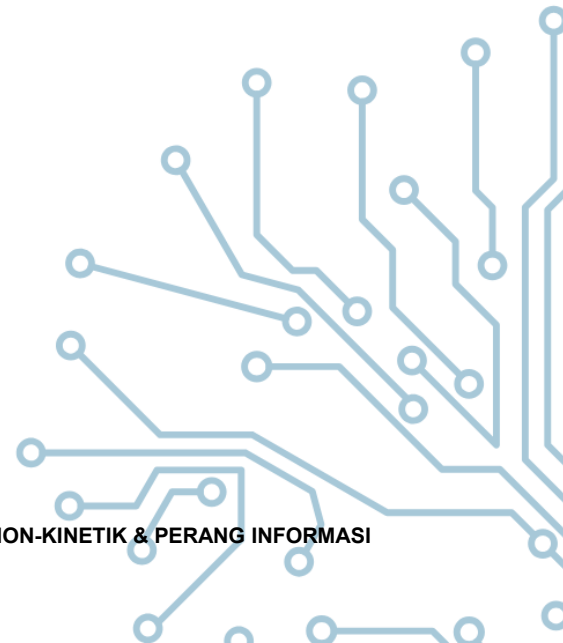
BUKU SAKU

MENGHADAPI ANCAMAN NON-KINETIK & PEPERANGAN INFORMASI

TNI ANGKATAN UDARA



KATA PENGANTAR

Perkembangan lingkungan strategis global menunjukkan bahwa spektrum ancaman terhadap kedaulatan negara tidak lagi didominasi oleh kekuatan bersenjata konvensional. Perang modern kini juga berlangsung di ruang siber dan ruang informasi, senyap, masif, dan mampu memengaruhi opini, moral, serta stabilitas nasional tanpa satu pun tembakan dilepaskan. Dalam konteks tersebut, konsep perang non-kinetik dan perang informasi menjadi tantangan nyata yang harus dipahami dan diantisipasi oleh setiap prajurit Tentara Nasional Indonesia Angkatan Udara (TNI AU).

Perang non-kinetik merujuk pada bentuk ancaman yang tidak menggunakan kekuatan fisik secara langsung, melainkan memanfaatkan teknologi, informasi, disinformasi, propaganda, serangan siber, hingga manipulasi persepsi untuk melemahkan pertahanan dan persatuan bangsa. Sementara itu, perang informasi berfokus pada penguasaan narasi, pengendalian opini publik, serta eksploitasi ruang digital guna memengaruhi cara berpikir dan bertindak suatu institusi maupun masyarakat.

Menyadari kompleksitas ancaman tersebut, Pimpinan Tertinggi TNI Angkatan Udara melalui Perintah Harian Kepala Staf Angkatan Udara menegaskan pentingnya *"Cybersecurity Awareness* dan Ketahanan Informasi: Tingkatkan *cybersecurity awareness* dan ketahanan informasi agar seluruh personel TNI Angkatan Udara mampu bersikap cerdas, waspada, serta bijak dalam menghadapi ancaman non-kinetik." Penekanan ini bukan sekadar imbauan, melainkan arahan strategis untuk memperkuat daya tangkal institusi di era digital.

Buku saku ini disusun sebagai panduan praktis dan ringkas bagi seluruh personel TNI AU dalam memahami serta menghadapi ancaman non-kinetik dan perang informasi. Materi yang disajikan mencakup tiga pilar utama, yaitu *Cybersecurity Awareness*, Ketahanan Informasi, dan Bijak Bersosial Media. Ketiganya dirancang untuk membangun kesadaran, meningkatkan kewaspadaan, serta menanamkan sikap profesional dalam memanfaatkan teknologi dan ruang digital.

Diharapkan buku saku ini menjadi pedoman operasional yang aplikatif, mudah dipahami, dan dapat diterapkan dalam kehidupan kedinasan maupun pribadi, sehingga setiap prajurit TNI AU tidak hanya unggul di udara, tetapi juga tangguh di ruang siber dan ruang informasi. Dengan kesiapan kolektif seluruh personel, TNI Angkatan Udara akan semakin adaptif, responsif, dan berdaya tangkal tinggi dalam menghadapi dinamika ancaman modern.

Semoga buku saku ini memberikan manfaat nyata dan memperkuat komitmen kita bersama dalam menjaga kehormatan, profesionalisme, serta ketahanan informasi TNI Angkatan Udara.

DAFTAR ISI

BAB I CYBERSECURITY AWARENESS

1.1 Pemahaman Dasar

Perkembangan teknologi informasi telah mengubah karakter ancaman terhadap pertahanan negara. Jika dahulu serangan identik dengan kekuatan fisik dan persenjataan, kini ancaman dapat datang melalui jaringan komputer, sistem komunikasi, dan perangkat digital yang digunakan sehari-hari. Inilah yang disebut sebagai ancaman siber dalam konteks perang non-kinetik. Serangan siber dapat berupa pencurian data, peretasan sistem, sabotase digital, hingga manipulasi informasi yang berdampak pada operasi dan reputasi institusi.

Bentuk ancaman siber semakin beragam, semakin kompleks, dan kian sulit dikenali karena pelaku terus mengembangkan metode yang lebih canggih, terselubung, serta mampu memanfaatkan celah teknis maupun kelengahan manusia, sehingga serangan tidak lagi mudah dideteksi secara kasatmata dan sering kali baru disadari setelah menimbulkan dampak terhadap sistem, data, maupun operasional organisasi. Berikut adalah serangan yang umum dilakukan:

a. ***Phishing***. Serangan dengan cara menyamar sebagai pihak resmi atau tepercaya melalui email, pesan singkat, atau tautan palsu untuk mengelabui korban agar memberikan data pribadi, kata sandi, atau informasi kedinasan.

b. ***Malware***. Perangkat lunak berbahaya yang disusupkan ke dalam sistem atau perangkat untuk merusak, mencuri data, memantau aktivitas, atau mengambil alih kendali tanpa sepengetahuan pengguna.

c. ***Ransomware***. Jenis malware yang mengunci atau mengenkripsi sistem dan data korban, kemudian meminta tebusan agar akses dapat dipulihkan, sehingga berpotensi mengganggu operasional satuan.

d. ***Social Engineering***. Teknik manipulasi psikologis yang memanfaatkan kelengahan, rasa percaya, atau kepanikan korban untuk memperoleh akses informasi penting tanpa harus meretas sistem secara teknis.

e. ***Insider Threat*** **(Ancaman dari Dalam)**. Ancaman yang berasal dari individu di dalam organisasi, baik disengaja maupun akibat kelalaian, yang menyebabkan kebocoran atau penyalahgunaan informasi.

Memahami pola dan karakter masing-masing serangan tersebut merupakan langkah awal dalam membangun pertahanan diri yang kuat di ruang siber.

1.2 Ancaman Nyata bagi Personel TNI AU

Bagi personel TNI AU, ancaman siber bukanlah sesuatu yang abstrak, melainkan nyata dan dapat terjadi kapan saja. Email dinas maupun pribadi dapat menjadi pintu

masuk serangan apabila tidak diverifikasi dengan cermat. Lampiran atau tautan yang tampak resmi bisa saja merupakan upaya penyusupan. Perangkat pribadi seperti telepon genggam dan laptop yang terhubung dengan jaringan dinas juga berpotensi menjadi celah keamanan apabila tidak dilindungi dengan baik.

Penggunaan Wi-Fi publik tanpa pengamanan yang memadai dapat membuka peluang penyadapan data. Selain itu, pendekatan melalui media sosial oleh pihak asing atau akun anonim dapat menjadi bagian dari upaya pengumpulan informasi. Percakapan ringan yang tampak tidak berbahaya bisa saja diarahkan untuk menggali detail tentang tugas, lokasi, atau aktivitas satuan. Oleh karena itu, kewaspadaan harus menjadi sikap dasar setiap prajurit dalam setiap interaksi digital.

1.3 Prinsip Dasar Keamanan Siber

Membangun kesadaran siber berarti menerapkan prinsip keamanan secara konsisten dalam aktivitas sehari-hari. Penggunaan kata sandi yang kuat dan berbeda untuk setiap akun merupakan langkah mendasar yang sering diabaikan. Autentikasi multi-faktor perlu diaktifkan untuk menambah lapisan perlindungan. Setiap tautan, lampiran, atau permintaan data harus diverifikasi sebelum direspons.

Pembaruan sistem operasi dan aplikasi secara berkala penting untuk menutup celah keamanan yang dapat dimanfaatkan pihak tidak bertanggung jawab. Pemisahan antara perangkat dinas dan pribadi juga harus dijaga guna mencegah pencampuran data yang berisiko. Dalam konteks militer, prinsip "*need to know*" harus diterapkan secara disiplin, yaitu informasi hanya dibagikan kepada pihak yang memang berwenang dan membutuhkan. Sikap saling percaya tetap penting, namun dalam keamanan siber berlaku prinsip kewaspadaan menyeluruh terhadap setiap akses dan permintaan informasi.

1.4 Tindakan Saat Terjadi Insiden Siber

Kesadaran siber tidak hanya berhenti pada pencegahan, tetapi juga pada respons yang tepat ketika insiden terjadi. Apabila ditemukan indikasi peretasan, kebocoran data, atau aktivitas mencurigakan pada perangkat, langkah pertama adalah tetap tenang dan tidak mengambil tindakan spekulatif. Jangan menyebarluaskan informasi insiden sebelum ada klarifikasi resmi, karena hal tersebut dapat memperburuk situasi.

Segera laporkan kejadian melalui jalur komando atau satuan kerja yang berwenang menangani keamanan siber. Dokumentasikan gejala atau pesan mencurigakan sebagai bahan bukti dan analisis. Hindari mencoba memperbaiki atau menyelidiki sendiri tanpa kompetensi dan kewenangan, karena dapat menghilangkan jejak digital yang diperlukan untuk investigasi. Respons yang cepat, terkoordinasi, dan sesuai prosedur merupakan bagian penting dari ketahanan siber institusi.

BAB II KETAHANAN INFORMASI

2.1 Konsep Ketahanan Informasi

Dalam era perang modern, informasi telah menjadi aset strategis yang nilainya setara dengan kekuatan persenjataan. Siapa yang mampu menguasai, mengamankan, dan mengendalikan informasi, dialah yang memiliki keunggulan dalam membentuk persepsi, memengaruhi opini, dan menjaga stabilitas. Ketahanan informasi merupakan kemampuan individu dan institusi untuk melindungi, mengelola, serta mempertahankan integritas informasi dari upaya manipulasi, kebocoran, maupun eksploitasi pihak lawan.

Bagi institusi militer, ketahanan informasi tidak hanya berkaitan dengan dokumen rahasia, tetapi juga menyangkut moral prajurit, kepercayaan publik, dan citra institusi. Serangan terhadap informasi dapat diarahkan untuk menurunkan kepercayaan, menciptakan keraguan, memecah soliditas, atau mengganggu pengambilan keputusan. Oleh karena itu, ketahanan informasi harus dipahami sebagai bagian dari sistem pertahanan menyeluruh, yang melibatkan kedisiplinan setiap personel.

2.2 Klasifikasi dan Pengamanan Informasi

Langkah utama dalam membangun ketahanan informasi adalah memahami bahwa tidak semua informasi bersifat terbuka. Dalam lingkungan militer, terdapat tingkatan klasifikasi yang mengatur siapa yang berhak mengakses dan menyebarkan informasi tertentu. Informasi operasional, data personel, rencana kegiatan, spesifikasi alutsista, hingga dokumentasi fasilitas merupakan bagian dari informasi yang harus dikelola dengan prinsip kehati-hatian.

Pengamanan informasi harus dilakukan secara menyeluruh dan konsisten, baik terhadap dokumen fisik maupun dokumen digital, karena keduanya memiliki nilai strategis dan berpotensi menjadi sasaran eksploitasi apabila tidak dikelola dengan disiplin serta sesuai prosedur keamanan yang berlaku.

a. **Pengamanan Dokumen Fisik.** Dokumen fisik, khususnya yang berkaitan dengan kedinasan dan operasional, memiliki nilai strategis yang harus dijaga dengan penuh tanggung jawab. Pengelolaan yang disiplin dan sesuai ketentuan menjadi kunci untuk mencegah kebocoran maupun penyalahgunaan informasi. Oleh karena itu, pengamanan dokumen fisik perlu memperhatikan hal-hal sebagai berikut:

1) Simpan dokumen cetak pada tempat yang aman dan sesuai ketentuan klasifikasi.

2) Jangan meninggalkan dokumen tanpa pengawasan di meja kerja atau ruang terbuka.

3) Hindari memotret, menyalin, atau menggandakan dokumen tanpa izin.

4) Pastikan dokumen sensitif tidak terlihat oleh pihak yang tidak berkepentingan.

b. **Pengamanan Dokumen Digital.** Seiring dengan meningkatnya penggunaan teknologi dalam mendukung pelaksanaan tugas, dokumen digital menjadi bagian yang tidak terpisahkan dari aktivitas kedinasan. Oleh karena itu, pengamanan data dan file elektronik harus dilakukan secara disiplin, sistematis, dan sesuai prosedur, guna mencegah kebocoran maupun akses oleh pihak yang tidak berwenang. Adapun langkah-langkah pengamanan dokumen digital meliputi hal-hal sebagai berikut:

1) Lindungi file digital dengan sistem keamanan yang memadai, termasuk kata sandi dan enkripsi bila diperlukan.

2) Jangan memindahkan data ke media penyimpanan eksternal tanpa izin dan prosedur resmi.

3) Kunci layar komputer atau perangkat setiap kali meninggalkan meja kerja.

4) Hindari membagikan detail kegiatan satuan, data operasional, atau informasi sensitif melalui platform digital yang tidak resmi.

Disiplin dalam menjaga dokumen fisik maupun digital merupakan bagian penting dari ketahanan informasi, karena kelalaian sekecil apa pun dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

2.3 Ancaman Perang Informasi

Perang informasi merupakan bagian dari perang non-kinetik yang bertujuan memengaruhi cara berpikir dan bertindak suatu institusi atau masyarakat. Bentuknya dapat berupa disinformasi, yaitu penyebaran informasi palsu secara sengaja, maupun misinformasi yang tersebar akibat ketidaktahuan. Propaganda dan operasi pengaruh sering dirancang untuk menciptakan narasi tertentu yang merugikan institusi militer, melemahkan kepercayaan publik, serta memecah soliditas internal.

Perkembangan teknologi juga memungkinkan munculnya rekayasa konten digital seperti manipulasi gambar, video, maupun suara yang sulit dibedakan dari aslinya. Informasi yang dipelintir, dipotong sebagian, atau dikeluarkan dari konteksnya dapat membentuk persepsi keliru di ruang publik. Jika tidak diantisipasi, kondisi ini berpotensi menurunkan kepercayaan masyarakat dan memengaruhi moral prajurit.

Selain itu, kemajuan kecerdasan buatan (*Artificial Intelligence*/AI) semakin memperkuat kompleksitas ancaman perang informasi. Teknologi AI mampu menghasilkan teks, gambar, audio, dan video yang tampak autentik dalam waktu singkat dan skala besar. Konten deepfake, bot otomatis penyebar opini, hingga manipulasi percakapan digital dapat digunakan untuk membangun narasi tertentu secara sistematis.

AI juga dapat dimanfaatkan untuk menganalisis perilaku pengguna media sosial guna menargetkan pesan propaganda secara lebih presisi dan personal.

Dalam konteks ini, ancaman tidak lagi sekadar informasi palsu, tetapi informasi yang dirancang secara cerdas, terstruktur, dan sulit dideteksi. Oleh sebab itu, setiap personel harus memiliki literasi digital yang memadai, meningkatkan kemampuan verifikasi sumber, serta tidak mudah terprovokasi oleh konten yang bersifat emosional atau sensasional. Kewaspadaan, pengendalian diri, dan disiplin informasi menjadi benteng utama dalam menghadapi perang informasi berbasis teknologi dan kecerdasan buatan.

2.4 Membangun Daya Tahan Informasi

Ketahanan informasi tidak lahir secara otomatis, melainkan dibangun melalui budaya disiplin dan literasi yang berkelanjutan. Setiap informasi yang diterima perlu diverifikasi sebelum dipercaya atau disebarkan. Sumber resmi dan kredibel harus menjadi rujukan utama dalam memahami suatu peristiwa. Kebiasaan menyaring informasi sebelum membagikannya merupakan bentuk tanggung jawab moral sekaligus profesional, karena satu tindakan yang keliru dapat berdampak luas terhadap institusi.

Di era kecerdasan buatan (*Artificial Intelligence*/AI), kemampuan verifikasi menjadi semakin penting. Teknologi AI mampu menghasilkan konten yang terlihat meyakinkan, mulai dari tulisan, gambar, hingga video yang seolah-olah autentik. Oleh karena itu, personel harus meningkatkan literasi digital dengan memahami bahwa tidak semua konten yang tampak nyata adalah benar. Diperlukan sikap kritis dalam menilai sumber, memeriksa keaslian visual maupun audio, serta tidak langsung mempercayai informasi yang bersifat provokatif atau emosional. AI juga dapat dimanfaatkan secara positif, seperti untuk mendukung analisis informasi dan deteksi anomali, namun penggunaannya harus tetap berada dalam koridor etika dan keamanan yang berlaku.

Selain itu, ketahanan informasi perlu diperkuat melalui edukasi berkelanjutan kepada personel dan keluarga, karena ancaman dapat masuk dari lingkungan terdekat, termasuk melalui media sosial dan aplikasi berbasis AI. Kesadaran kolektif akan pentingnya menjaga informasi akan menciptakan sistem pertahanan yang lebih kokoh dan adaptif terhadap perkembangan teknologi. Dalam konteks militer, komunikasi publik harus dilakukan secara terukur, disiplin, dan sesuai kewenangan, sehingga tidak menimbulkan celah yang dapat dimanfaatkan pihak lain dalam operasi pengaruh berbasis teknologi digital dan kecerdasan buatan.

BAB III BIJAK BERSOSIAL MEDIA

3.1 Media Sosial sebagai Ruang Operasi Baru

Perkembangan media sosial telah mengubah cara manusia berinteraksi, berbagi informasi, dan membentuk opini. Bagi institusi militer, media sosial bukan sekadar sarana komunikasi pribadi, melainkan bagian dari ruang informasi yang memiliki dampak strategis. Apa yang diunggah oleh seorang prajurit dapat dengan cepat tersebar luas, disalin, disimpan, dan dianalisis oleh berbagai pihak, termasuk yang memiliki kepentingan tertentu. Jejak digital bersifat permanen dan sulit dihapus sepenuhnya, sehingga setiap unggahan harus dipertimbangkan secara matang.

Dalam konteks perang non-kinetik, media sosial kerap dimanfaatkan sebagai alat pengumpulan informasi, penyebaran propaganda, maupun pembentukan persepsi negatif terhadap institusi pertahanan. Oleh karena itu, kesadaran bahwa media sosial merupakan bagian dari domain informasi pertahanan harus tertanam pada setiap personel. Kehati-hatian dalam bermedia sosial merupakan bagian dari disiplin militer di era digital.

3.2 Etika dan Disiplin Bermedia Sosial

Sebagai prajurit TNI AU, identitas pribadi tidak dapat sepenuhnya dipisahkan dari identitas institusi. Setiap unggahan, komentar, atau interaksi di ruang digital berpotensi mencerminkan sikap dan profesionalisme satuan. Oleh sebab itu, penting untuk menghindari unggahan yang berkaitan dengan tugas operasional, lokasi penugasan, jadwal kegiatan, fasilitas militer, maupun informasi lain yang bersifat sensitif.

Selain itu, personel perlu menjaga sikap netral dan tidak terlibat dalam perdebatan yang bersifat provokatif, terutama yang berkaitan dengan isu politik praktis atau isu yang dapat menimbulkan polarisasi. Menyampaikan pendapat secara emosional atau tanpa verifikasi dapat merugikan diri sendiri dan institusi. Sikap profesional, santun, dan terukur harus menjadi pedoman dalam setiap aktivitas bermedia sosial. Disiplin digital adalah cerminan disiplin sebagai prajurit.

3.3 Kenali Pola Rekrutmen dan Provokasi

Media sosial sering digunakan sebagai sarana pendekatan oleh pihak yang memiliki kepentingan tertentu. Akun anonim atau identitas palsu dapat mencoba menjalin komunikasi dengan dalih pertemanan, diskusi, atau kerja sama. Percakapan yang awalnya tampak ringan dapat diarahkan untuk menggali informasi tentang aktivitas satuan, kebijakan internal, atau kondisi personel. Modus lain dapat berupa survei daring, kuis berhadiah, atau permintaan data pribadi yang sesungguhnya bertujuan mengumpulkan informasi strategis.

Selain itu, provokasi digital juga sering dilakukan untuk memancing reaksi emosional. Konten yang menyinggung institusi atau memutarbalikkan fakta dapat

dirancang untuk menguji respons personel. Dalam situasi seperti ini, reaksi spontan justru dapat dimanfaatkan untuk memperluas isu. Oleh karena itu, pengendalian diri, kewaspadaan, dan keteguhan sikap menjadi kunci dalam menghadapi upaya rekrutmen maupun provokasi di ruang digital.

3.4 Prinsip Saring – Simpan – Sebarkan

Sebagai pedoman praktis, setiap personel dapat menerapkan prinsip sederhana: Saring, Simpan, dan Sebarkan. Saring berarti memeriksa kebenaran informasi sebelum mempercayai atau membagikannya. Perhatikan sumber, konteks, dan keakuratan isi. Jangan mudah terpancing oleh judul sensasional atau potongan informasi yang belum tentu lengkap.

Simpan berarti menjaga data pribadi maupun data kedinasan dengan bijak. Hindari menyimpan dokumen dinas pada platform pribadi tanpa pengamanan yang memadai. Pastikan pengaturan privasi akun media sosial diatur dengan baik untuk membatasi akses pihak yang tidak dikenal.

Sebarkan berarti hanya membagikan informasi yang aman, positif, dan tidak merugikan institusi. Jika ragu terhadap suatu konten, pilihan terbaik adalah tidak menyebarkannya. Prinsip kehati-hatian ini sederhana, namun memiliki dampak besar dalam menjaga keamanan informasi dan citra institusi.

BAB IV HIMBAUAN BAGI PRAJURIT TNI AU

Bedasarkan telegram Kepala Staf Angkatan Udara tentang pencegahan terhadap kebocoran dokumen kegiatan hasil rapat/berita/laporan dan kegiatan operasi TNI AU yang bersifat rahasia di lingkungan TNI AU baik melalui online ataupun hard copy, dengan ketentuan:

a. Memanfaatkan fasilitas pengiriman dokumen elektronik yang berklasifikasi rahasia melalui jaringan sanapati yang ada di kamar sandi.

b. Menekankan kepada Prajurit dan PNS TNI AU agar tidak mempublikasikan hasil rapat/berita/laporan atau dokumen dan kegiatan operasi yang bersifat rahasia di lingkungan TNI AU tanpa izin dari atasannya.

c. Memberlakukan pembatasan akses hanya kepada pengguna yang terdaftar untuk mengetahui hal apa saja yang dilakukan ketika masuk ke dalam sistem guna memperkecil kemungkinan peretas ke dalam jaringan sistem info yang ada.

d. Lengkapi perangkat android, iphone, dan komputer dengan *software* resmi serta antivirus yang ter-update setiap saat, proteksi perangkat dengan passcode, serta gunakan *two factor authentication* dan *password* yang kuat dan unik minimal 8 karakter yang diperbarui secara berkala.

e. Mengabaikan tautan yang dikirim via surel, sms pesan dari pengirim yang tidak dikenal untuk menghindari masuknya virus *malware.*

f. Setelah penggunaan aplikasi chat (facebook, whatsapp, twitter, youtube) agar *logout* guna menghindari terjadinya bocornya percakapan.

g. Memperhatikan dan mempedomani mekanisme maupun protap penghancuran dokumen sesuai dengan peraturan.

h. Laporkan kepada komando atas apabila ada Prajurit dan PNS TNI AU yang melanggar terkait kebocoran dokumen serta memproses/menghukum sesuai prosedur dan mekanisme yang berlaku.

PENUTUP

Perang modern tidak lagi selalu ditandai dengan dentuman senjata, tetapi dapat berlangsung senyap melalui ruang siber dan ruang informasi. Dalam situasi tersebut, setiap personel TNI AU memiliki peran strategis sebagai garda terdepan pertahanan non-kinetik. Kesadaran siber, ketahanan informasi, dan kebijaksanaan dalam bermedia sosial bukan sekadar pengetahuan tambahan, melainkan bagian dari disiplin dan profesionalisme prajurit di era digital. Buku saku ini diharapkan menjadi pedoman praktis yang membangun kewaspadaan, memperkuat tanggung jawab, serta menanamkan budaya keamanan informasi dalam setiap aktivitas kedinasan maupun pribadi. Dengan komitmen dan kesiapan kolektif, TNI Angkatan Udara akan semakin tangguh, adaptif, dan berdaya tangkal tinggi dalam menjaga kedaulatan negara di seluruh domain, termasuk ruang siber dan ruang informasi.

Kontak Pelaporan Insiden Siber

Satuan Siber TNI AU

a. WhatsApp Piket Siaga Siber (24/7): +62 822-9529-8226
b. Email: idaf-csirt@tni-au.mil.id
c. Instagram: @satsiberau