IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

28 giugno 2021

Machine Learning e Cybersecurity al servizio dell'Aerospaziale per il supporto alla protezione aziendale

Anna Capoluongo

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

MACHINE LEARNING E CYBERSECURITY AL SERVIZIO DELL'AEROSPAZIALE PER IL SUPPORTO ALLA PROTEZIONE AZIENDALE

Anna Capoluongo[1]

ABSTRACT: In un momento storico - quale quello odierno - caratterizzato da un vero e proprio cambio di paradigma che sta sfociando in una modifica radicale della visione del "*mondo dei dati*", le informazioni assurgono a centro di interesse, anche e soprattutto nell'ambito dell'illecito e del *cybercrime*.

Chiariti, *in primis*, alcuni concetti tecnici imprescindibili, il *focus* del presente contributo va a concentrarsi sull'*Artificial Intelligence* pensata in relazione con l'ambito industriale-aerospaziale.

E così, passate in rassegna alcune tematiche preliminari, quali quelle – ad esempio – del *machine learning*, *deep learning*, *generative adversarial networks* e dei *massive natural language models*, ci si sofferma successivamente sull'applicazione dell'Intelligenza Artificiale a supporto della "*Space Economy*", con particolare riguardo alle criticità, alla *safety*, alla *cybersecurity* e agli standard ISO/EN e guidelines concretamente applicabili.

La disamina, dopo un passaggio su alcuni esempi di *machine learning* applicato alla tutela della *cybersecurity*, si conclude, infine, con un breve *focus* sulla sicurezza informatica e nello specifico sullo Standard ED-202A (Aviation Cyber-Security Essential).

ABSTRACT: *In a historical moment - such as the present one - characterized by a real paradigm shift that is leading to a radical change in the vision of the "*data's world*", information becomes a center of interest, also and above all in the field of offence and cybercrime.*

[1] Avvocato, DPO, Professore a c., Vice-presidente dell'Istituto di Ricerca per gli Studi Giuridici, Economici e Sociali (I.R.L.E.S.S.), Membro del Gruppo di Lavoro sull'Intelligenza Artificiale di ANORC.

Having clarified, first of all, some certain essential technical concepts, the focus of this contribution goes to concentrate on the Artificial Intelligence conceived in relation to the industrial-aerospace field.

And so, after reviewing some preliminary themes, such as - for example - machine learning, deep learning, generative adversarial networks and massive natural language models, we then dwell on the application of Artificial Intelligence in support of the "Space Economy", with particular regard to criticalities, safety, cybersecurity and the concretely applicable ISO/EN standards and guidelines.

The examination, after a passage on some examples of machine learning applied to the protection of cybersecurity, concludes, finally, with a brief focus on computer security and specifically on the Standard ED-202A (Aviation Cyber-Security Essential).

* * *

SOMMARIO: 1. Introduzione – 2. Parallelismi tra settore industriale e aerospaziale con riferimento alle criticità, alla safety e alla cybersecurity – 3. Esemplificazioni di machine learning a tutela della cybersecurity – 4. Brevi cenni ai riferimenti sulla sicurezza informatica con focus sullo Standard ED-202A (Aviation Cyber-Security Essential)

1. Introduzione

Data la sempre maggiore rilevanza del valore[2] dei dati e delle informazioni[3], è fisiologico che gli interessi (soprattutto in ambito di operazioni illecite) si siano fortemente spostati verso tali *asset*, tanto da determinare un aumento esponenziale di casi di *cybercrime* a danno, non solo e non tanto dei privati, ma soprattutto delle aziende.

[2] A. CAPOLUONGO, "*Il trattamento dei dati personali nelle operazioni societarie straordinarie*", in Compliance, luglio 2021 n. 2, pp. 47-52, ed. SEAC.
[3] Intese come insieme di dati significativi

Le aree di rischio sono, dunque, sempre più connesse agli ambiti della privacy e della sicurezza del dato/informazione, anche a causa della forte dipendenza dell'industria dall'infrastruttura digitale, senza dimenticare le criticità legate al *fattore umano*[4], tutt'ora anello più debole della catena del trattamento dei dati e della sicurezza informatica, e alle ricadute in termini di responsabilità[5] (civile, penale e anche ex D.lgs. 231/2001), danni e *brand reputation*.

Fa riflettere, peraltro, come tale scenario non sia limitato solo a determinate tipologie di imprese, trovando invece terreno fertile in quasi tutti i campi, tanto privati, quanto di riflesso nazionale ed internazionale e anche pubblico.

A siffatta sorte non sfugge, difatti, neppure un ambito ritenuto – correttamente all'inizio, ma erroneamente al giorno d'oggi – "al sicuro" quale quello aerospaziale, che per sua stessa natura è certamente a sé stante, isolato e basato su tecnologie proprietarie, ma che presenta ad ogni modo dei punti di attacco sfruttabili dai cyber-criminali.

La cosiddetta "space economy", portata alla ribalta da ultimo da Elon Mask, è infatti caratterizzata dal combinarsi di tecnologie spaziali e digitali, che però sono ancora connesse e controllate da siti a terra, tanto che i segmenti terrestri dei sistemi spaziali sono diventati le nuove "vittime" dei cyber-attacchi.

Ancora peggio se ci si sofferma a pensare che l'implementazione dei protocolli di sicurezza è di norma esternalizzata a soggetti terzi. E così le responsabilità derivanti, anche sotto il profilo della *data protection*.

O se si riflette circa gli aspetti legati alla *cyber warfare* e quindi agli attacchi sponsorizzati a livello (e per finalità) prettamente politiche o econo-

[4] Si pensi, ad esempio, al recente (2017) caso di trafugamento di dati per 10 giga (ossia 100.000 file di gestione amministrativo-contabile, progettazione di componenti aeromobili civili e velivoli militari) ad opera di un ex collaboratore responsabile della cybersecurity e un dipendente di Leonardo S.p.A.

[5] Cfr. A. CAPOLUONGO**,** *AI, la giurisprudenza guarda al danno da algoritmo*, https://www.ai4business.it/intelligenza-artificiale/ai-la-giurisprudenza-guarda-al-danno-da-algoritmo/; *Etica ed Intelligenza Artificiale. Il caso Replika: "Always here to listen and talk. Always on your side"*, https://www.cyberlaws.it/en/2020/etica-intelligenza-artificiale/.

miche, quali ad esempio gli APT (Advanced Persistent Threat)[6], caratterizzati dall'elevata competenza tecnica (e dalle grandi risorse umane e finanziarie) dell'avversario che li scatena.

Allo stato dell'arte, a correre in aiuto alle imprese possono essere certamente i sistemi di intelligenza artificiale (AI), nel cui insieme vanno ricompresi i concetti di *machine learning*, *deep learning*, *generative adversarial networks* (GANs o reti generative avversarie) e *massive natural language models*.

Il proseguio della presente trattazione presuppone una familiarità – quanto meno di base - con i concetti sopra espressi, pertanto sembra utile proporne a seguire un breve inquadramento al fine di facilitare la lettura e la comprensione.

Anzitutto, va distinta una prima Intelligenza Artificiale (anche, *deep A.I.*), imperniata sull'idea che un computer possa raggiungere livelli di intelligenza pari a quelli degli esseri umani ed essere del tutto autonomo, da una seconda (anche, *narrow A.I.*) in cui il *focus* è sulla simulazione – non autonoma – del pensiero o dei processi di pensiero umani.

[6] Focalizzati su attacchi su larga scala, invisibili (stealthy), dalla durata molto estesa e finalizzati a carpire informazioni riservate o di rendere inutilizzabili alcuni servizi dell'entità attaccata.

A seguire, per maggior comprensione della tematica, si riportano una prima figura di sintesi del ciclo vitale di un sistema di Intelligenza Artificiale e una relativa alla trasformazione dei dati, riprese dal report dell'ENISA (European Union Agency for Cybersecurity) del Dicembre 2020 dal titolo "AI Cybersecurituy challenges":

Figure 1: AI lifecycle generic reference model

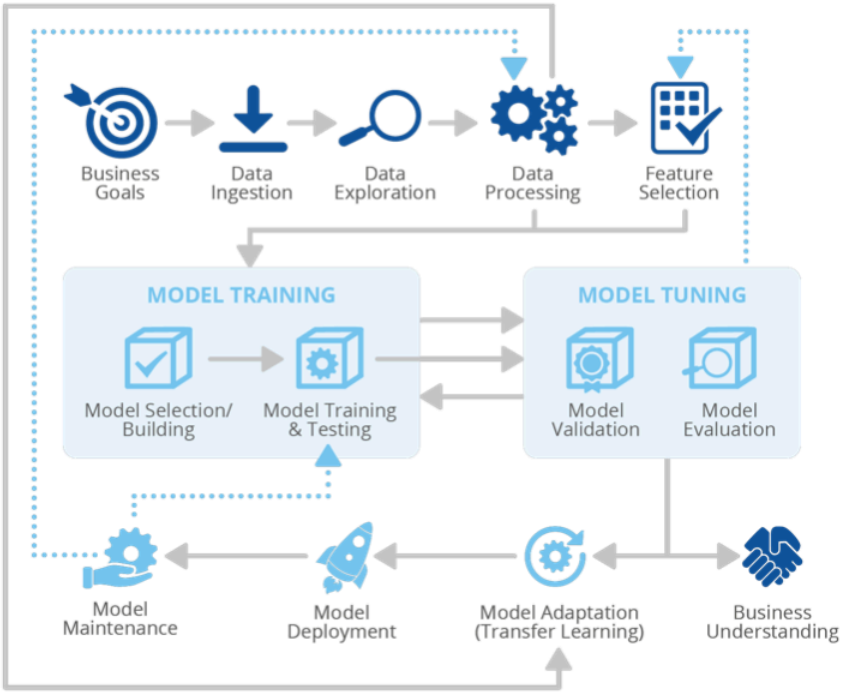


Figure 2: Data transformation along AI Lifecycle development stages

Ciò chiarito, e con riferimento ai metodi strutturati su reti neurali artificiali detti di *machine learning* (basati sull'addestramento di un modello mediante *dataset*) e *deep learning*[7] (noti come apprendimento profondo o strutturato profondo), gli stessi possono essere distinti in ulteriori "sottoinsiemi": supervisionato (basato su dati strutturati/classificati), semi-supervisionato (in cui di tutti i dati presenti nel training set, solo pochi vengono etichettati in precedenza), non supervisionato (basato su dati non strutturati) o per rinforzo (in cui il sistema migliora da solo le prestazioni, sulla base dell'interazione con l'ambiente).

Alla base di questo triangolo 'sommerso', sta l'insieme di tecniche che prende il nome di *data mining*, e che permette l'estrazione di informazioni utili da grandi quantità di dati, per mezzo di metodi (tra cui il *machine learning* e *deep learning*) basati su specifici algoritmi[8] addestrati a riconoscere relazioni causali"[9].

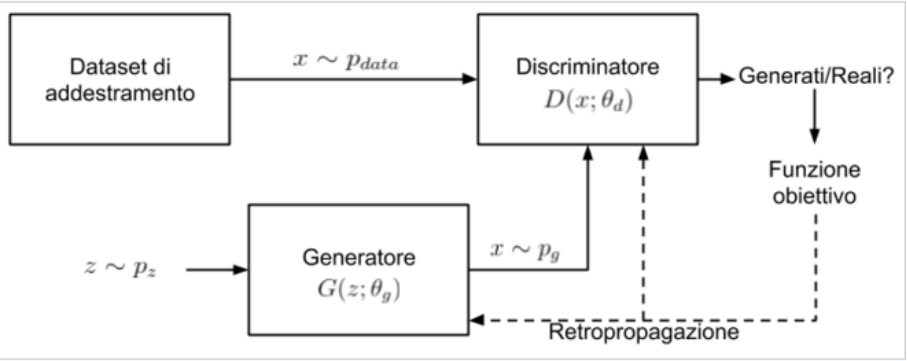
Un GAN, invece, è composto da due reti neurali: un cd. "generatore" che utilizza un input (dati) casuale per creare nuovi input e un "discriminatore" che cerca di distinguere gli input reali da quelli "fittizi" generati.

[7] Il deep learning è un approccio che consiste nell'utilizzare reti neurali molto profonde, cioè costituite da un numero elevato di strati. Ciò permette di creare sistemi più potenti, in quanto ogni strato può gestire un sotto-problema diverso dagli altri. Ad esempio, se applicato al riconoscimento di immagini, al primo livello competerebbe l'estrazione dei bordi, al secondo il riconoscere determinate forme semplici, al terzo forme complesse, al quarto ulteriori specifiche.

[8] Ad esempio quelli cd. euristici, progettati per risolvere problemi di particolare difficoltà.

[9] A. CAPOLUONGO, "*Internet of Bodies, neuroscienze e programmazione: dall'Habeas Corpus all'Habeas Mentem*", tesina per il Corso di Perfezionamento "Coding for Lawyers e Legal Tech", Università Statale di Milano, in fase di pubblicazione.

A seguire uno schema esemplificativo[10] di una rete generativa avversaria:



Rete generativa avversaria

Infine, i citati modelli di elaborazione del linguaggio si caratterizzano per l'unione di informatica, intelligenza artificiale e linguistica al fine di fornire ai sistemi la capacità di comprendere ed elaborare il linguaggio naturale (umano).

Ciò detto, e pur premesso che un'Intelligenza Artificiale propriamente intesa – e quindi scevra dalla supervisione umana, capace di totale autonomia - ancora non esiste e che neppure sulla definizione[11] stessa del termine vi è concordanza a livello globale, appare certamente condivisibile il rilievo che il supporto di *smart agent*, automazioni ed algoritmi possa consentire di in-

[10] Fonte Wikipedia, https://it.wikipedia.org/wiki/Rete_generativa_avversaria.

[11] Per Russell e Norvig (S. RUSSELL e P. NORVIG, *Artificial intelligence: a modern approach*, 2002), ad esempio, coincide con "*la progettazione e la costruzione di agenti intelligenti che ricevono percezioni dall'ambiente e compiono azioni che influenzano quell'ambiente*". Nella comunicazione sull'A.I. per l'Europa, invece, la Commissione ha proposto una definizione perfezionata, poi, nei termini che seguono: "*I sistemi di intelligenza artificiale (AI) sono sistemi software (e possibilmente hardware) progettati da esseri umani e che, avendo ricevuto un obiettivo complesso, agiscono nel mondo reale o digitale percependo il loro ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, applicando il ragionamento alla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di intelligenza artificiale possono utilizzare regole simboliche o apprendere un modello numerico. Possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti*" (Gruppo di esperti ad alto livello sull'IA, *Definizione dell'IA*, p. 8).

tercettare gli attacchi alla sicurezza e di contrastarli prima che gli stessi si trasformino in vere e proprie violazioni.

Ma tutto ciò come si mette in relazione con l'ambito industriale-aerospaziale? A vari livelli.

Le applicazioni concrete di tale mercato[12] vanno, infatti, ad incidere sui più disparati aspetti quali, ad esempio, il monitoraggio dei rifiuti, delle strade, delle ferrovie e delle reti idriche, il controllo dei valori di inquinamento, la verifica della stabilità di edifici, ponti, viadotti etc., i servizi basati sugli *space-data*, l'abilitazione di soluzioni IoT, le previsioni meteorologiche, le telecomunicazioni, i servizi audiovisivi, il controllo di eventi naturali/catastrofi, la navigazione marittima, aerea e terrestre.

2. Parallelismi tra settore industriale e aerospaziale con riferimento alle criticità, alla safety e alla cybersecurity

La realtà industriale è certamente un campo di gioco favorevole per l'introduzione e l'utilizzo dei sistemi di intelligenza artificiale, basati su algoritmi programmati per introitare importanti volumi di informazioni (*big data*), e questo perché l'ambiente noto e "controllato" permette un migliore addestramento dell'AI ed un maggior dominio dei *data base* di riferimento. C'è poi da rilevare come l'apprendimento automatico raggiunga le sue massime performance all'aumentare della grandezza del set di dati. Si dice infatti che tali sistemi migliorano le proprie prestazioni *in maniera adattiva* all'aumentare degli esempi da cui apprendono, secondo l'adagio *the more you do, the better you get.*

A tal proposito si pone, però, il problema di concedere l'accesso all'AI a tutte queste informazioni, consentendole di operare qualsiasi azione in "autonomia", poiché ciò comporterebbe l'inevitabile presentarsi di ampie zone di rischio quali: pregiudizi (*bias* o distorsione in gergo tecnico), errori, discriminazioni, effetto *black box*[13], conseguenze legali, danni economici,

[12] Ad esempio piccolo satelliti e servizi connessi ai lanci in orbita.

[13] "*i sistemi di IA sono in grado di produrre risultati, ma il processo con cui i risultati sono prodotti e le ragioni per cui l'algoritmo prende decisioni specifiche non sono pie-*

all'immagine e alla reputazione, falsi positivi o negativi, *overfitting*[14] (adattamento eccessivo) o *underfitting* (sotto-adattamento) del modello[15]. Sotto quest'ultimo profilo va ricordato che una buona *generalizzazione* richiede che il modello addestrato sia in grado di riconoscere la differenza tra segnale[16] e rumore[17], laddove per generalizzazione "*si intende l'abilità di una macchina di portare a termine in maniera accurata esempi o compiti nuovi, che non ha mai affrontato, dopo aver fatto esperienza su un insieme di dati di apprendimento*"[18].

Vi è poi l'aspetto del cd. *poisoning* o "avvelenamento" del sistema che ne comporta la manipolazione direttamente via data set (ad esempio modificando dei parametri) oppure mediante tecniche che agiscono sugli input al fine di portare (forzatamente) ad errori.

Ma gli attacchi informatici non si limitano a questo, investendo anche la *data protection* più ampiamente intesa - e quindi ricomprendente tanto le attività di trattamento di dati ed informazioni - quanto la sicurezza, capeggiata dalla triade C-I-A (confidenzialità, Integrità e Accessibilità) e seguita a ruota dall'interoperabilità e riutilizzabilità dei dati.

Tutto ciò assume un significato ulteriore se messo in relazione agli utilizzi concreti che ne vengono fatti nei settori della logistica, dei trasporti, navale, della missilistica, dove gran parte dei trattamenti avvengono grazie alle connessioni satellitari o sfruttandone il GPS. Pare evidente, dunque, come

---

*namente comprensibili per gli esseri umani. La trasparenza è quindi particolarmente importante per garantire l'equità nell'uso degli algoritmi e per identificare potenziali distorsioni nei dati di formazione" (*European Parliamentary Research Service (EPRS*), European framework on ethical aspects of artificial intelligence, robotics and related technologies*, 2020, raggiungibile al link: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU(2020)654179_EN.pdf).

[14] Sta ad indicare il sovraddattamento di un modello che include un numero eccessivo di parametri rispetto al numero di osservazioni e che quindi finisce per divenire disfunzionale.

[15] Si ha quando un modello viene addestrato in maniera molto (troppo) accurata su un training set specifico di dati, tanto da funzionare bene solo all'interno di quello e male adattandosi a set diversi. Quasi come se avesse imparato a memoria i dati del training.

[16] Semplificando, si intende il vero modello che si vuole imparare/riconoscere.

[17] O noise. I dati del mondo reale contengono dati irrilevanti o privi di significato definiti come rumore che possono influenzare in modo significativo varie attività di analisi dei dati dell'AI.

[18] Fonte: Wikipedia.

riuscire a disturbare i segnali GPS dei satelliti, oppure avere accesso a collegamenti non protetti (ad esempio da crittografia) o ancora il verificarsi di casi di *jamming*[19], potrebbe facilmente esporre ad altissimi rischi sistemi di guida, comunicazioni, operazioni militari e civili etc.

Vi è poi da valutare anche un'altra serie di aspetti, che emergono in seconda battuta. Quando il danno si produce proprio come conseguenza dell'utilizzo dell'AI, chi risponde? Per cosa? Secondo quali regole? E quali norme si applicano per la protezione delle informazioni?

Da una parte vengono in soccorso normative quali il D.lgs. 231/2001 sulla responsabilità penale degli enti, dall'altra il già citato GDPR con applicazione specifica alla tutela nel trattamento dei dati personali delle persone fisiche.

Ma la normazione più prettamente tecnica-ICT? Se è pur vero che vi sono standard, linee guida e raccomandazioni (es. ENISA), una regolamentazione vera e propria, *ad hoc*, riconosciuta, da applicarsi ad oggi sembra mancare.

Quanto, invece, alla verifica della rispondenza dell'AI utilizzata a determinati standard di etica (argomento da ultimo assai dibattuto) e di valutazione impatto sul trattamento dei dati personali (DPIA), allora i riferimenti cui guardare saranno – per il primo profilo - l'European Parliamentary Research Service, con le *EU guidelines on ethics in artificial intelligence: Context and implementation* del 2019; il Parlamento Europeo, con la *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))*; la Commissione Europea, con le *Linee guida etiche per una intelligenza artificiale affidabile* del 2019 e la Commissione Europea, con il *White paper on Artificial Intelligence* del 2020. Relativamente alla DPIA, i punti cospicui da menzionare sono, invece, *le indicazioni sulla redazione di una DPIA ai sensi dell'Opinion 4/2020*[20] *dell'EDPS sul "White Paper on Artificial Intelligence, i*

[19] In radiofonia, disturbo provocato intenzionalmente con interferenze e rumori.

[20] EDPS, *Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, 2020, raggiungibile al link: https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf.

suggerimenti del Garante del Regno Unito (ICO)[21]*, un sistema di autovalutazione mutuato dal framework del CSF e CSFP del NIST*[22] *e dalla linea guida Assessment List for Trustworthy AI (ALTAI)*[23], e l'AIA[24] canadese.

Senza dimenticare, ovviamente, la proposta di Regolamento sull'Intelligenza Artificiale[25] del 2021, dalla quale emerge l'obiettivo del mantenimento della *leadership* tecnologia (evitando *barrage*), affiancato alla necessità di bloccare effetti nefasti connessi all'uso non regolamentato dell'AI.

A ben vedere, l'approccio alla gestione di questi (ed altri) rischi è il medesimo tanto nell'industria comunemente intesa, quanto in quella più di "nicchia", come quella navale o aerospaziale.

Ecco che, quindi, i controlli applicabili – cui potersi riferire – saranno i più famosi ISO/IEC (principalmente 27001/27005) e NIST, basati su approcci suddivisi in più fasi, dalla identificazione (delle minacce, dei rischi, delle vulnerabilità), alla valutazione e *assessment,* al trattamento del rischio mediante l'individuazione di misure adeguate, alle *policies*, alla risposta alla minaccia per arrivare sino al monitoraggio e all'aggiornamento nel tempo.

Si ripete identica anche la netta separazione – soprattutto a livello di protezione – della parte relativa ai sistemi OT (*Operation Technology*)[26] da quella dei *Support Systems* e *IT Systems*.

Si deve puntare, in buona sostanza, alla *perimetrazione degli asset critici*.

Merita in tal senso farsi una digressione circa l'ambito dei sistemi di normazione volontaria europei ed internazionali, in particolare mettendo in

---

[21] ICO, *Guidance on the AI auditing framework*, 2020, raggiungibile al link: https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf, p. 16 ss.

[22] Si veda https://www.nist.gov/cyberframework.

[23] Si veda: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[24] Il *tool* è raggiungibile al link: https://open.canada.ca/aia-eia-js/?lang=en.

[25] Raggiungibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.

[26] Software e hardware direttamente connessi con la produzione, trasporto e trasformazione di beni. Un attacco cyber verso tali sistemi è particolarmente critico perché i potenziali impatti di ordine economico (mediante alterazione del funzionamento di un processo) possono poi tradursi anche nel danneggiamento di oggetti fisici.

correlazione lo standard di riferimento per il settore aerospaziale e della difesa (EN 9100[27]) con altri standard inerenti i principali sistemi di gestione, con *focus* sulle risorse ICT (ISO 27001, 20000-1 e 22301) che ormai rivestono sempre maggiore importanza, e con il GDPR.

Partendo, appunto, dall'ICT il primo *link* è con la ISO 20000-1 che affronta la tematica nel senso di definire determinati processi per la gestione dei servizi IT[28]. Sul punto è interessante rilevare come lo standard ISO 200000-1 si applichi a tutti i servizi ICT, inclusa la progettazione e lo sviluppo del software, con ciò che ne consegue anche a livello di correlazione con i requisiti di cui al GDPR, e nello specifico con i principi di *privacy by design* e *by default* ex articolo 25.

A tal proposito, è giusto il caso di ricordare che la norma volontaria non sostituisce la norma cogente (GDPR nel caso di specie), ma va intesa come mezzo e strumento tecnico per gestirne i requisiti.

Con espresso riguardo alla EN 9100 è opportuno in tal senso evidenziare come questa preveda espressamente che l'Organizzazione debba avere cura della proprietà dei clienti o dei fornitori, chiarendo che i *dati personali* dei clienti e dei fornitori debbano essere considerati proprio tra quelle proprietà di cui aver cura.

Con riferimento, invece, allo standard ISO 27001, recante requisiti per la gestione della sicurezza delle informazioni, questo si caratterizza per elencare una serie di controlli operativi applicabili per mitigare o prevenire il rischio di perdita di obiettivi di sicurezza delle informazioni, tanto per il perimetro di sicurezza organizzativo e delle risorse umane, quanto per quello fisico ambientale e di sicurezza IT.

Ancora una volta, la correlazione non si ferma a questi aspetti, ma va a coinvolgere anche l'ambito dei dati personali, dal momento che tra i controlli operativi dello standard ISO 27001 sono ricompresi anche quelli volti ad assicurare *compliance* in materia di privacy, cui si aggiungono quelli circa la

[27] La EN 9100 può ritenersi la declinazione nel settore aerospaziale e della difesa del più noto standard ISO 9001 recante i requisiti per un sistema di gestione per la qualità.
[28] Inclusi i processi per la gestione della sicurezza delle informazioni (ISO 27001) e per la gestione della continuità operativa (ISO 22301).

continuità operativa del trattamento delle informazioni (ISO 22301) o *business continuity*.

Venendo, poi, a quest'ultimo standard, si può dire che abbia assunto da ultimo una particolare rilevanza proprio nel settore aerospaziale e della difesa, anche alla luce dell'emergenza sanitaria mondiale (Covid-19) che ha necessariamente richiesto l'attivazione di meccanismi di continuità operativa sia all'interno dell'Organizzazione, sia all'esterno (ad es. lungo tutta la *supply chain*). La ISO 22301, infatti, aiuta ad individuare e gestire minacce attuali e future, adottando un approccio proattivo al fine di minimizzare l'impatto delle interruzioni (riducendo i tempi di fermo), salvaguardando l'operatività delle funzioni chiave, migliorando il tempo di risposta e la capacità di resilienza.

Non sfugge al richiamo del GDPR (art. 32 sulle misure di sicurezza) neppure questo standard, che difatti prevedere espressamente la resilienza del trattamento dei dati personali quale aspetto di rilievo.

Ancora, e con riferimento a tematiche che attraversano trasversalmente tutti i sistemi di gestione citati, non si può omettere di riportare due riflessioni in punto di *risk management* e *compliance*. E così, relativamente al primo profilo, è bene ricordare che la tematica viene declinata nelle linee guida dello standard ISO 31000 nonché in ulteriori linee guida su specifici aspetti (quali ad esempio ISO 27005 per i rischi inerenti la sicurezza delle informazioni), poiché sempre più, specialmente nel settore aerospaziale e della difesa, i rischi inerenti obiettivi di qualità, di servizi IT (Service Level Agreements), di continuità operativa (ad es. RPO, RPT, etc.), di sicurezza delle informazioni risultano tra loro inestricabilmente correlati.

Quanto alla tematica della *compliance*, va chiarito come questa non sia da intendersi solo in senso prettamente "Legal", bensì anche regolamentare, contrattuale e tecnico, così come testimonia sempre crescente convergenza tra il primo ambito (ricomprendente anche le leggi "LACO" o Leggi ad Alto Contenuto Organizzativo, quali ad es. il d.lgs. 231/01, la L.190/12 e il GDPR) e l'ambito più tipicamente tecnico normativo. In tale visione si inquadra, infatti, anche la recente emanazione da parte dell'International Standardization Organization dello standard ISO 37301 recante requisiti per la gestione della compliance nell'ambito dell'Organizzazione.

Infine, *last but not least*, con riferimento al mondo della data protection in ottica privacy – che può certamente rientrare nell'alveo dei trattamenti oggetto dei processi industriali – è d'obbligo citare due standard: la ISO 29134 riferita alla valutazione d'impatto (DPIA) e quindi all'analisi dei potenziali rischi impattanti sul trattamento di dati personali e la ISO 27701 che, sostanzialmente, estende la 27001 ai dati personali, assurgendo a sistema di gestione per la privacy.

I meccanismi di sorveglianza da utilizzarsi dovranno, dunque, essere realizzati nel rispetto degli standard consolidati appena esaminati, ma anche degli European Space Standards dell'European Cooperation for Space Standardization (ECSS[29]), dell'EF2000 (Eurofighter)-Software development standards[30], e di ulteriori specifici requisiti (tra i quali uno dei più rilevanti è l'*Hazard Analysis standard*).

3. Esemplificazioni di machine learning a tutela della cybersecurity

Nel momento in cui le applicazioni dell'intelligenza artificiale iniziano ad avere un impatto maggiore nel mondo reale è evidente che le stesse verranno sfruttate sempre di più anche per scopi malevoli[31]. È proprio il caso di quanto sta succedendo con i più recenti attacchi da parte degli hacker in tutto il mondo, come quelli ransomware dilagati nel 2020 e 2021.

[29] L'ECSS ha lo scopo di presentarsi quale standard per la gestione in qualità dei progetti spaziali. Le norme citate sono state sviluppate unitamente all'Agenzia Spaziale Europea (ESA) e si avvicinano allo standard ISO 12207 dal momento che prevedono i seguenti tre livelli: Space Project Management relativo a principi generali, organizzazione del progetto, fasi e pianificazione, gestione della configurazione e della documentazione; Space Product Assurance, relativo ad assicurazione qualità, sicurezza, materiali, qualità del prodotto software (standard ECSS-Q-80) e Space Engineering, relativo all'ingegneria di sistema, elettronica, software (standard ECSS-E-40). Le indicazioni per lo sviluppo del software sono concentrate proprio in questo documento.

[30] Per software di diversa natura: di bordo, di manutenzione, di training, del sistema di supporto a terra, etc.

[31] Esempi già in uso sono: indovinare password, rompere Captcha e clonare le voci.

Il report "*Malicious Uses and Abuses of Artificial Intelligence*"[32], ad esempio, avverte che i sistemi di intelligenza artificiale sono sviluppati per migliorare l'efficacia dei malware e per bloccare i sistemi anti-malware.

Ma l'AI potrebbe essere utilizzata a stretto giro anche per realizzare attacchi di social engineering su larga scala, progettare malware per il furto di documenti, evitare il riconoscimento facciale o biometrico, lanciare attacchi ransomware che sfruttano una profilazione intelligente, inquinare i dati, identificando falle nelle regole di rilevamento[33].

E, allora, in questo scontro aperto tra cyber-attack e cyber-defence, questi sistemi come possono essere usati per difendere i propri asset?

Iniziamo dall'evidenziare come 7 siano i principali ambiti in cui l'AI è in grado di incidere in maniera significativa, ovverosia:

- nell'**analisi delle minacce**, monitorando il traffico di rete per individuare attività sospette e classificarle;
- nella **rilevazione di malware**, identificandone nuovi tipi e rilevandone la presenza prima dell'apertura dell'eventuale file dannoso;
- nell'**analisi della sicurezza**, anche mediante la loro integrazione in *tool* e sistemi di gestione delle informazioni e degli eventi, grazie all'immensa capacità di calcolo connaturata all'AI;
- nella mitigazione delle minacce, mediante strumenti di "sicurezza aumentata";
- nella "**difesa attiva**"[34] che a sua volta si suddivide in
  - ***deception***, ossia fingere intenzionalmente qualcosa per fuorviare e rallentare gli aggressori. Per esemplificare, la generazione di documenti o profili di attività dall'aspetto realistico è un'area in cui l'apprendimento automatico eccelle.
  - ***Threat Intelligence o Cyber Threat Intelligence (CTI)***, che consiste nella raccolta di informazioni sulle minacce al fine di consentire, ad

[32] Realizzato da Europol, United Nations Interregional Crime and Justice Research Institute (Unicri) e Trend Micro

[33] https://www.corrierecomunicazioni.it/cyber-security/non-solo-deep-fake-ecco-come-lai-facilita-la-vita-degli-hacker/.

[34] Per approfondimenti, "*Machine Learning and Cybersecurity, hype and reality*", Giugno 2021, Center for security and emerging technology, Georgetown Walsh School.

esempio, di identificare gli exploit *zero-day*[35] prima che vengano implementati. Tra questi sistemi possiamo citare l'*early warning mechanism*, ossia un meccanismo di allerta precoce[36] capace di stimare il livello di rischio prima del verificarsi di un attacco (informatico o fisico) permettendo una risposta efficace.

- ***Attribution***, ossia l'attribuzione dell'attacco ad uno specifico avversario, al fine di determinare le probabili motivazioni e quindi migliorare la difesa e ridurre gli effetti dannosi.

Ciò premesso, e venendo ad esempi pratici di applicazione dell'AI in questo settore, come non citare il progetto di ricerca Cruise (Cyber security in Uas missions by Satellite link) finanziato dall'Agenzia spaziale europea (Esa) e dedicato alla valutazione della vulnerabilità e resistenza dei droni rispetto agli attacchi informatici. Fine ultimo quello di poter utilizzare i risultati per garantire la sicurezza nei trasporti aerei, ferroviari, navali e sulle autovetture a guida autonoma. Nello specifico questi gli obiettivi dei test: attacchi hardware (accesso ai sistemi di pilotaggio del drone); attacchi wireless; attacchi ai sensori, attacchi jamming e spoofing[37].

Ancora, a beneficiarne negli ultimi anni è stato anche il settore assicurativo, che inizia a sfruttare la precisione dei dati satellitari con lo scopo di redigere polizze sempre più "tailored" ed effettuare perizie da remoto attraverso le immagini satellitari.

Il monitoraggio di flussi di merci mediante tecnologie di localizzazione spaziale ha, inoltre, aperto nuove frontiere per l'industria dei trasporti, così come per l'Agrifood in cui le potenzialità dell'Ai possono essere sfruttate a pieno per il monitoraggio dei campi e del raccolto e l'implementazione dell'agricoltura di precisione.

---

[35] Un exploit zero-day è un attacco digitale che sfrutta le vulnerabilità zero-day al fine di installare software dannosi su un dispositivo. Una vulnerabilità zero-day rappresenta una falla nella protezione di un software presente su un browser o un'applicazione, non nota o conosciuta ma non gestita e per questo particolarmente rischiosa.

[36] Che può essere implementato come una catena di sistemi di comunicazione delle informazioni e comprende sensori, sottosistemi di rilevamento degli eventi e delle decisioni.

[37] Intercettazione di informazioni riservate.

4. Brevi cenni ai riferimenti sulla sicurezza informatica con *focus* sullo Standard ED-202A (Aviation Cyber-Security Essential)

In ambito di sicurezza informatica, come già brevemente accennato, il riferimento più noto è sicuramente quello del NIST, il quale suddivide l'analisi circa la valutazione dei livelli di rischio in 5 funzioni principali: *identify, protect, detect, respond and recover*, come da immagine che segue.

Sebbene sia indubbia la valenza del citato framework sulla cybersicurezza, ad onor del vero lo stesso non si adatta del tutto all'ambito del machine learning e dunque chiama a gran voce la ricerca di uno strumento più adeguato all'area di riferimento.

Il CSET[38], ad esempio, ha di recente elaborato (a sua volta) un modello che tenta di colmare alcune delle lacune cui si accennava, strutturato su 4 livelli, di cui uno innovativo rispetto al NIST, come si evince dalla tabella[39] che segue:

[38] Center for security and emerging technology, Georgetown Walsh School.
[39] "*Machine Learning and Cybersecurity, hype and reality*", Giugno 2021, pag. 3.

TABLE 1

A Comparison of Our Model and the NIST Cybersecurity Framework

NIST FUNCTIONS	OUR MODEL
Identify	Prevention
Protect	
Detect	Detection
Respond	Response and Recovery
Recover	
N/A	Active Defense

La cd. "active defence", infatti, viene definita così dal CSET: "*This term is used analogously to the way the SANS Institute has used it: as a spectrum of activity that includes annoyance, attribution, or outright counter-attack.14 Active de- fense can be thought of as an "other" category that includes any attempt to delib- erately engage or study external actors rather than simply responding to problems as they arise. This category can be broken down into a few more clearly defined subcategories, of which this report emphasizes three: (1) deception, or attempts to mislead and slow down adversaries; (2) threat intelligence, or attempts to actively study potential adversaries to better anticipate their actions; and (3) attribution, or attempts to connect multiple events to a single entity that can then be studied in more*

detail. Active defense, done well, can allow defenders to stay ahead of their ad- versaries and can potentially create disincentives against attacking in the first place*".

Ciò premesso, è il caso di soffermarsi brevemente sugli standard D-326A (USA) e ED-202A (Europa) intitolati "Specifiche del processo di sicurezza dell'aeronavigabilità"[40], a cui dovranno rifarsi produttori e operatori che vogliano certificare[41] sistemi e reti sotto il punto di vista della sicurezza informatica, dell'accesso non autorizzato, e dell'interruzione delle interfacce o delle informazioni dei sistemi elettronici degli aeromobili.

Il cd. "Set DO-326/ED-202" include anche dei documenti di accompagnamento, ossia il DO-356A/ED-203 "Metodi e considerazioni sulla sicurezza dell'aeronavigabilità"[42], il DO-355/ED-204 "Guida alla sicurezza delle informazioni per il mantenimento dell'aeronavigabilità"[43], l'ED-201 "Aeronautical Information System Security (AISS) Framework Guidance"[44] e l'ED-205 "Standard di processo per la certificazione di sicurezza / Dichiarazione del traffico aereo Servizi di gestione/navigazione aerea (ATM/ANS) Ground Systems".

[40] Questi rientrano nel "Set DO-326/ED-202" e sono strumenti di conformità accettati dalla FAA (Federal Aviation Administration) e dall'EASA (Agenzia Europea per la Sicurezza Aerea) per la certificazione della sicurezza informatica dell'aeronavigabilità, a partire dal 2019. "Airworthiness Security Process Specification", con l'edizione originale pubblicata nel 2010 e la sua revisione A nel 2014, definisce il processo di sicurezza informatica per lo sviluppo di aerei e sistemi, comprese le azioni da intraprendere per la certificazione in sé.

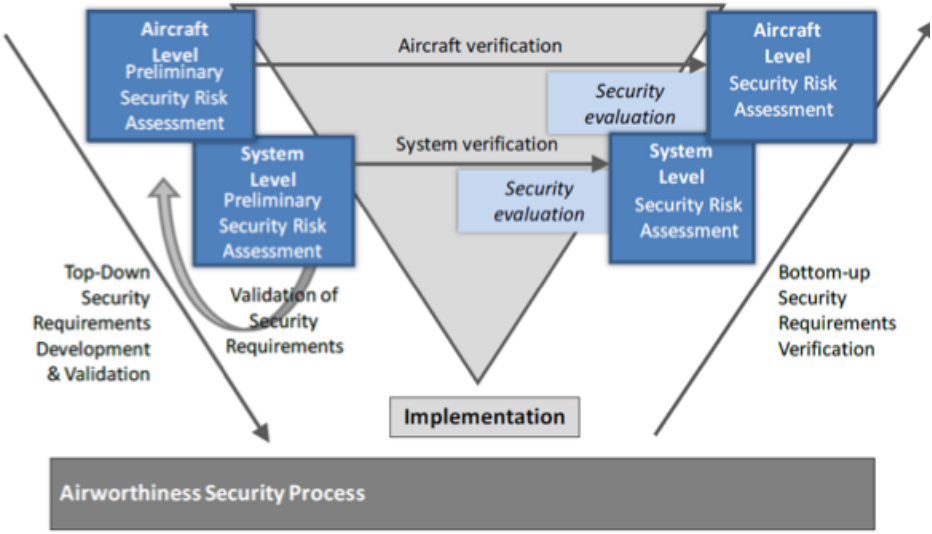
[41] L'EASA ha identificato sette diverse aree di specifiche di certificazione, compresi i requisiti tecnici normativi.

[42] "Airworthiness Security Methods & Considerations", con le edizioni originali rilasciate nel 2014 e 2015, e la sua revisione A nel 2018, è una guida pratica e dettagliata per l'implementazione di DO-326A/ED-202A.

[43] "Information Security Guidance for Continuing Airworthiness", pubblicata nel 2014, è una guida per la sicurezza informatica dell'aeronavigabilità.

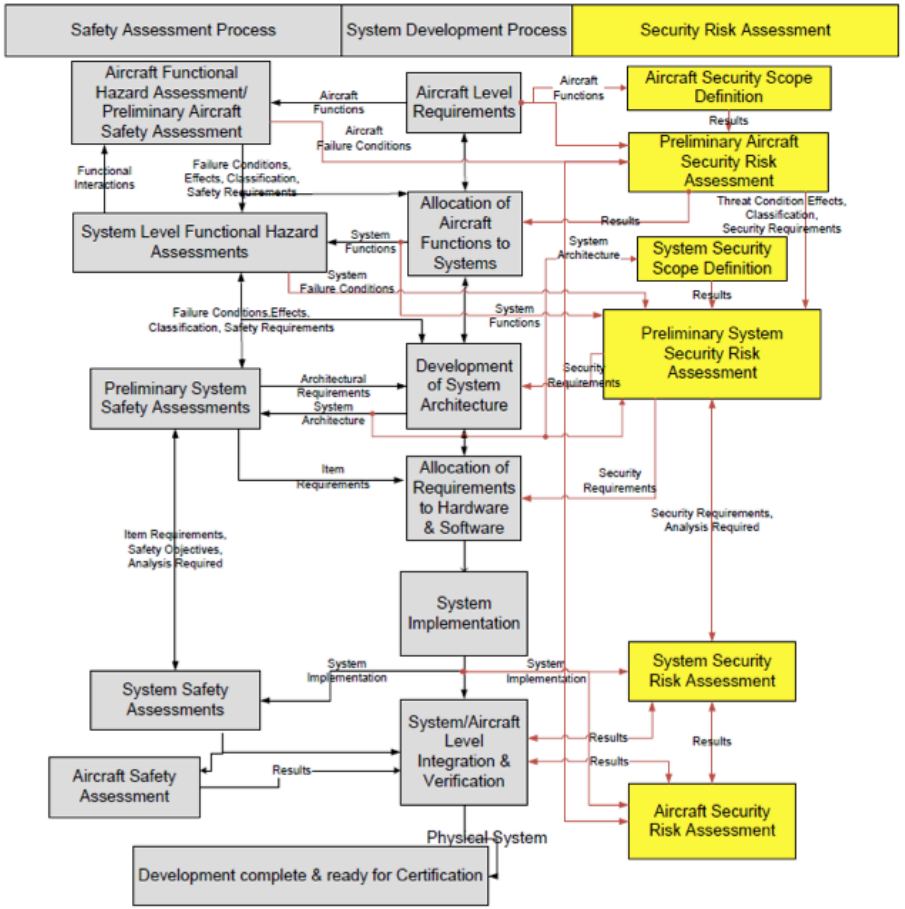
[44] "Aeronautical Information System Security (AISS) Framework Guidance", pubblicato nel 2015, è un documento "di alto livello" (non uno standard pratico) che delinea il "quadro generale" della Cyber-Security aeronautica per le varie parti interessate dell'aviazione.

Il DO-326A fornisce una chiara spiegazione del processo[45] di sicurezza dell'aeronavigabilità e della relazione tra i processi standard (Safety Assessment Process e System Development Process) e il nuovo processo per la Cyber Security (Security Risk Assessment)[46].



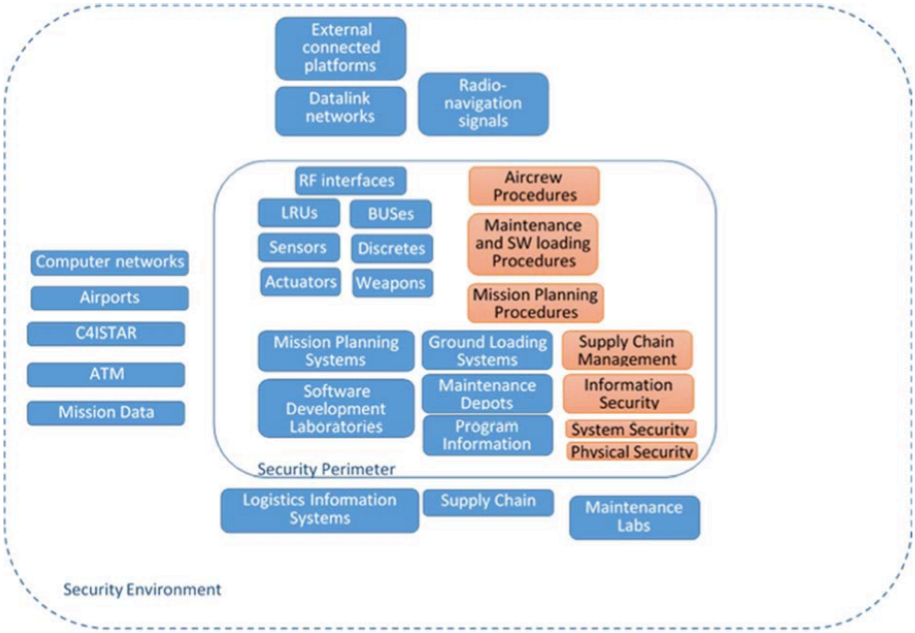
[45] "*Nella fase di progettazione/sviluppo, seguendo un approccio top down, le condizioni di minaccia identificate durante la valutazione iniziale della vulnerabilità vengono esaminate per definire nuovi requisiti di sicurezza e valutate per capire l'impatto sulla sicurezza del sistema aereo. Nella fase di verifica (valutazione della sicurezza), un approccio bottom-up viene effettuato per definire altri requisiti di sicurezza in un processo iterativo fino a raggiungere un livello di sicurezza accettabile", http://www.difesa.it/SGD-DNA/Staff/DT/ARMAEREO/Biblioteca/7Categoria/Documents/AER_EP_DT_2020_026_Ed_02072020.pdf.*

[46] Fonte: http://www.difesa.it/SGD-DNA/Staff/DT/ARMAEREO/Biblioteca/7Categoria/Documents/AER_EP_DT_2020_026_Ed_02072020.pdf.



Questo standard, ripartendo dai citati principi presenti nella ISO/IEC 27001, ripartisce ancora una volta le operazioni di analisi su differenti livelli, ma su 3 elementi specifici, ossia l'asset critico da proteggere, il perimetro di sicurezza e l'ambiente esterno che incide o può incidere sull'asset. Per ogni livello del perimetro potranno, poi, essere definiti gli asset fisici e logici maggiormente esposti a rischi cyber, gli effetti e le conseguenze. Quindi, una volta selezionato il *Target Object* per la valutazione, si definisce il Perimetro di sicurezza per la valutazione e, su questi elementi, si conduce il Cyber Security Analysis Process.

Si riporta per maggiore comprensione un esempio a quella che potrebbe essere l'analisi dell'ambiente di sicurezza per un sistema aereo:



Per concludere, è giusto il caso di rilevare come le sfide alla sicurezza in ambito industriale (e nello specifico nell'aerospaziale) possano provenire dai più disparati ambiti, fisici, logici, cyber, umani. L'unica soluzione che sembra poter portare a risultati validi è quella di un approccio olistico alla materia, che tenga conto, appunto, di differenti approcci e delle diverse direzioni da cui possono partire gli attacchi e le minacce, senza dimenticare di far rientrare nelle proprie misure di sicurezza anche una formazione pro-attiva del fattore umano e una "strong evaluation" del perimetro legal (anche e soprattutto di responsabilità) e di normazione, punto sul quale certamente sarebbe auspicabile l'emanazione quanto meno di linee guida che abbraccino tanto gli aspetti giuridici quanto quelli tecnici.

Una regolamentazione "ibrida", tra diritto e tecnologia.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future.
a cura di Alessio Persiani

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

ISSN (Online Edition): 2239 -7442