CYBER SECURITY in Ambito Trasporti Aereo

VITROCISET
a LEONARDO company

Cyber Security *"fast moving topic"*

La Cyber-Security è considerata da tutti gli attori dell'Aviazione Civile (Istituzioni, Industria, Operatori) su vari livelli (legislativo, regolamentazione, standardizzazione, ricerca e sviluppo) come un "fast moving topic" di assoluta priorità per garantire la sicurezza del trasporto aereo

CYBER ATTACK: OBIETTIVI

Nel settore dell'aviazione civile sono tre gli obiettivi principali che possono essere soggetti ad un attacco di natura informatica:

- i sistemi interni di un aeroporto,
- I sistemi di controllo di un aeroplano in volo,
- i sistemi di gestione del traffico aereo.

CYBER ATTACK: EVENTI SIGNIFICATIVI

- **2006**: un attacco informatico costringe la FAA a disattivare alcuni sistemi ATC in Alaska.
- **2008**: all'aeroporto di Madrid-Bajaras, un trojan in uno dei sistemi principali della compagnia Spanair impedisce la ricezione e l'attivazione di un messaggio d'allarme proveniente dal volo 5022. La mancata segnalazione è fra le cause della collisione dell'aeromobile (154 vittime).
- **2009**: un attacco ai sistemi FAA permette a hacker ignoti di accedere a 48.000 file del personale.
- **2013**: il sistema di controllo dei passaporti agli aeroporti di Istanbul Ataturk e Sabiha Gökçen viene arrestato da un attacco cibernetico, causando il ritardo di numerosi voli.
- **2013**: secondo un rapporto del Centre for Internet Security (CIS), nel corso del 2013 circa 75 aeroporti americani sono stati attaccati da prolungate campagne di spear phishing.
- **2014**: il volo Malaysia Airlines MH370 scompare dai radar dei controllori di volo. Il Boeing 777-200ER viene dato per disperso; tra le ipotesi (mai confermata) l'aereo sarebbe stato dirottato attraverso un telefono cellulare e/o una penna USB.
- **2015**: un attacco al network della compagnia di bandiera polacca Lot lascia a terra 10 voli diretti verso Danimarca, Germania e Polonia, provocando il ritardo per altri 10. L'attacco ha compromesso i sistemi che creano i piani di volo.
- **2016**: il malware BlackEnergy, colpisce le centrali elettriche Ucraine e alcuni server all'interno dell'aeroporto di Kiev.
- **2017**: attacco ransomware ai siti web dell'aeroporto ucraino a Odessa causando rallentamenti nella fornitura di servizi.
- **2018**: attacco ransomware al sito web dell'aeroporto di Bristol mandando in tilt le pagine degli arrivi e partenze anche all'interno dei terminal.

Rif : IAI ***The defence of civilian air traffic systems from cyber threats***

STAKEHOLDER

- 12th Amendment Annex 17
- ATM Security Manual
- WG on Threat and Risk
- Aviation Security Panel
- Security Audit Programme

- Doc 30
- Study Group Cyber Security

- Standardisation

- Coop with CERT

- Reg CE 300/2008 (Comm Rules)
- Reg CE 1035/2011 (Comm Reqs)

- ATM Security

EUROCONTROL

- Direttiva NIS 2016/1148
- GDPR

EU REGULATION

REGIONAL SERVICE PROVISION

- SESAR 2020

- D.Lgs. 65/2018

NATIONAL REGULATION

LOCAL SERVICE PROVISION

- SMS
- SOC

- Adeguamento GDPR e Cybersecurity

- Recepimento Annex ICAO

CSIRT Computer Security Incident Response Team

ICAO

- L'**ICAO** (**International Civil Aviation Organization**) è un'agenzia specializzata dell'ONU, istituita dalla Convenzione di Chicago nel 1944 da 52 Stati, al fine di creare le basi per lo sviluppo dell'aviazione civile internazionale
- Compito primario dell'ICAO è quello di promuovere la cooperazione tra gli Stati membri e la comunità aeronautica e di fissare regole che assicurino uno sviluppo dell'aviazione sicuro, efficiente e sostenibile
- Tra i compiti dell'ICAO vi è l'emissione e la raccolta di regolamentazioni suddivise in:
  - Norme e Raccomandazioni ovvero le **SARPs** (Standards and Recommended Practices) che costituiscono la regolamentazione tecnico giuridica dell'ICAO emesse sotto forma di allegati tecnici o **Annessi** che vengono adottati dagli Stati membri.
  - Procedure (**PANS** - Procedures for Air Navigation Services)
  - Procedure Supplementari (**SUPPS** - Supplementary Procedures)
  - Manuali Tecnici, ovvero documenti dettagliati utili per facilitare l'applicazione degli annessi e delle Procedure
  - Circolari, contenenti informazioni su argomenti specifici

ICAO: CYBER SECURITY

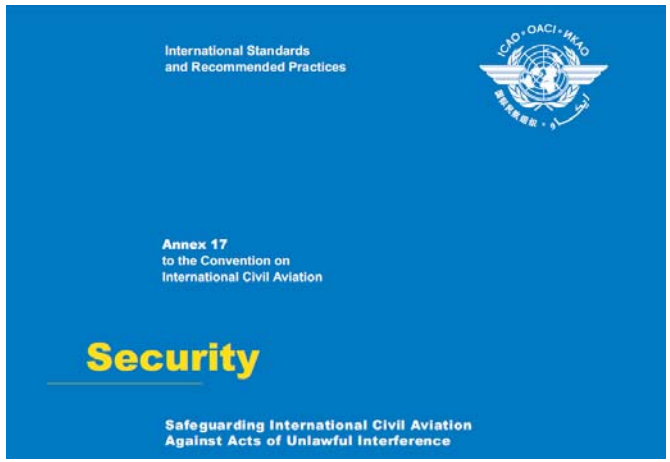
- L'ICAO nel 2013 ha introdotto in **Annex 17** (**Security**) la seguente Recomended Practice:

  «*Each Contracting State should develop measures in order to protect information and communicatione technology systems used for civil aviation purposes from interference that may jeopardise the safety of civil aviation*»

- **Doc 9985** (**ATM Security Manual**):

  «Protection of ATM system from security threats and vulnerabilities»

- L'ICAO ha istituito:
  - Aviation Security Panel (**AVSEC Panel**),un gruppo di esperti incaricati di individuare possibili minacce cyber per la sicurezza dell'aviazione civile e di sviluppare apposite Recomendations e security policies da adottare per tutti gli stati membri.
  - Secretariat Study Group on Cybersecurity (**SSGC**) e vari Working Group correlati, composti da esperti provenienti dagli Stati membri e dall'industria con l'obiettivo di promuovere lo sviluppo e la partecipazione a partnership e meccanismi governativi/industriali, a livello nazionale e internazionale, per la condivisione sistematica di informazioni su minacce informatiche, incidenti, tendenze e sforzi di mitigazione in tutta la comunità aeronautica.



EASA

- **EASA** (**European Aviation Safety Agency**) è un'Agenzia istituita dall'Unione Europea che fornisce consulenza tecnica alla UE nella stesura dei regolamenti e nella conclusione di accordi internazionali riguardanti la sicurezza aerea ed avente funzioni di carattere esecutivo, prima svolte dalle Autorità Aeronautiche dei paesi membri, quali:
  - L'omologazione dei prodotti aeronautici (certificazione dei prodotti e delle organizzazioni coinvolte nelle loro progettazione).
  - L'emissione delle Prescrizioni di Aeronavigabilità (le azioni da eseguire a carico di un aeromobile al fine di ripristinare un adeguato livello di sicurezza, laddove il livello di sicurezza di detto aeromobile rischi palesemente di essere compromesso).

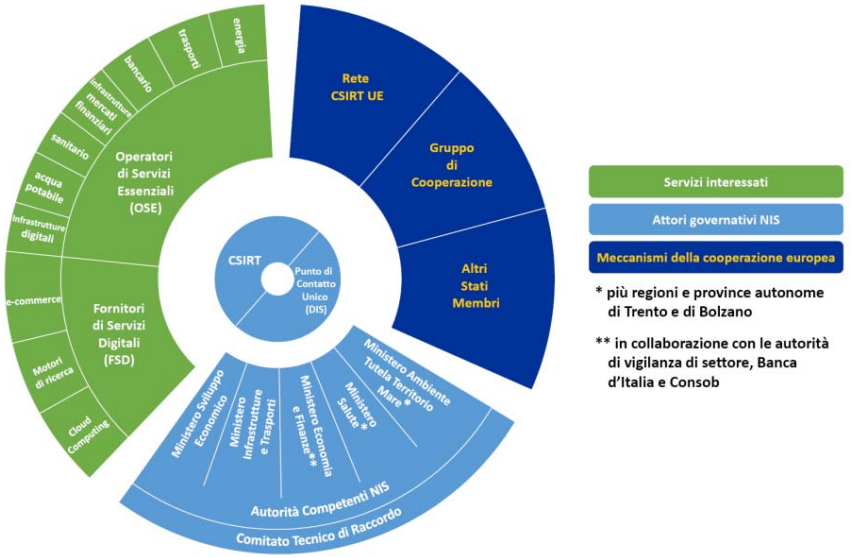
EASA: CYBER SECURITY

- Il nuovo Regolamento (UE) 2018/1139 di Base applicabile a tutti i domini EASA che definisce i requisiti essenziali norme comuni nel settore dell'aviazione civile, ha introdotto per la prima volta nella normativa europea la necessità di proteggere tutto il sistema aviazione civile dagli attacchi informatici, dal progetto al mantenimento del sistema/impianto nel corso delle operazioni
- Nel 2017 EASA ha firmato un memorandum di cooperazione con il Computer Emergency Response Team (**CERT-UE**) delle istituzioni UE. La missione di CERT-EU è sostenere le istituzioni europee per proteggersi dagli attacchi intenzionali e malevoli che ostacolerebbero l'integrità delle loro risorse IT e danneggerebbero gli interessi dell'UE.
- Frutto della collaborazione EASA e CERT-EU è il Centro Europeo per la Sicurezza Informatica nell'Aviazione (**European Centre for Cyber Security in Aviation - ECCSA**). La missione di ECCSA è quella di fornire informazioni e assistenza ai produttori europei di aeronautica, compagnie aeree, organizzazioni di manutenzione, fornitori di servizi di navigazione aerea, ecc. per proteggere gli elementi critici come aerei, sistemi di navigazione e sorveglianza, collegamenti dati, aeroporti.

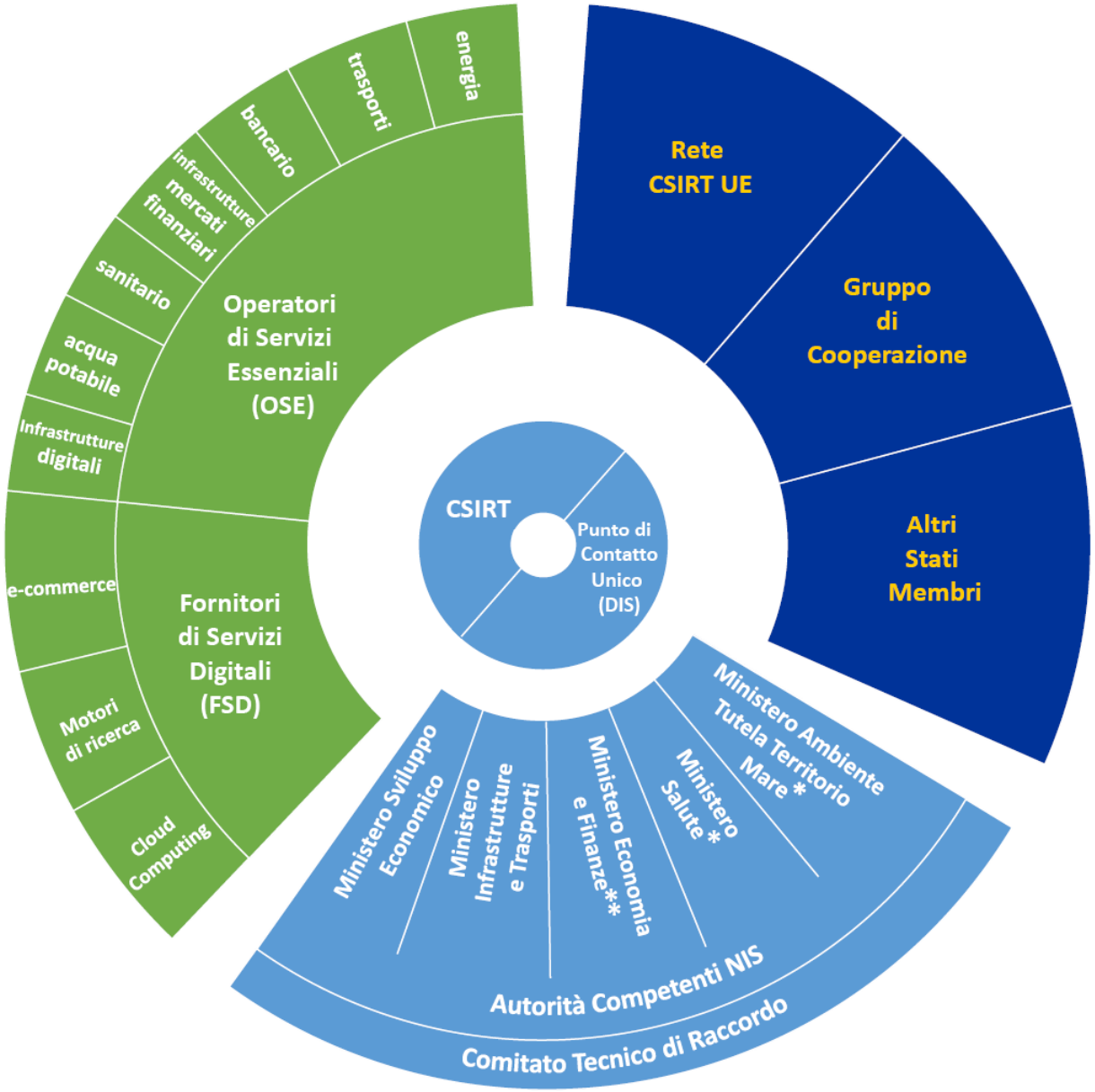
ECCSA
European Centre for Cyber Security in Aviation
Supported by EASA

UE: DIRETTIVA NIS

- Con il **D.Lgs 18/05/2018, n.65**, pubblicato su GU n.132 del 9/06/2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, (**Direttiva NIS Network and Information Security)** , intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli **Operatori di Servizi Essenziali (OSE)** e ai **Fornitori di Servizi Digitali (FSD)**.
- Gli **OSE** sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori **sanitario**, dell'**energia**, dei **trasporti**, **bancario**, delle **infrastrutture dei mercati finanziari**, della **fornitura e distribuzione di acqua potabile** e delle **infrastrutture digitali**.
- Gli **FSD** sono le persone giuridiche che forniscono servizi di *e-commerce*, *cloud computing* o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.



UE: DIRETTIVA NIS



Servizi interessati

Attori governativi NIS

Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

UE: GDPR

- Il **Regolamento generale per la protezione dei dati personali** n. 2016/679 (General Data Protection Regulation o **GDPR**) è la normativa europea in materia di protezione dei dati.
- Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta nel **maggio 2018**.
- Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati dell'Unione e sarà attuato allo stesso modo in tutti gli Stati dell'Unione senza margini di libertà nell'adattamento. Il suo scopo è, infatti, la **definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea**.

GDPR e NIS: APPLICAZIONI AERONAUTICHE

- **NIS -> Infrastrutture Critiche tra cui:**
  - Aeroporti e Compagnie Aeree.
  - Esistono esenzioni per le compagnie aeree e gli aeroporti più piccoli, ma ci si aspetta che il campo di applicazione si espanda nel futuro e spetta a ciascuno Stato membro dell'UE definire tali esenzioni.
- **GDPR**
  - Qualsiasi azienda che elabora i dati dai residenti nell'UE, indipendentemente dalla sede della società. Si applica a entità non UE.
- L'obiettivo è la prevenzione da attacchi informatici contro sistemi di gestione aeroportuale, in-flight Entertainment, sistemi WiFi per passeggeri, sistemi di informazione, sistemi di comunicazione da aereo a terra e sistemi TVCC.

SINGLE EUROPEAN SKY

- Il **Single European Sky** o **SES** («**Cielo Unico Europeo»**) è un'iniziativa lanciata dalla Commissione Europea nel 2000 per cui la progettazione, gestione e regolazione dello spazio aereo andranno armonizzate in tutta l'UE con l'obiettivo di rafforzare la sicurezza e l'efficienza del traffico aereo in Europa, di ridurre i ritardi e di ottimizzare la capacità degli spazi aerei.
- Nel contesto SES sono stati emanati dall'UE i seguenti Regolamenti:
  - il Regolamento CE n. 300/2008 del Parlamento Europeo e del Consiglio dell'11 marzo 2008 che istituisce norme comuni per la sicurezza dell'aviazione civile.
  - Regolamento Di Esecuzione (Ue) N. 1035/2011 Della Commissione del 17 ottobre 2011 che stabilisce i requisiti comuni per la fornitura di servizi di navigazione aerea.
- Il pilastro tecnologico dell'iniziativa SES è il progetto **SESAR (Single European Sky ATM Research)**.

SESAR

- **SESAR** (**Single European Sky ATM Research**) è il progetto di studio e realizzazione di un sistema di gestione del traffico aereo nell'ambito del SES volto a revisionare completamente lo spazio aereo europeo e il suo sistema di gestione del traffico aereo.
- Obiettivo del Programma SESAR è superare la frammentazione nazionale esistente e convogliare gli sforzi di Ricerca e di Sviluppo del settore verso sistemi di controllo di traffico aereo omogenei e moderni, in grado di garantire una capacità di traffico tre volte superiore a quella attuale, con costi unitari di rotta dimezzati, coefficienti di sicurezza 10 volte maggiori e ricadute ambientali 10 volte minori.
- Il Programma è gestito dal consorzio **SESAR JU** (**Joint Undertaking**) costituito dalla CE, EUROCONTROL, membri fondatori, 16 membri (fra cui **LEONARDO** e **ENAV**) più 16 partner associati, ovvero i principali service provider europei e le più importanti industrie del settore, che si sono impegnate affinché SESAR divenga la piattaforma di riferimento su cui ridisegnare il futuro sistema ATM europeo.

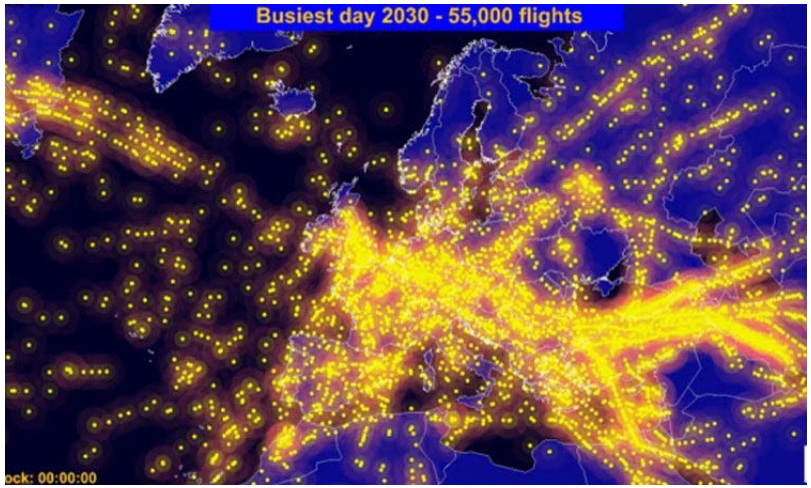
SESAR: CYBER SECURITY

- Il programma **SESAR 2020** (2016-2024) è il programma di innovazione e ricerca per il futuro dell'ATM in Europa volto a sviluppare soluzioni tecnologiche high-performing operational. Con un budget di 1.6 billion, SESAR 2020 supporterà progetti di sviluppo in 4 Aree:
  - **Airport operations**
  - **Network operations**
  - **Air traffic services**
  - **Technology enablers**.
- Il Programma SESAR 2020, gestito da SESAR JU, rappresenta la naturale evoluzione della prima fase (SESAR 1) e ha l'obiettivo di proseguirne il lavoro continuando gli sviluppi tecnico-operativi secondo le priorità europee dettate dall'European ATM Master Plan, riducendo sempre più il gap fra la fase R&D e quella di Deployment. Il programma prevede progetti Industrial Research & Validation, Very Large Scale Demonstrations, Exploratory Research
- Il Programma ha identificato la **Cyber Security** come «**Research Topic**» da indirizzare in tutte le Aree**.**
- L'obiettivo è di collaborare con EASA alla definizione e attuazione di una strategia europea per la sicurezza informatica nell'aviazione civile.

EUROCONTROL

- **EUROCONTROL** (European Organization for the Safety of Air Navigation) è l'organismo europeo istituito nel 1960 allo scopo di sviluppare e coordinare programmi e strategie mirate ad ottenere un efficiente e sicuro sistema di controllo del traffico aereo europeo.
- In particolare nella sede di Bruxelles risiede il **NMOC** - Network Manager Operations Centre (ex **CFMU** Central Flow Management Unit) ovvero l'unità centralizzata a livello europeo preposta alla gestione dei flussi di traffico aereo (ATFM).
- Tra i servizi operazionali forniti da NMOC rientra la validazione e distribuzione dei piani di volo e dei relativi messaggi associati (ARR, CHG, CNL, DEP e DLA) per conto degli Stati dell'area ECAC partecipanti al sistema centralizzato (41 Stati europei).
- Inoltre NMOC svolge la funzione di ottimizzazione in tempo reale del flusso di traffico nelle aree dove la domanda di traffico eccede la capacità disponibile valutando il re-routing per dei voli e l'assegnazione automatizzata degli Slots e gestendo i ritardi degli aerei al fine di offrire alternative per minimizzare i tempi di attesa.

EUROCONTROL



EUROCONTROL: CYBER SECURITY

- L' **ATM Security** di EUROCONTROL ha l'obiettivo di fornire**:**
  - Self-protection dei sistemi ATM.
  - Supporto implementativo e corsi di formazione.
  - Supporto Collaborativo a Istituzioni e Operatori.
- **In particolare viene dato supporto a:**
  - La Commissione europea, nel contesto del SAGAS (Stakeholders Advisory Group for Aviation Security), che identifica le infrastrutture critiche nell'ATM, implementa nuovi regolamenti per la sicurezza delle merci e della posta aerea da paesi terzi e progetti di R&S, ad es. GAMMA (Global ATM Security Management).
  - ICAO nello sviluppo e nella revisione del Manuale di sicurezza ATM e nello sviluppo di valutazioni di minacce e rischi per ATM.
  - ICAO threat and risk working group per cyber e CNS security.
  - ECAC nella revisione di ATM Security guidance (Doc 30).
  - Stati membri di EUROCONTROL.
  - Ricerca e sviluppo (SESAR).

EUROCAE

- **EUROCAE** (**European Organisation for Civil Aviation Equipment**) è l'organizzazione non profit nata nel 1963 composta da stakeholder nel settore del trasporto aereo: produttori, Air Navigation Services Provider, autorità nazionali di vigilanza, vettori aerei, gestori aeroportuali e altri utenti.
- I documenti EUROCAE hanno come scopo quello di sviluppare le specifiche operative per gli attori coinvolti nel settore e fungono da punto di riferimento per le idoneità agli standard europei (European Technical Standard Orders). Al fine di garantire una interoperabilità su scala globale, la documentazione prodotta dall'assemblea è in linea con la normativa ICAO e con il corrispettivo Ente di standardizzazione statunitense RTCA. Lo sviluppo della documentazione avviene nell'ambito di gruppi di lavoro (Working Groups) composti da specialisti di settore.
- EUROCAE ha istituito il **Working Group 72** (Aeronautical Information Systems Security) che recentemente ha pubblicato le Specifiche **ED-205** (Process Standard for Security Certification and Declaration of ATM/ANS Ground Systems). L'ED-205 descrive il processo utilizzato per identificare, valutare e gestire gli impatti sulla sicurezza dei sistemi ATM/ANS. Questo documento è usato per la certificazione o la dichiarazione di conformità ai requisiti di sicurezza applicabili.

ECAC

➢L'**European Civil Aviation Conference (ECAC)** è un organismo intergovernativo fondato nel 1955 dagli Stati che compongono il Consiglio d'Europa e che lavora in stretta collaborazione con l'ICAO, con lo scopo di promuovere un sistema di trasporto aereo sicuro, efficiente e sostenibile a livello europeo, perseguendo l'armonizzazione delle politiche dell'aviazione civile degli Stati membri e l'attenzione alle reciproche politiche aeronautiche tra gli Stati membri e altre parti del mondo.

➢**Doc 30 ECAC** è un documento che contiene, in chiave molto dettagliata, le misure e procedure di sicurezza ritenute necessarie per proteggere l'Aviazione Civile da atti di illecita interferenza. Le disposizioni in materia di sicurezza in volo, ATM, sicurezza informatica, gestione delle minacce e dirottamenti sono anch'esse incluse nel Doc 30, parte II. Le disposizioni del Doc 30 sono state recepite dalla UE e rese vincolanti con il Regolamento n. 2320 del 2002.

➢ ECAC ha inoltre istituito tre task force (Technical, Guidance Material and Training) e diversi gruppi di studio (ad esempio, rilevamento del comportamento, cani per la rilevazione di esplosivi, Cyber Security) per lo sviluppo di raccomandazioni a supporto per tutti gli Stati membri

ENAC

- L'Ente Nazionale per l'Aviazione Civile (**ENAC**), è l'unica Autorità di regolazione tecnica, certificazione, vigilanza e controllo nel settore dell'aviazione civile in Italia; è stato istituito il 25 luglio 1997 con Decreto Legislativo 250/97.
- Nei rapporti con i maggiori organismi sovranazionali (ICAO, ECAC, UE, EASA) è accreditato quale autorità competente per la sicurezza dell'Aviazione Civile.
- L'Italia ha aderito all'ICAO con D.Lgs 616/1948. Tuttavia il recepimento completo degli Annessi ICAO si è avuto tramite il D.Lgs 8/05/2005 che ha apportato modifiche al Codice della Navigazione (modificato ulteriormente in Mar/2006), per cui ENAC è stato autorizzato (Art. 690 C.N.) a recepire tutti gli Annessi ICAO con propri specifici Regolamenti.

ENAC
ENTE NAZIONALE PER L'AVIAZIONE CIVILE

ENAC: CYBER SECURITY

- **L'ENAC quale autorità di regolazione tecnica dell'aviazione civile ha la responsabilità di essere proattiva nel prevenire le nuove minacce cyber**. In particolare tra le azioni intraprese:
  - Sviluppare le conoscenze del personale addetto alla sorveglianza delle organizzazioni sulle tematiche generali che riguardano la cyber security.
  - Partecipare attivamente ai gruppi di lavoro sia nazionali che internazionali al fine di acquisire un'adeguata consapevolezza sulle tematiche inerenti la cyber security con particolare riguardo alle possibili minacce.
  - Assicurare il necessario e immediato scambio di informazioni con le istituzioni competenti in caso di attacchi informatici.
  - Pianificare e provvedere alla formazione iniziale in materia di cyber security tutto il personale addetto alla sorveglianza delle imprese che ricadono nei domini aeronautici di competenza ENAC.
  - Pianificare e monitorare i piani di sorveglianza sulle imprese certificate al fine di verificare l'adeguatezza della gestione delle situazioni di crisi, la capacità di individuare le cause all'origine e l'attuazione delle necessarie azioni correttive.
  - Assicurare il necessario coordinamento e scambio di informazioni con gli organismi nazionali e internazionali che si occupano di cyber security.
  - Partecipare attivamente ai test di simulazione di attacchi malevoli condotti sia a livello nazionale che europeo e internazionale.

ENAV

- L'Ente Nazionale Assistenza al Volo (**ENAV**) è la Società a cui lo Stato italiano demanda la gestione e il controllo del traffico aereo civile in Italia.

- Interamente controllata dal Ministero dell'Economia e delle Finanze e vigilata dal Ministero delle Infrastrutture e dei Trasporti, ENAV S.p.A. deriva dalla trasformazione nel 2000 dell'Ente Nazionale Assistenza al Volo in Società per Azioni, dopo la precedente trasformazione del 1996 in Ente Pubblico Economico.

- ENAV è una componente del sistema ATM (Air Traffic Management) internazionale, pertanto partecipa alle attività di ricerca e sviluppo in coordinamento con gli organismi di controllo internazionali del settore quali ICAO, EUROCONTROL e di categoria (CANSO).

ENAV: CYBER SECURITY

➢ENAV persegue una ***Security Policy*** per assicurare la sicurezza dei propri impianti e del personale, in modo da prevenire qualsiasi indebita interferenza nella fornitura dei servizi della navigazione aerea, e la protezione dei propri sistemi e dati dalle minacce alla sicurezza delle informazioni

➢ENAV ha sviluppato un proprio:

- ***Security Management System***, certificato UNI EN ISO 27001:2014:
- ***Security Operation Center***, in carico di monitorare la sicurezza informatica del gruppo che costituisce il motore operativo dei processi di prevenzione, rilevazione, contenimento, risposta e concorso alla *recovery*, nell'ipotesi di eventi pregiudizievoli per la sicurezza.

➢ENAV partecipa alla strategia di sicurezza cibernetica nazionale ed al quadro di protezione degli interessi di sicurezza e difesa nazionali, nella sua dimensione di infrastruttura critica e soggetto erogatore di servizi essenziali.

➢ Come membro del **CANSO** (Civil Air Navigation Services Organisation) ne condivide il Doc «CANSO Cyber Security and Risk Assessment Guide" documento contenente le linee guida per l'implementazione del programma di cyber security
di tutti gli ANSP associati.

canso
civil air navigation services organisation

IATA

- La **International Air Transport Association** (**IATA**) è un'organizzazione internazionale di Compagnie Aeree con sede a Montreal. Questa associazione unisce ed integra le varie reti di servizi delle compagnie associate permettendo, ad esempio, di poter controllare i prezzi e le disponibilità dei voli delle compagnie stesse anche da parte dei viaggiatori.
- Nel 2014 IATA, ICAO, Airports Council International (**ACI**), Civil Air Navigation Services Organisation (**CANSO**), e International Coordinating Council of Aerospace Industry Associations (**ICCAIA**), hanno condiviso una roadmap per allineare le proprie azioni circa le cyber threats.
- In particolare IATA ha sviluppato una “three-pillar strategy” (Risk Management, Advocacy, Reporting and Communication) per comprendere definire e valutare le minacce e i relativi rischi di attacchi cyber.

ASSAEROPORTI

- L'**Assaeroporti** (Associazione Italiana Gestori Aeroporti) è l'associazione delle 35 società di gestione aeroportuale operanti presso 42 aeroporti civili italiani.
- La cyber security è diventata una priorità di investimento per le compagnie aeree e gli Aeroporti, che soltanto nel 2018 hanno dedicato a questo capitolo di spesa 3,9 miliardi di euro (FONTE: SITA Indagine **2018 Air Transport Cybersecurity Insights**).
- Nello specifico a chiusura dell'anno le aerolinee destineranno alla sicurezza informatica il 9% della loro spesa IT complessiva (nel 2017 era il 7%), mentre per gli scali si arriverà al 12% rispetto al 10% dell'anno precedente.
- Tra le priorità di spesa più comuni ci sono per i prossimi tre anni, la consapevolezza e la formazione del personale (76%), l'adeguamento dell'infrastruttura ICT ai requisiti richiesti dalla normativa GDPR e Cybersecurity (73%) e la gestione di accessi e identità (63%), mentre tra le aree da monitorare e su cui sviluppare sistemi di difesa proattivi compaiono la rete, la sicurezza dell'extended enterprise (Cloud, Internet delle cose), la protezione da minacce interne come la fuga di dati, implementazione del Security Operation Center (SOC) per il monitoraggio proattivo.

ASSAEROPORTI
Associazione Italiana Gestori Aeroporti

TREND di MERCATO

- **AEROPORTI**:
  - Proteggere business e passeggeri dagli **attacchi informatici**
  - Perseguire maggiore efficienza con i servizi cloud, che riducono i costi di gestione
  - Offrire nuovi servizi self-service ai passeggeri (Check-in digitale)
  - Migliorare l'efficienza (tracciamento bagagli)

- **AEROPLANI**
  - Connessioni On-line
  - **Protezione da attacchi informatici**
  - Vettori unmanned
  - Data-link satellitari

- **ATM**
  - Sistemi ATM su piattaforme SWIM (System Wide Information Management) basate su Architetture Service Oriented (SOA).
  - Applicazione di Machine Learning per l'Automazione in ATM
  - **Strategia condivisa di Cyber Security**
  - Digital Information Management in ATM (Big Data)