah satu hambatan utama dalam peningkatan kapasitas keamanan siber nasional adalah tidak adanya kebijakan nasional yang mendukung pelatihan dan sertifikasi siber secara sistemik (Jeremy Jurgens, 2022). Tanpa kebijakan tersebut, pembangunan SDM siber akan bersifat reaktif dan terfragmentasi, yang menyebabkan organisasi tidak memiliki standar kompetensi minimum yang terukur. Tanpa regulasi yang mendorong pembelajaran berkelanjutan dan sertifikasi, organisasi siber akan mengalami hambatan dalam membentuk postur keamanan siber yang resilien dan adaptif terhadap perubahan ancaman.

Selain keterbatasan jumlah dan kapasitas personel bersertifikasi, akar permasalahan lain yang turut melemahkan kemampuan pencegahan siber dalam membangun *cyber resilience* di lingkungan TNI AU adalah belum adanya sistem deteksi dini yang terintegrasi secara menyeluruh dalam arsitektur keamanan informasi militer. Sistem deteksi dini yang ideal seharusnya mampu mengumpulkan, menganalisis, dan menyajikan informasi mengenai ancaman siber secara *real-time*, sehingga dapat memberikan peringatan awal dan memfasilitasi respons cepat sebelum serangan berkembang. Prinsip ini sejalan dengan kerangka *Cyber Threat Intelligence (CTI)* yang dijelaskan dalam *MITRE ATT&CK Framework*, di mana deteksi proaktif terhadap taktik, teknik, dan

prosedur (TTPs) lawan menjadi kunci dalam mencegah eskalasi serangan (MITRE Corporation, 2021). Hal ini juga didukung oleh panduan *NIST SP 800-61 Revision 2*, yang menegaskan bahwa sistem deteksi efektif harus terintegrasi dengan pemantauan log, analisis lalu lintas jaringan, serta respons insiden yang cepat dan tepat (NIST, 2012). Namun, saat ini deteksi keamanan siber yang tergelar di Satsiber Dispamsanau masih bersifat parsial dan *stand alone*, belum terhubung secara interoperabel dengan system lain. Para pemangku kewenangan belum sepenuhnya menyadari urgensi pembangunan sistem deteksi dini yang terintegrasi, karena hingga kini sistem deteksi keamanan siber yang tergelar di Satsiber Dispamsanau masih bersifat parsial serta belum terhubung secara interoperabel dengan sistem yang dimiliki Satsiber TNI maupun BSSN. Kondisi tersebut menyebabkan keterbatasan dalam pertukaran data ancaman secara *real time*, sehingga memperlambat proses identifikasi pola serangan dan pengambilan keputusan respons yang tepat. Akibatnya, potensi serangan siber yang sebenarnya dapat dicegah sejak dini justru berkembang menjadi insiden yang berdampak luas terhadap keamanan siber di lingkungan TNI AU.

Belum memadainya sistem monitoring yang adaptif dan bersifat prediktif ini juga diperburuk oleh rendahnya perhatian dan kesadaran dari pejabat pemangku kewenangan terhadap urgensi investasi dalam teknologi intelijen siber berbasis *threat intelligence platform*. Teknologi ini memiliki peran penting dalam memetakan *tren* serangan global dan lokal. Tanpa data intelijen yang akurat dan kontekstual, satuan siber di lingkungan TNI AU kesulitan menyusun skenario mitigasi berbasis bukti (*evidence based mitigation*). Selain itu, rendahnya integrasi antara sistem keamanan digital dengan sistem pendukung keputusan pada level komando juga menyebabkan kurangnya kesadaran situasional (*cyber situational awareness*) yang menjadi kunci dalam pengambilan langkah preventif. Oleh karena itu, pembangunan sistem deteksi dini yang bersifat terpusat, adaptif, dan interoperabel dengan entitas pertahanan siber nasional serta

dukungan *threat intelligence platform* mutlak diperlukan untuk mewujudkan postur *cyber resilience* yang solid dan responsif di lingkungan TNI AU.

Langkah strategis untuk mewujudkan *cyber resilience* dalam tugas pencegahan siber harus diarahkan pada pembangunan kapabilitas sumber daya manusia melalui tiga pilar utama dengan mengedepankan prinsip profesionalisme, diantaranya:

1) Penyusunan *Roadmap* Kompetensi Teknis Personel Siber. Penyusunan *roadmap* kompetensi teknis siber merupakan langkah strategis dalam membangun kapabilitas personel yang responsif terhadap kebutuhan operasional Dispamsanau, khususnya peran pencegahan atau pertahanan siber. Strategi ini dirancang melalui pendekatan bertahap, terukur, dan berbasis analisis kebutuhan organisasi. Adapun segmentasi dalam kompetensi teknis personel siber dikelompokkan ke dalam level kompetensi berdasarkan fungsinya:

a) Level Dasar. Level ini dikelompokkan bagi personel pemula yang memerlukan pelatihan fundamental seperti keamanan jaringan dan *cyber hygiene*.

b) Level Menengah. Level ini diperuntukkan bagi personel operasional yang ditargetkan mengikuti sertifikasi dengan peran pertahanan siber, diantaranya CEH, CND, dan CSA.

c) Level Advance. Level ini diperuntukkan bagi personel *cyber analyst* dengan sertifikasi tingkat tinggi seperti CPENT, CHFI, CTIA, atau SANS GIAC.

2) Penyusunan Kebijakan Kompetensi Personel Siber TNI AU. Penyusunan kebijakan kompetensi bagi personel siber dilaksanakan untuk menetapkan standar kompetensi teknis yang harus dimiliki personel siber (Jerman, R. S., & Setiawan 2020). Regulasi ini penting untuk

membentuk kerangka kerja profesionalisme siber yang konsisten di seluruh satuan. Kebijakan yang disusun ini menetapkan beberapa kriteria, diantaranya:jenis sertifikasi yang diwajibkan untuk setiap jenjang jabatan atau penugasan dalam satuan siber ketentuan jenjang karier berbasis kompetensi dan sertifikasi.

3) Peningkatan Kualitas Pendidikan dan Latihan Siber. Langkah peningkatan kualitas pada pendidikan dan latihan (diklat) siber menjadi instrumen penting dalam membangun kapabilitas personel siber TNI AU, khususnya di lingkungan Satsiber Dispamsanau. Pendidikan dan latihan tidak hanya berfungsi sebagai sarana transfer pengetahuan teknis, tetapi juga sebagai mekanisme pembentukan pola pikir strategis, responsif, dan adaptif terhadap dinamika perang siber. Mekanisme diklat harus bersifat bertahap dan terstruktur, yaitu:

a) Diklat Dasar. Metode pendidikan melalui pengenalan keamanan informasi, konsep dasar jaringan, dan kesadaran keamanan siber.

b) Diklat Lanjutan. Metode yang dilakukan adalah simulasi penanganan insiden, forensic investigation, penetration testing, dan SOC operations.

c) Diklat Spesialisasi. Metode yang dilakukan adalah *threat hunting*, *malware analysis*, *red teaming* dan *blue teaming*, serta operasional *cyber defense system* TNI AU.

4) Pembangunan sistem deteksi dini yang terpusat, adaptif, dan terintegrasi secara interoperabel dengan Satsiber TNI dan BSSN. Sistem ini harus mampu mengumpulkan, menganalisis, dan menyajikan informasi ancaman secara *real time*, sebagaimana prinsip dalam *MITRE ATT&CK Framework* dan panduan *NIST SP 800-61 Rev.2*, yang menekankan pentingnya integrasi antara *log monitoring*, analisis lalu lintas jaringan, serta mekanisme respons insiden yang cepat dan akurat.

b. **Peran Pemulihan Pasca Serangan Siber**

Kegiatan pemulihan pasca serangan merupakan proses penting yang bertujuan untuk mengembalikan fungsi sistem informasi ke kondisi normal setelah mengalami gangguan akibat serangan (Dasgupta, S., & Kumar, 2021). Peran pemulihan pasca serangan siber (*recovery*) merupakan elemen esensial dalam membangun ketahanan siber TNI Angkatan Udara yang berkelanjutan. Dalam *Cyber resilience Theory*, kemampuan untuk memulihkan fungsi kritikal setelah insiden siber merupakan indikator utama tingkat resiliensi organisasi. Hal ini membutuhkan sumber daya manusia yang tidak hanya memiliki kapasitas teknis dalam pemulihan system (Nissenbaum, 2020), tetapi juga mampu menjalankan *incident response*, *forensik digital*, dan *threat* prosedur teknis pemulihan merupakan bagian dari *incident response plan* yang harus dirancang secara terstandar *intelligence* dan terkoordinasi.

Indikator terhadap kemampuan pemulihan pasca serangan siber dapat dilihat dari waktu pemulihan yang dibutuhkan, efektivitas respons, serta kemampuan restorasi sistem secara cepat. Bagi TNI AU yang mengandalkan infrastruktur digital dalam tugas operasional pertahanan udara, keterlambatan dalam proses pemulihan dapat berimplikasi langsung pada operasional satuan bahkan gangguan komando, komunikasi, kontrol, dan intelijen, serta potensi eksposur terhadap kerentanan yang lebih luas pada sistem. Kajian empiris maupun kebijakan internal yang secara khusus mengatur tentang strategi pemulihan pascainsiden siber di lingkungan TNI AU masih sangat terbatas. Penulis mencermati bahwa hingga saat ini belum terdapat prosedur baku yang mendetail mengenai manajemen insiden, pemulihan data, hingga pemulihan layanan (*service continuity*) pada sistem pertahanan udara berbasis digital. Akibatnya, tindakan pemulihan yang dilakukan cenderung reaktif dan tidak sistematis, bergantung pada improvisasi teknis dan pengalaman lapangan yang tidak seragam antar satuan.

Tahap *recovery* merupakan fase untuk menguji kemampuan organisasi siber yang tidak hanya memulihkan kondisi semula, tetapi juga untuk melakukan *adaptasi* dan *transformasi* ke kondisi yang lebih kuat dari sebelumnya. Hal ini sejalan dengan konsep *resilience engineering* dalam pertahanan siber, yang menekankan kemampuan sistem untuk tidak hanya bertahan, tetapi juga pulih dan beradaptasi setelah gangguan terjadi (Kott, 2018). Namun, dalam realitas operasional, fungsi pemulihan siber di lingkungan Satsiber Dispamsanau masih belum dilengkapi dengan infrastruktur penunjang seperti sistem *backup dan restore real-time*, maupun skenario *disaster recovery plan* (DRP) yang teruji secara periodik. Selain itu Satsiber Dispamsanau masih menghadapi sejumlah tantangan nyata. Salah satu tantangan utama adalah keterbatasan sumber daya manusia yang memiliki kompetensi khusus dalam bidang pemulihan pasca serangan siber. Permasalahan kecakapan dibidang forensik digital, *disaster recovery*, serta manajemen insiden siber hanya berjumlah 2 personel karena personel dengan sertifikasi teknis seperti CHFI (*Computer Hacking Forensic Investigator*) dan CTIA (*Certified Threat Intelligence Analyst*) menunjukkan bahwa kemampuan analisis pasca insiden dan perencanaan pemulihan belum optimal.

Hal ini menjadi tantangan besar, karena dampak dan implikasinya dapat mengganggu kesinambungan operasional sistem pertahanan udara yang sangat bergantung pada integritas, ketersediaan, dan kerahasiaan informasi digital. Ketidaksiapan dalam pemulihan yang cepat dan terstruktur dapat menyebabkan meluasnya efek domino, mulai dari kebocoran data strategis, keterlambatan dalam pengambilan keputusan taktis, hingga penurunan efektivitas komando dalam situasi krisis. Lebih jauh, keterbatasan personel bersertifikasi di bidang pemulihan siber juga menimbulkan implikasi strategis terhadap ketergantungan pada pihak eksternal dalam penanganan insiden, yang secara tidak langsung membuka celah bagi risiko keamanan baru. Dalam jangka panjang, jika tidak segera ditangani melalui penguatan kapasitas SDM, pengembangan prosedur baku, serta investasi pada sistem pemulihan digital yang andal, maka

kemampuan Satsiber Dispamsanau untuk menjaga kedaulatan ruang siber nasional akan terus berada dalam posisi rentan. Oleh karena itu, diperlukan langkah sistematis untuk membangun ekosistem pemulihan siber yang resilien, adaptif, dan mampu mengantisipasi dinamika ancaman ke depan.

Pentingnya peran pemulihan dengan kesiapan sumber daya manusia yang tersedia jika dianalisis dalam perspektif teori profesionalisme menunjukkan lemahnya proses profesionalisasi dalam ketahanan siber. ketimpangan antara tugas dan kompetensi menunjukkan bahwa aspek pengembangan profesional SDM belum dioptimalkan, khususnya dalam dimensi *responsibility and accountability*. Profesionalisme dalam konteks pemulihan bukan hanya soal kemampuan teknis, tetapi juga menyangkut kesiapan mental, kemampuan pengambilan keputusan, dan integritas personel dalam menangani insiden dengan tingkat kerahasiaan dan tekanan tinggi. Ketidaksiapan dalam aspek pemulihan ini akan berdampak luas, karena tanpa keahlian yang memadai, proses pemulihan berpotensi lambat, tidak efisien, atau bahkan keliru, sehingga memperpanjang waktu henti sistem (*downtime*), menyebabkan kehilangan data strategis, serta membuka celah serangan lanjutan. Belum memadainya kemampuan dalam *post-incident analysis* akan menghambat proses pembelajaran dan pencegahan serangan berulang di masa mendatang. Pemulihan menjadi tahap kritis dalam siklus respons terhadap serangan siber karena menyangkut keberlangsungan fungsi komando, kendali, dan komunikasi dalam ruang siber militer. Peran pemulihan mencakup tiga dimensi utama, yaitu prosedur teknis pemulihan, penguatan SDM dan organisasi, serta pengembangan sistem manajemen insiden terintegrasi.Oleh karena itu dibutuhkan strategi penguatan *cyber resilience* pada Satsiber Dispamsanau yang menuntut kesiapan dalam aspek pemulihan (*recovery*) guna menjamin kelangsungan operasional sistem informasi pertahanan pasca insiden siber.

Prosedur teknis pemulihan merupakan bagian dari *incident response plan* yang harus dirancang secara terstandar (NIST 2020) termasuk di seluruh satuan

TNI AU yang berada di bawah koordinasi Dispamsanau. Namun, penelitian ini menemukan bahwa Satsiber Dispamsanau belum memiliki Standar Operasional Prosedur (SOP) pemulihan pasca insiden yang terdokumentasi secara sistematis dan diuji secara berkala. Tanpa SOP yang jelas, respons terhadap insiden siber akan cenderung bersifat reaktif dan tidak terkoordinasi. Hal ini dapat menyebabkan waktu pemulihan yang lebih lama dan tidak efisien, karena setiap satuan atau personel mungkin memiliki pendekatan berbeda dalam menangani insiden, yang pada gilirannya dapat memperburuk situasi. Tanpa SOP yang terstandarisasi, akan berpeluang memperbesar risiko kebocoran data sensitif atau kerusakan pada data strategis. Pemulihan yang lambat atau tidak terkoordinasi dapat membuka celah bagi serangan lanjutan atau eksposur terhadap kerentanan sistem yang lebih luas.

Aspek SDM dan organisasi menjadi aspek vital yang harus terpenuhi, keberhasilan pemulihan pasca-serangan sangat bergantung pada kesiapan personel yang memiliki kompetensi teknis, kemampuan analisis situasional, serta keterampilan dalam pengambilan keputusan cepat berbasis protokol keamanan siber. Namun, data penelitian ini menunjukkan bahwa pelatihan teknis pemulihan insiden siber masih belum menjadi bagian integral dari kurikulum pelatihan di Skadik Siber maupun program pengembangan profesi di lingkungan Dispamsanau. Akibatnya, ketika serangan terjadi, proses penanggulangan dan pemulihan kerap bersifat reaktif, tidak terkoordinasi, dan rawan menimbulkan eskalasi gangguan yang lebih luas. Selanjutnya dari sisi sistemik, dibutuhkan peningkatan kualitas koordinasi dalam organisasi *Indonesian Air Force Computer Security Incident Response Team* (IDAF-CSIRT) yang telah terbentuk saat ini yang mampu mengkoordinasikan seluruh elemen terkait dalam pemulihan operasional, baik pada tataran taktis maupun strategis. Sistem ini harus didukung oleh *Command Cyber Recovery Center* (CCRC) yang berfungsi sebagai pusat kendali teknis dan strategis dalam menavigasi proses pemulihan. Saat ini, belum terdapat satuan kerja khusus yang menjalankan fungsi ini secara

menyeluruh di lingkungan TNI AU, sehingga koordinasi lintas satuan dalam fase pemulihan belum optimal. Oleh karena itu, pemulihan bukan sekadar tahapan teknis pasca-insiden, tetapi merupakan pilar fundamental dalam menjamin kontinuitas pertahanan digital. Penguatan aspek pemulihan harus dilakukan secara simultan dengan pencegahan melalui peningkatan kapasitas SDM, penguatan infrastruktur pemulihan, serta pembentukan kerangka manajemen insiden yang terintegrasi.

Langkah strategis untuk mewujudkan *cyber resilience* dalam tugas pemulihan pasca insiden siber harus diarahkan pada pembangunan kapabilitas sumber daya manusia melalui tiga pilar utama, diantaranya:

1) Penyusunan dan Pengujian SOP Pemulihan Pasca Insiden. Hal ini mutlak terpenuhi sebagai langkah kritis dalam membangun kesiapsiagaan dan ketahanan siber suatu organisasi setelah terjadi serangan atau gangguan siber. Prosedur ini dirancang untuk memastikan bahwa organisasi dapat dengan cepat dan efisien memulihkan sistem dan infrastruktur yang terpengaruh, meminimalkan kerusakan, serta menghindari terjadinya insiden lebih lanjut. Penyusunan dan pengujian SOP Pemulihan Pasca Insiden adalah proses yang tidak hanya memerlukan perhatian terhadap teknis dan detail, tetapi juga membutuhkan koordinasi yang baik antar tim dan pelatihan yang berkelanjutan untuk memastikan kesiapan organisasi menghadapi ancaman siber. Dengan prosedur yang terstandarisasi, sistem pemulihan dapat dilaksanakan secara cepat dan efektif, yang pada akhirnya akan mendukung kelangsungan operasional dan meminimalkan dampak dari insiden siber yang terjadi.

2) Peningkatan Kompetensi SDM Siber. Peningkatan kompetensi sumber daya manusia (SDM) di bidang siber merupakan salah satu aspek yang krusial dalam membangun ketahanan siber yang efektif dan berkelanjutan. Keberhasilan organisasi dalam menghadapi dan mengatasi

ancaman siber sangat bergantung pada kualitas dan keahlian personel yang terlibat dalam manajemen dan pemulihan pasca-insiden. Oleh karena itu, peningkatan kompetensi SDM siber tidak hanya berfokus pada keterampilan teknis, tetapi juga pada kemampuan analisis situasional, pengambilan keputusan yang cepat, serta kemampuan untuk beradaptasi dengan dinamika ancaman yang terus berkembang. Peningkatan kompetensi SDM siber sangat penting dalam memastikan bahwa organisasi dapat menghadapi ancaman dan serangan siber secara efektif. Melalui program pelatihan yang terstruktur, peningkatan profesionalisme, serta penguatan aspek koordinasi dan pengambilan keputusan, organisasi akan memiliki tim yang lebih siap dalam menangani insiden siber dan pemulihan pasca-insiden.

3) Penguatan Infrastruktur dan Sistem Pemulihan Digital. Penguatan infrastruktur dan sistem pemulihan digital adalah langkah strategis yang sangat penting untuk memastikan kelangsungan operasional organisasi dalam menghadapi ancaman siber yang semakin kompleks dan canggih. Organisasi siber seperti satsiber Dispamsanau harus memiliki infrastruktur yang kuat dan sistem pemulihan yang efektif untuk memitigasi dampak insiden siber dan menjaga agar data serta layanan digital tetap dapat diakses meskipun terjadi serangan atau gangguan. Penguatan infrastruktur dan sistem pemulihan digital adalah fondasi yang sangat penting bagi organisasi untuk menjaga kelangsungan operasional, melindungi data sensitif, dan meminimalkan dampak yang timbul akibat insiden siber. Dengan menerapkan sistem cadangan yang handal, menyusun rencana pemulihan bencana yang matang, serta menguji dan memperkuat ketahanan sistem secara berkala, organisasi akan lebih siap dalam menghadapi serangan atau kegagalan sistem yang tak terduga.

5. Kesimpulan

Penelitian ini mengidentifikasi dan menganalisis berbagai tantangan yang dihadapi oleh Satsiber Dispamsanau dalam membangun kapasitas *cyber resilience* yang optimal, serta menyarankan langkah-langkah strategis yang dapat ditempuh guna memperkuat ketahanan siber TNI AU. Hasil penelitian menunjukkan bahwa meskipun Satsiber Dispamsanau telah memiliki fondasi yang baik dalam aspek *pencegahan* ancaman siber, terdapat beberapa kendala signifikan yang mempengaruhi efektivitasnya, baik dari sisi keterbatasan personel bersertifikasi, minimnya kebijakan yang terarah dalam pengembangan SDM, hingga perlunya peningkatan pemahaman tentang teknologi terbaru dalam mitigasi ancaman siber. Peningkatan kemampuan dalam aspek *pencegahan* sangat penting, mengingat ancaman siber yang semakin kompleks dan terdiversifikasi. Oleh karena itu, penguatan melalui program sertifikasi dan pendidikan lanjutan bagi personel, serta implementasi kebijakan yang mengarah pada pengembangan kompetensi berbasis sistem pelatihan yang terpadu, menjadi prioritas utama. Selain itu, pendekatan berbasis teknologi simulasi dan integrasi dalam jaringan *cyber defense* TNI AU yang lebih luas juga harus didorong untuk meningkatkan kesiapan menghadapi ancaman siber secara lebih efektif dan terukur.

Peran pemulihan (*recovery*) juga merupakan komponen kritis yang harus mendapatkan perhatian sebanding. Pemulihan pasca serangan siber merupakan komponen krusial dalam membangun ketahanan siber TNI Angkatan Udara yang berkelanjutan. Tahapan recovery tidak hanya berfungsi untuk mengembalikan sistem ke kondisi semula, tetapi juga menguji kapasitas adaptif dan transformasional organisasi dalam menghadapi gangguan. Sistem pemulihan yang efektif memungkinkan TNI AU untuk kembali beroperasi dengan cepat dan tanpa gangguan berarti setelah insiden siber. Satsiber Dispamsanau perlu memperkuat kebijakan pemulihan dengan mengembangkan sistem respons insiden yang komprehensif dan berkelanjutan, termasuk rencana pemulihan data, redundansi sistem, serta cadangan sistem komando yang dapat dipulihkan secara cepat. Strategi penguatan pemulihan siber harus diarahkan pada tiga pilar utama yaitu melalui penyusunan prosedur teknis

pemulihan yang terstandar dan teruji, peningkatan kapasitas dan profesionalisme SDM melalui pelatihan berkelanjutan, serta pengembangan sistem manajemen CSIRT TNI AU.

Daftar Pustaka

1. Buku

Dasgupta, S., & Kumar, A. 2021. *Cybersecurity and Cyber Resilience: A Comprehensive Approach to Organizational Security.* Edited by Wiley-Blackwell.

Dasgupta, S., & Kumar, P. (2021). *Cyber resilience: Fundamentals, applications, and strategies*. Springer.

Jason Healey. 2012. *Cyber Security Policy Guidebook*. Edited by Weley. 1'st.

Jerman, R. S., & Setiawan, S. 2020. Strategi Pertahanan Siber Di Indonesia. Edited by Jakarta: Penerbit Keamanan.

Kott, Alexander S. 2018. *Cyber Resilience of Systems and Networks*. https://dl.acm.org/doi/book/10.5555/3243348?utm.

Liu, D., & Wu, J. 2017. *Cybersecurity and Defense: Protection, Detection, and Recovery. Springer.*

Schneier, B. 2019. *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World.* Edited by Norton & Company.

2. Jurnal

Evans Linda. 2008. "*Professionalism, Professionality and the Development of Education Professionals*." *British Journal of Educational Studies*, 20-38.

Liu, D., & Wu, M. (2017). *Enhancing cyber security through preventive strategies: A resilience-based approach*. *Journal of Information Security and Applications, 37*, 1–9. https://doi.org/10.1016/j.jisa.2017.10.001

Nissenbaum, H. (2020). *Resilience in cyber security: From risk to readiness*. In E. Popescu et al. (Eds.), *Cybersecurity and resilience in the digital age* (pp. 25–40). Springer.

Nissenbaum, Gill &. 2020. *The Role of Human Factors in Cybersecurity*.

3. Media Online

Jeremy Jurgens. 2022. "*Global Cybersecurity Outlook 2022*." https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

Jurgens, J. (2022). *Global Cybersecurity Outlook 2022*. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

5. Sumber Dokumen

MITRE Corporation. (2021). *MITRE ATT&CK® framework*. https://attack.mitre.org/

NIST. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2). National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. 2020. *Cybersecurity Framework.*