Desain Konseptual Sistem Keamanan Siber Pada Industri Kedirgantaraan

(Conceptual Design of Cyber Security System of the Aerospace Industry)

Chadziqatun Najilatil Mazda[1*]

[1] Teknologi Rekayasa Logistik, Fakultas Teknik, Universitas Nurtanio Bandung
E-mail: mazdacha97@gmail.com

Abstract— ***The development of the aerospace industry is one of the transitions in the second mission of Asta Cita, namely to strengthen the national security protection system. Aerospace industry management in supporting Indonesia Emas 2045 requires several strategic steps. These include strengthening the industrial ecosystem through government-private collaboration and increased investment. The aerospace industry is one of the sectors that has an urgent need for information and communication technology. Therefore, cybersecurity is crucial for protecting strategic assets and sensitive information. This study aims to develop a cybersecurity management concept design that can be applied to the aerospace industry. This model was developed based on an analysis of cybersecurity threats faced by the aerospace industry, as well as existing cybersecurity best practices and standards. This qualitative study employed research and development methods using primary and secondary data. The results show several elements of the aerospace industry cybersecurity system, including cybersecurity system stakeholders consisting of government, industry, academia, and organizations. Furthermore, there are also challenges and focuses of cybersecurity in the aerospace industry. Through the design of the cybersecurity system concept for the aerospace industry, it is hoped that it can contribute to the development of cybersecurity policies and strategies in the aerospace industry.***

Keywords— **Conceptual Design, Cyber Security, Aerospace Industry**

Abstrak— ***Pembangunan industri kedirgantaraan merupakan salah satu perwujudan pada misi kedua Asta Cita, yaitu untuk memantapkan sistem pertahanan keamanan Negara. Manajemen industri kedirgantaraan dalam mendukung Indonesia Emas 2045 perlu melakukan beberapa langkah strategis. Antara lain penguatan ekosistem industri melalui kolaborasi pemerintah dengan swasta dan peningkatan investasi. Industri kedirgantaraan merupakan salah satu sektor yang memiliki urgensi terhadap teknologi informasi dan komunikasi. Oleh karena itu, keamanan siber menjadi sangat penting untuk melindungi aset-aset strategis dan informasi sensitif. Penelitian ini bertujuan untuk menyusun desain konseptual manajemen keamanan siber yang dapat diterapkan pada industri kedirgantaraan. Model ini dikembangkan berdasarkan analisis terhadap ancaman keamanan siber yang dihadapi oleh industri kedirgantaraan, serta best practice dan standar keamanan siber yang ada. Penelitian kualitatif ini menggunakan metode research and development menggunakan data primer dan sekunder. Hasil penelitian menunjukkan terdapat beberapa elemen sistem keamanan siber industri kedirgantaraan, antara lain stakeholder sistem keamanan siber yang terdiri atas pemerintah, industri, akademisi dan organisasi. Selain itu, terdapat pula tantangan dan fokus dari keamanan siber industri kedirgantaraan. Melalui desain konseptual sistem keamanan siber industri kedirgantaraan yang terbentuk, diharapkan dapat memberikan kontribusi pada pengembangan kebijakan dan strategi keamanan siber di industri kedirgantaraan.***

Kata Kunci— **Desain Konseptual, Keamanan Siber, Industri Kedirgantaraan**

**Chadziqatun Najilatil Mazda*
E-mail: mazdacha97@gmail.com

p-ISSN 2685-8991
e-ISSN 2808-2540

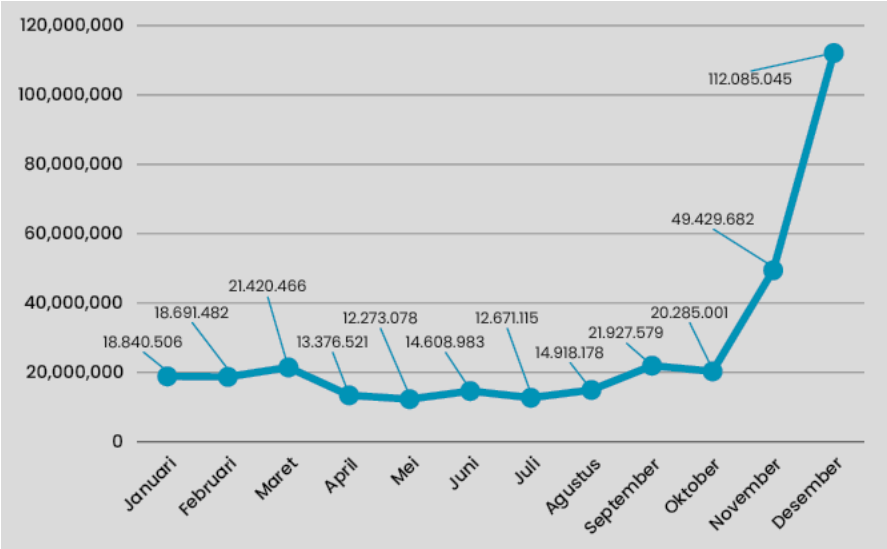
I. PENDAHULUAN

Indonesia memiliki misi abadi sebagai Negara yang merdeka, bersatu, berdaulat, adil dan makmur yang menjadi empat pilar Indonesia Emas 2045. Beberapa bagian yang menjadi sector pembangunan Indonesia adalah industrialisasi, sumber daya manusia, teknologi, infrastruktur, dan pendidikan [1]. Presiden Prabowo Subianto telah menetapkan delapan misi Asta Cita untuk mewujudkan visi "Bersama Indonesia Maju Menuju Indonesia Emas 2045". Pembangunan industri kedirgantaraan merupakan salah satu perwujudan pada misi kedua Asta Cita, yaitu untuk memantapkan sistem pertahanan keamanan Negara [2]. Industri kedirgantaraan juga menjadi sasaran dari program kerja meningkatkan jumlah anggaran pertahanan secara bertahap untuk memenuhi kekuatan optimal dan melakukan modernisasi Alat Utama Sistem Senjata TNI, serta mempercepat peningkatan kemampuan industri strategis nasional dalam memenuhi kebutuhan Alat Utama Sistem Senjata bagi TNI/ Polri.

Industri kedirgantaraan nasional memiliki visi menjadi industri kedirgantaraan yang tangguh dan berdaya saing menuju Indonesia Emas 2045. Terdapat empat pilar ekosistem industri kedirgantaraan, yaitu pesawat terbang, komponen dan rantai pasok, MRO dan jasa purna jual, serta jasa penerbangan dan kebandarudaraan. Industri kedirgantaraan memiliki prospek melalui nilai tambah domestik maupun devisa keluar. Tantangan utama industri kedirgantaraan adalah perubahan geopolitik dan geoekonomi yang mempengaruhi stabilitas rantai pasok, serta persaingan global yang ketat [2]. Manajemen industri kedirgantaraan dalam mendukung Indonesia Emas 2045 perlu melakukan beberapa langkah strategis. Antara lain penguatan ekosistem industri melalui kolaborasi pemerintah dengan swasta dan peningkatan investasi, membangun kemitraan strategis internasional dan aktif dalam inisiatif kedirgantaraan ASEAN untuk menciptakan pasar regional yang terintegrasi, dan meningkatkan penelitian dan pengembangan pada penguasaan teknologi kritis pesawat. Kemitraan strategis terbukti mampu meningkatkan kinerja industri dalam mencapai tujuan. Salah satunya adalah pada industri aluminium yang melibatkan kemitraan strategis industri bahan baku guna terpenuhinya kebutuhan alat peralatan pertahanan dan keamanan (Alpalhankam) [3].

Ekosistem penerbangan pada dasarnya terdiri dari sistem pemangku kepentingan yang kompleks, termasuk Maskapai Penerbangan, Bandara, Manajemen Lalu Lintas Udara, Manajemen Lalu Lintas Nirawak, dll. Sektor ini sedang mengalami transformasi digital besar-besaran dengan meningkatnya konektivitas dan ketergantungan antar-sektor. Akibatnya, ancaman siber baru dan pelanggaran keamanan bermunculan, yang membutuhkan pendekatan yang lebih holistik yang mencakup keamanan siber proaktif dan reaktif. Dampak insiden keamanan siber pada dasarnya bersifat finansial, di sektor penerbangan, insiden ini berpotensi memengaruhi aspek-aspek penting seperti operasional, kepatuhan, reputasi, atau bahkan keselamatan [4].

Pada tahun 2024, Indonesia memiliki lanskap keamanan siber yang cenderung meningkat dari Januari hingga Desember. Hal tersebut menunjukkan bahwa traffic serangan siber yang terjadi juga cenderung meningkat sehingga memerlukan desain sistem keamanan siber yang tepat. Adapun grafik trafik anomali siber di Indonesia disajikan pada gambar 1. sebagai berikut:



Gambar 1. Trafik Anomali Siber 2024

Berdasarkan gambar 1, total trafik anomali di Indonesia pada tahun 2024 adalah 330.527.636 anomali. Anomali trafik tertinggi terjadi pada bulan Desember dengan jumlah 112.085.045 anomali, sedangkan anomali terendah terjadi pada bulan Mei dengan jumlah 12.273.078 anomali. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi [5]. Industri penerbangan berpotensi menghadapi risiko keamanan siber tertinggi. Dipengaruhi oleh ketergantungan global pada teknologi dan komunikasi, keamanan siber rentan terhadap traffic anomali kejahatan siber yang meliputi gangguan IT, serangan malware/ransomware, pelanggaran data, serta denda dan penalti terkait. Industri penerbangan mengalami peningkatan serangan siber sebesar 24%, dengan 52 serangan dilaporkan pada tahun 2020, 48 serangan pada tahun 2021, dan 55 serangan pada tahun 2022. Beberapa serangan berkaitan dengan militer, sementara yang lain melibatkan metode pasif seperti pemindaian port, ping, dan pemantauan lalu lintas. Menurut TAC, 71% serangan melibatkan penyalahgunaan kredensial login dan infrastruktur IT yang tidak sah. Sementara itu, serangan DDoS yang menargetkan layanan daring maskapai penerbangan dan bandara mewakili 25% dari insiden siber. Insiden ini meningkat karena berbagai faktor, termasuk ketegangan geopolitik, peningkatan digitalisasi, dan meluasnya permukaan serangan [6].

Ketahanan infrastruktur dan keamanan siber dalam industri kedirgantaraan sangat penting karena kesalahan kecil atau kelalaian mengakibatkan berbagai kerusakan dan kerugian yang signifikan, misalnya kematian, hilangnya atau terungkapnya pemangku kepentingan, informasi identitas pribadi staf dan pelanggan, pencurian kredensial, kekayaan intelektual, dan intelijen [7]. Untuk membangun sistem keamanan siber diperlukan desain konseptual manajemen keamanan siber yang tepat. Penelitian tentang pemodelan sebelumnya pernah dilakukan oleh Prasetyo tahun yang menggunakan model Kano untuk mengembangkan inovasi produk pakan lele [8]. Sebuah model terbukti diperlukan dalam merepresentasikan sistemnyata. Penelitian ini, dimaksudkan untuk menyusun desain konseptual sistem keamanan siber pada industri kedirgantaraan.

p-ISSN 2685-8991
e-ISSN 2808-2540

II. LANDASAN TEORI

A. Pertahanan Siber

Berdasarkan Peraturan Menteri Pertahanan No 82 Tahun 2014 tentang Pedoman Pertahanan Siber menjelaskan bahwa pertahanan siber merupakan suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan Negara [9]. Pertahanan siber dilakukan untuk mengantisipasi datangnya ancaman dan serangan siber yang terjadi. Bentuk ancaman siber yang terjadi saat ini diantaranya.

a. Serangan *Advanced Persistent Threats* (APT), *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), biasanya dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Sehingga sistem menjadi terlalu sibuk dan crash, akibatnya menjadi tidak dapat melayani atau tidak dapat beroperasi. Permasalahan ini merupakan ancaman yang berbahaya bagi organisasi yang mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya.
b. Serangan *Defacement*, dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web korban sehingga isi dari halaman web korban berubah sesuai dengan motif penyerang.
c. Serangan *Phishing*, dilakukan dengan cara memberikan alamat website palsu dengan tampilan persis sama dengan website aslinya. Tujuan dari serangan *phishing* ini adalah untuk mendapatkan informasi penting dan sensitif seperti *username*, *password* dan lain-lain.
d. Serangan *Malware*, yaitu suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer. Biasanya program *malware* telah dirancang untuk mendapatkan keuntungan finansial atau keuntungan lain yang direncanakan. Jumlah serangan *malware* terus berkembang, sehingga saat ini telah menjadi pandemi yang sangat nyata. *Malware* telah terjadi dimana-mana dan mempengaruhi semua orang yang terlibat dalam setiap sektor kegiatan. Istilah virus generik digunakan untuk merujuk setiap program komputer berbahaya yang mampu mereproduksi dan menyebarkan dirinya sendiri.
e. Penyusupan siber, yang dapat menyerang sistem melalui identifikasi pengguna yang sah dan parameter koneksi seperti *password*, melalui eksploitasi kerentanan yang ada pada sistem.
f. Spam. Spam adalah pengiriman *e-mail* secara massal yang tidak dikehendaki dengan tujuan komersial, memperkenalkan perangkat lunak berbahaya, spam menyerupai serangan bom e-mail, dengan akibat mail server mengalami kelebihan beban, *mailbox user* penuh dan ketidaknyamanan dalam pengelolaan. Sebelumnya spam hanya dianggap sebagai gangguan, tapi saat ini e-mail spam merupakan ancaman nyata. Hal tersebut telah menjadi vektor istimewa untuk penyebaran virus, worm, trojans, *spyware* dan upaya *phishing*.
g. Penyalahgunaan Protokol Komunikasi. Sebuah serangan *spoofing Transmision Control Protocol* (TCP) bergantung pada kenyataan bahwa protokol TCP menetapkan koneksi logis antara dua ujung sistem untuk mendukung pertukaran data.

B. Desain Konseptual

Desain konseptual adalah tahap awal dari proses desain yang berfokus pada pengembangan ide-ide tingkat tinggi dan kerangka kerja strategis untuk sebuah proyek. Pada fase desain konseptual ini terdapat aktivitas mengubah gagasan awal menjadi sebuah cetak biru yang mendefinisikan masalah, tujuan, dan visi keseluruhan, sebelum merinci detail teknis yang

spesifik. Tujuannya adalah untuk menciptakan landasan yang koheren dan selaras dengan tujuan yang ditetapkan organisasi maupun perusahaan, baik untuk produk, layanan, atau sistem yang kompleks.

Dalam industri produk, desain konseptual adalah *framework* yang sering digunakan. Biasanya digunakan pada tahap awal proses desain, membantu mengembangkan ide dan konsep utama. Tujuan dari desain konseptual adalah untuk menghasilkan model konseptual untuk domain yang diselidiki. Maps perjalanan pengguna, blueprints layanan, model objek, dan model entitas adalah model konseptual yang biasa digunakan untuk mengeksplorasi dan mengembangkan ide serta sebagai dokumentasi setelah dirancang. Strategi, ruang lingkup, dan struktur elemen Garrett dari model UX dibahas dalam desain konseptual ini. Ini juga membahas tujuan layanan atau sistem, tujuan konten, dan fungsi yang akan dimiliki layanan atau sistem, serta desain interaksi dan arsitektur informasi [10]. Tahap penyusunan desain konseptual adalah sebagai berikut:

a. Menentukan tujuan utama desain konseptual

   Untuk menentukan tujuan utama desain konseptual, desainer dan tim harus mengetahui alasan di balik pembentukannya. Tujuan utama dapat ditentukan dengan menetapkan target atau pencapaian yang ingin tercapai dari desain konseptual yang terbentuk, serta sasaran user / pengguna desain tersebut.

b. Melakukan riset desain

   Riset desain berkaitan dengan unsur-unsur atau elemen-elemen yang melekat pada user / pengguna desain konseptual. Termasuk pula berkaitan dengan sifat-sifat, nilai-nilai dan maupun karakter dari unsur-unsur yang berkaitan.

c. *Verbal Ideation*

   Verbal ideation ini adalah tahap komunikasi dalam proses desain konseptual. Pada tahap ini bisa dilakukan dengan wawancara, *focus group discussion,* maupun *brainstorming* untuk memperoleh informasi yang diperlukan dalam penyusunan desain konseptual.

d. *Visual Ideation*

   Pada tahap ini ide dan informasi yang diperoleh dituangkan dalam rancangan desain baik berupa gambar, diagram, maupun jenis desain lainnya.

C. Pemodelan Sistem

Proses membuat sebuah model sistem disebut pemodelan. Model adalah representasi dari bentuk nyata [11]. Sistem adalah hubungan antar elemen yang membentuk sebuah kesatuan yang biasanya dibangun untuk mencapai tujuan tertentu. Sistem, yang berasal dari kata "*systēma*" dalam bahasa Latin dan "*sustēma*" dalam bahasa Yunani, berarti suatu kesatuan yang terdiri dari komponen atau elemen yang dihubungkan menjadi satu untuk memudahkan aliran informasi, materi, atau energi untuk mencapai tujuan tertentu.

Sebelum sistem diterapkan di lapangan, tujuan pemodelan adalah untuk melakukan analisis dan membuat prediksi yang sebanding dengan kenyataan. Jika model dapat memformulasikan sebuah proses tertentu tetapi tidak memungkinkan untuk melakukan analisis untuk mendapatkan solusi yang tepat, maka perlu dilakukan lagi perbandingan atau validasi antara pemodelan matematik dengan kondisi lapangan. Hal tersebut akan menjadi masalah untuk memprediksi dan mengamati proses tertentu pada lapangan [12].

p-ISSN 2685-8991
e-ISSN 2808-2540

III. METODE

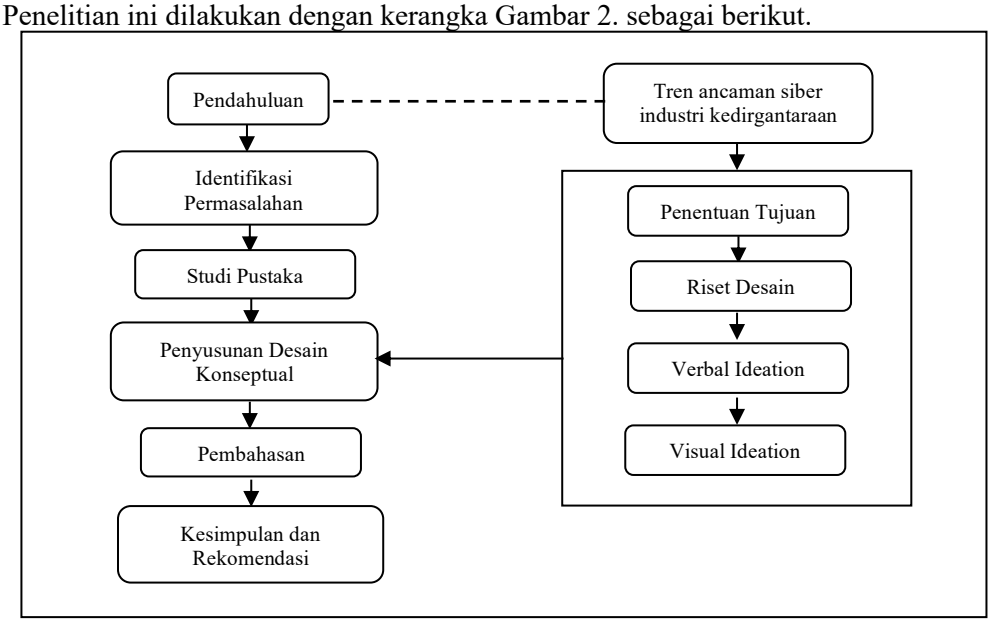
A. *Jenis Penelitian*

Jenis penelitian ini adalah kualitatif. Peneliti menggunakan jenis penelitian *research and development* (RnD) untuk membentuk desain konseptual yang tepat pada sistem keamanan siber Industri Kedirgantaraan. Data yang digunakan adalah data primer dan sekunder. Data primer adalah data yang diperoleh secara langsung melalui observasi dan wawancara. Data primer diperoleh pada pengamatan langsung pada 28 Agustus 2025. Adapun data sekunder adalah data yang diperoleh dari sumber kedua baik berupa landasan hukum, buku, jurnal, maupun berita yang berkaitan dengan siber dan industri kedirgantaraan.

Data yang telah terkumpul dilakukan keabsahan data menggunakan triangulasi metode, yaitu membandingkan informasi yang diperoleh dari sumber yang satu dengan sumber lainnya. Selanjutnya, data yang sudah valis digunakan sebagai landasan dalam menyusun desain konseptual sistem keamanan siber pada industri kedirgantaraan. Desain konseptual yang terbentuk kemudian dianalisis dan dibahas berdasarkan perspektif keamanan siber industri kedirgantaraan untuk ditarik kesimpulan dan rekomendasi penelitian.

B. *Diagram Alir Penelitian*

Penelitian ini dilakukan dengan kerangka Gambar 2. sebagai berikut.



Gambar 2. Diagram alir penelitian

IV. HASIL DAN PEMBAHASAN

A. *Desain Konseptual*

Desain konseptual sistem keamanan siber pada industri kedirgantaraan berarti keterikan antar elemen-elemen dalam sebuah sistem yang bertujuan untuk menciptakan keamanan siber pada industri kedirgantaraan. Penyusunan desain konseptual dilakukan dengan langkah-langkah strategis sebagai berikut:

1. Menentukan tujuan utama

Tujuan utama penyusunan desain konseptual sistem keamanan siber pada industri kedirgantaraan adalah membentuk suatu desain konseptual yang menampilkan sistem keamanan siber di industri kedirgantaraan, meliputi elemen-elemen sistem dan dan interaksi yang terjadi di dalamnya. Sasaran dari terbentuknya sistem tersebt adalah keamanan siber industri kedirgantaraan.

2. Melakukan riset desain

   Penyusunan desain konseptual sistem keamanan siber pada industri kedirgantaraan melibatkan beberapa elemen sistem keamanan siber, antara lain sebagai berikut:

   a. Stakeholder keamanan siber kedirgantaraan

      Stakeholder sistem keamanan siber pada industri kedirgantaraan meliputi:

      - Pemerintah Indonesia, melalui lembaga seperti Kementerian Badan Usaha Milik Negara (BUMN), Badan Siber dan Sandi Negara (BSSN), Kementerian Pertahanan, dan Kementerian Komunikasi dan Digital (Komdigi).
      - Industri, yaitu perusahaan yang bergerak di industri kedirgantaraan, seperti PT Dirgantara Indonesia, PT INTI, PT Len, PT Yogya Presisi Teknikatama Industri (YPTI), dan startup teknologi kedirgantaraan.
      - Akademisi, yaitu universitas dan lembaga penelitian seperti Insititut Teknologi Bandung, Politeknik SSN, Universitas Pertahanan, Universitas Nurtanio Bandung melalui Unnur Aero Maintenance Training Center (UAMTC), Universitas Dirgantara Marsekal Suryadarma (UnSurya) yang bekerja sama dengan Pusat Studi Air Power Indonesia (PSAPI), Universitas Jenderal Achmad Yani, Akademi Angkatan Udara dan lembaga pendidikan lainnya.
      - Komunitas Organisasi seperti Indonesia *Computer Emergency Response Team* (ID-CERT), Indonesia *Cyber Security Forum* (ICSF), Asosiasi Digitalisasi dan Keamanan Siber Indonesia (ADIGSI), Indonesia Network Security Association (IdNSA), Computer Security Incident Response Team (CSIRT) Indonesia, Penyelenggara Sistem Elektronik (PSE) Penerbangan, Ethical Hacker Indoensia, maupun industri jasa konsultan.

   b. Fokus keamanan siber kedirgantaraan

      - Fokus Industri Kedirgantaraan

        Pada industri kedirgantaraan, system keamanan siber dilakukan secara keseluruhan, dan lebih diutamkan pada bagian-bagian yang bersifat krusial, seperti pada database, desain, mesin, material, sdm, panduan, dll. Bagian tersebut memerlukan keamanan siber terkait sistem deteksi intruksi untuk melindungi infrastruktur kedirgantaraan, teknologi anti-*jamming* untuk melindungi komponen maupun alat komunikasi, serta protokol autentikasi untuk keamanan ruang udara.

      - Fokus teknologi keamanan siber

        Sistem keamanan siber dalam industri kedirgantaraan memerlukan kombinasi teknologi canggih untuk melindungi sistem kritis, data sensitive. Teknologi tersebut antara lain sebagai berikut:

        i. Enkripsi Data, untuk melindungi data sensitif, baik yang sedang dikirim maupun disimpan (data *at rest* dan *in transit*) dari akses tidak sah.

        ii. *Firewall* dan Keamanan Jaringan, digunakan untuk mengontrol dan memfilter lalu lintas jaringan antara sistem kedirgantaraan yang berbeda (misalnya, jaringan operasional dan jaringan TI perusahaan), mencegah akses yang tidak sah dan serangan siber dari luar.

p-ISSN 2685-8991
e-ISSN 2808-2540

iii. Autentikasi dan Otorisasi Pengguna (*Identity and Access Management - IaM*), untuk memastikan bahwa hanya personel yang berwenang yang dapat mengakses sistem dan data kritis, seperti kontrol lalu lintas udara (ATC) atau sistem kontrol pesawat.

iv. Pemantauan dan Deteksi Ancaman *Real-time*, digunakan untuk menggunakan alat pemantauan dan manajemen keamanan dalam mendeteksi aktivitas mencurigakan atau serangan siber secara langsung. Termasuk sistem peringatan dini untuk mengidentifikasi potensi pelanggaran keamanan.

v. *Artificial Intelligence* (AI) dan *Mechine Learning* (ML), kolaborasi AI dan ML dapat membantu mengotomatisasi deteksi ancaman, menganalisis data dalam jumlah besar, mengidentifikasi pola serangan siber, dan merespons insiden keamanan dengan cepat.

vi. Manajemen Kerentanan dan Pengujian Penetrasi (*Vulnerability Management and Penetration Testing*), digunakan untuk melakukan penilaian kerentanan dan pengujian penetrasi secara berkala untuk mengidentifikasi dan memperbaiki kelemahan keamanan sebelum dieksploitasi oleh penyerang.

vii. *Antimalware* dan Antivirus, yaitu perangkat lunak yang mendeteksi, mencegah, dan menghapus perangkat lunak berbahaya (*malware*) yang dapat menginfeksi sistem komputer dan jaringan di seluruh ekosistem kedirgantaraan.

viii. Pencadangan dan Pemulihan Data (*Backup and Disaster Recovery*), digunakan untuk cadangan data yang aman dan rencana pemulihan bencana untuk memastikan kelangsungan operasional jika terjadi serangan siber atau kehilangan data.

ix. Intelijen Ancaman (*Threat Intelligence*), digunakan untuk mendapatkan informasi terkini tentang ancaman siber yang muncul dan kerentanan spesifik industri kedirgantaraan untuk proaktif dalam pertahanan siber.

x. Keamanan Operasional Teknologi (OT), peran penting dari Teknologi Operasional membuat perlindungan terhadap sistem ini sangat penting untuk mencegah gangguan operasional.

c. Tantangan keamanan siber industri kedirgantaraan

Industri kedirgantaraan masih memiliki beberapa tantangan dalam mewujudkan

- Sumber daya manusia yang meliputi kebutuhan talenta digital yang besar.
- Aspek regulasi, belum ada undang-undang tunggal yang mengatur keamanan siber di Indonesia.
- Pada aspek teknologi masih diperlukan pengembangan industri lokal untuk mengurangi ketergantungan pada pemasok asing

3. Verbal *ideation*

Verbal ideation menunjukkan rancangan ide desain konseptual yang diusulkan. Pada tahap ini dijelaskan mengenai berjalannya siklus desain konseptual yang disusun. Desain konseptual keamanan siber industri kedirgantaraan disusun untuk menyusun keamanan siber pada industri kedirgantaraan yang memiliki 2 fokus utama, yaitu fokus industri kedirgantaraan dan fokus teknologi keamanan siber. Keterkaitan beberapa elemen dalam desain konseptual sistem keamanan siber pada industri kedirgantaraan di Indonesia merupakan kolaborasi multifaset yang krusial untuk menjaga keamanan dan kedaulatan nasional. Pemerintah Indonesia, melalui Kementerian/Lembaga seperti Kementerian

Badan Usaha Milik Negara (BUMN), Badan Siber dan Sandi Negara (BSSN), berperan sebagai regulator dan pengarah strategi keamanan siber industri kedirgantaraan, bekerja sama dengan Kementerian Pertahanan dan Kementerian Komunikasi dan Digital (Komdigi) untuk menetapkan kebijakan yang relevan dengan industri kedirgantaraan. Pelaku usaha, seperti PT Dirgantara Indonesia, PT INTI, PT LEN, PT YPTI maupun perusahaan teknologi kedirgantaraan lainnya, menjadi implementor utama yang mengembangkan dan mengoperasikan sistem keamanan siber untuk melindungi infrastruktur kritis seperti sistem komunikasi udara dan kontrol lalu lintas penerbangan.

Akademisi dari universitas seperti Insititut Teknologi Bandung, Politeknik SSN, Universitas Pertahanan, Universitas Nurtanio Bandung melalui Unnur Aero Maintenance Training Center (UAMTC), Universitas Dirgantara Marsekal Suryadarma (UnSurya) yang bekerja sama dengan Pusat Studi Air Power Indonesia (PSAPI), Universitas Jenderal Achmad Yani, Akademi Angkatan Udara dan lembaga pendidikan lainnya yang memberikan kontribusi signifikan melalui penelitian dan pengembangan doktrin, seperti Air Power Generasi Keenam, yang mengintegrasikan aspek keamanan siber dalam strategi kedirgantaraan. Selain itu, komunitas seperti Indonesia Computer Emergency Response Team (ID-CERT) dan Indonesia Cyber Security Forum (ICSF) berperan dalam pertukaran informasi dan peningkatan kesadaran keamanan siber.

4. Visual *ideation*

Pada tahap ini dilakukan visualisasi ide dan informasi yang diperoleh ke dalam rancangan desain berupa gambar. Pada desain konseptual sistem keamanan siber pada industri kedirgantaraan, kolaborasi Quad Helix yang melibatkan pemerintah, industri, akademisi, dan komunitas menjadi pendekatan strategis untuk memperkuat ekosistem keamanan siber kedirgantaraan Indonesia, dengan tujuan meningkatkan ketahanan terhadap ancaman siber dan mengembangkan industri lokal yang berdaya saing global terutama dalam mewujudkan misi industri kedirgantaraan pada Indonesia Emas 2045. Sinergi ini penting untuk menghadapi tantangan seperti kebutuhan sumber daya manusia yang mumpuni, regulasi yang adaptif, dan pengembangan teknologi indigenous demi kedaulatan dan keamanan nasional. Desain konseptual sistem keamanan siber pada industri kedirgantaraan melalui kolaborasi *Quad Helix* dapat digambarkan sebagai berikut:

Gambar 3. Desain Konseptual Sistem Keamanan Siber Industri Kedirgantaraan

p-ISSN 2685-8991
e-ISSN 2808-2540

Gambar di atas menunjukkan bahwa desain konseptual sistem keamanan siber industri kedirgantaraan memiliki beberapa fokus seperti fokus pada database, desain, mesin, material, SDM, panduan dan lain-lain. Sistem tersebut memiliki sejumlah ancaman seperti APT, Dos, DDos, defacement, malware, ransomware, phissing, dan lain-lain. Di Indonesia, sistem keamanan siber juga menghadapi tantangan berupa kesiapan dari sumber daya manusia (SDM) yang ahli di bidang siber, kesiapan teknlogi keamanan siber, serta regulasi keamanan siber yang belum memiliki Undang-Undang Keamanan dan Ketahanan Siber sebagai payung hukum yang sah.

Desain konseptual sistem keamanan siber industri kedirgantaraan melibatkan kolaborasi *Quad Helix* terdiri atas pemerintah, industri, perguruan tinggi dan organisasi. Dalam pelaksanaannya, diperlukan sinergi dan kolaborasi yang kuat antar stakeholder, serta peningkatan teknologi pertahanan siber yang diperlukan oleh industri kedirgantaraan, seperti *threat intelligence, firewall,* enkripsi data, *Identity and Access Management* (IaM), pemantauan dan deteksi *real time*, operational technology (*OT)*, *vulnerability management and penetration testing,* dan *back up technology.*

B. Pembahasan

Keamanan siber industri kedirgantaraan memiliki peran krusial dalam mewujudkan visi industri kedirgantaraan nasional yang tangguh dan berdaya saing menuju Indonesia Emas 2045. Di era digital ini, di mana sistem penerbangan sangat terhubung dan bergantung pada data, keamanan siber menjadi fondasi utama untuk melindungi infrastruktur kritis, data sensitif, dan keselamatan operasional. Sistem keamanan siber yang kuat akan meminimalisir risiko serangan siber yang dapat mengganggu operasional industri kedirgantaraan, membahayakan keselamatan personal, atau bahkan mencuri data rahasia teknologi maupun desain pesawat yang krusial bagi daya saing industri nasional.

Industri kedirgantaraan merupakan salah satu sektor kritikal yang sangat bergantung pada sistem teknologi informasi dan komunikasi yang kompleks. Ancaman siber terhadap industri kedirgantaraan semakin meningkat, mencakup potensi serangan terhadap sistem kontrol pesawat, jaringan komunikasi penerbangan, serta data sensitif terkait operasional dan keamanan. Oleh karena itu, desain konseptual sistem keamanan siber yang robust menjadi sangat penting untuk melindungi aset-aset vital industri ini dari ancaman seperti peretasan, malware, dan serangan *denial-of-service* yang dapat berakibat fatal terhadap keselamatan dan integritas data.

Desain konseptual sistem keamanan siber pada industri kedirgantaraan harus mempertimbangkan aspek-aspek seperti arsitektur jaringan yang aman, enkripsi data, mekanisme autentikasi yang kuat, serta kemampuan deteksi dan respons terhadap insiden siber. Selain itu, kolaborasi antara berbagai stakeholder termasuk regulator, operator penerbangan, dan penyedia teknologi juga krusial untuk memastikan implementasi keamanan siber yang efektif. Dengan pendekatan proaktif dan desain konseptual yang matang, industri kedirgantaraan dapat meningkatkan ketahanan terhadap ancaman siber dan menjaga keselamatan operasional penerbangan di tengah tantangan keamanan digital yang terus berkembang.

Dalam desain konseptual sistem keamanan siber industri kedirgantaraan, terdapat beberapa elemen kunci yang berperan penting dalam menjaga keamanan dan ketahanan sistem. Salah satu elemen vital adalah stakeholder sistem keamanan siber yang terdiri atas pemerintah, industri, akademisi, dan organisasi terkait. Pemerintah berperan dalam regulasi dan kebijakan, industri sebagai pelaksana dan pengembang teknologi, akademisi yang berkontribusi dalam penelitian dan inovasi, serta organisasi yang mendukung koordinasi dan implementasi. Selain itu, industri kedirgantaraan juga menghadapi tantangan seperti kompleksitas sistem yang tinggi, interoperabilitas teknologi, ancaman siber yang terus berkembang, dan kebutuhan akan kepatuhan terhadap standar keamanan. Fokus utama keamanan siber dalam konteks ini mencakup perlindungan data kritikal, pengamanan sistem kontrol penerbangan, deteksi dini ancaman, serta

peningkatan kesadaran dan kapasitas sumber daya manusia dalam menghadapi dinamika ancaman siber yang terus berubah. Semua elemen sistem keamanan siber industri kedirgantaraan harus saling berkolaborasi dan bersinergi. Pada tingkat industri pertahanan nasional, pentingnya kolaborasi terbukti mampu mewujudkan ekosistem industri pertahanan yang kuat dan solid [13].

V. KESIMPULAN

Manajemen industri kedirgantaraan dalam mendukung Indonesia Emas 2045 perlu melakukan beberapa langkah strategis. Antara lain penguatan ekosistem industri melalui kolaborasi pemerintah dengan swasta dan peningkatan investasi. Industri kedirgantaraan merupakan salah satu sektor yang memiliki urgensi terhadap teknologi informasi dan komunikasi. Oleh karena itu, keamanan siber menjadi sangat penting untuk melindungi aset-aset strategis dan informasi sensitif.

Desain konseptual keamanan siber industri kedirgantaraan disusun untuk menyusun keamanan siber pada industri kedirgantaraan yang memiliki 2 fokus utama, yaitu fokus industri kedirgantaraan dan fokus teknologi keamanan siber. Terdapat beberapa elemen sistem keamanan siber industri kedirgantaraan, antara lain stakeholder sistem keamanan siber yang terdiri atas pemerintah, industri, akademisi dan organisasi. Selain itu, terdapat pula fokus dan tantangan dari keamanan siber industri kedirgantaraan. Melalui desain konseptual sistem keamanan siber industri kedirgantaraan yang terbentuk, diharapkan dapat memberikan kontribusi pada pengembangan kebijakan dan strategi keamanan siber di industri kedirgantaraan.

Kolaborasi Quad Helix pada desain konseptual sistem keamanan siber industri kedirgantaraan yang terbentuk, melibatkan pemerintah, industri, akademisi, dan komunitas sebagai stakeholder dalam pendekatan strategis untuk memperkuat ekosistem keamanan siber kedirgantaraan Indonesia, dengan tujuan meningkatkan ketahanan terhadap ancaman siber dan mengembangkan industri lokal yang berdaya saing global terutama dalam mewujudkan misi industri kedirgantaraan pada Indonesia Emas 2045. Rekomendasi yang dapat peneliti berikan hendaknya pemerintah bisa mengesahkan RUU Keamanan dan Ketahanan Siber sebagai payung hukum yang kuat dalam pengaturan dan pengimplementasian sistem keamanan siber, termasuk keamanan siber di industri kedirgantaraan.

UCAPAN TERIMA KASIH

Atas berlangsungnya penelitian ini, peneliti mengucapkan terimakasih kepada Akademi Angkatan Udara (AAU) yang telah menyelenggarakan SENASTINDO 7 di Yogyakarta, pada 27 November 2025 dan ITSEC Cyber Security Summit 2025 yang secara tidak langsung memfasilitasi berjalannya penelitian pada 26-28 Agustus 2025 di Ritz Carlton-Pacific Place, Jaarta Selatan.

REFERENSI

[1] Mazda, Chadziqatun Najilatil; Nurhayati, Ema; Putra, Rivaldi Ananda Dwi. Study Behaviour of Prabowo Subianto's Leadership as the President of Indonesia. *Southeast Asia Development Research*, 2025, 1.2: 25-36.

[2] Kementerian PPN/ Bappenas, *Peta Jalan Pengembangan Ekosistem Industri Kedirgantaraan Indonesia 2022-2045.* Jakarta: Kementerian PPN/ Bappenas.

[3] Mazda, Chadziqatun Najilatil, et al. *Kemitraan Strategis Industri Aluminium Dalam Memenuhi Kebutuhan Bahan Baku Alat Peralatan Pertahanan Dan Keamanan (Alpalhankam)*. 2024. PhD Thesis. UIN Sunan Kalijaga Yogyakarta.

[4] (2025). Thales Group. [Online]. Available: https://www.thalesgroup.com/en/markets/aerospace/air-traffic-management/cybersecurity-aerospace.

p-ISSN 2685-8991
e-ISSN 2808-2540

[5] Badan Siber Dan Sandi Negara, *Lanskap Keamanan Siber Indonesia 2024*, Jakarta: BSSN, 2024.
[6] (2025). Airways Magazine. [Online]. Available: https://www.airwaysmag.com/new-post/aviation-cybersecurity-threats-in-2025.
[7] E. Ukwandu, M. A. B. Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andovonic, and X. Bellecen, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends", *Information,* vol. 13, no. 3, pp. 1-22, 2022.
[8] M. A. Prasetyo, C. N. Mazda, T. Aji, dan K. Dwijayanti, "Design Development of Catfish Chips using the Kano Model and Quality Function Deployment (QFD) at the Pelemadu Rempeyek Industrial Center", in *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 2024, pp. 2360-2369.
[9] Peraturan Menteri Pertahanan No 82 Tahun 2014 tentang Pedoman Pertahanan Siber.
[10] (2023). BINUS University. [Online]. Available at: https://sis.binus.ac.id/2023/08/02/apa-itu-desain-konseptual/.
[11] C. N. Mazda, D. A. Kurniawati, dan M. W. Musthofa, "Optimasi Keuntungan Digital preneur Hampers Minuman Menggunakan Aplikasi CPLEX", in *Proceedings of the National Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media*, 2023, Vol. 3, No. 1, pp. 215-220.
[12] Suradi, *Pemodelan Sistem (Sebuah Pengantar)*. Makassar: CV Tohar Media, 2022.
[13] Mazda, Chadziqatun Najilatil; Perdana, Yandra Rahadian; Jupriyanto. The Alliance Strategy in Supply Chain Management of Indonesia's Defense Industry. In: *Global Congress on Manufacturing and Management*. Cham: Springer Nature Switzerland, 2023. p. 80-87. https://doi.org/10.1007/978-3-031-80341-3_7.