



UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA “GIORGIO FUÀ”

Corso di Laurea Triennale in Economia e Commercio

RISK MANAGEMENT NELL'INDUSTRIA
AVIATION/AEROSPACE

Caso studio: Leonardo S.p.A. e CTNA

RISK MANAGEMENT IN THE
AVIATION/AEROSPACE INDUSTRY

Case study: Leonardo S.p.A. and CTNA

Relatore: Chiar.mo
Prof. Attilio Mucelli

Rapporto Finale di:
Andrea Dipaolo

Anno Accademico 2025/2026

Indice

Introduzione	3
Capitolo I – L’industria <i>aviation</i> / <i>aerospace</i> e i rischi del settore.....	4
1.1 Inquadramento e caratteristiche del settore.....	4
1.2 La filiera produttiva e i principali attori	7
1.3 Quadro generale dei rischi d’impresa nell’ <i>aviation/aerospace</i>	10
Capitolo 2 – I nuovi rischi nell’industria <i>aviation/aerospace</i>.....	16
2.1 <i>Cybersecurity</i> e rischi informatici	16
2.2 Intelligenza artificiale e nuovi profili di rischio.....	20
2.3 Supply chain globale e rischi operativi	23
2.4 <i>Business continuity</i>	26
Capitolo 3 – Il caso Leonardo S.p.A. e CTNA.....	28
3.1 Il ruolo di Leonardo nello sviluppo della rete CTNA.....	28
3.2 Il CTNA come piattaforma di supporto alla filiera aerospaziale.....	29
3.3 Dalla valorizzazione della rete al vantaggio competitivo.....	31
Conclusioni	34
Bibliografia	35
Sitografia	37
Ringraziamenti	38

INTRODUZIONE

L'industria *aviation/aerospace* rappresenta uno dei settori più rilevanti a livello globale, sia per il valore economico generato sia per il ruolo strategico che ricopre. La sua peculiarità risiede nell'integrazione tra tecnologia avanzata, requisiti di sicurezza e logiche industriali complesse. Essa svolge un ruolo fondamentale non solo per la mobilità di persone e merci, ma anche per la difesa nazionale, la ricerca scientifica e lo sviluppo tecnologico. Le imprese che operano in questo ambito si trovano a gestire un contesto articolato, in cui il rischio non è un elemento accessorio ma una componente strutturale delle decisioni aziendali.

Negli ultimi decenni, il settore è stato interessato da profondi mutamenti strutturali, legati alla globalizzazione dei mercati, alla digitalizzazione dei processi produttivi e all'emergere di nuove minacce di natura tecnologica, economica e geopolitica. In questo scenario, il rischio non può più essere letto in modo limitato ai soli aspetti operativi o finanziari, ma deve essere considerato in una prospettiva più ampia, che include anche fattori esterni e dinamiche di interdipendenza lungo la filiera. Il primo capitolo ha l'obiettivo di fornire un quadro introduttivo del settore, analizzandone le caratteristiche strutturali, la filiera produttiva e le principali tipologie di rischio. Tale analisi costituirà la base per l'approfondimento del *risk management assicurativo* con i nuovi rischi emergenti legati alla *cybersecurity*, all'intelligenza artificiale, alla *supply chain* e alla *business continuity* (Capitolo 2) e per un approfondimento delle dinamiche aziendali in Italia (Capitolo 3).

CAPITOLO I

L'INDUSTRIA AVIATION/ AEROSPACE E I RISCHI DEL SETTORE

1.1 Inquadramento e caratteristiche del settore

L'industria *aviation/aerospace* si distingue per un elevato grado di complessità, dovuto all'integrazione di processi produttivi avanzati, filiere globali e requisiti normativi particolarmente stringenti. Con il termine *industria aerospaziale e aviation* si fa riferimento all'insieme delle attività legate alla progettazione, produzione, manutenzione e commercializzazione di aeromobili civili e militari, sistemi spaziali, satelliti, veicoli di lancio, droni e relativi componenti e servizi.

A livello globale, il settore aerospaziale e dell'aviazione ha registrato una significativa ripresa dopo la crisi legata alla pandemia da COVID-19. Secondo recenti analisi di settore, nel 2024 i ricavi globali dell'industria aerospaziale hanno superato gli 850–900 miliardi di dollari, sostenuti principalmente dalla ripresa del traffico aereo commerciale, dall'aumento degli ordini di nuovi aeromobili e dalla crescita della spesa nel comparto difesa.¹

Il comparto comprende diverse macroaree:

- aviazione civile (aerei di linea, regionali, business jet);
- difesa e aeronautica militare;
- spazio e *space economy* (satelliti, osservazione della Terra, telecomunicazioni, lanciatori);
- servizi di manutenzione, riparazione e revisione (MRO).

Negli ultimi anni, la crescente integrazione tra ambito aeronautico e spaziale ha favorito la diffusione del concetto di “Aerospace & Defense (A&D)”, ormai

¹ Deloitte Insight, Prospettive sull'industria aerospaziale e della difesa, Centro di Ricerca Deloitte per l'Energia e l'Industria, 2025

ampiamente utilizzato sia a livello industriale sia nelle analisi economiche. Un elemento distintivo del settore è la struttura della filiera produttiva, che si sviluppa su più livelli ed è composta da attori altamente specializzati, tra loro fortemente interdipendenti, organizzata su più livelli (*tier*). Al vertice si collocano i prime contractor o OEM (*Original Equipment Manufacturer*), come Airbus, Boeing, Leonardo, Lockheed Martin, responsabili dell'integrazione finale dei sistemi complessi. A questi si affianca una rete estesa di fornitori di primo, secondo e terzo livello, spesso costituita da PMI altamente specializzate.²

Tabella 1 – I numeri dell'industria aerospaziale italiana³



Fonte: Osservatorio iCRIBIS sull'industria aerospaziale italiana, 2023

La dipendenza reciproca tra gli attori della filiera rende il settore particolarmente sensibile a interruzioni nelle catene di approvvigionamento, carenze di manodopera qualificata e difficoltà di coordinamento internazionale, elementi che incidono in modo diretto sui costi e sui tempi di produzione⁴.

Intensità tecnologica e investimenti in R&S: Il settore aerospaziale è tra quelli con la maggiore intensità di ricerca e sviluppo. In media, le imprese del comparto

² UHY LLP, *Aerospace Industry Market Analysis*, 2025

³ CRIBIS, *I numeri dell'industria aerospaziale italiana*, 2025

⁴ McKinsey & Company, *Affrontare la turbolenza continua: la catena di approvvigionamento commerciale-aerospaziale 2024* | Articolo

investono tra il 5% e il 10% del fatturato in R&S, percentuale superiore a quella di molti altri settori manifatturieri. Tali investimenti sono fondamentali per garantire:

- elevati standard di sicurezza;
- innovazione tecnologica (materiali compositi, digitalizzazione, intelligenza artificiale);
- riduzione dell'impatto ambientale;
- sviluppo di nuove piattaforme e servizi⁵ (eVTOL, *urban air mobility*, *space economy*).

L'innovazione è inoltre fortemente influenzata dalla cooperazione pubblico-privata, con un ruolo centrale svolto da governi e agenzie spaziali nazionali e sovranazionali (NASA, ESA).

Dal punto di vista macroeconomico, l'industria *aviation/aerospace* è un importante moltiplicatore di valore, in grado di attivare occupazione diretta e indiretta lungo l'intera filiera. A livello globale, il settore sostiene decine di milioni di posti di lavoro e contribuisce in modo significativo al commercio internazionale, in particolare nel trasporto aereo di merci ad alto valore aggiunto.⁵

In Italia, il comparto aerospaziale rappresenta un settore strategico del manifatturiero avanzato, con un fatturato compreso tra 13 e 19 miliardi di euro, oltre 50.000 addetti diretti e una forte prevalenza di PMI, affiancate da grandi gruppi industriali integrati nei programmi europei e internazionali.

Prime implicazioni in termini di rischio settoriale: Le caratteristiche strutturali descritte – elevata complessità tecnologica, dipendenza dalla filiera globale, ciclicità della domanda e forte regolamentazione – rendono il settore *aviation/aerospace* particolarmente esposto a rischi industriali, finanziari e geopolitici, che verranno analizzati nei paragrafi successivi. In particolare,

⁵ Accenture, *Navigating uncertain skies Commercial Aerospace Insight Report*, 2025

assumono rilievo i rischi legati alla volatilità della domanda, ai vincoli regolatori, alle tensioni geopolitiche e alla sostenibilità ambientale.⁶

L'industria aerospaziale dimostra fondamentali solidi nonostante i vincoli operativi. Diverse metodologie di ricerca producono proiezioni variabili, ma tutte indicano una crescita sostanziale:

Tabella 2 – numeri del mercato⁷

Segmento di mercato	Valore 2024	Valore 2025	Valore previsto per il 2030	CAGR	Fonte
Mercato globale A&D	885,20 miliardi di dollari	846,94 miliardi di dollari	1,3 trilioni di dollari	8.2-8.64%	Ricerca di mercato Zion
Produzione aerospaziale	N/A	789,25 miliardi di dollari	900+ miliardi di dollari	2.76%	Statista
Industria A&D USA	N/A	995 miliardi di dollari	1,2 trilioni di dollari	N/A	AIA <i>Aerospace</i>
Aerospaziale commerciale	322,77 miliardi di dollari	340,04 miliardi di dollari	420,06 miliardi di dollari	5.3%	Ricerca e Mercati

Fonte: Economia dello Spazio Magazine, *crescita del comparto aerospaziale italiano, 2025*

L'industria aerospaziale e della difesa statunitense ha contribuito con 443 miliardi di dollari in valore economico,⁸ 257 miliardi di dollari in reddito del lavoro e ha mantenuto un surplus commerciale di 73,86 miliardi che sottolinea la posizione di leadership globale degli Stati Uniti.

1.2 La filiera produttiva e i principali attori

La filiera produttiva dell'industria *aerospace* in Italia si configura come un sistema articolato e multilivello, caratterizzato da una forte integrazione tra grandi

⁶ PwC, *2025 Aviation Industry Review and Outlook*

⁷ Economia dello Spazio Magazine, *Cristina Leone al 3° Forum Space&Blue: crescita del comparto aerospaziale italiano, 2025*

⁸ The Business Research Private Ltd, *Rapporto sul mercato aerospaziale e della difesa 2026*

imprese, fornitori specializzati, piccole e medie imprese, centri di ricerca e istituzioni pubbliche. A differenza di altri settori manifatturieri, essa non segue una logica lineare, bensì si sviluppa come un ecosistema complesso in cui i diversi attori operano in modo interdipendente, contribuendo con competenze altamente specializzate alla realizzazione di sistemi tecnologicamente avanzati.

Al vertice della filiera si collocano i prime contractor, ovvero grandi gruppi industriali responsabili della progettazione, integrazione e gestione di programmi complessi. In Italia, tra i principali attori si distinguono Leonardo, Thales Alenia Space, Avio e Telespazio. In particolare, Leonardo rappresenta il fulcro industriale del sistema *aerospace* nazionale: il gruppo opera lungo l'intera catena del valore, dall'aeronautica agli elicotteri, dall'elettronica per la difesa alla *cybersecurity*, assumendo un ruolo centrale sia nell'integrazione dei sistemi sia nel coordinamento della supply chain. La sua funzione non è limitata alla produzione, ma si estende alla gestione integrata dei rischi, inclusi quelli tecnologici, operativi e di filiera, rendendolo un attore chiave nella resilienza dell'intero ecosistema industriale.

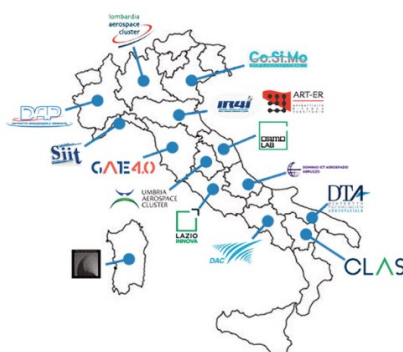
A un livello intermedio si collocano i fornitori di primo e secondo livello (Tier 1 e Tier 2), che contribuiscono alla realizzazione di componenti critici e sottosistemi ad alta complessità tecnologica. Tra questi si possono citare Avio Aero, Mecaer Aviation Group e OHB Italia. Questo livello rappresenta un nodo strategico per l'innovazione, ma è anche esposto a rischi significativi, legati alla qualità, alla continuità produttiva e alla dipendenza da tecnologie avanzate.

La base della filiera è costituita da una vasta rete di piccole e medie imprese altamente specializzate, che rappresentano la componente numericamente più rilevante del sistema industriale *aerospace* italiano. Tali imprese operano principalmente come subfornitori, offrendo lavorazioni di precisione, componentistica meccanica ed elettronica, sviluppo software e servizi di ingegneria. La loro elevata specializzazione costituisce un elemento distintivo, ma

introduce al contempo elementi di vulnerabilità, in particolare in relazione alla gestione dei rischi lungo la supply chain e alla sicurezza informatica. Un elemento distintivo della filiera *aerospace* italiana è rappresentato dal sistema della ricerca e dell'innovazione, che include università, centri di ricerca e cluster tecnologici. In questo ambito, il Cluster Tecnologico Nazionale Aerospazio svolge un ruolo centrale come piattaforma di coordinamento tra imprese, ricerca e istituzioni. Il CTNA riunisce grandi aziende, tra cui Leonardo, insieme a università, centri di ricerca e distretti tecnologici regionali, con l'obiettivo di rafforzare la coesione della filiera e promuovere lo sviluppo tecnologico. Attraverso attività di mappatura delle competenze, supporto all'innovazione e partecipazione a programmi europei, il cluster contribuisce a ridurre la frammentazione del sistema industriale e a migliorare la capacità di gestione dei rischi lungo la filiera, in particolare quelli legati alla supply chain e alla resilienza operativa.

Infine, un ruolo cruciale è svolto dalle istituzioni e dagli enti regolatori, tra cui l'ENAC e l'Agenzia Spaziale Italiana, che definiscono il quadro normativo e garantiscono il rispetto degli standard di sicurezza e affidabilità. In questo contesto, la gestione del rischio assume una dimensione non solo aziendale, ma anche sistemica e regolatoria.

Figura 1 – Distribuzione dei distretti regionali del CTNA⁹



Fonte: CTNA, *Viaggio tra i distretti*, 2025

⁹CTNA, *Viaggio tra i distretti*, 2025

La rappresentazione evidenzia come la filiera *aerospace* italiana non sia una semplice catena produttiva, ma un sistema interconnesso in cui il valore viene generato attraverso la collaborazione tra i diversi livelli. In tale contesto, Leonardo svolge un ruolo di integratore e coordinatore, mentre il CTNA contribuisce a rafforzare la coesione del sistema, favorendo l'integrazione tra industria e ricerca.

Questa configurazione implica che il rischio non sia circoscritto a singoli attori, ma si distribuisca lungo l'intera filiera, assumendo una natura sistemica. Le principali criticità riguardano la dipendenza da fornitori altamente specializzati, la vulnerabilità delle PMI e la crescente esposizione ai rischi cyber e di interruzione della supply chain.

A livello internazionale, la filiera *aerospace* presenta caratteristiche analoghe, pur con differenze nei modelli industriali. In Europa prevale un approccio collaborativo, rappresentato da gruppi come Airbus, mentre negli Stati Uniti si osserva una maggiore integrazione verticale, con attori come Boeing e Lockheed Martin. In entrambi i contesti, tuttavia, emerge una crescente attenzione alla gestione integrata dei rischi lungo la filiera.

1.3 Quadro generale dei rischi di impresa nell'industria *aviation/aerospace*

Dal punto di vista teorico e metodologico, i rischi dell'industria *aviation/aerospace* possono essere ricondotti alle principali categorie comunemente utilizzate nei framework di risk management (ISO 31000, COSO ERM), ossia:

- rischi operativi;
- rischi tecnologici;
- rischi finanziari;
- rischi regolatori e legali;
- rischi strategici e reputazionali;

- rischi di continuità operativa;
- rischi geopolitici e macroeconomici.

Tuttavia, nel settore *aviation/aerospace* queste categorie assumono caratteristiche specifiche, strettamente legate ai requisiti di sicurezza, al contesto normativo e alla bassa tolleranza al rischio che contraddistingue il comparto. Un aspetto distintivo del settore è il legame storico tra gestione del rischio e sicurezza del volo, che rappresenta da sempre una priorità non negoziabile. La sicurezza non è considerata un rischio tra gli altri, ma un obiettivo primario e non negoziabile, attorno al quale si strutturano processi, controlli e investimenti. Questo approccio ha portato allo sviluppo dei sistemi definiti *Safety Management Systems* (SMS)¹⁰, oggi obbligatori per operatori e autorità aeronautiche, che rappresentano uno dei modelli di gestione del rischio più maturi e avanzati a livello industriale. Negli ultimi anni, tuttavia, l'emergere di nuove minacce – in particolare digitali, geopolitiche e di supply chain – ha ampliato il perimetro del risk management, richiedendo una visione più ampia e interdisciplinare.

Nei capitoli successivi saranno approfonditi le seguenti tipologie di rischio:

- cyber e rischio informatico;
- tecnologico e rischio legato all'Intelligenza Artificiale;
- di supply chain e rischio industriale;
- di business *continuity* e resilienza operativa.

Di seguito sono riportate le principali caratteristiche delle altre tipologie di rischio che occorrono le imprese del settore.

¹⁰ ICAO, Annex 19 – *Safety Management*, Montréal, International Civil Aviation Organization, 2013 (e succ. amm.)

Rischio operativo e rischio di safety

- Questi aspetti costituiscono storicamente il nucleo centrale del *risk management* aeronautico ed è strettamente connesso al concetto di *safety*. Esso comprende tutti gli eventi che possono compromettere la sicurezza delle operazioni di volo, tra cui:

- guasti tecnici e strutturali dei velivoli;
- errori umani (piloti, manutentori, controllori del traffico aereo);
- carenze nei processi di manutenzione;
- malfunzionamenti dei sistemi di navigazione e comunicazione;
- criticità infrastrutturali aeroportuali.

L'ICAO ha reso obbligatoria l'adozione dei *Safety Management Systems*, fondati su quattro pilastri: policy e obiettivi di sicurezza, gestione del rischio per la *safety*, *assurance* e promozione della sicurezza. Tale modello ha consentito all'industria di raggiungere livelli di sicurezza estremamente elevati, riducendo il tasso di incidenti nonostante la crescita esponenziale del traffico aereo.

Rischio finanziario¹¹

- Nell'industria *aviation/aerospace* assume una rilevanza particolarmente elevata a causa dell'elevata intensità di capitale, dei lunghi cicli di sviluppo dei programmi e della forte esposizione a fattori macroeconomici e geopolitici. Tali caratteristiche rendono la sostenibilità finanziaria un elemento critico per la continuità operativa e per la capacità competitiva delle imprese del settore.

Rischio di liquidità e di struttura finanziaria

- Le imprese *aviation/aerospace* sono caratterizzate da ingenti investimenti

¹¹ McKinsey & Company, *Managing inventory and financial exposure in aerospace and defense, 2025*

iniziali in ricerca, sviluppo e certificazione, che precedono di molti anni la generazione dei ricavi. Ciò espone le organizzazioni al rischio di insufficiente liquidità, soprattutto in presenza di ritardi nei pagamenti, slittamenti delle consegne o interruzioni nei programmi. La gestione del capitale circolante e l'accesso a fonti di finanziamento stabili rappresentano quindi un fattore critico.

Rischio di esposizione ai tassi di cambio e ai tassi di interesse

- Il settore opera tipicamente su scala globale, con costi e ricavi denominati in valute differenti. Ne deriva una significativa esposizione al rischio di cambio, in particolare per le imprese esportatrici o coinvolte in programmi internazionali. Analogamente, l'utilizzo di finanziamenti a medio-lungo termine rende rilevante il rischio di tasso di interesse, specialmente in contesti di elevata volatilità finanziaria.

Rischio di programma e di sovracosti

- Un elemento distintivo del settore *aerospace* è il cosiddetto *program risk*, legato alla gestione di grandi programmi industriali complessi. Ritardi nella fase di sviluppo, difficoltà tecnologiche, modifiche normative o problemi nella supply chain possono generare extra-costi significativi, erosione dei margini e, nei casi più gravi, svalutazioni di asset o perdite su commessa.

Rischio di dipendenza da clienti istituzionali

- Una parte rilevante dei ricavi del settore, in particolare nel comparto *aerospace* e *defence*, deriva da clienti governativi o istituzionali. Ciò espone le imprese al rischio di:

- revisione o cancellazione dei programmi;
- riduzione dei budget pubblici;
- ritardi nei flussi di pagamento.

Questo tipo di dipendenza amplifica l'impatto delle decisioni politiche e macroeconomiche sulla performance finanziaria.

Rischio regolatorio, legale e reputazionale¹²

- L'industria *aviation/aerospace* è soggetta ad un quadro normativo estremamente articolato, a livello nazionale, europeo e internazionale. Cambiamenti normativi in ambito *safety*, *cybersecurity* (es. NIS2), sostenibilità ambientale ed export control rappresentano una fonte costante di rischio.

La non conformità può comportare:

- sanzioni economiche;
- limitazioni operative;
- perdita di certificazioni;
- danni reputazionali significativi.

Il rischio reputazionale, in particolare, è amplificato dalla visibilità mediatica del settore: incidenti, attacchi cyber o problemi di sicurezza vengono rapidamente amplificati, con effetti duraturi sulla fiducia degli stakeholder.

Rischi geopolitici e macroeconomici:

- Sono un'ulteriore categoria di rilievo nel quadro generale dei rischi d'impresa dell'industria *aviation/aerospace*. Tali rischi sono riconducibili all'instabilità politica internazionale, ai conflitti armati, alle tensioni tra Stati, alle politiche commerciali protezionistiche e alle oscillazioni delle principali variabili macroeconomiche, quali tassi di interesse, inflazione e cambio. Il settore *aviation/aerospace*, per sua natura fortemente internazionale e interconnesso, risulta particolarmente esposto a queste dinamiche. Le imprese operano infatti su

¹² Deloitte Insight, *Aerospace and Defense Industry Outlook*, 2026

mercati globali, dipendono da catene di fornitura transnazionali e sono spesso coinvolte in programmi industriali e contratti di lungo periodo con governi e istituzioni pubbliche. Eventi geopolitici avversi possono determinare restrizioni all'export, l'introduzione di sanzioni economiche, l'interruzione dei flussi di approvvigionamento o la riduzione della domanda di trasporto aereo e di investimenti nel comparto difesa. Dal punto di vista macroeconomico, una fase di recessione o un aumento dei costi di finanziamento può incidere negativamente sulla capacità delle imprese di sostenere ingenti investimenti in capitale fisso e ricerca e sviluppo, tipici del settore. Tali fattori accentuano l'incertezza operativa e strategica, rendendo necessarie politiche di gestione del rischio volte a migliorare la resilienza aziendale e la flessibilità finanziaria.

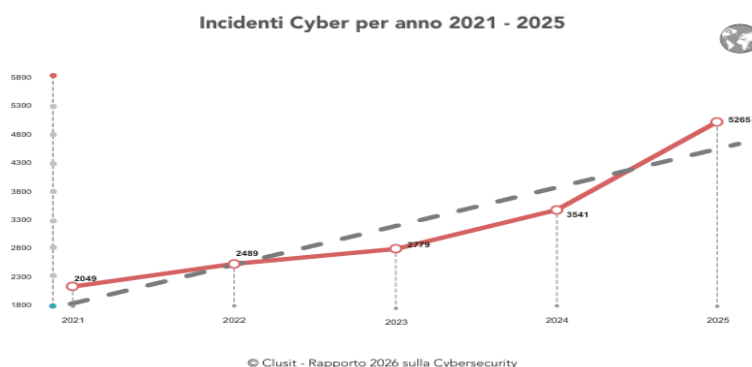
Capitolo II.

I nuovi rischi nell'industria *aviation/aerospace*

2.1 *Cybersecurity* e rischi informati

Negli anni la *cybersecurity* si è trasformata da disciplina di nicchia a un'urgenza globale. Gli incidenti informatici, dai ransomware alle violazioni massive di dati, non sono più eventi relegati alla cronaca specialistica: hanno un impatto sulla fiducia delle persone comuni, sulla stabilità economica e sulla sicurezza delle infrastrutture critiche. I dati annuali raccolti da Clusit¹³ evidenziano una tendenza in costante crescita degli attacchi, sia in termini di frequenza sia di sofisticazione. A livello globale, il numero di violazioni confermate e di eventi ransomware continua ad aumentare, spesso con impatti economici nell'ordine di miliardi di dollari l'anno e con ripercussioni su servizi essenziali. Anche in Italia, sebbene il quadro sia in parte mitigato da normative più stringenti e migliori prassi di resilienza, l'ecosistema digitale nazionale non è immune: istituzioni pubbliche, aziende e cittadini si confrontano quotidianamente con nuove minacce e la crescita esponenziale dei dispositivi connessi amplifica il raggio d'azione degli aggressori.

Figura 2 – incidenti cyber¹⁴



Fonte: ICAO, International Civil Aviation Organization

¹³ Rapporto CLUSIT sulla *cybersecurity* in Italia (edizioni 2025–2026).

¹⁴ Rapporto CLUSIT sulla Cybersicurezza in Italia, *Andamento degli incidenti cyber nel periodo 2021 - 2025*

L'industria *aviation/aerospace* è oggi uno dei settori industriali più altamente digitalizzati e interconnessi. Negli ultimi anni l'adozione di tecnologie digitali avanzate ha interessato l'intero ciclo operativo: dalla progettazione e produzione aerospaziale, alla gestione dei voli, fino alla manutenzione, ai servizi aeroportuali e all'esperienza del passeggero. Sistemi avionici digitali, piattaforme di *air traffic management* (ATM), manutenzione predittiva basata su big data, cloud computing e intelligenza artificiale hanno incrementato l'efficienza e la sicurezza operativa, ma hanno anche ampliato in modo significativo la cosiddetta superficie di attacco informatico dell'industria. A differenza di altri comparti economici, nel settore *aviation* i sistemi digitali non supportano soltanto funzioni amministrative o commerciali, bensì processi critici per la *safety*.

L'ICAO¹⁵ sottolinea come la crescente dipendenza da infrastrutture digitali renda l'aviazione un target particolarmente attrattivo per attori criminali e statuali, imponendo un ripensamento strutturale dei modelli di gestione del rischio informatico.

Il cyber risk nell'industria *aviation/aerospace* presenta una natura sistemica, in quanto coinvolge simultaneamente più soggetti e livelli della filiera: compagnie aeree, aeroporti, fornitori tecnologici, produttori aeronautici, autorità di controllo e servizi di navigazione aerea. Tale interdipendenza implica che un singolo evento informatico possa produrre effetti a cascata, propagandosi rapidamente tra sistemi, organizzazioni e Paesi diversi.

Secondo l'EASA¹⁶, la criticità del rischio informatico deriva anche dal progressivo superamento della separazione tradizionale tra Information Technology (IT) e Operational Technology (OT). L'integrazione tra reti operative e sistemi di business rende più complesso isolare le infrastrutture critiche, aumentando l'esposizione a

¹⁵ ICAO, International Civil Aviation Organization

¹⁶ EASA, Agenzia Europea per la Sicurezza dell'Aviazione 2026

minacce quali ransomware, accessi non autorizzati e sabotaggio digitale.

Principali categorie di cyber threat nel settore *aviation/aerospace*:

Attacchi alle infrastrutture critiche di terra

- Una delle categorie di rischio più frequenti riguarda gli attacchi ai sistemi informativi aeroportuali e delle compagnie aeree. Tali infrastrutture includono:

- sistemi di check-in e boarding;
- gestione bagagli;
- crew scheduling e flight operations;
- sistemi di manutenzione e logistica.

Rischi informatici sui sistemi avionici e di navigazione

- Un'area di particolare rilevanza riguarda i sistemi di navigazione e comunicazione, i quali dipendono sempre più da segnali esterni e infrastrutture satellitari. Fenomeni quali GPS spoofing e jamming costituiscono una minaccia emergente, in grado di alterare le informazioni di posizionamento ricevute dagli aeromobili. EASA e ICAO hanno sottolineato come tali minacce possano compromettere la sicurezza delle operazioni di volo, specialmente in condizioni di visibilità ridotta o in prossimità delle fasi di atterraggio. L'aumento di questi eventi ha spinto le autorità a considerare la resilienza cibernetica come parte integrante delle politiche di *safety*.¹⁷

Data breach e tutela dei dati sensibili

- Il settore *aviation* gestisce ingenti quantità di dati sensibili, tra cui informazioni personali dei passeggeri, dati biometrici, piani di volo e proprietà intellettuale industriale. Le violazioni informatiche possono comportare:

¹⁷Accenture, *Cybersecurity in Aviation - State of Cybersecurity Resilience 2025*

- sanzioni regolamentari (in particolare in ambito GDPR),
- danni reputazionali di lungo periodo,
- perdita di fiducia da parte dei clienti e degli stakeholder.

Secondo ricerche di settore, la fiducia del consumatore nel brand aeronautico risulta particolarmente vulnerabile agli incidenti cyber, con conseguenze dirette sulla domanda e sul valore aziendale.

La crescente rilevanza del rischio informatico ha condotto a una significativa evoluzione del quadro normativo. A livello internazionale, l'ICAO ha introdotto Standard e Recommended Practices¹⁸ sulla *cybersecurity*, richiedendo agli Stati e agli operatori di identificare e proteggere i sistemi ICT critici per l'aviazione civile. In ambito europeo, l'EASA ha adottato il regolamento Part-IS, che impone alle organizzazioni aeronautiche l'adozione di un *Information Security Management System* (ISMS) proporzionato al profilo di rischio. Questo approccio integra la gestione del cyber risk all'interno dei sistemi di *safety e di business continuity*, segnando un passaggio da una logica reattiva a una logica preventiva e sistemica della sicurezza informatica.

Guardando al futuro, è evidente che la *cybersecurity* non potrà più essere concepita come un insieme di strumenti reattivi appresi “a posteriori” né come un dominio riservato ai tecnici. Ha un impatto sempre più trasversale che richiede a tutti (cittadini, organizzazioni, aziende) di sviluppare una cultura diffusa di “*cyber resilience*” a più livelli: di consapevolezza per i cittadini e, da parte di organizzazioni e aziende, di tecnologie evolute che integrino anche l'AI difensiva), di modelli di governance robusti, di collaborazione internazionale e formazione continua. I sistemi di difesa devono essere adattivi, le architetture zero-trust, la crittografia avanzata (con un occhio allo sviluppo del quantum *criptography*) e

¹⁸ ICAO, *Standard e Recommended Practices sulla cybersecurity*

framework di compliance dinamici per realizzare strategie preventive dei prossimi anni.

2.2 Intelligenza artificiale e nuovi profili di rischi

L'intelligenza artificiale (IA) rappresenta una delle trasformazioni più rilevanti degli ultimi anni nel settore *aviation e aerospace*, incidendo profondamente sui modelli operativi, sulla gestione della sicurezza e sull'organizzazione complessiva del sistema aeronautico. Le applicazioni dell'IA spaziano dalla manutenzione predittiva alla gestione del traffico aereo, fino al supporto decisionale per piloti e operatori, consentendo una gestione più efficiente dei dati e una maggiore capacità di anticipare situazioni di rischio. L'elemento distintivo dell'introduzione dell'IA nel settore aeronautico è costituito dalla capacità di analizzare grandi quantità di informazioni in tempo reale, individuando pattern invisibili ai sistemi tradizionali. Ciò consente di migliorare significativamente la sicurezza operativa, ad esempio prevedendo guasti tecnici prima che si verifichino o ottimizzando le rotte di volo per ridurre congestioni e rischi di collisione. Tuttavia, questa evoluzione tecnologica comporta anche un cambiamento nella natura del rischio, che diventa sempre più legato a fattori digitali, algoritmici e organizzativi. In questa prospettiva, è fondamentale considerare anche l'evoluzione futura dell'intelligenza artificiale nel settore *aviation*. Le principali autorità internazionali sottolineano come l'IA sia destinata a diventare un elemento strutturale dell'intero ecosistema aeronautico, contribuendo alla creazione di sistemi sempre più autonomi e interconnessi. In particolare, si prevede un progressivo sviluppo di applicazioni avanzate nell'ambito della mobilità aerea urbana (Urban Air Mobility) e dei sistemi autonomi, nonché una crescente integrazione tra intelligenza artificiale, comunicazioni e gestione del traffico aereo (AI/CNS/ATM).

Parallelamente, l'evoluzione tecnologica porterà a un crescente utilizzo di sistemi basati su apprendimento automatico direttamente “on-board”, ovvero integrati nei velivoli, con funzioni di supporto o sostituzione parziale delle attività umane.

Questo scenario implica un passaggio da un'aviazione assistita a un'aviazione progressivamente autonoma, in cui l'IA non sarà più solo uno strumento di supporto, ma un attore attivo nei processi decisionali. Nel medio-lungo periodo, è plausibile attendersi un'espansione del ruolo dell'IA anche in ambiti quali la gestione integrata dei dati aeronautici, la pianificazione strategica delle rotte globali e la sostenibilità ambientale, grazie all'ottimizzazione dei consumi e delle emissioni. Tuttavia, questa evoluzione comporterà una crescente complessità sistemica e un aumento dell'interdipendenza tra componenti tecnologiche, organizzative e umane.

Alla luce di tali sviluppi, il settore *aviation* si trova di fronte a una fase di transizione in cui i benefici dell'innovazione devono essere bilanciati con l'esigenza di mantenere livelli elevati di sicurezza e affidabilità. Proprio questa crescente pervasività dell'intelligenza artificiale rende necessario un approfondimento dei nuovi profili di rischio emergenti.

Uno dei principali elementi di criticità riguarda l'affidabilità dei sistemi basati su intelligenza artificiale. A differenza dei sistemi tradizionali, progettati secondo logiche deterministiche, i modelli di machine learning apprendono dai dati e possono quindi generare risultati difficilmente prevedibili o interpretabili. Questa caratteristica, spesso definita come “black box”, rende più complesso il processo di certificazione e validazione, soprattutto in un settore altamente regolamentato come quello aeronautico, dove la sicurezza rappresenta un requisito imprescindibile.

Inoltre, le prestazioni dei sistemi AI dipendono fortemente dalla qualità dei dati utilizzati per l'addestramento, il che introduce ulteriori vulnerabilità legata a errori, incompletezza o manipolazione delle informazioni.

Un ulteriore profilo di rischio riguarda l'interazione tra uomo e macchina. L'introduzione di sistemi automatizzati avanzati modifica il ruolo degli operatori umani, generando nuove criticità nei processi decisionali. In particolare, il fenomeno dell’*“automation bias”*¹⁹ porta gli individui a fidarsi eccessivamente delle indicazioni

¹⁹ Center for Security and Emerging Technology (CSET), *AI Safety and Automation Bias*, 2024

fornite dai sistemi automatici, anche quando queste risultano errate o incoerenti con l'esperienza diretta. Questo rischio è particolarmente rilevante nel contesto aeronautico, dove situazioni di emergenza richiedono una pronta capacità di intervento umano. Parallelamente, l'aumento dell'automazione può determinare una progressiva perdita di competenze operative (*skill degradation*), riducendo la capacità degli operatori di gestire condizioni critiche senza il supporto dei sistemi intelligenti.

La crescente digitalizzazione del settore *aviation*, unita all'adozione dell'IA, amplifica inoltre i rischi legati alla *cybersecurity*. I moderni aeromobili e le infrastrutture aeroportuali sono caratterizzati da un elevato livello di interconnessione tra sistemi informatici, rendendo possibile l'esposizione a cyberattacchi che possono compromettere sia la sicurezza dei dati sia le operazioni di volo. Le minacce includono accessi non autorizzati, manipolazione dei sistemi di navigazione e attacchi alle reti di gestione del traffico aereo. In questo contesto, l'utilizzo dell'IA da parte di attori ostili consente la realizzazione di attacchi sempre più sofisticati, difficili da rilevare e contrastare con strumenti tradizionali.

Accanto ai rischi tecnici e operativi, emergono anche rilevanti questioni etiche e legali. L'utilizzo di sistemi autonomi o semi-autonomi pone interrogativi sulla responsabilità in caso di incidenti, sulla trasparenza dei processi decisionali e sulla necessità di mantenere un adeguato controllo umano. In questo senso, le principali autorità di regolazione internazionale, come l'ICAO e l'EASA²⁰, sottolineano l'importanza di un approccio "*human-centric*", volto a garantire che l'essere umano rimanga al centro dei sistemi critici e che l'utilizzo dell'IA sia accompagnato da adeguati meccanismi di governance, trasparenza e accountability.

Per far fronte a queste nuove sfide, il quadro normativo è in continua evoluzione. Organismi come la Federal Aviation Administration (FAA) e l'EASA stanno sviluppando linee guida e roadmap specifiche per la certificazione e l'utilizzo sicuro dell'intelligenza artificiale nel settore aeronautico. L'obiettivo è quello di adattare i

²⁰ ICAO, Guidance on Artificial Intelligence in Aviation, 2024

tradizionali standard di sicurezza a tecnologie caratterizzate da elevata complessità e dinamismo, garantendo al contempo l'innovazione. Parallelamente, a livello europeo, il regolamento sull'intelligenza artificiale (AI Act)²¹ introduce un approccio basato sul rischio, classificando molte applicazioni nel settore *aviation* come sistemi ad alto rischio, soggetti a requisiti stringenti in termini di conformità e controllo.

In conclusione, l'intelligenza artificiale rappresenta una leva fondamentale per l'innovazione e la competitività del settore *aviation e aerospace*, ma introduce anche una nuova classe di rischi che richiede un'evoluzione dei modelli di gestione e regolazione. La sfida principale consiste nel bilanciare i benefici derivanti dall'automazione e dall'analisi avanzata dei dati con la necessità di garantire elevati standard di sicurezza, affidabilità e controllo umano. Solo attraverso un approccio integrato, che combini innovazione tecnologica, governance efficace e adeguati framework normativi, sarà possibile sfruttare appieno le potenzialità dell'IA minimizzando i rischi associati.

2.3 Supply chain globale e rischi operativi

La supply chain globale del settore *aviation e aerospace* rappresenta una delle strutture produttive più complesse e interconnesse dell'economia contemporanea. Negli ultimi anni, la crescente globalizzazione e frammentazione della filiera hanno accentuato la dipendenza da fornitori esterni e subfornitori, incrementando il livello di complessità del sistema. In questo contesto, la supply chain aeronautica è stata sottoposta a forti pressioni, dovute a fattori quali la pandemia, le tensioni geopolitiche, la carenza di materie prime e i problemi logistici. Secondo l'International Air Transport Association (IATA), le difficoltà nella supply chain stanno generando impatti economici significativi, con costi stimati superiori a 11 miliardi di dollari per il settore nel 2025, tra inefficienze operative, aumento dei costi di manutenzione e ritardi nelle consegne.

²¹ Regolamento (UE) 2024/1689 (AI Act)

Un elemento particolarmente critico riguarda i cosiddetti colli di bottiglia nella produzione. La difficoltà nel reperire componenti chiave, come motori e parti strutturali, ha determinato un aumento significativo del backlog globale, che ha superato le 17.000 unità di velivoli, con tempi di attesa che possono arrivare a oltre dieci anni. Tale situazione evidenzia la fragilità del sistema produttivo e la sua incapacità di adattarsi rapidamente a shock esterni.

Un ulteriore profilo di rischio è rappresentato dalla forte dipendenza da fornitori strategici. Nel settore *aerospace*, molti componenti altamente specializzati sono prodotti da un numero limitato di aziende, il che genera fenomeni di concentrazione e aumenta l'esposizione a interruzioni operative. Come evidenziato da analisi di settore, i problemi finanziari o produttivi di un singolo fornitore possono avere effetti a cascata sull'intera filiera, rallentando o bloccando la produzione. Questo fenomeno è ulteriormente aggravato dalla limitata visibilità sui livelli più profondi della supply chain (tier-2 e tier-3 suppliers), rendendo difficile l'identificazione preventiva delle vulnerabilità.

La crescente digitalizzazione della filiera introduce inoltre rischi legati alla *cybersecurity*, di cui abbiamo parlato in precedenza.

A livello operativo, la supply chain aeronautica è esposta anche a rischi di tipo logistico e organizzativo. Ritardi nelle consegne, inefficienze nei trasporti e problemi di coordinamento tra i diversi attori possono determinare interruzioni della produzione e impatti negativi sulla continuità operativa delle compagnie aeree. In alcuni casi, tali criticità hanno comportato la necessità di utilizzare aeromobili più datati, con conseguente aumento dei costi di manutenzione e riduzione dell'efficienza energetica.

Un ulteriore elemento di complessità è rappresentato dai rischi geopolitici e normativi. Il settore *aviation* è fortemente influenzato da politiche commerciali, regolamentazioni internazionali e rapporti tra Stati. Sanzioni economiche, restrizioni all'esportazione e conflitti internazionali possono interrompere i flussi

di approvvigionamento e rendere necessario il ripensamento delle strategie di sourcing. Secondo analisi di settore, queste dinamiche stanno spingendo le aziende verso modelli più resilienti, basati su una maggiore diversificazione dei fornitori e una progressiva regionalizzazione della supply chain.

L'impatto delle criticità nella supply chain non si limita a semplici inefficienze operative, ma genera una vasta gamma di effetti economici e strategici, distinguibili in danni diretti e indiretti. I danni diretti si manifestano immediatamente sul piano economico-operativo e riguardano principalmente l'aumento dei costi e le perdite di produzione. Nel settore *aviation*, i ritardi nella consegna di componenti o nella manutenzione dei motori possono comportare la messa a terra degli aeromobili (Aircraft on Ground), con conseguenti perdite di ricavi e aumento dei costi fissi. Secondo IATA²², le disfunzioni della supply chain genereranno oltre 11 miliardi di dollari di impatti economici nel 2025, tra costi di manutenzione più elevati, leasing di componenti e inefficienze operative. Inoltre, la necessità di utilizzare aeromobili più vecchi a causa dei ritardi nelle consegne comporta un aumento del consumo di carburante e dei costi operativi.

A tali effetti si aggiungono i danni legati alla gestione delle emergenze operative, come l'acquisto urgente di componenti sul mercato secondario, il ricorso a fornitori alternativi a costi più elevati e l'incremento delle scorte di sicurezza per compensare l'incertezza della filiera. Questi elementi incidono significativamente sulla redditività delle compagnie e degli operatori aeronautici.

I danni indiretti, invece, si manifestano nel medio-lungo periodo e riguardano aspetti strategici, reputazionali e competitivi. Tra questi, un ruolo centrale è svolto dalla perdita di affidabilità del servizio, che può tradursi in cancellazioni, ritardi e disservizi per i passeggeri, con conseguente riduzione della soddisfazione e della fiducia nei confronti delle compagnie aeree. Tali effetti si riflettono anche sul piano competitivo, determinando una possibile perdita di quote di mercato a favore di

²² International Air Transport Association (IATA) 2026, Aviation Supply Chain Art. 13.10.2025

operatori più efficienti o meglio organizzati.

Un ulteriore danno indiretto riguarda l'impatto sulla sostenibilità e innovazione. I ritardi nella supply chain limitano l'introduzione di nuovi aeromobili più efficienti e meno inquinanti, rallentando il percorso di transizione ecologica del settore. Inoltre, la pressione esercitata sulle imprese può ridurre le risorse disponibili per investimenti in ricerca e sviluppo.

Infine, i rischi legati alla supply chain possono avere conseguenze anche sul piano sistemico, contribuendo a incrementare la volatilità dei costi e l'incertezza del mercato. La presenza di interdipendenze elevate tra i diversi attori della filiera implica che un singolo evento critico possa propagarsi rapidamente lungo l'intero sistema, amplificando gli effetti negativi e rendendo più complessa la gestione del rischio. In questo senso, la fragilità della supply chain rappresenta non solo un rischio operativo, ma anche un fattore di vulnerabilità macroeconomica per l'intero settore *aviation/aerospace*.

In conclusione, la supply chain globale del settore *aviation e aerospace* rappresenta un elemento chiave per la competitività e l'innovazione, ma al tempo stesso costituisce una fonte significativa di rischi operativi. La crescente interconnessione e complessità del sistema richiedono un approccio integrato alla gestione del rischio, che tenga conto non solo degli aspetti tecnici e logistici, ma anche delle dimensioni economiche, tecnologiche e geopolitiche. Solo attraverso un rafforzamento della resilienza della supply chain sarà possibile garantire la continuità operativa e la sicurezza in un contesto sempre più incerto e dinamico

2.4 Business Continuity

In questo contesto, la *business continuity* (BC) assume un ruolo strategico: non si limita alla gestione delle emergenze, ma mira a garantire la continuità operativa, la sicurezza dei passeggeri e la stabilità economica del sistema aeronautico nel suo complesso. L'ICAO sottolinea infatti che qualsiasi interruzione nel settore può

avere effetti immediati e diffusi su economia, commercio e società.

Costi economici diretti e indiretti: nel 2022, ritardi e cancellazioni hanno generato un impatto economico globale stimato tra 75 e 88 miliardi di dollari considerando diverse regioni del mondo²³.

Solo negli Stati Uniti e in Europa, il costo combinato è stato compreso tra 58 e 68 miliardi di dollari. Le disruption rappresentano circa l'8% dei ricavi totali delle compagnie aeree (circa 60 miliardi di dollari). A livello operativo, anche micro-interruzioni hanno impatti rilevanti: un singolo minuto di ritardo nel block time può costare circa 100 dollari per volo, moltiplicandosi in perdite miliardarie su scala globale. La *business continuity* nel settore *aviation* non è opzionale, ma essenziale, rappresenta uno strumento fondamentale per garantire stabilità, sicurezza e competitività.

²³ Airhelp, *Cost of disrupted flights to the economy*, 2024

Capitolo III

Il caso Leonardo S.p.A. e CTNA: la valorizzazione della rete come strategia competitiva

3.1 Il CTNA come piattaforma di supporto alla filiera aerospaziale: riduzione delle fragilità e condivisione delle competenze.

Il Cluster Tecnologico Nazionale Aerospazio (CTNA) è un'associazione pubblico-privata senza scopo di lucro che si pone come interlocutore di riferimento nazionale per le industrie dell'aerospazio, per il mondo della ricerca e per gli attori istituzionali operanti nei settori dell'Aeronautica e dello Spazio.

Istituito nel 2012 dal MIUR nell'ambito della strategia di specializzazione nazionale e riconosciuto con la legge n. 123 del 3 Agosto 2017, il CTNA svolge un ruolo cruciale nel sintetizzare esigenze e priorità degli attori del sistema aerospaziale, anche con riferimento alle aspettative del mercato globale e delle politiche settoriali europee e internazionali. Il CTNA supporta la competitività del settore aerospaziale, contribuendo attivamente a moltiplicare le opportunità di business e di crescita per l'Italia; questo avviene attraverso una serie di azioni specifiche delineate nelle strategie pluriennali, in perfetta sintonia con la sua mission. Aderiscono al CTNA i 15 principali distretti tecnologici regionali e i maggiori players del settore industriale e del mondo della ricerca con i quali è instaurato un dialogo costante e una proficua condivisione di esperienze. Inoltre, aderiscono all'associazione anche La Federazione Italiana dell'Aerospazio e della Difesa (AIAD) e l'Agenzia Spaziale Italiana (ASI)²⁴. Oggi al CTNA sono associati in totale ventidue soggetti: quattordici distretti regionali che ne rappresentano la spina dorsale favorendo la collaborazione tra le imprese e gli enti di ricerca sul territorio; Leonardo e Avio Aero, che quali soci industriali di riferimento garantiscono un collegamento diretto con le esigenze della filiera; CNR, CIRA e INGV, che in quanto enti di ricerca forniscono competenze scientifiche e tecnologiche di altissimo livello; AIAD, che rappresenta le aziende del settore

²⁴ CTNA, www.ctna.it/profilo/

aerospaziale e della difesa, contribuendo a tutelare i loro interessi e a promuoverne lo sviluppo; e l'ASI che collabora con il CTNA per la definizione delle strategie di sviluppo del settore. I principali obiettivi del CTNA sono quelli di definire le strategie di innovazione e le priorità per programmi di ricerca e sviluppo tecnologico, coerenti con le agende strategiche a livello europeo; stimolare la creazione di talenti tra le giovani generazioni nelle discipline scientifiche; e sostenere le politiche di ricerca e innovazione, al fine di favorire una connessione stabile tra interventi e strumenti a livello nazionale e regionale²⁵.

Il CTNA si configura come una piattaforma di coordinamento della filiera aerospaziale italiana, favorendo l'integrazione tra grandi imprese, PMI, università e istituzioni. Attraverso questa rete, riduce le fragilità del sistema produttivo, migliorando il collegamento tra ricerca e industria e facilitando l'accesso a risorse e competenze condivise. La collaborazione strutturata consente di ottimizzare i processi di innovazione, diminuire i costi e aumentare la resilienza della supply chain. Inoltre, il cluster promuove la diffusione del know-how e lo sviluppo di progetti comuni, rafforzando la competitività complessiva del settore nazionale. In questo modo, il CTNA trasforma la cooperazione tra attori eterogenei in un vero vantaggio competitivo basato sulla condivisione delle competenze²⁶.

3.2 Il ruolo di Leonardo nello sviluppo della rete CTNA: coordinamento industriale e integrazione del sistema

Leonardo S.p.A. è un gruppo industriale internazionale che realizza capacità tecnologiche multi dominio per la sicurezza globale. Protagonista dei principali programmi strategici dell'Aerospazio, Difesa e Sicurezza, conta oltre 62.000 dipendenti nel mondo. L'azienda ha una significativa presenza industriale in Italia, Regno Unito, Polonia e Stati Uniti e opera in 150 Paesi anche attraverso controllate,

²⁵ Art. <https://www.pandorarivista.it/articoli/il-futuro-della-filiera-aerospaziale-italiana-la-visione-del-ctna-intervista-a-cristina-leone/>

²⁶ Agenzia spaziale Italiana, www.asi.it

joint venture e partecipazioni. Leonardo è partner tecnologico e industriale di Governi, Amministrazioni della Difesa, Istituzioni e imprese. Nel 2025 ha registrato ricavi consolidati pari a €19,5 mld, nuovi ordini per €23,8 mld e investito €3 mld in R&S. Innovazione, ricerca continua, industria digitale e sostenibilità sono i pilastri del suo business nel mondo.

Aree di business²⁷

- Elettronica per la difesa: Soluzioni multi-dominio per la sorveglianza, la sicurezza e la protezione delle forze in campo e delle infrastrutture critiche.
- Spazio: Asset spaziali e servizi satellitari che si avvalgono di avanzate tecnologie digitali, dall'intelligenza artificiale al cloud, dal supercalcolo alla *cybersecurity*.
- *Cyber & Security*: Realizzazione di piattaforme proprietarie basate su tecnologie trasformative - Intelligenza Artificiale, Cyber e Data Platform.
- Elicotteri: leader globale nel volo verticale attraverso elicotteri avanzati per missioni civili e militari.
- Aeronautica: velivoli: progettazione, sviluppo e produzione di velivoli di ultima generazione.

Leonardo S.p.A. svolge un ruolo centrale nello sviluppo del CTNA, configurandosi come attore guida e integratore della filiera aerospaziale italiana. In quanto grande impresa leader del settore, partecipa direttamente alla governance del cluster e ne orienta le priorità strategiche, contribuendo al coordinamento delle attività di

²⁷ www.leonardo.com, *LEONARDO AT A GLANCE*

ricerca e innovazione. Attraverso il CTNA, Leonardo favorisce l'integrazione tra grandi imprese, PMI, università e centri di ricerca, rafforzando la coesione del sistema industriale. Il gruppo promuove lo sviluppo di progetti collaborativi e l'accesso a finanziamenti nazionali ed europei, facilitando la crescita tecnologica dell'intera filiera. Inoltre, svolge un'importante funzione di trasferimento di competenze e know-how, contribuendo a ridurre le frammentazioni e a migliorare la competitività complessiva del settore²⁸. In questo modo, Leonardo valorizza il cluster come piattaforma strategica, trasformando la rete in una leva di coordinamento industriale e innovazione condivisa.

3.3 Dalla valorizzazione della rete al vantaggio competitivo: effetti sistemici per Leonardo nel contesto globale.

La valorizzazione della rete all'interno del CTNA rappresenta per Leonardo S.p.A. una leva strategica fondamentale per costruire un vantaggio competitivo sostenibile. Il cluster, infatti, integra imprese, centri di ricerca e istituzioni, favorendo la condivisione di competenze, tecnologie e infrastrutture lungo l'intera filiera aerospaziale. In questo contesto, l'adozione di progetti comuni di filiera consente di ridurre la frammentazione del sistema e di ottimizzare i processi di innovazione, evitando duplicazioni e dispersioni di risorse.

La standardizzazione di pratiche operative e la cooperazione strutturata generano una significativa riduzione dei costi, oltre a un miglioramento della qualità e dell'affidabilità dei prodotti. Questo porta l'intera filiera a un livello tecnologico più elevato, consentendo anche alle PMI di colmare gap competitivi e di inserirsi in programmi industriali complessi. Leonardo, come integratore di sistema, beneficia direttamente di questa evoluzione, potendo contare su partner più qualificati e su una supply chain più solida ed efficiente. [pandorarivista.it]

Un ambito particolarmente rilevante è quello della *cybersecurity*, cruciale nel

²⁸ <https://italianspaceindustry.it/cluster-tecnologico-nazionale-aerospazio-ctna/>

settore aerospaziale e della difesa. La condivisione di piattaforme, standard e informazioni sulle minacce consente di costruire un sistema di sicurezza integrato lungo tutta la filiera. Attraverso un approccio coordinato, le imprese possono sviluppare soluzioni comuni per la protezione di dati sensibili, infrastrutture critiche e sistemi digitali. Questo permette di evitare investimenti duplicati e di raggiungere economie di scala: ad esempio, la condivisione di centri di monitoraggio (SOC – *Security Operation Center*) e di protocolli di difesa può generare un risparmio ipotetico tra il 20% e il 30% dei costi di sicurezza IT per le singole imprese, aumentando al contempo la capacità di prevenzione e risposta agli attacchi. Inoltre, la condivisione in tempo reale delle informazioni sulle minacce rafforza la resilienza complessiva del sistema, riducendo il rischio di interruzioni della supply chain.

Un secondo esempio riguarda la gestione dei rischi assicurativi. In un contesto aerospaziale caratterizzato da investimenti elevati e alta esposizione al rischio, l'adozione di modelli condivisi di analisi e gestione consente di migliorare la valutazione delle vulnerabilità e di distribuire i rischi tra i diversi attori. La creazione di database comuni e di strumenti condivisi di risk assessment permette di negoziare condizioni assicurative più favorevoli, generando un potenziale risparmio ipotetico fino al 15-25% sui premi assicurativi. Inoltre, la maggiore trasparenza e collaborazione facilita la prevenzione dei rischi, riducendo la probabilità di incidenti e perdite economiche.

Questi esempi dimostrano come la condivisione di pratiche e strumenti all'interno del CTNA produca benefici sistemici per tutta la filiera. Le PMI accedono a tecnologie e competenze avanzate, mentre Leonardo rafforza il proprio ruolo di coordinatore e guida industriale. Ne deriva un ecosistema più efficiente, integrato e resiliente, in cui il valore creato è superiore alla somma delle singole componenti. In un contesto globale sempre più competitivo, questo modello consente a Leonardo S.p.A. di competere non solo come singola impresa, ma come espressione di un

sistema-paese avanzato. La capacità di valorizzare la rete e di implementare progetti di filiera condivisi diventa quindi un fattore chiave per ottenere un vantaggio competitivo duraturo, fondato su innovazione, efficienza e cooperazione.

CONCLUSIONI

Il settore *aviation/aerospace* si trova oggi al centro di una trasformazione profonda, guidata da innovazione tecnologica, interconnessione digitale e crescente complessità dei rischi. In questo scenario, il risk management evolve da funzione di controllo a vero e proprio driver strategico.

L'integrazione tra rischi aziendali e assicurativi consente di adottare una visione olistica, fondamentale per anticipare e mitigare minacce sempre più sofisticate. *Cybersecurity* e intelligenza artificiale non rappresentano solo ambiti di rischio, ma anche opportunità da governare con approcci strutturati e consapevoli. Allo stesso tempo, le criticità legate alla supply chain evidenziano la necessità di modelli più resilienti, flessibili e trasparenti.

La *business continuity*, infine, assume un ruolo chiave nell'assicurare la capacità dell'organizzazione di rispondere e adattarsi a eventi disruptivi, garantendo la continuità dei servizi e la tutela degli stakeholder.

Guardando al futuro, le organizzazioni che sapranno integrare competenze, tecnologie e strumenti di gestione del rischio in un framework coerente e proattivo saranno meglio posizionate per competere in un mercato sempre più instabile e sfidante.

BIBLIOGRAFIA

- Accenture (2025), Navigare cieli incerti – Rapporto di approfondimenti sull'aerospaziale commerciale.
- Accenture (2025), Stato della resilienza della *cybersecurity* nell'aviazione.
- AirHelp (2024), Costo dei voli interrotti verso l'economia.
- CLUSIT (2025–2026), Rapporto sulla cybersecurity in Italia.
- CRIBIS (2025), I numeri dell'industria aerospaziale italiana.
- CSET (2024), Sicurezza dell'IA e Bias di Automazione.
- CTNA (2025), Viaggio tra i distretti
- Deloitte Insight (2025), Prospettive sull'industria aerospaziale e della difesa.
- Deloitte Insight (2026), Prospettive sull'industria aerospaziale e della difesa.
- EASA (2024), Intelligenza Artificiale e Aviazione.
- EASA (2026), Panoramica sulla *cybersecurity* e Regolamentazione Parziale IS.
- FAA (2024), Roadmap per la Garanzia della Sicurezza dell'Intelligenza Artificiale.
- IATA (2026), Analisi della Supply Chain dell'Aviazione.
- IATA (2026), Strategia di Sicurezza Informatica dell'Aviazione.
- ICAO (2025), L'impatto dell'intelligenza artificiale sul settore dell'aviazione.
- McKinsey & Company (2024), Affrontare la turbolenza continua: la supply chain aerospaziale.
- McKinsey & Company (2025), Gestione dell'inventario e dell'esposizione finanziaria nell'aerospaziale e nella difesa.
- PwC (2025), Revisione e prospettive dell'industria aeronautica.

Rapporto annuale sulla sicurezza informatica dell'Associazione delle Industrie Aerospaziali.

SecurityScorecard, il panorama del rischio cibernetico dell'industria aeronautica globale.

The Business Research Company (2026), Aerospace and Defense Market Report.

SITOGRAFIA

<https://www.icao.int>

<https://www.icao.int/aviation-cybersecurity>

<https://www.easa.europa.eu>

<https://www.iata.org>

<https://www.aia-aerospace.org>

<https://www.leonardo.com>

<https://www.ctna.it>

<https://www.asi.it>

<https://italianspaceindustry.it>

<https://www.accenture.com>

<https://www.securityscorecard.com>

<https://www.pandorarivista.it/articoli/il-futuro-della-filiera-aerospaziale-italiana-la-visione-del-ctna-intervista-a-cristina-leone/>

RINGRAZIAMENTI

Desidero innanzitutto esprimere un sentito ringraziamento al Relatore Professor Attilio Mucelli per la disponibilità dimostrata e per il supporto fornito durante la stesura di questo lavoro.

Un ringraziamento speciale va alla mia famiglia, in particolare a mia madre, a mio padre e a mia sorella, per il sostegno, la vicinanza e la fiducia dimostrati nel corso degli anni. Anche nei momenti di difficoltà e durante il periodo di interruzione degli studi, la loro presenza è stata fondamentale per trovare la forza di riprendere e portare a termine questo percorso.

Un pensiero speciale va a mia moglie Sara, per la pazienza, la comprensione e la vicinanza dimostrate lungo tutto questo cammino; il suo sostegno quotidiano e la sua fiducia sono stati per me una motivazione costante, senza la quale il raggiungimento di questo traguardo non sarebbe stato possibile.

Questo risultato appartiene a tutte le persone che hanno creduto in me, spronandomi a non fermarmi e a rimettermi in gioco.