Jurnal TNI Angkatan Udara (Vol. 2 No.1, 2024)
ISSN: 2809-5464

PENGAMANAN DATA SISTEM INFORMASI DISINFOLAHTAAU

Sugeng Triharto[1] , Ricky Pratama[2], Dikatama T[3].

[1,2,3]dika.pratama0101@gmail.com

ABSTRAKS ━ Memasuki pertumbuhan kemajuan industry 4.0 sebagai *fase* revolusi teknologi, sistem informasi menjadi suatu hal yang menjadi kebutuhan. Mata dunia telah berubah menjadi lebih dekat dan berbagai kemudahan telah terwadahi dengan adanya perkembangan sistem informasi saat ini. Informasi memegang peranan penting dari setiap aspek kehidupan pribadi maupun organisasi. Oleh karenanya keamanan suatu informasi menjadi skala prioritas dalam pembangunan sistem yang ada saat ini. Disinfolahtaau sebagai pembinaan dan penyelenggaraan sistem informasi yang ada di TNI AU sudah seharusnya menjadi sebuah organisasi yang bukan hanya menyediakan aplikasi untuk memudahkan pelaksanaan tugas satuan kerja saja, namun harus menjadi organisasi yang berkemampuan menjamin keamanan data sistem informasi yang dibangun. Mengoptimalkan tugas pengamanan data sistem informasi memang bukanlah suatu hal yang mudah. Butuh perencanaan, pedoman, pelatihan serta keseriusan dari setiap unsur yang ada baik personel pelaksana di lapangan hingga pada level pimpinan. Untuk mencapai sasaran dalam pengoptimalan tugas Disinfolahtaau guna pengamanan data sistem infomasi dalam rangka mendukung tugas TNI AU, maka dibutuhkan langkah-langkah untuk meningkatkan kemampuan personel yang mengawaki organisasi dengan didukung peralatan infrastruktur yang dipadu dengan *prosedure* pengamanan yang ada menjadi faktor penting yang mutlak diperhitungkan serta direncanakan sehingga keamanan data sistem informasi lebih terjamin. Mewujudkan keamanan data sistem informasi pada hakekatnya merupakan serangkaian tahapan yang harus ditempuh dengan dukungan dari para pemangku kebijakan untuk merumuskannya. Hal ini dapat dimulai dari peningkatan kemampuan personel, revitalisasi infrastruktur data sistem informasi serta pembuatan prosedur keamanan data hingga organisasi baru yang khusus menangani kejahatan *cyber* hingga penguatan kepemilikan jaringan mandiri untuk mengintegrasikan seluruh sistem yang ada.

Kata Kunci : *Fase*, Revolusi, Teknologi Sistem Informasi

1. PENDAHULUAN

Tentara Nasional Indonesia Angkatan Udara (TNI AU) sebagai komponen utama alat pertahanan negara di udara bertugas yang menegakkan kedaulatan dan keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI) serta melindungi kehor matan dan keselamatan bangsa dari setiap ancaman yang datang dari luar negeri maupun dari dalam negeri. Fenomena kemajuan teknologi industri 4.0 sebagai *fase* revolusi teknologi, telah mengubah mata dunia pada era informasi. Informasi memiliki peranan penting di semua aspek kehidupan serta merupakan salah satu kebutuhan hidup baik secara individual maupun organisasi. Ancaman dan serangan siber khususnya perang siber (*cyber war*) saat ini telah masuk sebagai ancaman militer maupun ancaman nonmiliter karena berpotensi menimbulkan kerugian fatal terhadap keutuhan serta kedaulatan bangsa dan negara. Kejahatan teknologi informasi seperti *hacking, cracking, phising, malware* juga memicu bentuk dimensi ancaman perang baru yang saat ini dikenal dengan istilah perang siber (*cyber war*). Fasilitas yang sudah berada di Disinfolahtaau berupa perangkat sistem komputer, sistem informasi beserta perang kat jaringannya terhubung dengan *data center,* merupakan infrastrukturkritis TNI AU, sangat rentan terhadap ancaman dan harus dilindungi keamanannya. Semakin tingginya tingkat ketergan tungan organisasi terhadap suatu sistem informasi maka semakin tinggi pula tingkat ancaman dan kerawanan terhadap serangan data informasi tersebut.

Guna mengatasi kondisi dan permasalahan di atas, maka diperlukan upaya-upaya secara urgensi pemahaman mengenai kondisi lingkungan strategis terkini akan hal-hal yang menimbulkan ancaman dan kerawanan *cyber* terhadap data sistem informasi yang dibangun Disinfolahtaau. Perubahan serta perkembangan ilmu pengetahuan dan teknologi yang begitu cepat, menuntut Disinfolahtaau untuk segera merencanakan, merumuskan dan menyusun konsep dalam rangka pertahanan keamanan data yang dimulai dari mendidik personel, pembinaan kemampuan sumber daya personel, pengoptimalan sarana pra sarana infrastruktur jaringan komunikasi data yang aman, serta tata kelola prosedur organisasi yang khusus menangani bidang *cyber defense* agar dapat mengantisipasi ancaman kerawanan perang *cyber* yang dapat mengganggu pelaksanaan tugas TNI AU. Untuk itulah pengoptimalan tugas Disinfolahtaau agar dapat meningkatkan keamanan data sistem informasi harus menjadi prioritas penting, sehingga data sistem informasi dapat digunakan dengan aman dalam rangka mendukung tugas TNI Angkatan Udara kedepan.

2. LANDASAN FILOSOFIS

2.1. Landasan Idiil (Pancasila). Pancasila merupakan pandangan dan falsafah hidup bangsa Indonesia yang merupakan kris talisasi nilai-nilai norma yang diyakini kebenarannya, sehingga menimbulkan tekad untuk mewujudkannya melalui sikap, tingkah laku dan perbuatan dalam kehi dupan bermasyarakat, berbangsa dan bernegara.Pancasila memiliki peran penting dalam kehidupan berbangsa dan bernegara dalam pengem bangan serta pemanfaatan teknologi informasi sehingga harus selalu menjadi landasan pemikiran dalam peman faatan kebutuhan informasi tersebut.

2.2. Landasan Konstitusional (UUD 1945). UUD 1945 sebagai landasan konstitusional merupakan acuan bagi bangsa Indonesia dalam mewujudkan tujuan nasionalnya yaitu melindungi segenap bangsa Indonesia, seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, men cerdaskan kehidupan bangsa serta ikut serta melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan social. Atas dasar tersebut, setiap orang berhak untuk berkomunikasi dan memperoleh informasi yang aman agar dapat disimpan, diolah, sehingga dalam menyampaikan informasi menggunakan dengan segala jenis media yang tersedia secara aman.

3. LANDASAN KONSEPSIONAL

3.1. Wawasan Nusantara, Wawasan nusantaramerupakan cara pandang bangsa Indonesia dengan dijiwai nilai-nilai Pancasila berdasarkan UUD 1945 serta memperhati kan sejarah dan budaya tentang diri serta lingkungan keberadaan yang dimanfaatkan sebagai kondisi dan konstelasi geografi, dengan menciptakan tanggung jawab, motivasi, dan rangsangan bagi seluruh bangsa Indonesia dengan mengutamakan persatuan dan kesatuan bangsa serta kesatuan wilayah NKRI pada penyelenggara an kehidupan bermasyarakat, berbangsa, dan bernegara untuk mencapai tujuan nasional dapat menjamin keutuhan wilayah nasional dan melindungi sumber-sumber data serta pengelolaannya dari segala bentuk ancaman baik yang datang dari dalam maupun luar dengan peningkatan tugas Disinfolahtaau.

3.2. Ketahanan Nasional, merupakan suatu kondisi dari bangsa yang menggambarkan kemampuan untuk meng hadapi/mengatasi segala macam ancaman, tantangan, hambatan serta gangguan. Faktor penguat ketahanan nasional suatu bangsa yaitu ideologi, politik, sosial budaya, ekonomi dan pertahanan keamanan (ipoleksusbudhan kam). Terkait dengan hal tersebut, peran Disinfolahtaau dalam rangka menjaga sistem informasi TNI AU merupakan salah satu bentuk usaha serta berkewajiban dalam menciptakan ketahanan nasional, yaitu dengan melakukan berbagai bentuk upaya-upaya mewujudkan keamanan data sistem informasi.

3.3. Landasan Operasional, serbagai berikut:

- **Undang-undang Nomor 3 Tahun 2002** tentang Pertahanan Negara. Hakikat pertahanan negara merupakan segala daya upaya pertahanan bersifat semesta yang penyelenggaraannya didasarkan pada kesadaran atas hak dan kewajiban warga negara serta keyakinan pada kekuatan sendiri. Secara khusus di pasal 20 ayat 2 menjelaskan bahwa segala sumber daya nasional yang berupa sumber daya manusia, sumber daya alam dan buatan, nilai-nilai, teknologi dan dana dapat didaya gunakan untuk meningkatkan kemampuan pertahanan negara yang diatur lebih lanjut dengan Peraturan Pemerintah. Dikaitkan dengan Sistem Pertahanan Negara maka optimalisasi tugas dalam rangka penga manan pengelolaan sistem informasi yang baik adalah merupakan suatu kebutuhan dan keharusan yang dimiliki oleh TNI AU untuk meningkatkan daya tangkal dalam menghadapi segala bentuk ancaman/ kerawanan dari kejahatan siber terhadap data sehingga peran Disinfolahtaau dalam pengamanan data sistem informasi sangat diandalkan. Undang-undang Nomor 34 Tahun 2004 tentang TNI. Dalam undang-undang RI nomor 34 tahun 2004 Bab IV Pasal 6 ayat 1 dijelaskan bahwa TNI sebagai alat pertahanan negara berfungsi sebagai penangkal terhadap setiap bentuk ancaman militer dan ancaman bersenjata dari luar dan dalam negeri terhadap kedaulatan, keutuhan wilayah, dan kesela matan bangsa.
- **Undang-Undang ITE No. 19 Tahun 2016** tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pemerintah memfa silitasi pemanfaatan teknologi informasi dan transaksi elektronik sesuai dengan keten tuan peraturan perundang-undangan. Pada pasal 40 ayat 2b bahwa dalam melaku kan pencegahan, pemerintah berwenang mela kukan pemutusan akses atau meme rintahkan kepada penyelenggaraan sistem elektronik untuk melakukan pemutu san akses terhadap informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar hukum.
- **Peraturan Menteri Pertahanan Republik Indonesia** Nomor 82 tahun 2014 tanggal 17 Oktober 2014 tentang Pedoman Pertahanan Siber. Pedoman pertahanan siber ini digunakan sebagai penyamaan keinginan, prinsip dan kehendak dalam penye lenggaraan pertahanan siber pada sistem informasi, kendali dan komunikasi di TNI khususnya Disinfolahtaau. Pedoman ini merupakan langkah-langkah dalam penye lenggaraan pertahanan siber sebagai penyamaan pemahaman dan pedoman yang disesuaikan dengan tugas dan fungsi satuan masing-masing agar mempedomani dan diterapkan dalam pertahanan siber sehingga pola pikir, pola sikap, dan pola tindak dalam menjamin keamanan jaringan di sektor pertahanan dapat terwujud.

4. METODE PENELITIAN

4.1. Teori Keamanan Sistem Informasi, menurut Raymond McLeod dan George P. Schell Jr (2007). Menurut Raymond McLeod dan George P. Schell Jr dalam bukunya berjudul "*management information systems*" ber pendapat sistem informasi manajemen adalah sistem berbasis komputer yang dapat menyediakan penggu na dengan informasi yang dibutuh kan dan kebutuhan informasi tertentu yang dibutuh kan. Sistem informasi manajemen dapat digunakan untuk mengelola sumber daya yang terkandung didalamnya, seperti peralatan sistem informasi (termasuk perangkat keras dan lunak), jaringan komunikasi data, organisasi dan sumber daya manusia, serta peran pemimpin yang bertanggungjawab untuk memantau dan memastikan kesiapan operasi data untuk memastikan ke amanan data yang strategis di TNI AU.

4.2. Teori Manajemen, menurut George R. Terry, Dibagi menjadi empat fungsi manajemen dasar, yaitu *planning* (peren canaan), *organizing* (pengorgani sasian), *actuating* (pelaksanaan) dan *controlling* (pengawasan). Keempat fungsi manajemen ini disingkat dengan POAC. Mercer and Justine, dalam teori *human capital* menyebutkan sumber daya yang ada pada setiap orang atau kelompok adalah capital. Jika dalam dunia bisnis, capital diperoleh dengan mengkonversi bahan mentah menjadi barang setengah jadi atau barang jadi yang siap dijual. Akan tetapi, dalam

pendidikan, sumber daya manusia (*human capital*) didapat ketika seseorang mampu menguasai *skill* atau *knowledge* yang diinginkan selain sumber daya alam, modal, dan *enter preneur* sumber daya manusia (*human capital*) menjadi salah satu faktor produktifitas suatu negara. Artinya semakin tinggi tingkat kualitas sumber daya manusia pada suatu negara, semakin tinggi pula tingkat produktifitas, kesejahteraan, dan daya saingnya di tingkat global.

5. HASIL PENELITIAN DAN PEMBAHASAN

5.1. *Cyber War: The Next Threat To National Security And What To Do About It.* Menurut Richard Clark dalam bukunya tersebut menyatakan bahwa ancaman serangan *cyber* saat ini telah mengalami banyak perubahan apabila dilihat dari pola, teknologi maupun strategi yang digunakan. Seiring dengan perkembangan peralatan komunikasi data yang maju serta penemuan *fiber optic* yang memiliki kecepatan dalam mengirim paket data maka dapat dipastikan serangan *cyber* dapatdengan cepat menye rang infrastruktur jaringan komputer. Implikasinya dalam dunia militer, kemam puan *cyber* telah merubah media pepe rangan dari sistem pertahanan yang dioperasikan oleh manusia, kini sistem pertahanan tersebut dapat diakses melalui media komputer yang *online* tanpa harus mengalahkan terlebih dahulu alutsista persenjataan lawan. Adanya serangan ancaman *cyber* yang ditujukan kepada infrastruktur militer juga telah mengubah konsep doktrin dan strategi yang sebelum nya tidak mengadopsi perang informasi sehingga hal ini menjadi kebutuhan yang sangat mendesak untuk perlunya pembentu kan *cyber defense.* Dengan demikian maka pada zaman informasi ini militer harus mengubah tiga komponen dasar dalam penyesuaian kemajuan teknologi informasi yaitu strategi, tingkat integrasi serta pendekatan *command and control (C2)*.

5.2. Aprison, 2015. Optimalisasi *Data Center* Disinfolahtaau Guna Pengama nan Sistem Informasi Dalam Rangka Terwujudnya C*yber Defence System* Mabes TNI AU. Menurut Aplison, penambahan data *center disney* sangat diperlukan TNI AU untuk mencapai *cyber defence* dengan melaksanakan perbaikan pusat data di Disinfolahtaau dan meningkat kan sistem keamanan data serta membatasi keluarnya informasi yang tidak perlu/ meminimalis informasi yang kurang penting, serta fokus pada penggunaan teknologi *server virtual* untuk memastikan kesiapan data dan memastikan Indonesia memiliki data di TNI AU selalu aman. Memasuki revolusi Industri 4.0 merupakan fenomena yang mengkolaborasikan teknologi *cyber* dan teknologi sistem informasi khususnya di TNI AU meliputi bidang intelijen, operasi, personel, logistik, dan manajemen. Serangan dan acaman *cyber* saat ini senantiasa berevolusi semakin canggih, mengikuti perkembangan global teknologi informasi. Serangan dan ancaman *cyber* dapat secara rahasia melumpuhkan pusat data tanpa akan saling melengkapi. Teridentifikasi untuk melakukan pencurian dokumen-dokumen penting suatu organi sasi. Berbagai potensi ancaman seperti di atas akan benar-benar menjadi masalah jika Disinfolahtaau tidak menye imbangkan kemampuan tugasnya dalam memper kuat pertahanan *cyber defense* data sistem informasi yang berkembang pesat saat ini baik darisegi personel, perangkat maupun organisasi. Berdasarkan hasil analisis data dan fakta terkait kondisi tugas data di Disinfolahtaau saat ini masih kurang aman dan rawan dalam hal penyimpanan data.

5.3. *Transfer of Technology* (TOT) Sistem Informasi *Cyber* merupakan sistem yang sangat diperlukan sebagai proses pendele gasian kemampuan, pengetahuan dan teknologi sistem informasi serta jaringan yang sudah terbangun. Kondisi sekarang proses TOT ke personel dari mitra pengem bang dalam penguasaan teknologi sistem perangkat pengamanan aplikasi yang terbangun masih sangat terbatas. Banyak dari personel belum sepenuhnya terlatih untuk menguasai sistem perangkat aplikasi yang terbangun terutama dalam sisi dukungan pengamanan data sistem informasi. Menyebabkan Disinfolahtaau

masih bergantung kepada pihak luar untuk pemecahan permasalahan baik secara teknis dilapangan maupun interen seperti dalam pengkonfigurasian perangkat *data center* berupa *firewall*, *segment* pembagian jaringan aplikasi seluruh satker, tentang hak akses data sehingga penutupan celah kerawanan di masing-masing aplikasi meliputi aplikasi operasi, logistik, personel, dan manajemen yang jumlahnya tidak sedikit dan sangat penuh kompleksitas.

5.4. Infrastruktur Pengamanan Data Sistem Informasi. Kondisi infrastruktur terhadap pengamanan data SIM terutama *data center* belum sepenuhnya dapat mendukung pemenuhan kondisi yang ideal untuk melindungi infrastruktur kritis TNI AU. Sesuai fakta yang kami dapat dilapangan bahwa beberapa perangkat yang ada di *data center* sudah harus direvitalisasi karena sudah lebih dari lima tahun. Sesuai dengan ruang lingkup dan kewenangan serta skala prioritas, suatu kelembagaan pertahanan siber sangat memerlukan dukungan teknologi infrastruktur salah satunya *dissaster recovery center* (DRC), merupakan salah satu infrastruktur *data center* yang sudah di bangun mulai tahun 2013 yang ada belum dilengkapi dengan pengamanan data sistem informasi termasuk salah satunya adalah ruangan lab *monitoring* siber serta bangunan DRC untuk menangkal gangguan dari pihak asing yang membahayakan *data center.* Infrastruktur ini seharusnya bagian yang tidak boleh terpisahkan dalam membangun suatu pertahanan *cyber* TNI AU khususnya Disinfolahtaau dalam mengantisipasi kejadian sebenarnya jika terjadi *cyber attack*.

***Prosedure* Pengamanan**. *Prosedure* pengamanan data yang ada saat ini dalam *data center* belum menjadi fokus penting organisasi TNI AU. Terbukti dengan belum adanya organisasi khusus yang menangani permasalahan *cyber* sehingga mengakibat kan adanya masalah pengaman an data diwadahi denganprotap yang jelas. Saat Ini pengamanan data hanya mengandalkan peran tugas pokok Pusat Data Sistem Informasi (Pustasisinfo) yang tugasnya lebih kearahpemeliharaan perangkat *data center*. Disinfolahtaau tidak tertuang secara tertulis terkait pasal-pasal dalam meblokir situs-situs tertentu, *prosedure* upaya yang harus dilakukan untuk mendeteksi adanya *mal ware* yang berpotensi merusak jaringan komputer serta membuat kebijakan jalur hak akses user untuk masuk ke *data center.* Kondisi inilah yang mengakibatkan saat terjadinya peretasan akun sosial media *facebook* TNI AUdi 2019, TNI AU khususnya Disinfolahtaau tidak memiliki dasar untuk melakukan *prosedure* pemulihan data seperti apa karna tidak ada referensi untuk penyelesaiannya.

5.5. Kemampuan Personel dalam TOT Sistem Informasi *Cyber* Belum Optimal. Peningkatan kemampuan personel dalam TOT sistem informasi *cyber* untuk peng optimalan tugas Disinfolahtaau dalam penanganan keamanan data sistem infor masi harus menjadi prioritas. Mayoritas personel telah memiliki kemampuan dalam bidang sistem informasi dan teknologi komputerisasi, namun belum pada keilmuan bidang pengamanan data atau *cyber*.

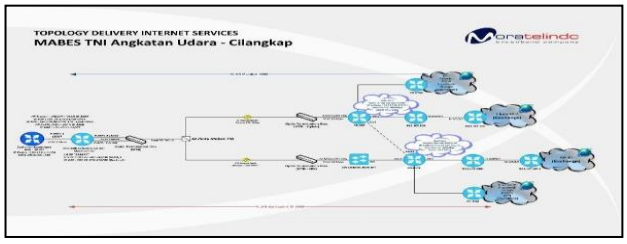
5.6. Ketidak optimalan permasalahan TOT sistem informasi *cyber* diatas disebabkan oleh:

- Kurangnya kesempatan personel dalam kursus pengamanan data. Beberapa personel Disinfolahtaau hanya sedikit yang berkesempatan mengikuti kursus pengamanan data dan kurangnya kesempatan untuk mengikuti kursus *cyber defense.*
- Minimnya jumlah personel yang memiliki keahlian khusus dibidang *data center* sehingga banyak konfigurasi data center terkait *cyber attack* tidak dapat ditangani.
- Kurangnya minat/kemauan dari personel Disinfolahtaau, dan lebih memilih untuk mempelajari selain bidang *cyber* seperti multimedia, *database.*
- Kurangnya budaya keamanan data sistem informasi.

Faktor perilaku budaya personel dalam bekerja juga menambah persoalan ketidak optimalan Disinfolahtaau dalam melaksa

nakan pengamanan data informasi, banyak diantara personel yang melakukan *login* ke suatu aplikasi baik aplikasi bidang operasi, logistik, personel dan manajemen dengan membuat *password* yang tingkat keamanan nya rendah/*weaknes* seperti NRP, tanggal lahir maupun nama sendiri. Selain itu budaya menyimpan *password* di *history browser* sebagai alasan agar tidak mengetik ulang jika login ke suatu aplikasi dapat membuka celah kerawanan jika komputer staf tersebut dibuka oleh orang yang tidak ber kepentingan.

5.7. Dukungan Kelengkapan Infra struktur tentang Pengamanan Data Sistem Informasi Belum Terpenuhi menjadi point penting yang harus terpenuhi. Kondisi saat ini perangkat pengamanan *data center* belum sepenuhnya terpenuhi. Hal tersebut ditunjukan dari infrastruktur pengamanan data sistem informasi serta fasilitas lainnya yang sangat menentukan guna mendukung optimalisasi tugas Disinfolahtaau belum lengkap. Persoalan infrastruktur penga manan data sistem informasi Disinfolahtaau saat ini sesuai data fakta yang menjadi penyebab lemahnya *cyber defense.* Jaringan Komunikasi *Data Center* yang Masih Bergantung Pada *Provider Luar*. Saat ini jaringan data yang masuk ke *data center* bergantung pada *provider* lain. Disinfolahtaau selama ini berlangganan selama satu tahun untuk mendukung jaringan internet Mabesau. Dengan keter gantungan tersebut maka keamanan data sistem informasi kita bergantung pada mitra dan menimbulkan kerawanan tersendiri dalam mendukung tugas TNI AU kedepan nya. Masih adanya Software Aplikasi *Client* yang *Unlisensi*. Ketidak optimalan *data center* saat ini juga dihadapi dan masih banyaknya *client* yang terhubung ke *data center* yang *unlisensi.* Software aplikasi yang *unlisensi* rata- rata dari sistem operasi *Windows*, *Office* serta Anti Virus yang *free* yang di instalasi di client-client. Ketidak originilan *software* aplikasi ini dapat berimplikasi pada kerentanan masuk nya virus, *spyware* maupun *malware* yang disusupi *cyber espionage.* Banyak pintu keamanan data center yang terbuka dengan melewati celah-celah *software unlisensi* atau bajakan ini, tentunya sangat membahayakan keamanan data TNI AU serta mempengaruhi tercapainya tugas TNI AU. *Software* sistem operasi aplikasi *data center* yang belum terintegrasi. Saat ini *data center* Disinfolahtaau berisi aplikasi yang telah di bangun dari tahun 2009 sebelum adanya data center. Setiap aplikasi dibangun dengan *platform* berbeda karena tidak adanya ketentuan terdahulu dari Disinfolahtaau untuk penyeragaman sistem operasi aplikasi maupun dari sisi *database* aplikasi. Dengan masalah tersebut menjadikan tugas Disinfolahtaau menjadi tidak optimal sehingga menjadi tantangan ke depan untuk pengintegrasian sistem informasi yang berbeda *platform* agar tugas TNI AU dalam mengakses semua sistem informasi yang aman dapat saling terintegrasi. Adapun data table perbedaan platform aplikasi sebagai berikut:



Revitalisasi Perangkat *Data Center* belum terlaksana. Revitalisasi perangkat *data center* sangat diperlukan untuk meningkat kan kemampuan operasional perangkat dikarenakan perangkat yang ada sekarang sudahberusia lebih dari 5 tahun. Selain usia beberapa perangkat yang ada saat ini sudah berbeda teknologi dengan yang terbaru saat ini seperi *rooter, switch, sfp , firewall, fiber optic* serta mikrotik memerlukan penggan tian, dikarenakan pimpinan masih memprio ritaskan pada pembangunan dan pere majaan pesawat serta alutsista lainnya. Selain itu mungkin para pimpinan masih beranggapan bahwa ancaman terhadap data sistem informasi khususnya *data center* Disinfolahtaau belum menjadi sesuatu prioritas suatu ancaman yang bernilai strategis. Fasilitas Ruang monitoring pengamanan sistem informasi (Pamsisfo) TNI AU yang Kurang terawat. Pada awal dibangunnya tahun 2016, ruanganpamsisfo

masih bisa memonitor trafik data dari luar yang mengakses sistem informasi di *data center.* Ruangan Pamsisfo ini memang dibangun oleh Kemenhan sebagai kepanjangan satuan siber yang telah di bangun Kemhan dengan harapan Kemhan juga dapat memonitor trafik data yang ada di TNI AU melalui Disinfolahtaau. Ketidak optimalan tugas Disinfolahtaau dalam perawatan ini dikarenakan tidak adanya struktur organisasi di Disinfolahtaau yang menangani khusus ruangan Pamsisfo tersebut sehingga ber implikasi pada rawannya gerbang pengamanan data yang langsung kearah *data center* tanpa ada yang *memonitoring* jalur *traffic* paket data. Pelaksanaan optimalisasi tugas Disinfolah taau dalam pengamanan data sistem informasi memerlukan suatu langkah yang komprehensif dan sistematis sehingga dapat di laksanakan secara efektif dan efisien. Untuk itu tugas Disinfolahtaau yang diharapkan dari pokok-pokok permasalahan tersebut harus berdasarkan Undang-Undang RI Nomor 3 Tahun 2002 Tentang Pertahanan Negara, Undang-undang Nomor 34 tahun 2004 tentang TNI, Undang-undang ITE No 19 tahun 2016 tentang informasi dan transaksi elektronik, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 tahun 2014 tanggal 17 Oktober 2014 tentang Pedoman Pertahanan Siber, Keputusan Kepala Staf Angkatan Udara Nomor Kep/402/XII/2019 tanggal 31 Desember 2019 Tentang Petunjuk Referensi Cetak Biru (*Blue Print*) Teknologi Informasi dan Sistem Informasi Tentara Nasional Indonesia Angkatan Udara serta didukung dengan teori tentang Sistem Informasi Manajemen.

5.8. Kemampuan Personel dalam TOT Sistem Informasi *Cyber* Optimal. Pembangunan sistem informasi yang handal baik dari sisi keamanan maupun manfaat kegunaannya tentunya memer lukan sumber daya manusia yang memiliki kapasitas serta kapabilitas dalam bidang teknologi informasi yang mumpuni. Pembinaan jenjang karier personel yang diharapkan harus disesuaikan dengan Peraturan Kepala Staf Angkatan Udara Nomor Perkasau/126/XII/2009 Tanggal 10 Desember 2009 Tentang Buku Petunjuk Teknis TNI AU Tentang Pembinaan Profesi dan Karier Perwira Korps Dinas Khusus Bidang Pengolahan Data Elektronik (PDE). Saat ini pembinaan personel pada tiap-tiap bagian subdis yang ada merupakan lulusan pendidikan sarjana sistem informasi serta jurusan IPA bagi para personel bintara dantamtama. Namun kondisi tersebut belum cukup, yang patut kita penuhi bahwa untuk seluruh personel Disinfolahtaau dengan berbagai level keahlian sebagai pranata komputer adalah dapat menangani *trouble shooting* maupun TOT pengetahuan *cyber* secara teknis.

5.9. Dukungan Kelengkapan Infrastruktur Pengamanan Sistem Informasi. Keleng kapan infrastruktur pengamanan terkait teknologi yang ideal ada di *data center* Disinfolahtaau antara lain *Network Operation Center (NOC)* serta laboratorium yang di lengkapi fasilitas pendukung lainnya. Jaringan Komunikasi *Data Center* yang Mandiri. Kedepannya jaringan data yang masuk ke *data center* harus bisa mandiri. Hal ini memang suatu pekerjaan yang levelnya hingga pemerintahan. Pengama nan data sistem informasi akan lebih terjamin jika kemandirian jaringan data seperti *provider* atau satelit dapat dimiliki TNI. Software Aplikasi *Client* yang *lisensi*. Banyaknya *client* yang terhubung ke *data center* diharapkan didukung sistem yang ber*lisensi* baik, dari sisi sistem operasi, *office*, antivirus maupun *database .* Hal ini dilakukan agar kedepannya *data center* tidak rentan pada masuknya benda asing seperti virus, *spyware* maupun *malware* yang dapat disusupi *cyber espionage.* Investasi software lisensi memang diawal sangat mahal dari sisi harga namun sebanding dengan manfaat dan keamanan data yang kita dapati karena dengan software yang *berlisensi* tentunya keamanan data TNI AU akan semakin terjamin dimana hal ini merupakan suatu yang sangat tidak ternilai harganya. Software Sistem Operasi Aplikasi *Data Center* yang Terintegrasi. Kondisi yang diharapkan dalam pengoptimalan tugas Disinfolahtaau yang lain yaitu adalah mewujudkan *data warehouse* dimana fungsi nya untuk meng integrasikan data sistem aplikasi dari berbagai platform untuk dapat

dibaca dan digabungkan terutama aplikasi yang sudah terpublis/online di internet. Revitalisasi Perangkat *Data Center* terlaksana. Dalam upaya mewujudkan keoptimalan *data center* tentunya perangkat keras yang ada saat ini diharapkan bisa di revitalisasi. Kemampuan operasional perangkat keras *data center* harus senantiasa *terupdate* untuk perangkat yang usianya lebih dari 5 tahun secara berkala. Selain perangkat keras, perangkat lunak keamanan harus terupdate setiap tahunnya karena *software* keamanan ini hanya berlisensi 1 tahun. Dengan direvitali sasi perangkat dan *software* yang ada seperi *rooter, switch, sfp* serta mikrotik dan penggantian kabel *fiber optic* dibeberapa gedung yang ada di Mabesau, maka dapat meningkatkan performa kecepatannya *data center* dalam menyajikan informasi yang aman. Dengan terbangunnya DRC *data center* maka TNI AU akan memiliki *backup* data sistem informasi dalam mendukung pengamanan jika sewaktu-waktu ada gangguan terhadap *data center* yang dimiliki saat ini.

5.10.Indikasi Keberhasilan. Pengamanan data sistem informasi merupakan bagian infra struktur kritis TNI AU yang harus dapat diwujudkan secara optimal dengan didukung dan melibatkan pihak-pihak lain yang terkait dalam pelaksanaannya yaitu masing-masing *stakeholder* seperti Sopsau, Slogau, Disminpersau, Diswatpersau serta *stake holder* pengguna aplikasi lainnya. Indikasi berhasilnya tugas Disinfolahtaau guna pengamanan data sistem informasi dalam rangka mendukung tugas TNI AU dengan optimal adalah:

5.11.Peningkatan kemampuan *skill* dan *awareness* personel. Penyerapan TOT sistem informasi *cyber* yang meningkat sangat berbanding lurus dengan meningkat nya *skill* atau kemampuan personel khususnya dalam penanganan keamanan data sistem informasi sehingga melahirkan *awareness* personel terhadap data sistem informasi khususnya personel yang di tempatkan di *data center* Dis infolahtaau, memiliki pengetahuan tentang penanganan sistem informasi, personel yang sangat sensitif yang terbiasa menangani masalah jaringan dan keamanan data sistem informasi yang mereka tangani, yang pada gilirannya akan mencegah informasi palsu atau melindungi data sistem informasi dan tugas utamanya adalah memberikan kontribusi aktif kepada TNI AU.

5.12.Terwujudnya dukungan keleng kapan infrastruktur pengamanan sistem informasi. Sistem informasi dapat terlak sana secara maksimal dengan dukungan kemandirian jaringan komunikasi data, *lisensi software*, integrasikan sistem aplikasi serta terbackupnya kemam puan perangkat karena adanya revitalisasi *data center* serta sarana fasilitas seperti DRC dan ruang monitoring, yang pada akhirnya akan berkontribusi terhadap tugas Disinfo lahtaau dalam pengamanan data sistem informasi dan tugas pokok TNI Angkatan Udara.

5.13.Terciptanya kebijakan pimpinan TNI AU tentang *prosedure* pengaturan keamanan data yang selaras, menjadi factor penting dalam menyusun beberapa *procedure* pengaturan keamanan data seperti terkait pengaturan fungsi *firewall* serta pemahaman yang kuat terkait *blue print* pembinaan sistem informasi yang diwujudkan dengan adanya validasi organi sasi *cyber*, yang pada akhirnya akan berkontribusi terhadap tugas Disinfolahtaau dalam pengamanan data sistem informasi dan tugas pokok TNI AU.

5.14.Strategi. Strategi pengoptimalan tugas Disinfolahtaau guna mengamankan data sistem informasi dalam rangka mendukung tugas pokok TNI AU. Sehubungan dengan hal tersebut maka strategi yang perlu dilaksanakan adalah sebagai berikut:

- **Pertama.** Mewujudkan kemampuan per sonel dalam TOT sistem informasi *cyber* yang optimal melalui peningkatan kemam puan kualitas, kuantitas sumber daya personel bidang pengamanan teknologi informasi menggunakan metode pendidikan kursus, pelatihan, pemben tukan minat, peningkatan budaya keamanan data sistem informasi, melalui sarana Kemhan, Pusinfolahta TNI, Mabesau, pada Satker Disdikau serta

Disinfolahtaau dengan tujuan menyiap kan personel yang memiliki kemampuan dalam menyerap ilmu penge tahuan sistem informasi *cyber* secara optimal sehingga mampu menangani ber bagai persoalan terkait gangguan dalam penanganan data sistem informasi yang ada di TNI AU.

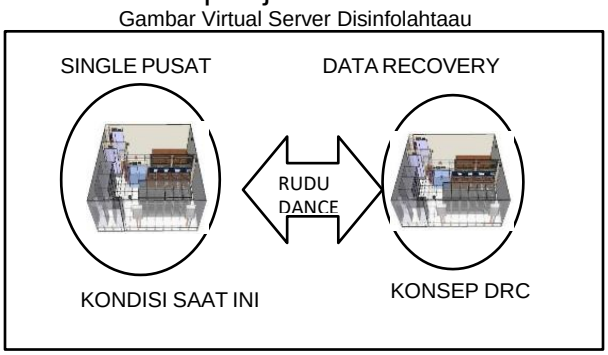
- **Kedua.** Mewujudkan dukungan infra struktur pengamanan sistem informasi yang memadai melalui pengadaan dan penam bahan sarpras, menggunakan metode riset penelitian dan pengembangan, pembelian *lisensi software,* pengintegrasian sistem operasi, revitalisasi perangkat, pem bangunan, pemeliharaan perangkat melalui sarana Kemhan, Mabes TNI, Mabesau melalui Srenaau dan Disinfolah taau dengan tujuan agar mampu mengoptimalkan tugas Disinfolahtaau dalam keamanan data sistem informasi TNI AU untuk menjaga serta menye diakan informasi kepada pimpinan dengan cepat dan aman.
- **Ketiga.** Mewujudkan *prosedure* kea manan data sistem informasi yang selaras melalui kajian, revisi dan pembuatan protap aturan pengamanan data sistem informasi menggu nakan metode pembuat an protap baru yang menuangkan konfigu rasi pengamanan data, sosialisasi *blue print* pembinaan sistem informasi, kajian validasi organisasi *cyber* melalui sarana Mabes TNI dan Mabesau melalui satker Srenaau, Disinfolahtaau, dan *Stake holder* serta Infolahtalanud dengan tujuan penataan *prosedure* sistem penanganan keamanan data sistem informasi dapat melindungi infrastruk tur kritis TNI AU berupa *data center* yang sudah dibangun saat ini.

5.15. Upaya Berdasarkan Strategi. Meng optimalkan kemampuan personel dalam TOT sistem informasi *cyber,* meningkatkan kualitas dan kuantitas sumber daya personel bidang pengamanan data sistem informasi dengan menggunakan metode pendidikan kursus, pelatihan, pembentukan minat, peningkatan budaya keamanan data sistem informasi antara Kemhan, PusinfolahtaTNI, Mabesau ber dasarkan undang-undang terkait. Upaya-upaya yang akandiwujudkan melalui strategi pertama sangat membutuh kan dukungan Menteri Pertahanan, Panglima TNI, Kasau melalui Kadisdikau dan Kadisinfolahtaau untuk melakukan langkah-langkah tindakan sebagai berikut:

Gambar Skema Kebutuhan Kompetensi SDM pertahanan Siber

Upaya Berdasarkan Strategi Kedua. Mewujudkan dukungan kelengkapan infra struktur pengamanan sistem informasi yang memadai melalui pengadaan dan penam bahan sarana prasarana, menggu nakan metode riset penelitian dan pengem bangan, pembelian *lisensi software,* pengintegrasian sistem operasi, revitalisasi perangkat, pembangunan, pemeliharaan perangkat melalui sarana Kemhan, Mabes TNI, Mabesau berdasarkan Permenhan No.82 Tahun 2014 tentang Pertahanan Siber, dengan melakukan beberapa tindakan sebagai berikut:

Gambar Konsep kajian DRC Disinfolahtaau



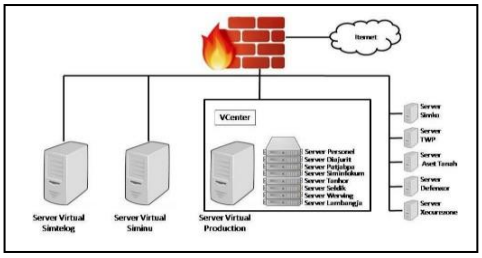
6. KESIMPULAN DAN REKOMENDASI

- Peran organisasi Disinfolahtaau dalam pengamanan data sistem informasi masih dibayangi akan ketidakoptimalan kemampuan personel, kelengkapan infra

struktur serta *prosedure* yang digunakan dalam pengamanan data dimana hal ini berdampak terhadap kelancaran pelak sanaan tugas dan fungsi Disinfolahtaau sebagai pembinaan sistem informasi TNI AU. Dibutuhkan penyusunan *grand strategy* TNI AU khusus nya peningkat an sumber daya personel dalam TOT sistem informasi, pembangunan DRC dan meleng kapi infrastruktur pengaman an data sistem informasi, serta validasi organisasi *cyber* sebagai wujud tata kelola pengamanan data yang selaras. Dinamika perkembangan dunia teknologi informasi 4.0 yang pesat secara global regional dan nasional di kawasan, telah mengubah bentuk ancaman perang yang menjadikan peluang serta kendala ter sendiri sebagai proyeksi kebutuhan kekuatan sistem infomasi TNI AU yang harus segera terwujud keamanannya.

- Dalam melindungi infrastruktur kritis berupa data sistem informasi sangatlah membutuh kan adanya upaya strategis dari para pemimpin organisasi mulai dari Menteri Pertahanan, Panglima TNI serta Kasau untuk merencanakan dan me wujudkan langkah-langkah strategis dalam meningkatkan kemampuan personel, kelengkapan infrastruktur pengamanan maupun piranti lunak berupa *prosedure* pengaturan keamanan data.

- Pemahaman *security awareness* per sonel TNI AU di masing-masing *stake holder* harus dapat dijadikan sebagai budaya untuk dapat mencegah bocornya data-data strategis TNI AU yang dapat digunakan oleh pihak yang tidak ber wenang untuk sesuatu yang mem bahayakan bagi pelaksanaan tugas pokok TNI AU.



7. REFERRENSI

[1]Clarke,Richard A. dan Robert K.Knake, 2010,*Cyber War-The Next Threat to National Security and What to Do About It*

[2]Doktrin Siber Tentara Nasional Indonesia Nomor KEP/1355/XII/2018, Lampiran C, Ancaman dan serangan Siber.

[3]Keputusan Kepala Staf Angkatan Udara Nomor Kep/722/XI/2016 tentang Keamanan Sistem Informasi.

[4]Mercer and Justine, 2010, *Human Resource Management In Education*. www.bps. go.id, diakses tanggal 15 April 2020.

[5]Perkasau Nomor 24 tahun 2014 tentang POP Disinfolahtaau Pasal 3.

[6]Peraturan Menteri Pertahanan Republik tentang Pedoman Pertahanan Siber.

[7]SistemPertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Media Informasi Dirjend Pothan. Kementrian Pertahanan RI.

[8]Undang-Undang RI Nomor 34 Tahun 2004, Pasal 10.

[9]Undang-Undang RI Nomor 3 Tahun 2002 tanggal 8 Januari 2002 tentang Pertahanan Negara.

[10]Undang-Undang RI Nomor 34 Tahun 2004 tanggal 16 Oktober 2004 tentang Tentara Nasional Indonesia.

[11]Undang-Undang ITE No. 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.