MINISTERO DELLA DIFESA

Strategia Digitale 2026-2030

Edizione 2026

PAGINA NON SCRITTA

On. Guido Crosetto
Ministro della Difesa

"*Il dato, la sua disponibilità, integrità, accessibilità e la sua protezione diventano, dunque, un tema centrale per il concetto di Sicurezza Nazionale nel suo senso più ampio.*"

Audizione presso la IV Commissione Difesa
della Camera dei deputati. 23 gennaio 2025

PAGINA NON SCRITTA

MINISTERO DELLA DIFESA

ATTO DI APPROVAZIONE

Approvo la presente "Strategia digitale della Difesa" – Edizione 2026.

Roma, li 27 aprile 2026

IL MINISTRO DELLA DIFESA

On. Guido Crosetto

PAGINA NON SCRITTA

INDICE

PAGINA NON SCRITTA

PERCHÉ UNA "STRATEGIA DIGITALE"

La Difesa riconosce l'esigenza di una specifica strategia, per attuare il proprio processo di trasformazione digitale e indirizzare la radicale transizione dal c.d. paradigma *net*-centrico a quello *data*-centrico[1].

Tale transizione sottende a sua volta, la centralità del processo decisionale *data-driven*, perseguendo un approccio di tipo *decision*-centrico[2], per il quale risulta essenziale massimizzare il valore del «dato», attesi i suoi impatti sulle decisioni dell'organizzazione.

In questa prospettiva, le nuove tecnologie giocano un ruolo determinante, fornendo gli strumenti necessari per trasformare il «dato» in decisioni strategiche.

Nell'attuale scenario di crescente instabilità e di continua evoluzione delle forme di competizione, la pronta implementazione dei citati paradigmi risulta indispensabile per gestire con rapidità ed efficacia l'incertezza dei contesti operativi.

L'obiettivo di questa Strategia Digitale è quello di consolidare l'efficacia dello Strumento militare nel suo complesso, garantendo superiorità informativa, processi di decision-making *guidati dai dati, interoperabilità – nazionale e internazionale – nonché la capacità di operare nel multi-dominio, in coerenza con le principali direttive dell'Alleanza Atlantica e dell'Unione Europea.*

I PILASTRI DELLA STRATEGIA

Il percorso strategico di trasformazione digitale della Difesa si fonda su tre pilastri:

---

valorizzazione del «dato»

connettività avanzata

sicurezza, resilienza e operazioni nel dominio cibernetico

Questi tre pilastri presentano una forte interdipendenza, tale per cui nessuno di essi può operare efficacemente in assenza degli altri. Ne consegue come un eventuale *deficit*, anche se limitato a un singolo pilastro, si ripercuota sull'intero dominio cibernetico, generando una vulnerabilità sistemica.

Pertanto, l'ambizione è quella di realizzare un **ecosistema digitale integrato, sicuro e resiliente** che sfrutta le nuove tecnologie per essere efficace nel supporto ai processi decisionali a tutti i livelli in ambito Difesa e si basa sul **«dato» quale centro di gravità**.

---

[1] Il passaggio dal paradigma *net*-centrico a quello *data*-centrico indica l'evoluzione concettuale dalla connessione delle piattaforme alla priorità di rendere i «dati» stessi il fulcro di qualsivoglia attività. In allegato *alfa*, è riportata la definizione di «dato» e i relativi "principi".

[2] Approccio che si concentra sull'identificazione, la strutturazione e l'automatizzazione delle decisioni chiave dell'organizzazione.

Con tale definizione si intende un'organizzazione complessa ove il «dato» è al centro dei processi decisionali e operativi, valorizzandolo come risorsa strategica primaria. In tale modello, ogni processo – dalla pianificazione strategica alla condotta delle operazioni, dalla gestione logistica all'addestramento – è alimentato da «dati» di qualità, accessibili, interoperabili e protetti. Ciò consente di prendere decisioni tempestive, informate e basate su evidenze oggettive, tali da collegare i «dati» al valore dell'organizzazione e tradurli in azioni concrete ed efficaci. Un'organizzazione *data-driven* sfrutta sistematicamente strumenti avanzati di *data analytics* [3] e di Intelligenza Artificiale (IA)[4] per estrarre valore dal proprio patrimonio informativo, abilitando capacità predittive, ottimizzazione delle risorse e vantaggio competitivo in scenari complessi e dinamici.

Quindi, l'obiettivo finale della Strategia è trasformare la Difesa in una **organizzazione "*fully digital, data-driven & decision-centric*"**, capace di operare con piena efficacia nel contesto multi-dominio. Questo significa evolvere da una cultura tradizionale, basata su procedure consolidate e gerarchie informative verticali, verso un modello agile, interconnesso e fondato sulla condivisione orizzontale dell'«informazione». In tal modo, il «dato» fluisce liberamente – nel rispetto delle classifiche di sicurezza – tra domini, livelli gerarchici e componenti dello Strumento militare, migliorando la qualità e la velocità delle scelte tattiche, operative e strategiche.

Tale trasformazione richiede non solo l'adozione di tecnologie all'avanguardia, ma anche un profondo cambiamento culturale e organizzativo, promuovendo competenze digitali, mentalità innovativa e un approccio collaborativo, quale fondamento della superiorità informativa e dell'efficacia operativa.

Al contempo, deve essere garantita la **piena coerenza in termini di sostenibilità**, affinché l'implementazione della Strategia possa essere declinata in un percorso concreto e pienamente rispondente alle esigenze operative.

LA STRATEGICITÀ DEL «DATO»

In analogia con quanto si osserva anche al di fuori del contesto militare, il «dato» della Difesa – e in particolare quello classificato – è un patrimonio strategico, tanto quanto lo sono i suoi *asset* convenzionali, e un abilitante trasversale. In quanto tale, il «dato» andrà vigilato lungo la *supply chain* e preservato durante il suo ciclo di vita, dalla creazione alla sua cancellazione.

Ciò eleva il «dato» a elemento imprescindibile per l'operatività delle Forze Armate. Infatti, una gestione del «dato» al passo coi tempi, porta a un vantaggio determinante nel c.d. "campo di battaglia digitalizzato" così come nel lavoro quotidiano, dove è sempre crescente lo spazio per strumenti di analisi e di IA.

Questi obiettivi si devono realizzare attraverso un percorso di sviluppo razionale, comprendendo valutazioni e scelte appropriate sulle info-strutture da realizzare e da impiegare, l'incentivazione della cultura *data*-centrica e la crescita della competenza, la ricerca del talento nonché l'aperta condivisione da parte di ogni Componente della Difesa.

---

[3] Gli strumenti di *data-analytics* sono *software* impiegati per elaborare, visualizzare e interpretare grandi quantità di dati grezzi provenienti da varie fonti. Attraverso un processo di raccolta, trasformazione e analisi, permettono di comprendere informazioni grezze con evidenze ed interpretazioni strategiche volte a migliorare l'efficienza dei processi di un'organizzazione.

[4] Cfr. Strategia della Difesa in materia di Intelligenza Artificiale – ediz. 2026.

Il tutto, mantenendo l'aderenza agli indirizzi delle principali Organizzazioni Internazionali cui l'Italia appartiene.

Altresì, va perseguita la virtuosa cooperazione inter-dicasteriale e inter-agenzia, finalizzata all'espletamento dei compiti di difesa e sicurezza militare dello Stato – così come previsti dal vigente quadro normativo – anche nel dominio cibernetico.

La Strategia contempla soluzioni a geometria variabile in ogni ambito e a ogni livello gestionale. In tal senso, è fondamentale anche il coinvolgimento dell'industria, delle istituzioni, del mondo accademico e di quello della ricerca, fornendo un ulteriore apporto al Sistema-Paese, nel costante impegno di salvaguardia degli interessi nazionali.

Le sfide si stratificano con crescente sofisticazione e indeterminatezza, minando sempre più le istituzioni democratiche e in generale, la sicurezza dei cittadini. Questo scenario richiede una partecipazione corale affinché il percorso di digitalizzazione sia tangibile anziché relegato a mera dematerializzazione. Ciò significa sostenere l'innovazione tecnologica e incoraggiare il cambio di paradigma nelle persone e nei processi, affinché la Difesa realizzi appieno le condizioni utili per la propria crescita in termini di capacità e competenze.

IL CONTESTO DI RIFERIMENTO

Il quadro internazionale

Da diversi anni, la NATO, l'UE e i Paesi di riferimento in termini di livello di ambizione – come Francia, Germania e Regno Unito – hanno indirizzato sforzi rilevanti per consolidare i propri processi di digitalizzazione.

In ambito **NATO**, l'indirizzo strategico è dato dalla *Digital Transformation Vision*:

"entro il 2030, il processo di trasformazione digitale consentirà all'Alleanza di condurre operazioni multidominio, di garantire l'interoperabilità, di migliorare la consapevolezza situazionale e di facilitare la consultazione politica e il processo decisionale basato sui dati".

Emanata nel 2022, il suddetto documento è stato integrato nel 2025 dalla *Data Strategy for the Alliance* (DSA) e dalla *Digital Transformation Implementation Strategy* (DTIS) 2.0.

La prima di esse definisce i *benchmark* per trasformare la NATO in un'organizzazione *data*-centrica, affinché i «dati» siano gestiti come risorsa strategica e condivisi in modo sicuro e interoperabile tra gli Alleati, al livello sia strategico sia operativo/tattico.
In generale, l'obiettivo della DSA è garantire «dati» di qualità, un modello di governo comune e un ecosistema di condivisione dei «dati», tale da supportare la superiorità

informativa e consentire decisioni *data-driven*, sfruttando anche modelli di IA e di *Machine Learning* (ML), in coerenza con i principi etico-valoriali[5].

Il secondo documento mira all'adozione coordinata delle tecnologie digitali, per modernizzare processi, forze e info-strutture dell'Alleanza. Esso definisce i risultati strategici da conseguire, i traguardi concreti e misurabili necessari a tradurre gli obiettivi in capacità nonché le attività operative, le responsabilità e le tempistiche per realizzare i *deliverable*, assicurando una progressione coordinata dell'intero processo di trasformazione digitale. In armonia con la *Data Strategy*, le sue finalità sono abilitare le operazioni multi-dominio, assicurare l'interoperabilità digitale, migliorare la consapevolezza situazionale e rendere più rapidi e informati i processi decisionali, attraverso strumenti come il c.d. *digital backbone* [6], l'*Alliance Data Sharing Ecosystem* (ADSE)[7] e una *digital-ready workforce* [8].
In generale, la DTIS 2.0 traguarda un'organizzazione *data-driven* e *digital-enabled* entro la fine del decennio, in accordo alla seguente *roadmap* (Fig. 1):

- 2026: (a) consolidamento delle una *digital-ready workforce*, attraverso programmi di formazione su *data science*, *cyber*, IA e tecnologie emergenti nonché scambi con industria e università; (b) sviluppo delle prime capacità operative[9] della *digital backbone*.
- 2027: disponibilità dell'ADSE per mettere a sistema «dati» provenienti da Alleati, NATO *Enterprise* e *partner* industriali, con particolare attenzione all'uso di «dati» di addestramento per i sistemi di IA.
- 2030: (a) piena operatività delle capacità di *digital-interoperability* e di operazioni multi-dominio abilitate dalla *digital backbone*; (b) disponibilità di una *digital-ready workforce* integrata, interoperabile e sicura, con almeno il 10% del personale NATO dotato di competenze avanzate.

Da rilevare come lo sfidante percorso sopra descritto interessi tutti i livelli di classifica del «dato», da NATO UNCLASSIFIED (NU) a NATO SECRET (NS).

Per la realizzazione di questi obbiettivi, la NATO ha attivato reti di acceleratori e centri di test come il *Defence Innovation Accelerator for the North Atlantic* (DIANA)[10] e il NATO

---

5 In tema di IA, la NATO dispone di una specifica strategia – dal contenuto classificato *RESTRICTED* – emanata nel 2021 e aggiornata nel 2025.

6 Il *digital backbone* della NATO è l'infrastruttura digitale di nuova generazione che integra sistemi, piattaforme e reti dell'Alleanza, assicurando connettività universale, trasporto sicuro dei «dati» e interoperabilità tra domini (terra, mare, aria, spazio e cyber).

7 L'*Alliance Data Sharing Ecosystem* (ADSE) è il meccanismo NATO concepito per favorire la condivisione sicura, protetta e interoperabile di «dati» e modelli IA/ML tra gli Alleati, la NATO *Enterprise* e i *Partner* qualificati.

8 Per *digital-ready workforce* si intende il personale – civile e militare – dotato di competenze, cultura e strumenti adeguati a operare efficacemente in un ambiente digitale e *data*-centrico.

9 Tali capacità comprendono reti federate, *cloud computing* (erogazione *on-demand* di servizi informatici tramite internet, per offrire un'innovazione più rapida, risorse flessibili ed economie di scala) e *data fabric* (architettura «dati» distribuita tale da consentire l'integrazione, la gestione e l'accesso uniforme a informazioni provenienti da fonti eterogenee, garantendo interoperabilità, sicurezza e *governance* centralizzata). In ambito "Difesa", tali capacità rappresentano il "tessuto connettivo" per consentire lo sfruttamento dei «dati» come risorsa strategica, rendendoli impiegabili in tempo reale per decisioni operative e multi-dominio.

10 Iniziativa NATO avviata nel 2021 per accelerare l'adozione di tecnologie emergenti e dirompenti (AI, autonomia, spazio, quantistico, biotech, materiali avanzati). Si fonda su una rete di acceleratori e centri di test sperimentali distribuiti tra gli Alleati, offrendo a start-up, PMI e centri di ricerca opportunità di sperimentazione in contesti *dual-use*, per stimolare la cooperazione pubblico-privato.

Innovation Fund (NIF)[11], allo scopo di contenere il c.d. *time-to-capability* [12]. DIANA e NIF costituiscono il pilastro del sistema innovativo NATO: il primo fornisce infrastrutture e *network* per la sperimentazione, il secondo risorse finanziarie per l'industrializzazione e la scalabilità delle soluzioni più promettenti.

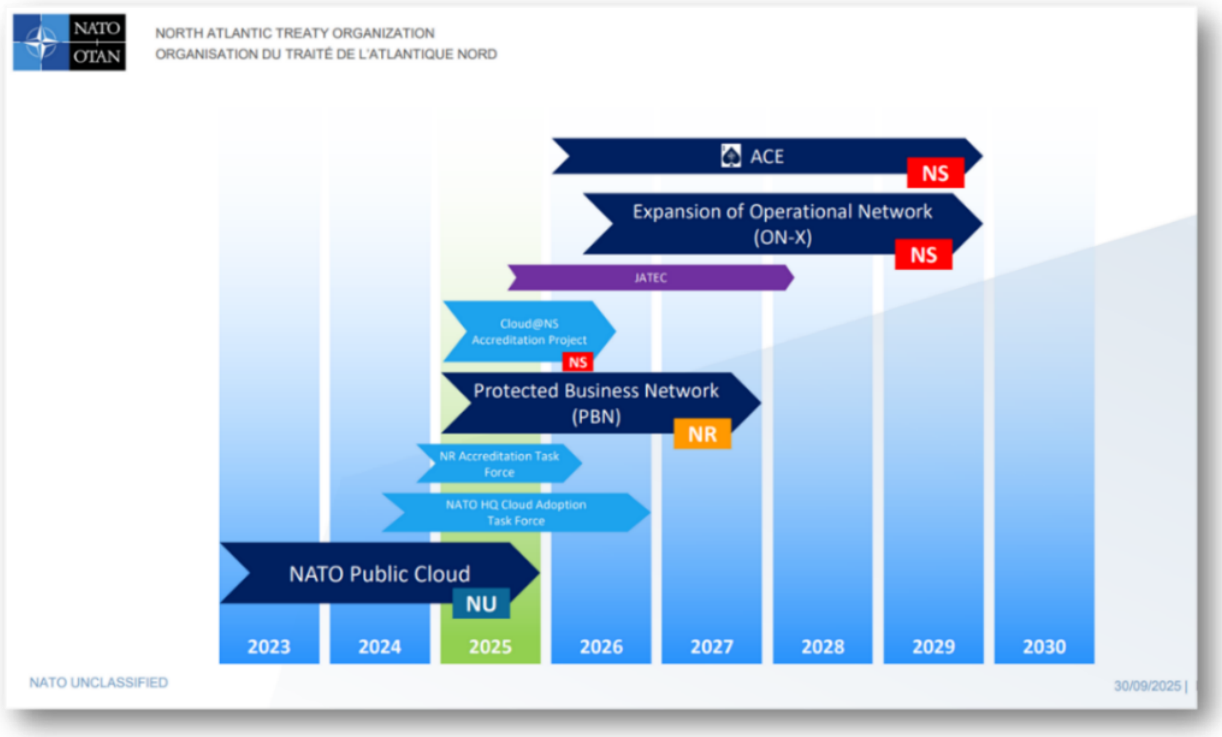


Fig. 1 - Piano di implementazione della migrazione in *cloud* dei servizi NATO, predisposto dalla neo-costituita *Cyber & Digital Transformation Division*.

A sua volta, l'**Unione Europea** contempla la digitalizzazione tra i pilastri dello *Strategic Compass* – con orizzonte 2030 – sostenendola con l'*European Defence Fund* [13], l'EU *Defence Innovation Scheme* [14] e la *Strategic Technologies for Europe Platform* [15]. Inoltre, si

[11] Fondo di investimento multinazionale lanciato nel 2022 con la partecipazione di 24 Paesi alleati che finanzia imprese tecnologiche e *start-up* ad alto potenziale, garantendo l'accesso a innovazioni strategiche.

[12] Per *time to capability* si intende l'intervallo di tempo necessario tra l'avvio di un programma di sviluppo/acquisizione e la sua effettiva disponibilità operativa, ossia quando la capacità è pienamente fruibile dalle Forze Armate.

[13] Strumento finanziario dell'Unione Europea dedicato a sostenere la ricerca collaborativa e lo sviluppo di capacità di difesa innovative tra gli Stati membri e l'industria europea.

[14] Iniziativa dell'Unione Europea volta a coordinare e valorizzare gli strumenti di sostegno all'innovazione nel settore della difesa, in particolare a favore di PMI, start-up e nuovi attori tecnologici.

[15] Iniziativa istituita con il Regolamento (UE) 2024/795 che mira a rafforzare la competitività industriale e l'autonomia strategica dell'UE sostenendo investimenti in tecnologie critiche (digitali, *deep tech*, pulite e biotecnologie). Utilizza fondi esistenti per finanziare progetti innovativi, offrendo un "marchio di sovranità".

annoverano diverse iniziative PESCO[16] tra cui i progetti *European Secure Software-Defined Radio* (ESSOR)[17] e *Robust Communication Infrastructure and Networks* (ROCOMIN)[18].

Da quanto accennato[19], seppur in un quadro frammentato, si evince come vi sia la convergenza sull'adozione di standard condivisi e di processi di *procurement* "*innovation-friendly*", sulla federazione dei «dati» e sul rafforzamento dei livelli di *cyber-resilience*. Inoltre, rilevano sforzi e investimenti volti alla creazione e alla professionalizzazione di una *cyber workforce* nazionale per supportare i processi di digitalizzazione che sono alla base degli sviluppi e competenze della società moderna.

Si evidenzia pertanto che, all'interno del perimetro NATO e UE, le nazioni con livelli di ambizione comparabili al nostro hanno intrapreso un analogo percorso *data-driven* abilitato da soluzioni *cloud*, sicurezza *by-design*, standard e cicli agili di *procurement*.

La situazione nazionale

L'Italia si trova in una fase di profonda riconfigurazione strutturale, il cui processo è guidato dalla Strategia nazionale "Italia Digitale 2026", la quale mira a collocare il Paese nel gruppo di testa dell'UE entro il termine del Decennio Digitale 2020-2030. In tale percorso, la presente Strategia mira a integrare il quadro di trasformazione digitale e innovazione tecnologica nazionale per gli aspetti di difesa e sicurezza militare, assicurando altresì un allineamento con le linee guida della NATO e dell'UE.

Al fine di mantenere il passo con le info-strutture e i programmi ad alta intensità tecnologica dei principali *partner*, sussiste l'esigenza di attuare investimenti mirati e di disporre di uniformità gestionale lungo tutto il processo di trasformazione digitale.

In particolare, l'impegno va profuso nella pronta implementazione di un modello di governo e gestione del «dato», nella migrazione in strutture cloud *pubbliche/qualificate/sovrane, nello sviluppo di sistemi per la sicurezza e la resilienza cibernetica, nell'acquisizione di competenze digitali e sulle* Emerging & Disrupting Technologies (EDT)[20]*, in accordo al ruolo istituzionale dello Strumento militare.*

---

[16] La *Permanent Structured Cooperation* (PESCO) è il meccanismo dell'Unione Europea, istituito nel 2017, per consentire agli Stati membri di sviluppare congiuntamente progetti di difesa e di potenziare la propria interoperabilità operativa e industriale.

[17] Il programma ESSOR riguarda lo sviluppo di *software-defined* radio (SDR) tali da permettere interoperabilità sicura tra forze europee nei domini terrestre, marittimo, aereo. Comprende lo sviluppo di forme d'onda specifiche, terminali radio e un'architettura comune per facilitare la portabilità del *software*.

[18] L'obiettivo del programma è potenziare le infrastrutture di comunicazione critiche e reti robuste per le forze armate europee, incluse soluzioni sicure e resilienti, dimostratori e iniziative tali da migliorare la mobilità operativa e la connettività sotto stress.

[19] Approfondimento in allegato *bravo*

[20] Tecnologie Emergenti e Dirompenti: sono innovazioni scientifiche e tecniche in rapida evoluzione che hanno il potenziale di trasformare radicalmente il modo in cui viviamo. Le EDT non si limitano a un singolo settore, ma hanno una natura orizzontale, influenzando settori come la difesa, la finanza, la salute e l'industria. A causa della loro natura radicale, le EDTs pongono sfide significative in termini di sicurezza (anche cibernetica), etica, regolamentazione e competizione geopolitica. Con riferimento agli argomenti trattati, tra le attuali EDT si evidenziano: IA, *Machine Learning* e tecnologie quantistiche.

Al contempo, la partecipazione a iniziative come la *Federated Mission Network* (FMN) [21], DIANA/NIF, EDF/EUDIS e il Polo Strategico Nazionale (PSN)[22] nonché la presenza di settori industriali e accademici di eccellenza (per esempio, navale, spaziale, cyber, robotica), garantiscono alla Difesa un potenziale rilevante e un vantaggio qualitativo in termini di dottrina, interoperabilità e cooperazione internazionale.

LA *VISION* PER I TRE PILASTRI DELLA TRASFORMAZIONE DIGITALE

Valorizzazione del «dato»

La Difesa dispone di un vasto **patrimonio informativo** cui va associato un appropriato grado digitalizzazione, coerente con le condizioni al contorno e le tendenze complessive dell'innovazione tecnologica.

La *Vision* per valorizzare il suddetto patrimonio dovrà pertanto sottendere un impianto digitale agile e interconnesso, dove l'informazione fluisce orizzontalmente tra domini e livelli decisionali per garantire la superiorità informativa.

Tale impianto dovrà basarsi su:
- un **modello di governo e gestione del «dato»**, a cui si devono correlare info-strutture e applicativi integrati, operanti su basi dati di qualità, funzionali all'adozione di soluzioni di *data-analytics* e di IA, in ottica di virtuosa diffusione di un ecosistema *data-driven*;
- la disponibilità di **info-strutture e infrastrutture tecnologicamente all'avanguardia**, quali **il *cloud* e l'*High Performance Computing* (HPC)**, con cui mirare al continuo potenziamento delle proprie capacità per valorizzare il «dato» nell'ottica di efficientamento dei processi decisionali;
- lo **sviluppo del "capitale umano"** attraverso programmi di formazione mirata nelle discipline STEM e la promozione di una cultura digitale a tutti i livelli.

Connettività avanzata

Le reti della Difesa, già diversificate e in continuo ammodernamento, devono risultare abilitanti per le operazioni multi-dominio, assicurando l'interoperabilità con i *partner* NATO e UE. In tale ottica, andranno garantiti gli standard di resilienza, sicurezza e continuità operativa connessi alle esigenze degli scenari militari e all'aumento esponenziale della quantità di «dati».

In particolare, la connettività dovrà prevedere:
- l'**unificazione delle reti nei diversi domini** per ottenere omogeneità da un punto di vista sia architetturale sia concettuale nonché per rendere più efficienti gli aspetti di impiego e gli articolati processi di certificazione;
- l'efficace **scambio dati tra differenti livelli di classifica** e in particolare, dal livello non-classificato ai livelli superiori;

[21] Iniziativa NATO per fornire un quadro comune di standard, capacità e specifiche tecniche volte a garantire l'interoperabilità digitale tra le Forze Armate alleate e partner. Basato sull'esperienza maturata nelle operazioni in Afghanistan, la FMN consente la creazione di reti federate sicure e scalabili, facilitando la condivisione di dati, comandi e servizi ICT in contesti coalizionali. La FMN è basata su spirali evolutive, ciascuna delle quali definisce parametri da conseguire entro il 2030

[22] Il Polo Strategico Nazionale (PSN) è l'infrastruttura *cloud* ad alta affidabilità nata per ospitare i dati e i servizi critici e strategici della Pubblica Amministrazione italiana. Rappresenta il pilastro operativo della Strategia *Cloud* Italia, il piano che mira a migrare almeno il 75% dei dati della PA verso ambienti sicuri entro il 2026.

- l'eventuale realizzazione di una **rete a bassa classifica** da affiancare all'attuale **rete ad alta classifica**, per rispondere alle effettive **esigenze di gestione e classificazione dei «dati»** nonché per consentire il passaggio di dati non-classificati, di cui al punto precedente;
- costante **allineamento all'evoluzione della citata iniziativa FMN**;
- la fornitura di una **crescente disponibilità di banda**, con particolare riferimento all'uso di servizi satellitari multi-orbita e multi-*provider*.

Sicurezza, resilienza e operazioni nel dominio cibernetico

Lo scenario cibernetico presenta una crescente complessità: la tecnologia digitale compenetra ogni settore e la persistente competizione rende sempre più indefinito il confine tra pace e guerra. Da ciò deriva la necessità di affrontare inedite minacce e sfide.

Alla stregua di quanto avviene nei domini operativi tradizionali, lo Strumento militare è chiamato al compito primario della difesa e sicurezza militare dello Stato anche nel *cyber-space*.

In considerazione delle peculiarità del dominio cibernetico, l'assolvimento di tale compito richiede l'adozione di un modello operativo in grado di garantire la capacità di difendere, ingaggiare, contrastare e rendere inoffensive le iniziative malevoli.

Inoltre, tale modello deve prevedere un'integrazione sinergica e senza soluzione di continuità con gli altri Pilastri tecnico-operativi dell'architettura nazionale di sicurezza cibernetica[23], assicurando un approccio coordinato per la protezione dell'intero dominio cibernetico.

Ciò va perseguito tramite:
- l'arruolamento di **risorse umane qualificate e specializzate (talenti)** e la valorizzazione del personale in servizio, da accentrare per realizzare una "massa critica" di risorse (c.d. *cyber workforce*) caratterizzata da costante prontezza operativa e capacità tecnologiche avanzate, idonea a operare nell'ambito di una più ampia minaccia ibrida e "non convenzionale", tipica degli attuali scenari di confronto;
- lo sviluppo di capacità per la conduzione di **operazioni cibernetiche *full-spectrum***, anche in ottica di protezione delle infrastrutture critiche nazionali e di contrasto alla minaccia ibrida negli ambienti informativo e cognitivo, incrementando la deterrenza del Sistema Paese a tutela degli interessi strategici nazionali. Tale aspetto andrà perseguito, sfruttando le EDT per ampliare, automatizzare ed ottimizzare le capacità esprimibili;
- strumenti e processi che consentano l'**acquisizione di prodotti e servizi "allo stato dell'arte" nei settori ICT e Cyber** e l'**aggiornamento tecnologico delle capacità**, in maniera agile, coerente con la velocità dell'innovazione nonché con l'evoluzione della minaccia;

[23] La Strategia Nazionale di Cybersicurezza 2022-26 prevede quattro Pilastri tecnico-operativi. Essi sono: (1) L'Agenzia per la Cybersicurezza Nazionale (ACN), con compiti di coordinamento, resilienza, certificazione, protezione; (2) le Forze di Polizia e gli organismi interni al Ministero dell'interno per la prevenzione e il contrasto della criminalità informatica; (3) il Ministero della difesa, responsabile per la difesa dello Stato nello spazio cibernetico; (4) gli organismi del Sistema di Informazione per la Sicurezza della Repubblica a cui sono affidate le attività di ricerca e di elaborazione informativa per la tutela degli interessi nazionali.

un'**evoluzione** dell'attuale **impianto normativo** per abilitare la Difesa (e tutelare il proprio personale) a operare nel pieno delle proprie capacità ai fini dell'assolvimento dei compiti istituzionali, sin dal tempo di pace.

I – LA VALORIZZAZIONE DEL «DATO»

INTRODUZIONE

Il primo pilastro della Strategia si focalizza sulla valorizzazione del patrimonio informativo della Difesa (*data exploitation*), promuovendo un utilizzo ottimale dei «dati» come risorsa fondamentale per tutti i processi, siano essi di natura operativa, logistica o amministrativa.

In quest'ottica, è necessario adottare strumenti tecnologici avanzati tali da consentire una gestione efficace delle informazioni e un continuo sviluppo di capacità, integrando progressivamente anche le EDT.

Un patrimonio informativo di valore è una condizione necessaria per ottenere un vantaggio operativo, organizzativo e decisionale. Ciò è perseguibile con un cambio radicale nel modo di operare con l'«informazione» e nell'adattamento – anche del singolo militare o civile della Difesa – nelle azioni concrete di ogni giorno così come nelle esigenze operative sottese alle minacce multidimensionali e geopolitiche al contorno.

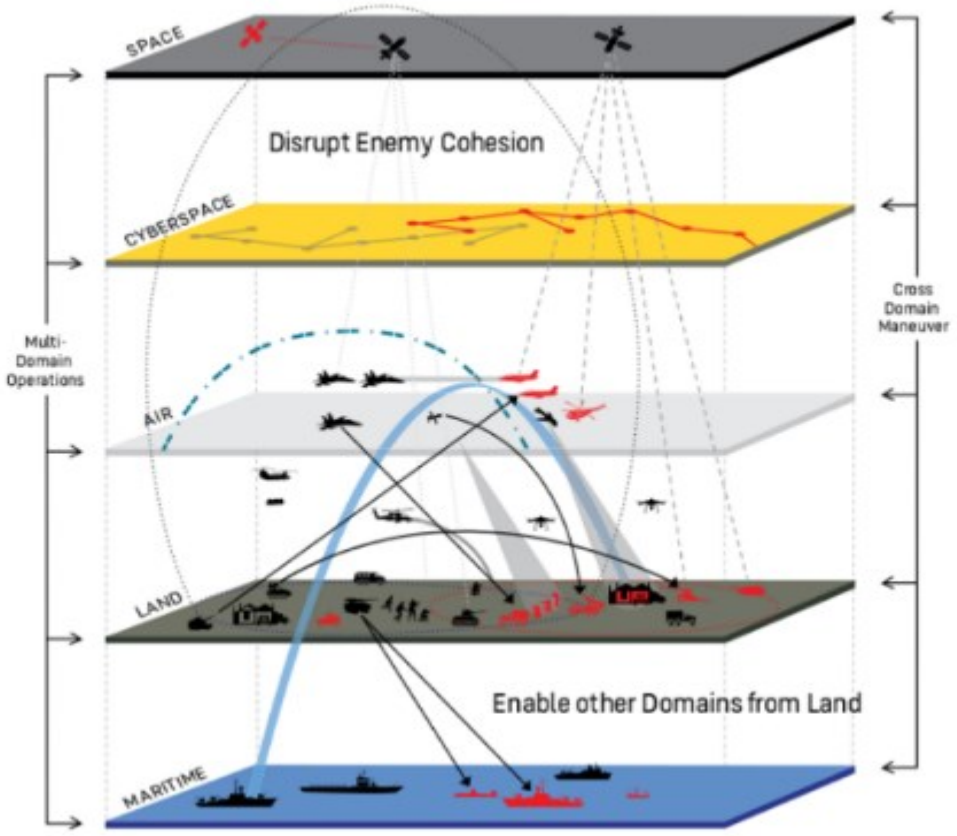


Fig. 2 - Rappresentazione delle operazioni multidominio.

Il punto di partenza è un «dato» di qualità e condiviso, funzionale a trarre il massimo beneficio dai citati strumenti tecnologici a livello strategico, operativo e tattico. In particolare, detti strumenti sono abilitanti del *data-driven decision-making process*, utile a supportare il decisore con un contributo strutturato, completando il peculiare – e insostituibile – istinto del "Comandante".

Nel suo complesso, la Difesa già dispone di un prezioso volume di «informazioni» e necessita di un sistema strutturato di *data governance* e *data management*, per massimizzare la valorizzazione del «dato», non-classificato e, soprattutto, classificato.

Infatti, migliorare la qualità, l'integrità, la disponibilità dei «dati» e garantirne la congruenza, è indispensabile per **produrre informazione di valore**, essenziale per il vantaggio strategico, operativo e tattico e per la leva sinergica delle Componenti della Difesa, in risposta alle minacce convenzionali e non convenzionali, nello spazio fisico, cibernetico e cognitivo.

Il traguardo è l'operatività trasversale di tutta la Difesa, raggiungibile solo tramite la qualificazione del «dato» come collante della c.d. manovra multi-dominio, in armonia anche con quanto perseguito in ambito NATO*.*

In particolare, un governo uniforme del «dato» a livello interforze, consentirà di realizzare il principio del *need to share* [24], garantendo un'efficace condivisione delle informazioni tra le diverse articolazioni della Difesa, abilitando i processi di analisi e i modelli decisionali guidati dai «dati», a tutti i livelli della catena di comando.

Tale approccio, integrato dall'adozione di tecnologie *cloud* e di calcolo ad alte prestazioni (i.e. HPC), garantirà:

Integrità del dato: le elaborazioni potranno avvenire su «dati» costantemente aggiornati e affidabili.

Riduzione della superficie d'attacco: i «dati» risiedono su architetture avanzate (quali i *data lakehouse*[25]) e applicazioni sviluppate secondo criteri di *security-by-design*, minimizzando i rischi di *data breach* e garantendo la conformità normativa, compreso il rispetto del principio di minimizzazione nella conservazione dei dati personali.

Abilitazione dell'IA: l'utilizzo efficace dell'IA richiede «dati» affidabili, integri e di qualità, obiettivo raggiungibile attraverso infrastrutture adeguate, siano esse tradizionali o in *cloud*.

[24] Nell'applicazione del paradigma *data*-centrico, fermo restando il rispetto del tradizionale principio di *need to know*, basato su una condivisione selettiva e gerarchica delle informazioni, si sta adottando il principio del *need to share*, che promuove la disponibilità del dato tra attori autorizzati lungo l'intero ciclo di vita informativo. Tale evoluzione non implica una riduzione dei livelli di sicurezza, ma un loro rafforzamento attraverso meccanismi di *governance* del dato, interoperabilità, classificazione, tracciabilità e controlli di accesso dinamici, finalizzati ad abilitare tempestività, coerenza e superiorità informativa.

[25] Un *data lakehouse* è un'architettura dati ibrida che combina le caratteristiche di un *data lake* (per la memorizzazione flessibile e a basso costo di dati grezzi, strutturati e non strutturati) con quelle di un *data warehouse* (per l'elaborazione efficiente di *query* analitiche e *business intelligence*). Consente l'integrazione e l'analisi unificata di dati eterogenei, supportando l'implementazione di una *governance* dati moderna come descritta nella presente Strategia.

Resilienza e adattabilità: sarà possibile rimodulare e riadattare rapidamente l'ambiente ICT in risposta a situazioni avverse, in ambito sia classificato sia non classificato, ricercando altresì ridondanza delle relative info-strutture.

Ottimizzazione delle risorse: una gestione uniforme e le economie di scala consentiranno di ottimizzare le disponibilità economiche, l'impiego del personale specializzato e i tempi di gestione, migliorando la sostenibilità complessiva e contenendo anche il traffico di rete.

Gestione delle classifiche agevolata: l'uso di info-strutture appropriate – anche in termini di certificazione – faciliterà la trattazione delle classifiche e delle qualifiche dell'informazione, garantendone il corretto grado di sicurezza e protezione.

Crescita di produttività e motivazione professionale: si faciliterà l'uso di soluzioni di *collaboration* per l'elaborazione dei «dati», capitalizzando il c.d. *Return on Future*[26];

Continuità operativa[27]: nel rispetto della sicurezza del dato e della resilienza dell'infrastruttura classificata e non-classificata, sarà garantito il pronto accesso ai «dati» anche da remoto, con particolare riguardo alle esigenze dei livelli dirigenziali e del *top management*.

Per rispondere alle esigenze operative e di gestione tecnico-operativa, tecnico-industriale e tecnico-amministrativa dell'Organizzazione, è indispensabile adottare un modello strutturato univoco di data governance *e* data management*, razionalizzando e standardizzando le info-strutture sul piano tecnologico e normativo. Ciò consentirà di realizzare una piena sinergia digitale tra le componenti terrestre, marittima, aerea, spaziale e cibernetica della Difesa.*

CONDIZIONI PER LA VALORIZZAZIONE DEL «DATO»

Ai fini del raggiungimento degli obiettivi sopra descritti, il percorso e le azioni da adottare dovranno essere indirizzati al conseguimento di specifiche condizioni di valorizzazione del «dato»[28]:

1. Accuratezza
2. Aggiornamento
3. Capacità di analisi (*data-analytics*)
4. Compatibilità
5. Completezza
6. Conformità
7. Conservazione
8. Portabilità tra piattaforme

---

[26] Il *Return on Future*, inteso come *expected Return of Investment*, è il rendimento atteso derivante da investimenti fatti oggi per ottenere benefici futuri. Nella fattispecie, si cita la sperimentazione di nuove piattaforme digitali (un'impresa adotta l'intelligenza artificiale o il cloud computing per essere competitiva in futuro) e la formazione del capitale umano: si investe in competenze digitali utili a un ritorno sulla capacità innovativa.

[27] Per continuità operativa si intende la capacità di svolgere una "lavorazione" senza interruzioni o intralci, anche di natura tecnologica o di interfaccia uomo-macchina.

[28] L'esplicitazione delle linee di azione è indicata in allegato *charlie*.

9. Protezione
10. Rilevanza
11. Sovranità
12. Standardizzazione
13. Tracciabilità
14. Organizzazione
15. Competenze digitali
16. Efficienza energetica
17. Sostenibilità

INFO-STRUTTURE CLOUD E HPC

Nel quadro della trasformazione digitale della Difesa, un *cloud* sovrano e i sistemi di calcolo ad alte prestazioni (HPC) non sono solo soluzioni tecnologiche, ma veri e propri moltiplicatori di forza all'interno di un c.d. "*cloud continuum*" integrato. Questa convergenza info-strutturale abilita la transizione verso un'organizzazione dove il «dato» deve essere un *asset* strategico nelle immediate disponibilità del decisore.

In particolare,

> *l'HPC fornisce la potenza necessaria per analizzare e sfruttare i* big data *nonché per simulazioni massive e l'addestramento di modelli di IA, mentre il* cloud *garantisce l'elasticità e l'accessibilità necessarie per erogare servizi avanzati su larga scala.*

La disponibilità di sistemi HPC rappresenta la condizione necessaria per gestire la complessità dei moderni scenari multi-dominio. In primo luogo, essa garantisce l'addestramento di modelli sovrani. Infatti, l'adozione di architetture "native IA" è fondamentale per lo sviluppo e l'addestramento di *Large Language Models* (LLM) e sistemi di IA generativa ad uso della Difesa, assicurando il supporto a compiti complessi di analisi di *intelligence* e simulazione. Allo stesso tempo, l'integrazione di supercomputer abilita la creazione di "gemelli digitali" (*Digital Twin*) di teatri operativi complessi, permettendo di testare politiche di adattamento e scenari tattici con una precisione senza precedenti.

Oltre a disporre di elevata potenza di calcolo, sarà necessario considerare il limite dell'architettura dei «dati», ponendo particolare attenzione allo *storage* strategico. Nella fattispecie, la valorizzazione del «dato» dipende dalla capacità di alimentare i processori senza interruzioni, evitando la cosiddetta "GPU *starvation*", ossia l'apporto carente di «dati» alle risorse di calcolo. È pertanto imperativo l'impiego di architetture di *storage* ad alte prestazioni in grado di garantire elevati *throughput* — dell'ordine di centinaia di GB/s se non di TB/s — essenziali per caricare in tempo reale modelli massivi o gestire *checkpoint* frequenti durante missioni critiche. A ciò si affianca l'adozione di modelli di *data lake intelligence*, tali da consentire la gestione di enormi volumi di «dati» non strutturati — quali segnali, immagini satellitari e dati IoT — ricchi di metadati, rendendoli accessibili in modo uniforme attraverso interfacce standardizzate.

Inoltre, la valorizzazione del «dato» in ambito militare richiede info-strutture computazionali capaci di adattarsi in modo dinamico ed efficiente all'urgenza della missione, garantendo l'agilità operativa, tramite l'elasticità del *cloud*.

Sul piano dell'interoperabilità e dell'interconnessione, l'efficacia di un'organizzazione complessa come la Difesa risiede nella capacità di far dialogare centri «dati» distribuiti, affinché l'informazione sia creata e condivisa una sola volta (principio "*once only*"). A tal riguardo, le info-strutture integrate dovranno assicurare la produzione, la validazione e la condivisione orizzontale dell'informazione tra tutte le articolazioni della Difesa, eliminando silos informativi e ridondanze costose. L'evoluzione della rete militare verso lo "standard Terabit" dovrà consentire poi l'interconnessione geografica dei *data center* come se fossero un unico ambiente logico.

Per quanto concerne la sovranità digitale e la sicurezza, dovrà essere implementato uno specifico **controllo giurisdizionale** – affinché i «dati» restino soggetti alle sole leggi nazionali ed europee – **e tecnologico**, per assicurare la protezione del «dato» nei confronti di soggetti esterni[29]. In particolare, per il dominio ad **alta classifica** è da prevedersi la migrazione verso **un cloud sovrano-disconnesso** al fine di mantenere l'assoluto controllo su «dati» e servizi. Per il dominio non-classificato e a bassa classifica si valuteranno – nel breve termine – architetture *cloud* tali da consentire il tempestivo transito dei «dati» su info-strutture qualificate[30].

Con specifico riguardo alla protezione del «dato», si prefigura l'**impiego di tecnologie di *confidential computing* e di gestione autonoma delle chiavi crittografiche** (*Bring Your Own Key/Hold Your Own Key*), al fine di isolare i «dati» all'interno di ambienti *cloud* non proprietari, garantendone la riservatezza anche durante l'elaborazione e consentendo, al contempo, di sfruttare i servizi offerti da infrastrutture *cloud* pubbliche (ad esempio, piattaforme di *collaboration*). In termini di controllo e conformità, si prevede l'adozione progressiva di tecnologie di cifratura omomorfa[31] — supportate da acceleratori *hardware* dedicati — per abilitare l'elaborazione sicura di «dati» cifrati senza necessità di esporli in chiaro. In prospettiva, si valuterà la realizzazione di architetture ibride in grado di integrare sistemi di calcolo quantistico con supercomputer classici, ampliando ulteriormente le capacità di protezione e di elaborazione crittografica. Il controllo esclusivo delle chiavi di cifratura da parte della Difesa, unitamente all'adozione del paradigma *zero trust* e di soluzioni di *data-centric security*, garantirà la protezione dei «dati» lungo l'intero ciclo di vita — dalla creazione alla cancellazione — indipendentemente dall'infrastruttura su cui risiedono.

Infine, lo sviluppo e l'implementazione di capacità HPC, considerando come tali sistemi siano "energivori"[32], dovrà affrontare la sfida della **sostenibilità e dell'efficienza energetica**. Pertanto, le future info-strutture HPC della Difesa dovranno rispondere a specifici requisiti di efficienza ed essere supportate da infrastrutture energetiche ad alte prestazioni — sia per l'alimentazione sia per il raffreddamento — adeguatamente ridondate in caso di emergenza.

Questo approccio garantirà che le **infrastrutture digitali** non siano semplici strumenti, ma **capacità di superiorità decisionale, di difesa e sicurezza nazionale**.

---

[29] Tra i soggetti esterni verso su cui deve essere assicurata la protezione del «dato» sono ricompresi anche i *cloud provider*, nazionali o esteri.

[30] In analogia al processo adottato dalla NATO.

[31] La cifratura omomorfa permette di elaborare dati crittografati senza decifrarli, garantendo massima *privacy* nel *cloud* in quanto i dati rimangono protetti anche durante l'elaborazione. L'integrazione di acceleratori *hardware* specifici è cruciale per rendere operativa la cifratura omomorfa, oggi molto dispendiosa dal punto di vista computazionale

[32] HPC6 di ENI, il supercomputer più potente d'Italia e tra i primi dieci al mondo, può consumare fino a 10 MW a pieno regime, equivalenti al fabbisogno di circa 3.000 abitazioni.

STRUMENTI PER IL GOVERNO E LA GESTIONE DEL «DATO»

Il governo condiviso del «dato» e la sua omogenea gestione sono alla base della Strategia.

> *La comprensione condivisa di ruoli, responsabilità e processi genera un clima di reciproca fiducia ed evita approcci disgiunti, tali da portare a silos informativi confinati in singoli domini o aree funzionali, con conseguente nocumento per l'operatività dello Strumento.*

Data Management e *Data Governance*

In conformità al *framework* DAMA[33], la funzione di *data management* comprende lo sviluppo, l'esecuzione e la supervisione dei piani, delle *policy* e delle procedure stabilite dalla *data governance*, con l'obiettivo di fornire, controllare, proteggere e accrescere il valore dei «dati» lungo l'intero ciclo di vita.

Di conseguenza, la *data governance* rappresenta l'esercizio dell'autorità e del controllo strategico sulla gestione dei «dati».

L'automazione dei processi di *governance* e *management* dei «dati» costituisce un obiettivo primario al fine di garantire – in modo continuativo e su larga scala – l'applicazione coerente dei principi del «dato», così come enunciati nell'allegato *alfa* alla presente Strategia.

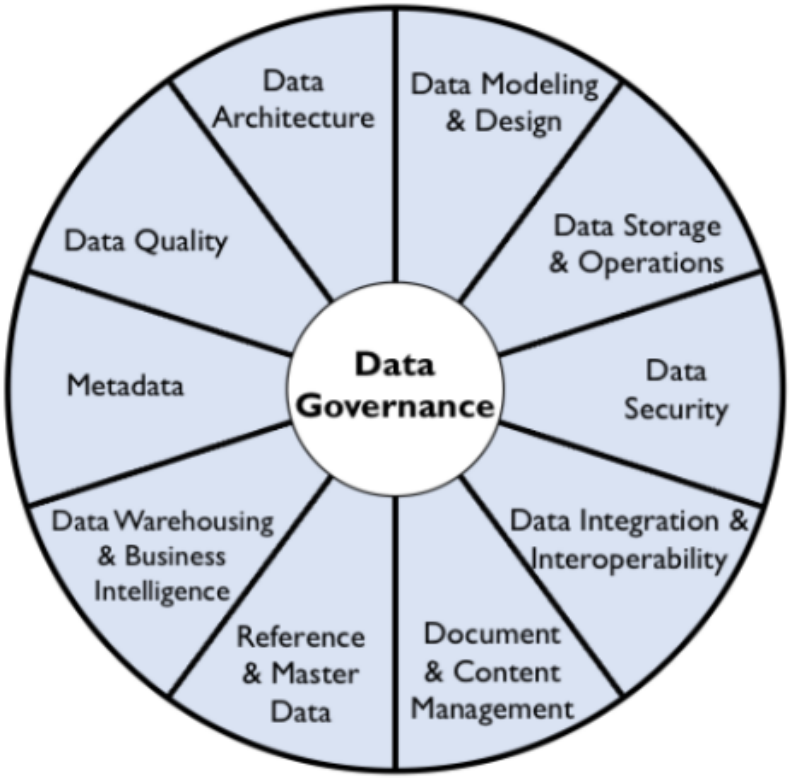


Fig. 3 - Insieme delle funzioni costituenti il *Data Management*

[33] "*Data Strategy for the Alliance*" e DMBoK 2nd Ed. – *Data Management Body of Knowledge* II.

Per realizzare le condizioni necessarie all'auspicata valorizzazione del «dato», si adotterà un percorso per implementare una *data governance* condivisa e un quadro normativo comune, tale da disciplinare gestione, conoscenza, qualità, sicurezza e disponibilità dei «dati». Una volta consolidata la struttura di governo, sarà possibile dare attuazione al *data management* mediante l'applicazione di direttive univoche e lo sviluppo di un approccio standardizzato.

Tale modello consentirà di promuovere la cooperazione tra le diverse componenti della Difesa, valorizzando le specifiche peculiarità che caratterizzano la generazione e la gestione dei «dati» in ciascuna di esse.

Nella fattispecie, un efficace *data management* è subordinato ai seguenti elementi:

1. Qualità dei «dati»;
2. Fattori abilitanti (tecnologia, standardizzazione e cultura digitale);
3. Strumenti di analisi, supportati da appropriate capacità computazionali, in accordo agli indirizzi strategici definiti per tali settori.

Il governo dei «dati»

L'individuazione di ruoli e figure cui assegnare specifiche responsabilità nell'ambito del governo dei «dati» è una condizione necessaria affinché le articolazioni della Difesa, nell'ambito dei «domini dati» di rispettiva competenza, operino secondo criteri di armonizzazione, uniformità, efficienza e ottimizzazione dei risultati, consentendo la tempestiva disponibilità dei «dati», dal livello politico a quello tattico.

Tra i differenti «domini dati» – nonché verso i domini esterni all'organizzazione Difesa – avverrà l'interscambio di *data product*, ovvero collezioni di «dati», corredate dal codice necessario per il loro consumo e dai metadati con cui si descrivono le caratteristiche[34], utili a soddisfare specifiche esigenze informative.

Responsabile Unico dei «dati» (RUD)

Al fine di realizzare il modello di *data governance*, si evidenzia il ruolo del Responsabile Unico dei Dati (RUD) quale figura cardine per impartire direttive di governo e di gestione dei «dati». Ai sensi del combinato disposto dell'art. 26 del COM e dell'art. 89 del TUOM, tale ruolo è assegnato al Capo di Stato Maggiore della Difesa.

In allegato *delta* è riportata la descrizione dettagliata degli elementi citati e le fasi logiche della funzione di *data management* e di *data governance*.

[34] Ad esempio: contenuto, categoria, modalità di utilizzo e fruizione, *ownership,* frequenza di aggiornamento ecc.

II – CONNETTIVITÀ AVANZATA

INTRODUZIONE

Per connettività avanzata si intende la capacità di trasporto del «dato» in maniera sicura, capillarmente distribuita, resiliente, ad alta velocità, bassa latenza, ampia banda e multi-vettore.

La connettività avanzata è un prerequisito fondamentale per l'implementazione della Strategia, perché imprescindibile per assicurare la continuità operativa anche in scenari contestati, congestionati o degradati.

Dal punto di vista tecnologico, ciò si traduce in un impianto di telecomunicazioni basato su tecnologie allo stato dell'arte, tra cui:
- standard di comunicazioni di 5ª e 6ª generazione (c.d. 5G e 6G), sia terrestre sia satellitare;
- connessioni satellitari multi-orbita e multi-*provider* (militare e commerciale);
- topologie di reti *mesh* [35];
- sistemi tattici e architetture *Software-Defined Network* (SDN)[36];
- *network slicing* [37].

La connettività avanzata collega dinamicamente sensori, piattaforme, sistemi d'arma e centri di comando e controllo, anche tra domini a classifica diversa, abilitando:
- lo scambio continuo, sicuro, affidabile e in tempo reale di grandi volumi di «dati»;
- l'integrazione di capacità automazione;
- la possibilità di operare in logica multi-dominio;
- l'interoperabilità coi *partner* alleati e le coalizioni internazionali.

Quindi, l'impianto di connettività avanzata è funzionale a:
- trasferire le informazioni – sia classificate sia non-classificate – in *real-time* o *near real-time*;
- supportare una *situational awareness* evoluta;
- garantire il comando e controllo distribuito anche in contesti di minaccia cibernetica o interdizione elettromagnetica;

[35] Una rete *mesh* è un'architettura di comunicazione in cui ciascun nodo (dispositivo o sistema) si collega direttamente ad altri nodi, creando percorsi multipli e ridondanti per la trasmissione dei dati, eliminando le zone morte e garantendo alta velocità nonché scalabilità in tutta la zona di copertura. Questa struttura aumenta la resilienza e l'affidabilità della rete, poiché i dati possono automaticamente instradarsi attraverso i nodi disponibili anche in caso di guasti o interferenze.

[36] Il *Software-Defined Networking* (SDN) è un'architettura di rete che separa il piano di controllo (che decide come instradare il traffico) dal piano dati (che fisicamente trasporta i pacchetti), permettendo di gestire in modo centralizzato e programmabile il comportamento della rete tramite software, con maggiore flessibilità, automazione e sicurezza.

[37] Il *network slicing* è una tecnologia che consente di suddividere un'unica infrastruttura di rete fisica in più reti virtuali (o "fette", c.d. *slice*), ognuna isolata, autonoma e configurata con risorse e caratteristiche dedicate (ad esempio capacità di banda, latenza e livelli di sicurezza), per supportare in parallelo servizi diversi con requisiti specifici su un'unica infrastruttura di rete. Attraverso le operazioni di "virtualizzazione" e "isolamento", basate su *Software Defined Networking* (SDN) e *Network Functions Virtualization* (NFV), vengono creati segmenti virtuali indipendenti, garantendo che il traffico di una "fetta" non interferisca con le altre.

- aumentare la resilienza e la capacità di adattamento operativo.

A livello NATO, la connettività avanzata è un pilastro per la FMN, ossia il citato principio su cui creare reti federate e interoperabili tra i Paesi membri, assicurando alle forze alleate la capacità condividere informazioni in tempo reale in qualsiasi teatro operativo, sin dai primissimi momenti (c.d. *zero-day interoperability*).

Infatti, la NATO considera la connettività avanzata essenziale per il conseguimento della superiorità informativa, per sostenere operazioni multi-dominio, per garantire la coerenza e la compatibilità tecnica delle architetture C5ISR nonché per proteggere i «dati» classificati attraverso cifratura e segmentazione logica delle reti.

Il concetto di connettività avanzata non è soltanto un'evoluzione tecnologica, ma rappresenta un prerequisito strategico per l'efficacia, la sicurezza e l'interoperabilità dei moderni Strumenti militari, coerente con le linee guida della NATO e con la visione di una Difesa digitalizzata, agile e integrata.

In coerenza con il quadro normativo europeo e nazionale[38], si riconosce il carattere strategico delle infrastrutture digitali e di connettività quali elementi essenziali per il mantenimento di funzioni vitali della società.

Analogamente, le infrastrutture di connettività della Difesa rivestono un ruolo critico per la continuità operativa dello Strumento militare e sono strategiche per la funzione di difesa e sicurezza militare dello Stato. Per tale motivo, le reti e i sistemi di telecomunicazione della Difesa devono garantire i più elevati standard di resilienza, sicurezza e disponibilità.

Inoltre, tale impianto connettivo non supporta esclusivamente le esigenze operative militari, ma costituisce anche un *asset* strategico per impieghi *dual use*, potendo fornire capacità di supporto, o addirittura sostituirsi, alle infrastrutture civili in scenari di crisi, emergenza o incidente su vasta scala.

In particolare, la capacità della Difesa di disporre di sistemi di comunicazione ridondanti, resilienti e operanti su molteplici vettori tecnologici (i.e. terrestri, satellitari e radio), rappresenta un elemento di garanzia per la sicurezza nazionale, supportando la continuità dei servizi essenziali anche in caso di perturbazione o collasso delle reti civili. Tale funzione di *back-up*, in coerenza anche con gli indirizzi strategici della NATO e dell'UE, riveste carattere prioritario nell'attuale scenario geopolitico, ove la protezione delle catene di approvvigionamento, la gestione delle interdipendenze intersettoriali e la capacità di risposta agli incidenti costituiscono elementi fondamentali per la resilienza complessiva del Sistema Paese.

Pertanto, lo sviluppo dell'impianto di connettività avanzata della Difesa, attraverso la realizzazione di infrastrutture digitali sicure, affidabili e interoperabili, idonee sia a operare in scenari contestati sia a contribuire, ove necessario, alla resilienza delle reti e dei servizi

[38] Direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici (c.d. CER) e la direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (c.d. NIS-2), recepite in Italia rispettivamente con il D.Lgs. 4 settembre 2024, n. 134, e con il D.Lgs. 4 settembre 2024, n. 138.

critici nazionali, si inserisce nella più ampia visione strategica di rafforzamento della difesa e sicurezza nazionale.

OBIETTIVI E CAPACITÀ

Il primo obiettivo è il conseguimento di continuità, resilienza e sicurezza delle comunicazioni attraverso infrastrutture terrestri, satellitari e radio, in grado di sostenere operazioni complesse, anche in ambienti contestati o degradati.

Entro il 2030, un traguardo misurabile sarà la realizzazione di una **copertura di rete sicura e ad alta capacità sul territorio nazionale e sulle principali aree di proiezione operativa**, riconducendo i tempi medi di ripristino delle comunicazioni a specifiche *recovery time objective guarantees*, variabili in relazione alla criticità delle stesse.

Il secondo obiettivo è la funzione di **"C2 distribuito"**, supportato da reti ad alta velocità, elevato *troughput* e bassa latenza tali da scambiare in tempo reale, flussi di «dati» tattici, informazioni *intelligence* e ordini operativi. Entro il 2030, ci si prefigge di integrare in un'unica architettura di rete federata/unificata i sistemi C5ISR e i sensori strategici nazionali, assicurando compatibilità con gli standard della FMN.

Il terzo obiettivo è la capacità di segmentare e assegnare priorità ai servizi di rete, attraverso l'**adozione del *network slicing***. Ciò al fine di per dedicare risorse affidabili a servizi *mission-critical* (bassa latenza ed alta affidabilità). Tutti i teatri operativi esterni devono essere supportati da almeno tre profili di *slice* di rete distinti, ottimizzati per priorità, sicurezza e *performance*.

Un ulteriore traguardo è la progressiva **implementazione di reti *mesh* tattiche e soluzioni di SDN** per aumentare la flessibilità, ridurre i costi di gestione e migliorare la capacità di riconfigurare dinamicamente i percorsi di comunicazione. Entro i prossimi quattro anni, si prevede l'integrazione di reti *mesh* nella maggior parte delle unità tattiche ad alta prontezza operativa, con procedure standard NATO di interoperabilità e cifratura *end-to-end*.

In generale, è necessario garantire la coerenza degli investimenti info-strutturali con i piani NATO di trasformazione digitale e di potenziamento delle reti di comando e controllo (vds. concetto NATO *Enterprise Networking*) nonché con il progressivo sviluppo delle capacità di coalizione basate su architetture *cloud* federate.

Linee di Azione

Per il conseguimento degli obiettivi, si prefigurano le seguenti azioni:

1. **Realizzare la connettività avanzata della Difesa**, secondo parametri di capillarità, scalabilità, prontezza, omogeneità e resilienza. Ciò si deve attuare sia in ambito nazionale sia nel c.d. «fuori area» ossia negli ambienti operativi comunque correlati alla salvaguardia degli interessi del Paese, includendo aree extra-regionali, contesti ad alto rischio e scenari di crisi.

   Attesa la fisionomia ibrida dello scenario di riferimento, volta a disarticolare anche le info-strutture, questa linea di azione sottende un'ampia diversificazione dei mezzi di trasmissione, in accordo anche ai principi NATO e dell'Unione Europea. A tal fine, l'architettura di connettività avanzata dovrà essere:
   - basata su standard condivisi;
   - sicura *by design* e funzionale ai principi del «dato»

- progettata per operare anche in ambienti degradati con percorsi alternativi e meccanismi di *failover* [39] automatici;
- scalabile e flessibile.

Ai fini della sostenibilità, sono da traguardare anche soluzioni del tipo ***Smart Military District***, intesi come ecosistemi integrati e intelligenti in cui infrastrutture, tecnologia e processi operativi sono ottimizzati per garantire efficienza energetica e resilienza logistica[40].

2. **Garantire l'interoperabilità nazionale e alleata**. Ciò include l'adesione – in ambito NATO – agli standard della FMN, volti a facilitare operazioni *combined*, rafforzando la capacità di *digital-Alliance*, così come indicato nella DTIS 2.0.
   In ambito nazionale, ciò si riflette nell'implementazione interforze di una rete "a bassa classifica" e di una rete unificata "ad alta classifica", superando il concetto di "comunità di sistemi" e prevedendo altresì l'impiego di soluzioni di *cross domain*, per mettere in comunicazione le reti a diversa classifica.
3. **Supportare la funzione C2 multi-dominio**, abilitando la condivisione dei «dati» e implementando architetture/protocolli tali da assicurare lo scambio sicuro di informazioni tra sistemi, sensori, piattaforme e personale – al livello strategico, operativo e tattico – in piena conformità al paradigma data-centrico.
4. Considerare **la sicurezza cibernetica come elemento intrinseco di ogni componente della rete e di ogni processo di connettività**. Questo include il consolidamento dell'adozione dell'approccio *secure by design* e dell'attuale capacità di *vulnerability assessment* nonché il continuo sviluppo e rafforzamento delle capacità di risposta attiva agli incidenti.
5. Sviluppare e implementare soluzioni tali da consentire un **uso efficiente e dinamico dello spettro elettromagnetico**, essenziale per la gestione delle comunicazioni e la conduzione delle c.d. *Cyber Electro-Magnetic Operations/Activities* (CEMO/CEMA)[41] in ambienti complessi e congestionati.
6. Adottare un approccio proattivo nel **monitoraggio**, nell'**identificazione** e nell'**integrazione di tecnologie emergenti nel campo della connettività**, al fine di mantenere un vantaggio tecnologico e adattarsi con immediatezza ai cambiamenti del panorama operativo.

L'IMPIANTO CONNETTIVO DELLA DIFESA

Il fondamento info-strutturale di connettività su cui poggia la Strategia non è solo un insieme di reti, ma è un **ecosistema interconnesso** di componenti fisici e logici, servizi e protocolli,

---

[39] Il **failover** è una modalità operativa di *back-up* in cui un sistema informatico, rete o componente *hardware*, in caso di guasto o malfunzionamento del componente primario, passa automaticamente a una componente di riserva (ridondante). Questo processo garantisce la continuità del servizio, minimizzando o eliminando i tempi di inattività per le utenze.

[40] Gli ***Smart Military District*** sfruttano tecnologie avanzate, come l'*Internet of Things* (IoT), l'intelligenza artificiale e sistemi di gestione automatizzati, per migliorare la gestione delle risorse, ridurre l'impatto ambientale e potenziare la capacità di risposta operativa. I principali vantaggi di tale approccio includono una maggiore flessibilità operativa, una riduzione dei costi di gestione e manutenzione, e la possibilità di adattarsi rapidamente a scenari in evoluzione, garantendo al contempo un elevato livello di sicurezza e sostenibilità.

[41] Argomento trattato nella parte III della Strategia.

tali da consentire il flusso sicuro e continuo delle informazioni attraverso i domini operativi e la rete *enterprise* della Difesa.

Questo impianto connettivo dovrà fungere da catalizzatore per un ambiente integrato e per l'effettiva cooperazione tra tutte le componenti della Difesa e quelle delle Forze Armate alleate.

In particolare, la realizzazione di un robusto impianto connettivo richiederà l'impiego e l'integrazione dei seguenti elementi.

Rete Integrata della Difesa (RID) - avanzata

Oggi, la Rete Integrata della Difesa è basata sulla Rete in Fibra Ottica Nazionale (RIFON), sulla *Metropolitan Area Network* (MAN) di Roma e sulla Rete Numerica Interforze (RNI). La RID costituisce la spina dorsale della connettività terrestre e fissa della Difesa.

La Rete in Fibra Ottica della Difesa (RIFON) deve fornire una capacità di trasmissione ad altissima velocità e bassa latenza per l'organizzazione *enterprise*, fondamentale per le applicazioni richiedenti elevate prestazioni, come i *data centre*, il *cloud* e i sistemi di comando e controllo distribuiti.

La Rete Numerica Interforze (RNI) – aggiornata con ponti radio ad elevata capacità – deve garantire l'interconnessione di *back-up* e l'estensione della RIFON alle zone nelle quali risulta non costo-efficace portare la connettività ottica.

Il potenziamento dell'attuale RID prevede:

- l'adeguamento capacitivo delle componenti in fibra ottica e ponti radio, la realizzazione di nuove dorsali e l'estensione della rete in fibra ottica ad altre articolazioni della Difesa
- l'integrazione della rete con *asset* satellitari, di connettività avanzata 5G, di connettività tattica (SDR, *Multi Data Link* e *Tactical Data Link*) e con le reti di missione (NATO, EU, coalizione).

L'integrazione di queste reti diviene cruciale per sostenere un appropriato flusso informativo all'interno della Difesa e per rendere la rete più sicura, resiliente e con capacità aderenti ai parametri della banda ultra-larga (velocità fino a 200-400 Gbps), sfruttando tecnologie che prevedono la piena integrazione del substrato ottico con quello di *routing* IP (*Routed Optical Networking* [42]).

Connettività Satellitare Multi-Orbita e Multi-*Provider*

Tale forma di connettività è fondamentale per garantire una copertura di comunicazione globale e resiliente, superando le limitazioni geografiche e assicurando la connettività anche in aree remote o contestate.

L'utilizzo di servizi di comunicazione satellitare basata su costellazioni in orbita bassa (LEO) e media (MEO), in aggiunta a quelli in orbita geostazionaria (GEO) e la complementarietà di *provider* militari e commerciali, garantiscono diversificazione, sinergia e prestazioni adeguate a supportare esigenze concorrenti e in generale, il trasferimento dei volumi di

[42] Il *Routed Optical Networking* (RON) è un'architettura di rete avanzata che converge i livelli IP (*routing*) e ottici (trasporto) in un'unica infrastruttura semplificata. Utilizzando ottiche coerenti inseribili direttamente negli apparati di rete, si elimina la necessità di *transponder* esterni, riducendo costi, consumi energetici, spazio fisico e complessità operativa.

«dati» richiesti per il *real-time* (in particolare per i sistemi autonomi e l'*edge-computing*), il video streaming, l'osservazione della terra, ecc.

Con tale prospettiva, emerge anche l'esigenza di spostare il baricentro verso l'utilizzo prevalente di reti classificate, dotate di servizi moderni, distribuiti e resilienti. In altri termini, occorre evitare la segregazione delle capacità avanzate al dominio "non-classificato", risultando conveniente:

- trasferire nel dominio "classificato" i servizi tecnologici più moderni (*cloud*, multi-orbita, distribuzione, *zero trust*);
- evitare *lock-in* tecnologico, perseguendo soluzioni federate e interoperabili in ambito NATO/UE;
- sviluppare connettività satellitare *class-based*, tale da garantire resilienza e continuità operativa, anche in scenari di crisi;
- integrare le reti classificate nei *backbone* digitali NATO (i.e. *Digital Backbone, Alliance Data Sharing Ecosystem*).

Connettività 5G e *Next Generation Network*

La connettività 5G offre un potenziale significativo, risultando integrabile all'interno di reti dedicate (es. per connettività tattica, sensori, IoT) quale complemento, all'interno di un'architettura di Difesa "*trusted*", ibrida e distribuita.

In tale ottica, la Difesa si sta predisponendo per operare quale *mobile network operator*, ottenendo i c.d. "*mobile country*" e "*network code*" per gestire in autonomia la propria rete radio dedicata, impiegando porzioni *ad hoc* di spettro elettromagnetico. È in fase di implementazione un *core network* 5G proprietario e centralizzato, corredato di *asset* fissi e portabili, anche a favore delle FF.AA.

Questa capacità – sviluppata dalla Difesa anche in seno a iniziative della NATO – può raggiungere uno stato di maturità tale da prevederne l'estensione sul territorio nazionale e in scenari operativi, attraverso la creazione di "bolle di connettività avanzata", funzionali a interconnettere apparati *Military Internet of Things* (MIoT), bisognevoli di alta velocità e bassa latenza (ad es. per esigenze di logistica avanzata, telemedicina sul campo, sorveglianza e supporto alle operazioni in aree urbane).

Parimenti, si dovrà considerare la necessità di evolvere l'intera capacità 6G, le cui caratteristiche avveniristiche, base della c.d. *tera economy* [43], sono già allo studio dei consessi di standardizzazione internazionale, nonché veicolo di importanti investimenti per l'industria di settore (*vendor*, integratori e *provider*), intenzionati a fornire tale capacità già a partire dal 2028.

Sistemi Tattici

I sistemi tattici sono essenziali per la connettività sul campo di battaglia, consentendo l'interscambio di «dati» in modo sicuro tra piattaforme aeree, terrestri e navali, per la costruzione e diffusione di una *joint common operational picture*.

L'impiego dei *data link* con capacità avanzate di resistenza alle contromisure elettroniche, alta resilienza e capacità di rete *ad hoc* è cruciale per mantenere la connettività e lo scambio

[43] Nuovo paradigma che vede nel *Terabit* (1000 miliardi di *bit*) l'unità di confronto per le comunicazioni dati, contro l'attuale *Gigabit* (1 miliardo).

di dati *real/near real-time* tra le piattaforme terrestri, navali e aeree in ambienti complessi e sotto attacco.

Infine, i sistemi *Identification Friend or Foe* (IFF) sono volti a identificare in modo rapido e sicuro le forze amiche e distinguerle quelle potenzialmente ostili.

Software Defined Radio (SDR)

I sistemi SDR offrono flessibilità operativa e capacità di adattamento a diversi scenari e protocolli di comunicazione. Le SDR permettono di riconfigurare le radio tramite *software*, supportando un'ampia gamma di forme d'onda e frequenze, inclusi nuovi standard e capacità di *networking*, facilitando l'interoperabilità tra diverse Forze e nazioni alleate.

Sistemi di C2 multidominio

I sistemi di C2 sono il cuore della capacità di integrare sensori, effettori e decisori attraverso i domini operativi. La connettività avanzata deve fornire la capacità di alimentazione «dati» in tempo reale per questi sistemi, permettendo la citata *joint common operational picture* nonché supportando processi decisionali distribuiti e collaborativi.

La loro efficacia dipende dalla robustezza e dalla disponibilità della sottostante infrastruttura di connettività.

Reti di Missione/Coalizione Federate

L'implementazione di standard comuni e condivisi di *network interconnection* è indispensabile per garantire un'interoperabilità c.d. *zero-day*[44] delle Forze in operazioni, sin dal tempo di pace nonché in tutte le fasi di pianificazione, preparazione e generazione delle Forze.

La federazione delle reti di missione/operative va ricercata mediante l'adesione a iniziative internazionali quali la FMN – in ambito NATO /*Partnership for Peace* (PfP) – e l'EU *Operations Wide Area Network*, in ambito europeo.

Questo consentirà la condivisione sicura e fluida delle informazioni in operazioni di coalizione, facilitando la collaborazione, la pianificazione congiunta e la *situational awareness* a supporto dell'integrazione multi-dominio.

Information Exchange Gateway

L'interazione tra reti non classificate e reti classificate dovrà perseguirsi tramite soluzioni certificate, al fine di garantire uno scambio sicuro e regolato di informazioni tra domini a diversa classifica di sicurezza.

Al momento, tali soluzioni sono subordinate alle valutazioni delle competenti autorità nazionali[45] per accertare l'adeguatezza, la conformità e l'applicabilità delle tecnologie disponibili (tra cui il cosiddetto "diodo dati"[46]) ai casi concreti di uso.

---

[44] Per *zero day*, si intende dal primo giorno di attività operativa, qualsiasi essa sia.

[45] L'Ufficio Centrale per la Segretezza (UCSe) del Dipartimento Informazioni per la Sicurezza presso la Presidenza del Consiglio dei Ministri.

[46] Un diodo dati (o *data diode*) è un dispositivo *hardware* in grado di realizzare un trasferimento di dati unidirezionale tra due domini di sicurezza (ad esempio da una rete di classificazione inferiore verso una di classificazione superiore, o viceversa), impedendo fisicamente qualsiasi comunicazione nel senso opposto. Questo garantisce che informazioni o potenziali minacce non possano propagarsi "a ritroso" verso il dominio più sensibile.

Infatti, queste soluzioni devono essere valutate dal punto di vista normativo, di affidabilità e di compatibilità operativa: gli *standard*, le procedure di certificazione, la robustezza del dispositivo e la gestione operativa (*logging*, *incident response*, ecc.) sono aspetti essenziali.

III – SICUREZZA, RESILIENZA E OPERAZIONI NEL DOMINIO CIBERNETICO

INTRODUZIONE

Se da un lato l'innovazione tecnologica prefigura benefici condivisi e su larga scala, dall'altro accelera la metamorfosi e la diffusione delle minacce.

> *Con una tendenza sempre più preoccupante, il dominio cibernetico si caratterizza per la presenza di una moltitudine eterogenea di nuovi attori – statuali e non – in grado di sfruttare la pervasività dell'innovazione tecnologica e dotarsi di strumenti sofisticati e sempre più accessibili per compiere finalità illecite. I loro fini sono minare le istituzioni democratiche, deviare l'opinione pubblica con attività di* cognitive warfare *ovvero manipolazione cognitiva e in generale, mettere a rischio la sicurezza dei cittadini.*

La natura trasversale e ibrida di queste minacce pone un accento inedito nel c.d. *continuum* della competizione[47] e amplia lo spettro di instabilità nel quadro delle relazioni internazionali, dove insistono nuovi fattori destabilizzanti e fenomeni revisionisti[48] dell'ordine globale.

Infatti, come evidenziato nel documento "Il contrasto alla guerra ibrida"[49], il dominio cibernetico funge da moltiplicatore di scala e di effetti, per una moltitudine di azioni ostili: dalla disinformazione agli attacchi contro infrastrutture critiche, dalla manipolazione dei processi democratici alle interferenze nei sistemi energetici, finanziari e di trasporto. La difficoltà di attribuzione e la c.d. *plausible deniability* rendono tali operazioni particolarmente insidiose, consentendo agli attori malevoli di operare "sotto soglia" senza dover rispondere delle proprie azioni.

Questa realtà impone alla Difesa di evolvere da una postura meramente reattiva a una capacità di azione predittiva e adattiva, volta non solo a contenere ma a prevenire, dissuadere e assorbire gli attacchi, operando senza soluzione di continuità. La risposta a questa minaccia richiede un approccio integrato *whole-of-government*, in cui lo Strumento militare – attraverso capacità operative *full-spectrum* – agisce in sinergia con gli altri pilastri della sicurezza cibernetica nazionale, sin dal tempo di pace.

Tutto ciò si riflette nella realtà interconnessa e digitalizzata di ognuno di noi, dove lo Strumento militare – baluardo della difesa e della sicurezza militare del Paese – è chiamato ad adattarsi alla mutevolezza delle condizioni al contorno, ricercando un agile aggiornamento delle capacità e delle modalità di impiego.

---

[47] Il *competition continuum* (ossia il continuum della competizione) è un concetto utilizzato nelle relazioni internazionali e si basa sull'idea per cui la competizione tra gli attori non si limita a un singolo tipo di interazione ma si estende lungo un continuum con diverse fasi: cooperazione, concorrenza, competizione aggressiva, conflitto latente, conflitto aperto.

[48] Revisionismo è un termine usato nel campo delle relazioni internazionali per descrivere lo scopo di un Paese di rivedere o cambiare l'ordine internazionale esistente e in particolare quello stabilito da potenze con un ruolo dominante. Le potenze revisioniste sfidano lo *status quo*, spesso in modo violento. Esempi storici di potenze revisioniste sono la Germania nella Prima e nella Seconda Guerra Mondiale e l'Unione Sovietica durante la Guerra Fredda.

[49] Non-paper del Ministro della Difesa "Il contrasto alla guerra ibrida: una strategia attiva", ediz. novembre 2025.

Con tale prospettiva, questa parte della Strategia fornisce gli indirizzi per l'assolvimento dei compiti di difesa e di sicurezza militare dello Stato nello spazio cibernetico di interesse nazionale[50].

LE PRIORITÀ PER LA DIFESA CIBERNETICA

In accordo ai compiti assegnati allo Strumento, si individuano quattro principali obiettivi:

1) incremento della sicurezza e della resilienza nel dominio cibernetico, nella dimensione cognitiva e nello spettro elettromagnetico;
2) capacità di svolgere operazioni *full-spectrum*[51], sin dal tempo di pace;
3) coerenza quantitativa e qualitativa degli organici;
4) consolidamento della cooperazione internazionale e della *cyber-capacity building*.

Sicurezza e resilienza nello spazio cibernetico

Attesa la pervasività della minaccia ibrida, il progressivo ampliamento delle superfici d'attacco e l'intensificarsi delle attività ostili richiedono una postura proattiva, per garantire la protezione delle infrastrutture critiche, siano esse civili o militari.

Pertanto, lo Strumento militare deve rafforzare le proprie capacità di identificazione, mitigazione e reazione alle minacce cibernetiche, dotandosi di architetture robuste e resilienti, per operare anche in ambienti degradati. Ciò significa adottare un approccio *security-oriented* per gli elementi costitutivi del proprio spazio cibernetico – incluse le catene di approvvigionamento – e promuovere un continuo dialogo a livello di Sistema Paese.

La sicurezza dello spazio cibernetico è una precondizione per l'operatività ovvero la libertà di azione in ottica multi-dominio e l'interoperabilità, nazionale e internazionale.

Pianificazione e conduzione di operazioni *full-spectrum*

Quale fattore abilitante, la Difesa deve saper pianificare, condurre e sostenere l'intero spettro di operazioni cibernetiche fin dal tempo di pace, garantendo la prontezza operativa in caso di aggressione, sabotaggio o compromissione degli *asset* critici nonché assicurare la difesa e la deterrenza nello spazio cibernetico di interesse nazionale.

Tale capacità muove da una robusta consapevolezza situazionale dello spazio cibernetico, includendo la dimensione elettromagnetica, cognitiva e ibrida. Infatti, la condizione di vantaggio si acquisisce con la meticolosa comprensione di quanto accade, avendo allo stesso tempo gli strumenti per negare e/o limitare tale facoltà all'avversario.

---

[50] Insieme delle infrastrutture informatiche IT, comprensive di *hardware*, *software*, capacità, dati, connessioni fisiche e elettromagnetiche, dei sistemi cyber-fisici OT comprensivi di sistemi attuatori di processo, sensori, sistemi di controllo industriale (ICS), apparecchiature mobili dotate di connessione di rete, nonché dei punti di interconnessione, delle rappresentazioni digitali, delle relazioni fisiche, logiche e cognitive stabilite tra essi, entro il quale il Ministero della Difesa opera per adempiere i propri compiti istituzionali anche al di fuori dei confini nazionali. La definizione è tratta dalle proposte di modifica del Codice dell'Ordinamento Militare (D.Lgs. 15 marzo 2010, n. 66).

[51] Le operazioni cibernetiche *full-spectrum* integrano azioni offensive, difensive e di *exploitation* (sfruttamento) in tutti i domini (terra, mare, aria, spazio, cyber) per garantire la sicurezza delle missioni, proteggere le reti informatiche e neutralizzare gli avversari. Combinano attività cyber, guerra elettronica e *intelligence* per proteggere/attaccare le infrastrutture critiche (proprie/avversarie) e ottenere un vantaggio militare.

Ciò richiede professionalità specializzate, efficaci forme di formazione e addestramento con appropriati strumenti[52], regole di ingaggio e norme coerenti nonché un complesso info-strutturale all'avanguardia, adottando processi di *procurement* più agili per l'implementazione di nuove capacità.

Coerenza organica

Per contribuire con efficacia alla difesa dello spazio cibernetico, alle iniziative delle Organizzazioni Internazionali e alla collaborazione nel contesto della cybersicurezza nazionale è necessario disporre di un'adeguata Forza specialistica, in termini sia quantitativi sia qualitativi.

Essa è da considerarsi abilitante per l'intero impianto capacitivo della Difesa e pertanto, dovrà essere sviluppata, considerando i *capability target* della NATO e dell'UE, le peculiarità dei *Force providers* – ovvero delle Forze Armate – e le specifiche attività, comprendenti le *Baseline Activities and Current Operations* (BACO)[53].

In particolare, sono fondamentali soluzioni a geometria variabile per l'alimentazione, l'impiego e il *retaining* del personale specialistico – civile e militare – nell'ambito di un percorso virtuoso di crescita professionale, tale da promuovere e valorizzare il talento e le competenze.

In questo perimetro, va altresì promossa la "cultura tecnologica" nella prospettiva di una continua formazione del personale.

Cooperazione internazionale e *Cyber Capacity Building* (CCB)

La cooperazione internazionale nel dominio cibernetico assume il carattere di leva strategica per la sicurezza nazionale. Pertanto, la Difesa deve essere parte attiva nelle iniziative internazionali, incoraggiando in particolare, le attività di CCB, attraverso programmi di rafforzamento dei partner di interesse nonché il consolidamento di una rete di sicurezza condivisa.

Queste attività contribuiscono a un ambiente cibernetico più affidabile, facilitando la condivisione di *know-how*, lo sviluppo di standard comuni e ultime, non per importanza, opportunità di crescita economica duale.

In tale ottica, andranno perseguite la cooperazione nella NATO e nell'UE, nonché iniziative bi-multilaterali, sostenendo una cultura della sicurezza cibernetica basata su condivisione, interoperabilità e mutuo supporto.

---

[52] Tra cui piattaforme di *cybersecurity awareness*, piattaforme di simulazione, *Cyber Range* ed iniziative quali *Cyber Challenge* (nel 2025 lo Stato Maggiore della difesa ha organizzato il primo evento, già programmato anche per il 2026) e *Training Camp*. In tale contesto, riveste particolare importanza, quale *asset* proprietario, il *Cyber Range* "UNAVOX" della Scuola di Telecomunicazioni delle Forze Armate (STELMILIT), ambiente di simulazione avanzato che costituisce un'eccellenza nazionale per la formazione e l'addestramento del personale della Difesa nelle operazioni cibernetiche. Tale infrastruttura consente di replicare scenari operativi realistici, favorendo lo sviluppo delle competenze tecniche e tattiche necessarie per operare efficacemente nel dominio cibernetico, in piena sinergia con le capacità interforze e in coerenza con gli standard NATO.

[53] Con l'acronimo BACO (*Baseline Activities and Current Operations*) la NATO, nella dottrina di *targeting* (AJP-3.9 – *Allied Joint Doctrine for Joint Targeting*), identifica l'insieme delle attività di base e delle operazioni correnti, costituenti il contesto di riferimento ("*steady state*") da cui partire nella pianificazione. Le BACO comprendono, da un lato, le attività routinarie di presenza, sorveglianza, deterrenza e sicurezza collettiva già in atto (*baseline activities*) e dall'altro, le operazioni correnti condotte in teatro (*current operations*). Questo livello rappresenta quindi la "situazione di partenza" rispetto alla quale vengono valutati fabbisogni, effetti e risorse addizionali da impiegare in caso di crisi o escalation operativa.

GLI ABILITANTI DELLA CAPACITÀ CIBERNETICA

Sistema cibernetico della Difesa

Per il conseguimento degli obiettivi è necessario uno specifico sistema cibernetico della Difesa**,** costituito dalle seguenti articolazioni:

- **Vertice politico-militare**: responsabile della definizione delle linee di indirizzo in materia nonché delle relazioni interministeriali e inter-agenzia;
- **Vertice strategico-militare**: responsabile dell'implementazione della Strategia e dello sviluppo delle capacità cibernetiche;
- **Vertice tecnico-industriale**; responsabile per la ricerca tecnico-scientifica e il *procurement*;
- **Comando Operativo di Vertice Interforze**: responsabile della pianificazione e direzione delle operazioni e delle esercitazioni militari in ambito nazionale e internazionale;
- **Forze Armate**: responsabili della sicurezza delle proprie info-strutture, *provider* degli *asset* specialistici nonché attori primari nella formazione di base e intermedia del personale;
- **Centro Alti Studi della Difesa (CASD) – Polo Formativo Cyber**[54]: referente per la formazione avanzata e la diffusione della cultura cibernetica[55].

Nel perimetro del sistema cibernetico della Difesa, emerge anche l'opportunità di un centro di collaborazione civile-militare, per lo studio, la formazione e lo sviluppo di soluzioni tecnologiche. Tale centro potrà avvantaggiarsi della collaborazione dell'industria nazionale, di altre istituzioni, del mondo accademico e della ricerca, esplorando paradigmi inediti come quello della *software defined defense* [56] e prevedendo la realizzazione di una specifica *software factory* [57].

Il dominio cibernetico e la funzione *intelligence*

È stato di recente istituito il Comando interforze Cyber-Intelligence-Reparto Informazioni e Sicurezza (COCI-RIS) per garantire l'aggregazione delle funzioni di *intelligence* tecnico-militare nella conduzione delle operazioni *full-spectrum*, nella dimensione cognitiva e nello spettro elettromagnetico nonché quelle di comprensione e contrasto della minaccia ibrida.

Con tale ottica, sono stati posti alle dipendenze del COCI-RIS il Comando per le Operazioni in Rete (COR), il Centro *Intelligence* Interforze e il Reparto Informazioni e Sicurezza.

---

[54] Oltre al CASD (riconosciuto quale Scuola Superiore Universitaria ad ordinamento speciale), il Polo è formato dalla Scuola di Telecomunicazioni delle Forze Armate (STELMILIT) e dal Centro Interforze di Formazione *Intelligence* e Guerra Elettronica (CIFIGE).

[55] I Corsi di Alta Formazione erogati dal CASD sono percorsi formativi di eccellenza nel settore della *cyber security* e delle tecnologie emergenti rivolti a personale militare e civile interessato a mantenere standard elevati di aggiornamento professionale e formazione.

[56] Già citata in premessa.

[57] Una *software factory* è un modello organizzativo e tecnologico funzionale alla centralizzazione e standardizzazione dello sviluppo del *software*, attraverso metodologie agili, pratiche DevSecOps e automazione. Una *software factory* consente un potenziale contenimento della dipendenza da fornitori esterni, l'aumento della sicurezza *by design*, la garanzia di riusabilità del codice e l'accelerazione del rilascio di soluzioni digitali innovative, a soddisfacimento delle esigenze operative.

Tale Comando deve caratterizzarsi per un livello tecnologico all'avanguardia, tale da consentirgli di operare in sinergia coi Pilastri dell'architettura nazionale di cybersicurezza e a supporto delle operazioni multi-dominio.

In tale contesto, sulla base dei compiti istituzionali della Difesa nel dominio cibernetico, tra cui quello di "autorità nazionale di gestione delle crisi informatiche", insieme all'Agenzia per la Cybersicurezza Nazionale[58], il COCI-RIS:

- dal tempo di pace fino a situazioni di conflitto armato, opera con approccio inter-agenzia e interministeriale, comprendendo, prevenendo e contrastando le minacce cibernetiche[59];
- contribuisce alla sicurezza cibernetica anche del segmento spaziale, con le articolazioni operanti nel dominio spazio;
- funge da autorità di coordinamento per l'impiego degli *asset* e capacità peculiari delle Forze Armate nel dominio cibernetico e nello spettro elettromagnetico;
- gestisce le risorse ICT e le info-strutture del dominio "classificato" e "non classificato" della Difesa;
- provvede allo scrutinio tecnologico e alla sicurezza delle catene logistiche;
- contribuisce alla sicura attuazione del processo di trasformazione digitale della Difesa.

Quadro Normativo

L'evoluzione del *framework* giuridico è essenziale per abilitare e accordare la missione della Difesa nel dominio cibernetico. Le relative proposte sono oggetto di uno specifico Disegno di Legge, funzionale all'evoluzione del contesto operativo di difesa e sicurezza militare dello Stato.

L'azione prioritaria perseguita riguarda l'adeguamento di ruoli e funzioni dello Strumento militare nello svolgimento dei compiti assegnati. In questo ambito, le azioni si concentrano su:

- garantire che lo Strumento militare sia operativo e capace di intervenire senza soluzione di continuità su tutto lo spettro delle minacce, sin dal tempo di pace, assicurando un'adeguata copertura giuridica per il personale militare impegnato nelle operazioni cibernetiche;
- predisporre norme per il reclutamento, l'alimentazione, la formazione, il trattenimento e l'impiego del personale specialistico, adottando una prospettiva interforze tale da garantire piena integrazione e sinergia tra le diverse componenti e con la possibilità di avvalersi di personale civile proveniente dagli istituti di formazione, dal settore industriale e dal mondo accademico e della ricerca;
- garantire la sicurezza e la protezione delle catene logistiche e delle relative infrastrutture che hanno impatto diretto sull'efficienza dello Strumento militare;

[58] Tale compito discende dal recepimento della direttiva (UE) 2022/2555 (c.d. *Network and Information Security* - NIS 2) relativa alle misure per garantire un livello comune elevato di sicurezza informatica nell'Unione Europea. La NIS2 è stata recepita col decreto legislativo 4 settembre 2024, n. 138.

[59] In particolare, questo compito sottende , le capacità di *due diligence* per vigilare sul proprio spazio cibernetico; *denial* per impedire, limitare, contrastare gli attacchi (statuali e non); *attribution* per contribuire, con valutazioni tecniche, a risalire con alta confidenza, agli autori di attacchi cibernetici; *punishment* per creare le premesse affinché chiunque attacchi un'infrastruttura vitale per la sicurezza dello spazio cibernetico sia soggetto a una legittima azione di contrasto, culminante in misure e sanzioni concrete, applicabili e credibili (deterrenza).

- sviluppare procedure di *procurement* in linea con le esigenze di sviluppo capacitivo, tenendo in debita considerazione le peculiarità e la rapidità dei processi di innovazione tecnologica;
- definire una condivisione, tempestiva, costante e strutturata, delle informazioni di sicurezza cibernetica tra i Pilastri dell'architettura nazionale affinché sia abilitato e garantito un approccio integrato per la sicurezza e difesa dello spazio cibernetico di interesse nazionale.

Organizzazione, procedure e relazioni

Al fine di sviluppare le capacità cyber in chiave interforze, inter-dicasteriale e inter-agenzia, sia al livello nazionale sia internazionale, risulta necessario perseguire il rafforzamento delle attività sul piano organizzativo, procedurale e su quello delle relazioni.

In particolare, nel perimetro operativo del citato COCI-RIS, devono essere implementate modalità di condivisione in tempo reale della situazione di sicurezza afferente alle reti interforze, delle Forze Armate e a quelle dei teatri operativi, tramite piattaforme e sistemi unificati. Tale condivisione è volta a mantenere il massimo livello di consapevolezza della minaccia e in maniera discendente, garantire la necessaria prontezza operativa dello Strumento.

Per quanto concerne l'integrazione operativa in ambito nazionale, è necessaria la strutturazione di processi funzionali alla condivisione di linee di indirizzo, procedure, modalità di risposta a eventi e crisi cibernetiche, nonché strategie per la formazione e l'acquisizione di competenze nel settore. Inoltre, occorre definire il perimetro di cooperazione tecnica in caso di evento, attacco o crisi cibernetica. Infine, è opportuno promuovere attività congiunte, quali ad esempio la pianificazione e la condotta di esercitazioni per incrementare la capacità di risposta in caso di evento o crisi cibernetica, la costituzione di team congiunti e altre attività collaborative.

Per quanto riguarda le iniziative in ambito NATO/UE, è necessario conseguire rilevanza nei progetti avviati, consolidando i processi necessari a impiegare le capacità cyber in sinergia con gli Alleati nonché le risorse messe a disposizione in ambito internazionale. Parimenti, è opportuno il consolidamento del ruolo nei meccanismi operativi dell'Alleanza Atlantica e dell'Unione Europea, con la finalità di salvaguardare gli interessi nazionali, con particolare riguardo alla deterrenza, alla difesa e alla sicurezza nello spazio cibernetico di interesse nazionale.

In generale, è necessaria la strutturazione di piani di cooperazione bi/multilaterali, rispondenti alle esigenze dei Paesi *partner* – in coerenza per esempio con l'approccio adottato dal Piano Mattei – attraverso attività di CCB, improntate alla logica *train, equip, sustain, infrastructure*.

In merito alle convergenze tra dominio cibernetico e spaziale, devono essere definite modalità per il rafforzamento della protezione cibernetica dei sistemi satellitari, sia in fase di progettazione sia durante l'operatività dei sistemi, al fine di prevenire limitazioni, interferenze o manipolazioni dei dati trasmessi. Inoltre, occorre individuare strumenti congiunti per il monitoraggio e la risposta alle minacce cibernetiche nello spazio, favorendo anche la condivisione di informazioni e la collaborazione tra le Organizzazioni internazionali di riferimento, quale ad esempio l'Agenzia Spaziale Europea e il settore privato.

Risorse umane

La realizzazione di una Forza credibile ed efficace nel dominio cibernetico è diretta responsabilità del Capo di Stato Maggiore della Difesa.

a. breve termine

È necessaria l'effettiva "interforzizzazione" dello Strumento e l'unificazione funzionale della Forza specialistica, costituita da personale sia civile sia militare. Tale unificazione rappresenta la precondizione per sviluppare una capacità efficiente ed efficace, in conformità agli indirizzi già delineati.

Per quanto attiene all'organico, si rende necessaria la definizione di nuovi meccanismi di reclutamento per individuare figure professionali, integrando competenze provenienti dal settore civile e dal mondo dell'industria. Parimenti, occorre definire meccanismi per l'alimentazione strutturata della forza specialistica, garantendo la continuità d'impiego nell'ambito di una filiera coerente nel tempo. Altresì, è fondamentale lo sviluppo delle competenze attraverso una formazione continua, unitamente alla valorizzazione e al riconoscimento economico delle competenze, seguendo il modello già adottato per le risorse pregiate a elevata connotazione specialistica.

Per quanto concerne la formazione avanzata, assume particolare rilevanza la valorizzazione del ruolo del Centro Alti Studi della Difesa quale ente di riferimento per il Dicastero, integrando le capacità formative interforze e delle Forze Armate. È necessario sviluppare percorsi di formazione per operatori, *management* e *leadership* attraverso percorsi nazionali e internazionali. Inoltre, occorre acquisire piattaforme avanzate per formarsi e addestrarsi, partecipando a esercitazioni anche di gestione di crisi nazionali, eventi e *workshop*. Infine, è opportuno sviluppare un portfolio di corsi e formazione da offrire ad altri Paesi, nell'ambito delle attività di relazione internazionale e di CCB.

b. medio termine

È importante procedere con le seguenti azioni:

- ridefinire, a livello qualitativo e quantitativo, il bacino specialistico *cyber* in accordo con l'aggiornato livello di ambizione e le discendenti esigenze operative;
- consolidare la valorizzazione delle capacità operanti negli Istituti di formazione militare di settore;
- perseguire la realizzazione di una riserva *cyber* con professionalità provenienti dal mondo civile (in particolare dal mondo universitario e della ricerca, nonché da quello industriale), complementare alle capacità esprimibili dalla Difesa.

Per il conseguimento degli scopi afferenti alle risorse umane è altresì necessaria la promozione dell'*appeal* della Difesa. Tale promozione si attua attraverso l'elaborazione di un piano comunicativo finalizzato a rendere attrattiva la Difesa in termini di reclutamento del personale, contribuendo alla cultura cibernetica e consolidando l'immagine dello Strumento militare come "frontiera tecnologica". Inoltre, occorre perseguire la fidelizzazione dei giovani appassionati del mondo cyber e tecnologico attraverso eventi attrattivi e innovativi[60] per facilitare l'incontro con i talenti del mondo della scuola, dell'università e della ricerca. Infine, è da perseguire la costituzione di un bacino di personale specialistico, costituito sia da militari sia da docenti universitari ed esperti

[60] *Cyber-Challenge*, *Open-day*, seminari, *Workshop*, *Cyber-Camp* e *Cyber-Lab* nonchè Cyber & IT *Talent Program*.

provenienti dalla società civile, per contribuire alla diffusione della cultura cibernetica all'interno del Dicastero.

Tecnologia

I processi di ammodernamento e rinnovamento dello Strumento militare richiedono maggior agilità nel modo di approcciare la tecnologia e l'innovazione.

a. breve termine

È necessaria la gestione delle risorse in accordo al mutato livello di ambizione, adottando architetture scalabili con approccio *security-oriented* e implementando tecnologie avanzate per il rilevamento delle minacce, crittografia avanzata come quella post-quantistica e soluzioni di sicurezza cibernetica quali il modello *zero trust* e le soluzioni *data-centric security*. In tale processo, si deve assicurare l'interoperabilità tra i sistemi *legacy* e quelli di nuova acquisizione.

Per quanto riguarda le soluzioni autonome e robotica, è necessario l'adeguamento delle capacità della Difesa alle nuove sfide operative, etiche e legali derivanti dal crescente utilizzo di tali sistemi. Infatti essi estendono il piano di complessità, costituendo un fattore strategico da governare con visione, rigore e responsabilità.

b. medio termine

Al fine di ottimizzare l'acquisizione degli elementi utili al tracciamento delle linee di sviluppo capacitivo, anche in chiave EDT, si reputano necessarie relazioni strutturate con le realtà industriali di settore.

Per quanto attiene all'*open innovation* [61], va perseguito un modello collaborativo tale da valorizzare competenze, tecnologie e soluzioni esterne, coinvolgendo attivamente cittadini, imprese, *start-up*, università e centri di ricerca. A tal riguardo, è necessaria l'implementazione anche di metodologie di *call for proposal* di tipo *solicited* [62], al fine di massimizzare il ritorno tecnologico sulle traiettorie individuate per soddisfare le specifiche esigenze della Difesa.

[61] Con *open innovation* si intende un approccio all'innovazione, prevedendo l'apertura dei processi di ricerca, sviluppo e sperimentazione a contributi esterni all'organizzazione, quali università, centri di ricerca, *start-up*, industria, comunità di esperti e partner pubblici-privati. In ambito *cyber*, l'*open innovation* favorisce la condivisione controllata di conoscenze, tecnologie e *best practice* per accelerare l'individuazione delle minacce, lo sviluppo di soluzioni di sicurezza avanzate e l'aumento della resilienza dei sistemi digitali, riducendo tempi e costi rispetto a modelli di innovazione esclusivamente interni.

[62] Una *call for proposal solicited* è un invito formale alla presentazione di proposte emesso da un'organizzazione su temi, requisiti e obiettivi specificamente definiti, con criteri di valutazione e scadenze prestabilite; le proposte presentate rispondono quindi a un'esigenza esplicita del committente. Una *call for proposal unsolicited*, invece, consiste nella presentazione spontanea di una proposta progettuale da parte di un soggetto esterno, non richiesta né guidata da un bando specifico, basata su idee o soluzioni innovative ritenute di potenziale interesse per l'organizzazione destinataria.

IV – DIRETTRICI STRATEGICHE E OBIETTIVI CAPACITIVI

Come indicato nell'introduzione, la Strategia Digitale si deve realizzare in un "percorso di sviluppo razionale, comprendendo valutazioni e scelte appropriate sulle info-strutture da realizzare e da impiegare" nonché l'aderenza agli indirizzi NATO/UE. In particolare, Ciò significa l'ineludibilità di soddisfare i c.d. *capability target* 2025 e quanto indicato dalla *Digital Transformation Implementation Strategy* 2.0.

Pertanto, sono di seguito delineate le Direttrici Strategiche (DS), suddivise per i tre pilastri della Strategia. Esse definiscono i principali ambiti di intervento verso i quali si intende orientare le azioni per l'implementazione del suddetto percorso, considerando l'arco temporale 2026 - 2030

Pilastro	Direttrice strategica	Obiettivo capacitivo
(VD) Valorizzazione del «dato»	(VD-DS-1) Modello di governo del «dato»	Entro il 2026 Esercizio dell'autorità e del controllo strategico sul *data management*.
	(VD-DS-2) Strumenti di *data management*	Entro il 2028 Realizzazione dei c.d. *data platform – data lakehouse* per fornire, controllare, proteggere e accrescere il valore dei «dati» lungo l'intero ciclo di vita.
	(VD-DS-3) Info-struttura *cloud*	Entro 1° semestre 2027 per soluzione *cloud* qualificato Entro 2028[63] per *cloud* sovrano-disconnesso Adozione di soluzioni *cloud*, tali da incrementare efficacia gestionale (tra cui la c.d. *collaboration*), scalabilità e sostenibilità, garantendo gli aspetti di sicurezza e controllo

[63] Le tempistiche di attuazione per i «dati» classificati sono subordinate ai relativi percorsi di certificazione.

		del «dato» in funzione del livello di classifica
	(VD-DS-4) Strumenti di *data-analytics*	Entro il 2027 Impiego di strumenti *off the shelf* e proprietari a supporto dei processi di *situational awarness* e *data-driven decision-making*.
(CA) Connettività avanzata	(CA-DS-1) Servizi satellitari multi-orbita e multi-*provider*	Entro 1° semestre 2027 Implementazione di soluzioni a garanzia di una connettività resiliente e in linea con le esigenze di dispiegamento dello Strumento.
	(CA-DS-2) Rete 5G proprietaria	Entro il 2029 Disponibilità di infrastrutture complementari nell'ambito dell'architettura di Difesa "*trusted*", ibrida e distribuita.
	(CA-DS-3) Sistemi avanzati C2, TLC e tattici	In continuità[64] Adozione di soluzioni per l'interscambio sicuro di «dati» tra piattaforme aeree, terrestri e navali e per disporre di un'appropriata *joint common operational picture*.
	(CA-DS-4) Reti classificate e non-classificate	Entro il 2028 Unificazione delle infrastrutture nei diversi domini, perseguendo omogeneità sia architetturale sia operativa.

[64] Termine impiegato per specificare che non c'è una scadenza predefinita ma è necessario porre in essere un processo di ammodernamento permanente e continuativo per il raggiungimento dell'obiettivo.

	(CA-DS-5) *Cross domain* monodirezionale	Entro il 2027 Adozione del c.d. *data diode*, per scambio «dati» tra i vari domini.
	(CA-DS-6) Standard NATO	In continuità Rispetto della coerenza con gli standard dell'Alleanza, per garantire un'interoperabilità c.d. *zero-day* delle Forze in operazioni.
(CY) *Cyber*	(CY-DS-1) Sicurezza e resilienza nel dominio cibernetico	Entro il 2029 (capacità iniziale) Adozione del paradigma *Zero Trust* per perseguire il controllo degli accessi, la segmentazione delle reti e la protezione degli *asset* critici secondo il principio *never trust, always verify*.
		In continuità Perseguimento di una robusta e univoca *cyber situational awarness,* massimizzando la sua condivisione a favore di tutto lo Strumento militare.
		In continuità Incremento del livello di consapevolezza da parte del fattore umano in materia di rischio cyber e impiego sicuro degli *asset* digitali.
		In continuità

		Sviluppo di strumenti tecnologici (e.g. cifranti ad alta capacità e «*quantum resistant*») per la continuità operativa e la protezione del perimetro digitale
	(CY-DS-2) Quadro normativo	Entro il 2027[65] Aggiornamento del vigente impianto di leggi e regolamenti per accordare la missione della Difesa nel dominio cibernetico, consentendone la piena e continua operatività, sin dal tempo di pace.
		In continuità Perseguimento della sicurezza e della protezione delle catene logistiche e delle infrastrutture che hanno impatto diretto sull'efficienza dello Strumento militare.
	(CY-DS-3) Operazioni cibernetiche *full spectrum*	In continuità Consolidamento della capacità di pianificare, condurre e sostenere operazioni cibernetiche per la difesa e la sicurezza militare dello spazio cibernetico di interesse nazionale.
		In continuità Coerenza organica della *cyber workforce*, in termini organizzativi, quantitativi e qualitativi.

[65] Percorso subordinato a *iter* legislativi

	(CY-DS-4) *Cyber Capacity Building*	In continuità Promozione della cooperazione all'interno delle Organizzazioni Internazionali di riferimento, nonché di iniziative bi-multilaterali, sostenendo una cultura della sicurezza cibernetica basata su condivisione, interoperabilità e mutuo supporto.

V – IMPLEMENTAZIONE DELLA STRATEGIA, MISURAZIONE DELLE *PERFORMANCE* E FATTORI DI RISCHIO

IMPLEMENTAZIONE DELLA STRATEGIA

L'attuazione della Strategia avverrà nell'ambito dei processi di pianificazione generale dello Stato Maggiore della Difesa[66], perseguendo il principio di ottimizzazione delle risorse e adottando un approccio *top-down* volto al conseguimento di effetti nel multi-dominio nonché al soddisfacimento degli obiettivi, nei tempi e modi indicati dal presente documento.

MISURAZIONE DELLE *PERFORMANCE*

Il processo sistematico che valuta – tramite *Key Performance Indicators* (KPI) – il raggiungimento degli obiettivi e l'efficacia delle misure previste da questa Strategia richiede l'utilizzo di metriche quantitative e qualitative per monitorare l'andamento, guidare le decisioni e attuare eventuali azioni correttive.

Quindi, per garantire un'adeguata misurazione dei risultati e il monitoraggio dell'avanzamento è opportuno applicare metodi riconosciuti, tra cui il NATO *Data Exploitation Maturity Model* (DEMM).

In allegato *echo*, è riportato un elenco dei principali KPI identificati.

FATTORI DI RISCHIO

Dall'analisi degli obiettivi e delle conseguenti linee di implementazione, emergono potenziali fattori di rischio che possono condizionare il soddisfacimento delle esigenze e che dovranno essere quindi mitigati per un'efficace implementazione della Strategia.

Tali **fattori di rischio**, riportati in allegato *foxtrot*, possono essere riassunti come di seguito.

In ambito **antropico**, emergono i rischi legati alla disponibilità – in termini qualitativi e quantitativi – di risorse umane con competenze digitali avanzate, unitamente a quelli di attrazione del "talento digitale", per via della forte competitività del settore privato. A ciò si somma la resistenza al cambiamento culturale e istituzionale, che si manifesta nella tendenza a mantenere silos informativi e nella difficoltà ad adottare approcci "*data-driven*" e "*cyber-aware*".

In ambito **tecnico/tecnologico**, le criticità risiedono nell'obsolescenza delle info-strutture ICT e nella persistenza di sistemi *legacy*, tali da ostacolare l'interoperabilità e la resilienza delle reti di fronte alle persistenti minacce. Ulteriori vulnerabilità derivano dal potenziale *vendor lock-in*, che vincola la libertà strategica a soluzioni proprietarie chiuse e non nazionali nonché dal rischio di una mancata acquisizione di capacità avanzate.

Infine, in ambito **gestionale e amministrativo**, i rischi sono legati alla frammentazione delle responsabilità nel governo del «dato», tali da generare ridondanze e scarsa *accountability*. Inoltre, la rigidità dei processi di *procurement* prefigura un disallineamento tra la velocità dell'innovazione e il soddisfacimento delle esigenze operative, mentre una limitata sinergia tra le componenti militari, civili e industriali potrebbe impedire la creazione di un efficace ecosistema digitale nazionale.

[66] In coerenza con il piano triennale per l'informatica e le attività discendenti dalle Linee Programmatiche del Ministro della Difesa in riferimento al dominio cibernetico.

VI – CONCLUSIONI

Questa strategia inquadra la trasformazione digitale della Difesa entro il 2030, non come una mera opzione tecnologica, ma come abilitatore fondamentale della sovranità nazionale e imperativo strategico imprescindibile per la difesa e sicurezza militare dello Stato. Infatti, il cuore di tale visione risiede nella necessità di perseguire l'incremento di autonomia e sovranità tecnologica, riducendo le dipendenze critiche da attori esterni.

Attraverso la valorizzazione del «dato» e un impianto di connettività avanzata, la Difesa si pone l'obiettivo di creare un ecosistema integrato e interoperabile, anche a livello internazionale, essenziale per garantire la libertà di azione nei sempre più complessi scenari multi-dominio.

In un contesto internazionale caratterizzato da una competizione permanente in ogni ambito e da minacce ibride sempre più insidiose, il dominio cibernetico emerge quale contesto primario e moltiplicatore di effetti, tali da paralizzare infrastrutture critiche e manipolare i processi democratici. Pertanto, è necessario evolvere da una postura meramente reattiva a una capacità predittiva, proattiva e adattiva, al fine di garantire resilienza, difesa e sicurezza. Il messaggio è netto: la sicurezza dello spazio cibernetico è, in modo estensivo, una precondizione per la libertà e la prosperità dello Stato.

A tal fine, è vitale investire nel capitale umano, promuovendo la formazione specialistica e una cultura della sicurezza basata sulla condivisione e sul mutuo supporto. Al contempo, la Difesa deve adottare un modello in grado di coinvolgere in sinergia, il mondo accademico e della ricerca nonché quello industriale, garantendo agilità nell'adozione di tecnologie emergenti e dirompenti, come l'intelligenza artificiale e le tecnologie quantistiche, da governare con visione e responsabilità.

La Difesa deve confermare il suo ruolo di "frontiera tecnologica" del Paese, un baluardo capace di adattarsi alla mutevolezza delle sfide moderne. Questo impegno richiede anche una solida cooperazione internazionale, in particolare in ambito NATO e UE, per consolidare una rete di sicurezza condivisa, a tutela degli interessi nazionali e della stabilità globale.

Solo attraverso il connubio tra innovazione e sovranità tecnologica, eccellenza professionale e sinergia strategica a livello di Sistema-Paese, si potranno proteggere efficacemente gli *asset* critici e i processi democratici, in una realtà sempre più interconnessa e contesa.

Bibliografia

Nazionale

- D.Lgs. 15 marzo 2010, n. 66 – Codice dell'Ordinamento Militare. Aggiornato al 23 giugno 2025, in corrispondenza della Legge 9 maggio 2025, n. 69
- D.Lgs 4 settembre 2024, n. 138 che recepisce la Direttiva (UE) 2022/2555 (conosciuta anche come *Network and Information Security* - NIS 2)
- Linee Programmatiche del Ministro Della Difesa – ed. 2023
- Atto di Indirizzo del Ministro della Difesa per l'avvio del ciclo integrato di programmazione della performance e di formazione del bilancio di previsione per l'E.F. 2025 e la programmazione pluriennale 2026-2027 – ed. 2025
- "Strategia *cloud* Italia" del Dipartimento per la trasformazione digitale del Governo italiano in collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN) (2021)
- Strategia di Cyber-sicurezza Nazionale 2022-2026 - emanata dal Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la Cybersicurezza Nazionale (ACN) e del Comitato Interministeriale per la Cybersicurezza (CIC), in attuazione del D.L. 14 giugno 2021, n. 82, che ha istituito l'ACN e definito il perimetro nazionale di cybersicurezza
- Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica (aka PSNC) – aggiornato a maggio 2024
- IA e Difesa: Strategia della Difesa in materia di Intelligenza Artificiale - edizione 2026

Nato

- *Digital Transformation Vision* – ed. 2022
- *Data Strategy for the Alliance* – ed. 2025
- *Digital Transformation Implementation Strategy* 2.0 – ed. 2025
- *Data Exploitation Framework Strategic Plan* – ed. 2022
- *Data Centric Security Implementation Plan* – ed. 2022
- *Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems* – ed. 2024
- *Artificial Intelligence Strategy* – ed. 2025 (R)

Unione Europea

- *Strategic Compass* – adottato dal Consiglio dell'UE il 21 marzo 2022
- *Strategic Implementation Plan for the Digitalisation of EU Forces* – ed. 2021

Cina

- Baughman, Josh. 2024. "*The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield*" The Cyber Defense Review
- Bitzinger, Richard, Yoram Evron, and Zi Yang. 2021. "*Roundtable China's Military-Civil Fusion Strategy: Development, Procurement, and Secrecy Asia Policy*"
- Lee, Jonathon. 2025. "*China Military Studies Review*" Usmcu.edu
- McFaul, Cole, Sam Bresnick, and Daniel Chou. 2025. "*Pulling Back the Curtain on China's Military-Civil Fusion | Center for Security and Emerging Technology*." Center for Security and Emerging Technology (CSET)

- Staff, SWJ. 2025. "*Military and Security Developments Involving the People's Republic of China December* 2024 | Small Wars Journal by Arizona State University."
- Sterling, Bruce. 2020. "'Accelerate the Development of Military Intelligentization" WIRED

Russia

- Nadibaidze, Anna. 2022. "*Russian perceptions of military AI, automation, and autonomy.*" Foreign Policy Research Institute (FPRI)
- "*Russia's National AI Strategy.*" 2024. Global Institute for National Capability.
- Sukhankin, Sergey. 2025. "*Russia capitalizes on development of artificial intelligence in its military strategy*" Jamestown.org
- Borchert, Heiko. 2024. The Very Long Game. Springer Nature
- "*Intersessional panel of the United Nations commission on science and technology for development* (CSTD)." 2024

Studi e analisi

Soare, Simona R. 2023 "*Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age*" - International Institute for Strategic Studies (IISS)

ALLEGATO A - Principi del «dato»

Per «dato» si intende "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di essi, anche sotto forma di registrazione sonora, visiva o audiovisiva*" [67].

In conformità alla dottrina dell'Alleanza Atlantica[68], la definizione di «dato» comprende:

- dati tabellari strutturati, inclusi dati numerici e categoriali;
- testo non strutturato e testo in linguaggio naturale;
- dati analogici o digitalizzati quali immagini, video, audio o contenuti multimediali;
- dati ottenuti da sensori e sistemi di segnalazione sensoriale;
- *metadati*, ossia informazioni su altri dati;
- prodotti derivati e basati su quanto sopra, tra cui analisi, riepiloghi e statistiche descrittive, nonché i risultati delle tecniche di sfruttamento ed elaborazione dei dati (per esempio IA/*Machine Learning* - ML).

Tra l'altro, questa definizione aggiorna la tradizionale distinzione tra «informazioni» e «dati». Infatti, l'«informazione» emersa dai «dati» in un determinato contesto può assumere il ruolo di «dato» per un altro contesto, poiché combinata con ulteriori «dati». Per esempio, un'«informazione» con specifica interpretazione e output al livello tattico, può essere un «dato» per i livelli superiori, concorrendo alla determinazione di scenari informativi più ampi e articolati.

I principi del «dato» – da rispettare all'unisono per conseguire gli obiettivi della Strategia – sono:

Visibilità

I «dati» devono essere registrati, reperibili e la loro esistenza deve essere visibile a persone o sistemi autorizzati. I metadati devono essere localizzabili attraverso *repository* [69] centralizzati virtualizzabili.

Accessibilità

I «dati» devono essere disponibili per l'uso da parte di persone, entità e sistemi autorizzati attraverso meccanismi appropriati e *policy* di accesso, con particolare attenzione a manutenzione e amministrazione dei *repository*.

Affidabilità

Gli utenti e i sistemi devono essere in grado di determinare e valutare l'integrità dei «dati» e dei processi relativi ai «dati» affinché gli stessi possano essere utilizzati con sicurezza nelle attività decisionali e di analisi. A tal fine, vanno considerati:

- l'integrazione di metadati e di una semantica condivisa[70], per facilitare l'identificazione, la tracciabilità, il recupero e la referenziazione dei «dati»

---

[67] DDL del Senato, 20 marzo 2025 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale".

[68] *Data Strategy for the Alliance*, febbraio 2025.

[69] Per *repository* di dati si intende un contenitore logico o fisico in cui i dati vengono archiviati, gestiti e resi disponibili secondo regole di accesso e sicurezza predefinite. A differenza di semplici archivi statici, un *repository* è progettato per garantire conservazione, integrità, reperibilità e condivisione dei «dati» lungo il loro ciclo di vita, anche tramite metadati e cataloghi centralizzati. In ambito Difesa, i *repository* possono assumere forme diverse – da database relazionali a sistemi documentali, da *data warehouse* a *data lake* (cfr. il glossario) – e costituiscono la base di un ecosistema data-centrico, orientato alla valorizzazione e interoperabilità delle informazioni.

[70] Per semantica si intende l'insieme delle regole e dei modelli tali da attribuire significato univoco ai «dati», distinguendoli dal mero livello sintattico o tecnico. In ambito di *governance* digitale, la semantica si realizza attraverso

- la creazione di sistemi di monitoraggio per garantire l'affidabilità lungo l'intero ciclo di vita del «dato»[71]
- il potenziamento del controllo e della registrazione attività sui «dati», migliorando trasparenza e *accountability*.

Regolamentazione

I «dati» devono essere regolati e gestiti secondo normative, *policy* e standard nazionali nonché NATO e UE.

Interoperabilità

I «dati», i sistemi e i processi relativi ai «dati» devono garantire l'interoperabilità all'interno della Difesa. Pertanto, è necessaria un'architettura comune/federata, dotata di interfacce standard tali da garantire la comunicazione e i requisiti di interoperabilità sintattica e semantica[72].

Qualità

La qualità dei «dati» deve essere garantita per tutto il ciclo di vita, attraverso l'implementazione di azioni di controllo esplicite, automaticamente implementate, catalogate, registrate e revisionate per garantire l'idoneità dei «dati» agli scopi e utilizzi previsti dalla Difesa.

Condivisibilità

I «dati» devono essere disponibili per utenti, sistemi e organizzazioni autorizzate, nel rispetto del *need to share.* Pertanto, si devono utilizzare meccanismi appropriati, sicuri e standardizzati, in modo da favorire collaborazione e cooperazione anziché silos informativi. L'implementazione di standard per i metadati facilita l'individuazione e l'accesso alle risorse di «dati» condivisibili (i.e. catalogo dati).

Sicurezza

I «dati» devono essere protetti e controllati durante l'intero ciclo di vita, al fine di garantirne riservatezza, integrità, disponibilità, autenticazione e non ripudio[73]. A tal fine, va considerata una gestione granulare dei privilegi di accesso ai «dati», delle identità digitali e delle condizioni di contesto nelle quali le richieste di accesso ai «dati» si materializzano[74].
I requisiti di sicurezza peculiari delle categorie di «dati» soggette a particolari discipline, quali la tutela del segreto di stato, la privacy e le specifiche regolamentazioni amministrative,

---

vocabolari, ontologie e metadati condivisi, per assicurare coerenza interpretativa, interoperabilità tra sistemi e corretto sfruttamento del patrimonio informativo della Difesa.

[71] Il "ciclo di vita del dato" si compone delle seguenti fasi: creazione, applicazione regole di standardizzazione e sicurezza, salvataggio, utilizzo, archiviazione, eliminazione.

[72] L'interoperabilità sintattica assicura che i sistemi possano scambiarsi «dati» secondo formati e codifiche standard (es. XML, JSON), garantendone la leggibilità strutturale; l'interoperabilità semantica garantisce invece che tali dati siano interpretati con lo stesso significato, grazie a vocabolari, ontologie e metadati condivisi (cfr. ISO/IEC 11179; W3C Semantic Web Standards).

[73] Con il termine non ripudio del «dato» si indica la garanzia per cui un'informazione, una transazione o una comunicazione digitale non possa essere negata dal soggetto che l'ha generata, trasmessa o ricevuta. In ambito giuridico e tecnico, il non ripudio è assicurato mediante meccanismi come firme digitali, certificati crittografici e log sicuri, tali da attribuire in modo certo la responsabilità di un'azione digitale, rafforzando così integrità, tracciabilità e *accountability*.

[74] Concetti relativi alla *Data Centric Security*. Essa si concentra sulla protezione dei dati, indipendentemente da dove si trovino, da chi li accede o da come vengono trasmessi. In altre parole, invece di basarsi solo sulla difesa di reti o dispositivi (difesa del perimetro), la *Data Centric Security* applica controlli di sicurezza e policy ai dati stessi, tramite: cifratura persistente, gestione dinamica dei diritti di accesso, classificazione, tracciamento dei dati, ecc.

devono essere applicati con marcature di sicurezza e tecnologie di prevenzione della perdita di «dati» nonché solidi meccanismi di auditing, tali implementare per i metadati, restrizioni di accesso e gestione in modo immutabile.

ALLEGATO B – Approfondimento del quadro internazionale

Il Regno Unito ha avviato la costruzione di una propria *digital backbone* ossia una rete digitale unificata e sicura per le Forze Armate. L'obiettivo è integrare oltre 2.000 sistemi *legacy* in un'infrastruttura modulare e *cloud-ready*, comprendendo una *Digital Foundry* [75] per la gestione e l'analisi dei «dati» nonché una *Defence Digital Function,* direttamente dipendente dal vertice politico-militare[76].

Nel quadro della "Legge di programmazione Militare 2024-2030", la Francia ha avviato una riforma organizzativa nel settore digitale della Difesa, con la creazione del *Commissariat au Numérique de Défense* (CND)[77] – operativo dal settembre 2025 – sotto l'autorità diretta del Ministro delle Forze Armate. Il CND integra le funzioni, le competenze e le risorse finora distribuite fra tre enti principali: la Direzione Generale del Digitale e dei Sistemi d'Informazione e Comunicazione (DGNum), la Direzione Interforze delle Reti e dei Sistemi d'Informazione della Difesa (DIRISI) e l'Agenzia del Digitale di Difesa (AND).

Nel 2026, è prevista il passaggio alle dipendenze della CND anche dell'Agenzia Ministeriale per l'Intelligenza Artificiale di Difesa (AMIAD), consolidando l'intera catena di comando digitale, dalle infrastrutture alla gestione dei «dati» e applicazioni avanzate. Inoltre, la Francia ha sviluppato il programma *Architecture for Processing and Massive Exploitation of Multi-source Information and Artificial Intelligence* (ARTEMIS.IA). Nella fattispecie, si tratta di un'info-struttura tipo *digital backbone* nazionale per le Forze Armate, con focus su autonomia tecnologica e sovranità dei «dati», nell'intento di affrancarsi quanto possibile, dalle soluzioni extra-UE. ARTEMIS.IA integra capacità di IA per funzioni di *Intelligence, Surveillance and Reconnaissance* (ISR)[78], pianificazione operativa e superiorità informativa, presentandosi come uno dei modelli europei più avanzati di trasformazione digitale della Difesa.

Nel 2025, la Germania ha creato il Ministero Federale per la Trasformazione Digitale e la Modernizzazione dello Stato (BMDS)[79] e nell'ambito della Difesa, è impegnata in rilevanti iniziative. Tra esse, si annoverano il programma *AI4Defence* volto a sviluppare un'infrastruttura federata per l'impiego sicuro e sovrano dell'IA in ambito militare e il contratto plurimiliardario *Digitalisierung Landbasierter Operationen* (D-LBO), per la digitalizzazione delle operazioni terrestri. Inoltre, la Germania sta perseguendo il c.d. paradigma *Software Defined Defence* (SDD), già richiamato nell'*Alliance Digital Strategy*.

---

[75] La *Digital Foundry* è una struttura dedicata a sperimentare, sviluppare e integrare con rapidità soluzioni digitali innovative in ambito Difesa. Opera come laboratorio agile per combinare competenze di *data science*, intelligenza artificiale, *cloud* ed *edge computing*, con l'obiettivo di trasformare i «dati» in capacità operative concrete.

[76] La *Defence Digital Function* è la struttura inglese di governo incaricata di guidare la trasformazione digitale della Difesa. Riunisce competenze, policy e standard relativi a «dati», architetture, *cloud*, sicurezza cibernetica e innovazione, assicurando coerenza tra i programmi e favorendo l'adozione di soluzioni digitali comuni. In sostanza, rappresenta il "cuore organizzativo" della digitalizzazione, complementare alle *Digital Foundry* (laboratori di sperimentazione) e al *Digital Backbone* (infrastruttura tecnologica).

[77] https://www.defense.gouv.fr/actualites/commissariat-au-numerique-defense-nouveau-vecteur-puissance-numerique.

[78] ISR indica l'insieme delle attività di raccolta, analisi e diffusione di informazioni ottenute tramite fonti di *intelligence*, sistemi di sorveglianza (sensoristica, satelliti, UAV, radar, ecc.) e piattaforme di ricognizione, finalizzate a supportare il processo decisionale e le operazioni militari.

[79] BMDS è l'acronimo di *Bundesministerium für digitale Transformation und Staatsmodernisierung* ossia il citato Ministero istituito col compito di coordinare le politiche digitali, l'innovazione tecnologica e la modernizzazione di tutta la pubblica amministrazione.

Detto paradigma si basa sul concetto di disaccoppiare le funzionalità operative dall'*hardware* fisico, rendendo i sistemi di comando, controllo, comunicazione e combattimento programmabili, riconfigurabili e aggiornabili tramite *software*. In tal modo, la capacità militare non è più vincolata al ciclo di vita dell'*hardware*, ma può evolvere in modo agile grazie ad aggiornamenti digitali, automazione e IA. Il modello SDD consente la gestione dinamica di reti, sensori e piattaforme attraverso un'architettura *cloud-edge* federata e mira a una Difesa per l'appunto, "*software-defined*" ossia abilitata dai «dati».

Sul versante dei potenziali *competitor*, emerge l'esperienza della *Military-Civil Fusion* cinese ossia la strategia lanciata per integrare il settore civile con quello militare, favorendo il trasferimento di tecnologie *dual-use* tramite un "sistema strategico integrato nazionale" di *procurement*. Con tale prospettiva, la Cina è impegnata in un proprio percorso di transizione da "meccanizzazione", a "informatizzazione e intelligentizzazione" della guerra, adottando l'impiego sistemico di IA, calcolo quantistico, realtà virtuale/aumentata, *cloud*, sistemi autonomi e IoT, per condurre operazioni multi-dominio e cognitive.

L'Esercito Popolare di Liberazione cinese descrive questo approccio come una nuova "rivoluzione negli affari militari", fino a concepire scenari di meta-war, in grado di fondere campo fisico, virtuale e cognitivo.

Sul fronte russo, si può citare il parco tecnologico militare "ERA Technopolis", inaugurato dal Ministero della Difesa russo nel 2018 ad Anapa sul Mar Nero. Esso è concepito come hub di ricerca e sviluppo per l'integrazione di IA, robotica, *big data* e guerra elettronica.

Presentato come la "*Silicon Valley* militare russa", il complesso coinvolge università, centri di ricerca e imprese nazionali con l'obiettivo di accelerare l'adozione di tecnologie duali a supporto delle funzioni di "Comando & Controllo" (C2), ISR e sistemi autonomi, in coerenza con la strategia russa di IA al 2030.

ALLEGATO C - Condizioni per la valorizzazione del «dato»

Per il conseguimento degli obiettivi indicati nella parte I della Strategia, si individuano le seguenti linee di azione, associate alle "condizioni" e/o "caratteristiche chiave".

1. Accuratezza
   - Integrare meccanismi di *data-quality* e *data management* su standard condivisi, definiti nel perimetro della *data governance*.
   - Definire metadati e semantica in conformità con gli standard NATO.
   - Sviluppare – in accordo alla specifica Strategia della Difesa – sistemi di IA per la validazione continua dei «dati».
2. Aggiornamento
   - Realizzare piattaforme «dati» automatizzate, basate su tecnologie volte a garantire aggiornamenti costanti e accessibilità a «dati» affidabili, con un basso impatto in termini di personale[80].
   - Integrare all'interno di dette piattaforme, *framework* di monitoraggio dinamico (*data curation*) dei controlli riguardanti la completezza, la qualità e l'affidabilità dei «dati», contenuti nei *repository* della Difesa.
3. Analisi
   - Acquisire strumenti di *data-analysis* e IA per la valorizzazione e lo sfruttamento di volumi elevati di «dati» in accordo a riferimenti NATO per la *data-centric architecture*.
   - Dimensionare le architetture per la *data-analysis* sulle caratteristiche qualitative e quantitative dei «dati» trattati, c.d. 5V dei *big data* (Volume, Velocità, Varietà, Veridicità, Valore), per guidare le analisi.
   - Supportare l'analisi nelle tre dimensioni: fisica, virtuale e cognitiva.
   - Acquisire capacità computazionali ad alte prestazioni coerenti con le esigenze di valorizzazione del patrimonio informativo, "classificato" e "non- classificato".
4. Compatibilità
   - Realizzare un modello organizzativo di *data management* comune (insieme condiviso di principi, standard, strumenti e *framework* tecnologici per un'infrastruttura coerente, interoperabile e scalabile).
   - Implementare un catalogo di *Application Programming Interface* (API) – ossia connettori standard – per supportare l'integrazione di soluzioni analitiche e operative.
   - Individuare sistemi flessibili per compatibilità a lungo termine tra tecnologie emergenti e *legacy*, supportando scenari di operazioni multi-dominio.
   - Integrare IA e HPC in accordo alla specifica Strategia della Difesa, con finalità di analisi su grandi volumi di «dati» – classificati e non-classificati – provenienti da piattaforme eterogenee.
   - Assicurare l'interoperabilità per evitare duplicazioni, inutili conversioni e spreco di risorse, a supporto anche della sostenibilità energetica.

[80] Le soluzioni tecnologiche saranno individuate in fase di implementazione della Strategia.

5. Completezza
   - Costruire un ecosistema di «dati» tale da integrare fonti multiple, perseguendo altresì la raccolta dei «dati» prodotti da tutte le piattaforme e asset della Difesa.
   - Adottare il citato modello *data management*, considerando l'intero ciclo di vita del «dato» e assicurando trasversalità per tutti i domini.
   - Automatizzare per ridurre il rischio errore umano.
   - Eliminare «dati» duplicati e obsoleti per evitare sprechi computazionali: minore consumo energetico nei *data centre* grazie a un uso ottimizzato dello *storage*. A tal fine, lo Stato Maggiore Difesa è chiamato a definire le linee implementative per la pronta razionalizzazione dei *data centre* interforze e della Difesa nonché l'adozione di tecnologie *cloud* [81]. Ciò deve avvenire nel breve termine per il dominio "non classificato" e nel medio termine per il dominio "classificato".

6. Conformità
   - Adottare piattaforme automatizzate per il monitoraggio della conformità normativa, l'allineamento a direttive e linee guida europee e NATO, l'adattamento ai cambiamenti legislativi.

7. Conservazione
   - Considerare il «dato» come *asset* duraturo. I «dati» devono persistere oltre i singoli progetti ed essere mantenuti per utilizzi futuri.
   - Adottare nel breve termine, tecnologie di archiviazione distribuita[82] e – quando applicabili – sistemi di *quantum-safe cryptography,* per garantire la sicurezza ai massimi livelli disponibili sul mercato.
   - Prevenire fenomeni di *lock-in* tecnologico, adottando soluzioni diversificate, flessibili e scalabili.
   - Definire regole di conservazione, catalogazione e monitoraggio dei «dati» tali da ridurre i rischi legati alla loro aggregazione e divulgazione, nonché garantire il riutilizzo dei «dati» (principio fornitura *once only)*.
   - Perseguire il *repository* dei «dati» conformi e accessibili per le articolazioni interforze e delle Forze Armate, senza silos informativi.
   - Adottare soluzioni di *business continuity* e *disaster recovery* per garantire l'integrità dei «dati» anche in situazioni di reset estremi, di natura cibernetica, cinetica o disastro naturale.
   - Monitorare e rimuovere «dati» inutilizzati per ottimizzazione delle risorse.

8. Portabilità tra piattaforme
   - Realizzare ecosistemi di «dati» aperti e scalabili, tali da consentire la piena integrazione dei *data lakehouse* in uso nella Difesa in accordo a procedure automatizzate.
   - Individuare tecnologie eventualmente *open-source* e soluzioni di *collaboration* digitale non solo all'interno della Difesa ma anche in chiave interministeriale e inter-

[81] Le tecnologie individuate dovranno soddisfare i principi del «dato» e in particolare, soddisfare i parametri di sicurezza e adottare meccanismi di mitigazione secondo standard, normative e framework condivisi in ambito NATO/UE (cfr. art. 89 del "Codice dell'ordinamento militare").

[82] Le tecnologie di archiviazione impiegate dalle Forze Armate sono oggi eterogenee (es. veeam, rubrik, veritas, commvault, ecc.). Pertanto, è necessaria la standardizzazione delle modalità con cui sono realizzati i *back-up* (quando, dove e come) nonché l'individuazione di una piattaforma unica di gestione per tutta la Difesa, risultando un unico *data lake* e un unico punto di accesso e controllo del *back-up*.

agenzia. Ciò deve essere garantito con prontezza per i «dati» del dominio "non classificato", adottando soluzioni in *cloud*.
- Integrare sensori IoT e tecnologie avanzate come il 5G/6G nonché costellazioni di satelliti a bassa orbita (SatLEO[83]) per garantire connettività e accesso continuo ai «dati»[84].

9. Protezione
- Garantire la sicurezza «dati» in accordo alla classifica e in ogni fase di creazione, gestione, trattamento, archiviazione e trasmissione. Realizzazione di ambienti logici *secure by design*, integrando approcci proattivi come l'IA predittiva (identificazione e mitigazione minacce) e le architetture *zero trust.*
- Applicare modelli di *data centric security* basati sulla triade *Confidentiality – Integrity – Availability* (CIA).
- Registrare le operazioni di accesso, uso e modifica dei «dati» per garantire sicurezza e trasparenza.
- Adottare sistemi di autenticazione avanzati come l'*Identity, Credential, and Access Management* (ICAM).
- Gestire i privilegi di accesso, *account, labeling* e crittografia nel rispetto delle normative delle Organizzazioni Internazionali di appartenenza.
- Considerare il «dato» come risorsa rispondente al paradigma *need to share* oltreché a quello del *need to know*.
- Realizzare sistemi nel rispetto dei principi di *privacy by design* e *privacy by default,* minimizzando i «dati» personali trattati e il loro periodo di conservazione.

10. Rilevanza
- Valorizzare i «dati» come motore strategico, operativo e tattico, integrando il «dato» nei processi decisionali e nei modelli predittivi per anticipare scenari futuri.
- Utilizzare IA e ML adattivo non solo per migliorare la rilevanza nei contesti applicativi ma anche per abilitare modelli predittivi.
- Strutturare la semantica avanzata: oltre alla standardizzazione del «dato», creazione di ontologie e *knowledge graphs* per una rappresentazione più intelligente e relazionale delle informazioni.
- *data-driven operations*: incentivare processi decisionali basati su *insight data-driven*, riducendo la dipendenza da analisi *ex-post* e decisioni manuali.

11. Sovranità del dato
- Ricercare ed adottare soluzioni e tecnologie *cloud* che soddisfino i principi di sovranità tecnologica e digitale, in particolare per il «dato» classificato.
- Assicurare il pieno controllo dei flussi «dati» dalle fonti autoritative (*data producer*) agli utenti finali (*data consumer*) attraverso le politiche di *data governance*, per garantire accuratezza e responsabilità nell'accesso e utilizzo dei «dati».
- Contrastare le minacce *cyber* come esplicitato nella III parte della presente Strategia.

[83] Sistemi satellitari del tipo *Low Earth Orbit*.

[84] Il tema è trattato nella II parte della Strategia, riguardante la "connettività avanzata".

12. Standardizzazione
    - Adottare *framework* di interoperabilità anche duale, basati su *standard* aperti e condivisi tra le Forze Armate. In tal senso, è promossa la standardizzazione secondo i NATO *Interoperability Standards and Profiles* (NISP)[85] e UE.

13. Tracciabilità
    - Implementare soluzioni volte a garantire tracciabilità affidabile e verificabile.
    - Integrare sistemi tali da coprire l'intero ciclo di vita del «dato» e adottare strutture logiche di *data-topology* per localizzare e gestire i «dati» attraverso l'organizzazione.

14. Organizzazione
    - Istituire il modello interforze di governo e gestione del «dato».
    - Condividere i «dati» per evitare *silos* informativi.

15. Formazione
    - Promuovere un investimento mirato sul capitale umano, affinché la Difesa disponga di *Knowledge, Skill, Ability* (KSA)[86] funzionali al conseguimento degli scopi della Strategia. Tale prospettiva sottende l'opportunità di:
      a. orientare la formazione di base, includendo aliquote di discipline STEM[87] e moduli di cultura digitale nei corsi delle Accademie per Ufficiali e delle Scuole Sottufficiali, così da creare un potenziale bacino e un *mindset* "*digital-ready*" già nelle prime fasi della carriera;
      b. sviluppare formazione specialistica a più livelli, prevedendo syllabus correlati ai ruoli professionali per alfabetizzazione digitale diffusa, percorsi su *data management*, *analytics*, intelligenza artificiale e *cyber-security*. In tal senso, la Strategia contempla anche l'integrazione delle strategie nazionali vigenti sulla trasformazione digitale con il supporto dell'Agenzia per l'Italia Digitale nel caso di applicazioni duali;
      c. esplorare inedite formule di formazione e reclutamento a "geometria variabile", ricorrendo a risorse dell'industria, del mondo accademico e della ricerca, per la condivisione e il trasferimento osmotico di competenze.

[85] I NATO *Interoperability Standards and Profiles* (NISP) costituiscono il quadro di riferimento tecnico adottato dall'Alleanza Atlantica per garantire la coerenza, l'interoperabilità e la standardizzazione dei sistemi di comando, controllo, comunicazione, *computer*, *intelligence*, sorveglianza e ricognizione (C4ISR).

[86] *Knowledge, Skills and Abilities* sono le tre dimensioni su cui si articola la preparazione del personale. "*Knowledge*" rappresenta l'insieme delle conoscenze teoriche e tecniche, "*Skills*" le competenze pratiche per applicarle efficacemente, mentre "*Abilities*" le capacità cognitive e personali (es. *problem solving*, adattabilità); esse consentono di operare in contesti complessi e dinamici. La tassonomia KSA è ampiamente utilizzata in ambito HR, formativo e operativo, nel settore pubblico e quello privato, costituendo un riferimento anche nei *framework* NATO ed UE per lo sviluppo di una *work-force digital-ready*.

[87] Per STEM si intende *Science, Technology, Engineering and Mathematics*, ovvero l'insieme delle discipline tecnico-scientifiche (Scienze, Tecnologia, Ingegneria e Matematica). L'acronimo è utilizzato a livello internazionale per indicare i percorsi formativi e professionali che costituiscono la base per lo sviluppo tecnologico, l'innovazione e la competitività, con applicazioni centrali anche in ambito Difesa e sicurezza.

16. Efficienza energetica

- Razionalizzare le info-strutture della Difesa, privilegiando, ove possibile, l'adozione di soluzioni in outsourcing ad alta efficienza, così da contenere i consumi energetici e idrici, ottimizzare l'impiego delle risorse e beneficiare delle più avanzate tecnologie sostenibili messe a disposizione dagli operatori specializzati.
- Integrare in modo sistematico i principi della *green information technology* [88], orientando progettazione, gestione e utilizzo delle info-strutture verso criteri di sostenibilità ambientale e riduzione dell'impatto energetico.

17. Sostenibilità

- Adottare soluzioni in grado di ottimizzare e conciliare le relazioni tra l'esigenza operativa individuata, la discendente capacità attesa e l'effettiva sostenibilità della stessa, considerando l'insieme di tutte le condizioni al contorno (i.e. offerta e *ramp up* tecnologica/industriale e prospettive di "ricerca e sviluppo", disponibilità di risorse – umane, finanziarie, tempo – ma anche vincoli burocratici esogeni quali le procedure indicate dal "codice degli appalti").

[88] Per *green information technology* (green IT) si intende l'insieme di pratiche, tecniche e soluzioni tecnologiche volte a ridurre l'impatto ambientale dei sistemi informativi lungo l'intero ciclo di vita: dalla progettazione delle infrastrutture, alla gestione energetica dei data center, fino al corretto smaltimento e riciclo delle apparecchiature elettroniche. L'obiettivo è garantire sostenibilità, efficienza e risparmio energetico, senza compromettere le prestazioni operative.

ALLEGATO D - Implementazione del governo e della gestione del «dato»

QUALITÀ DEI «DATI»

Tutte le capacità analitiche richiedono «dati» affidabili, di qualità e tali da scongiurare distorsioni involontarie, per supportare lo sviluppo di sistemi efficaci e interoperabili. Grazie alla qualità, i «dati» possono essere valutati, catalogati e comunicati in modo appropriato a utenti e applicazioni, garantendone l'idoneità agli scopi previsti e abilitando *data-analytics* e IA.

La qualità dei «dati» è misurabile attraverso gli indicatori della norma ISO 8000, la quale individua una qualità intrinseca e una qualità estrinseca dei «dati»[89]. Tuttavia, qualunque capacità relativa ai «dati» lungo tutto il ciclo di vita, dovrà rispondere ai citati principi del «dato».

La prima azione da attuare è incrementare la qualità del «dato», riconoscendolo come il primo valore dell'«informazione». L'ecosistema *data-driven* deve garantire a ogni entità "*consumer*" in possesso del *need to know* e autorizzato all'accesso[90] in base alle politiche di *data governance*, di trovare e accedere ai «dati» provenienti da qualsivoglia fonte e dominio operativo, per sviluppare analisi e *dashboard* funzionali alle esigenze della sua "missione".

A tal fine, dovranno essere favorite basi dati centralizzate e/o federate (per esempio, i *data lakehouse*), utilizzando la raccolta e l'aggregazione strutturata e automatizzata dei «dati» in tutta la Difesa nonché collegando le fonti di «dati», per consentire la prontezza informativa.

Quindi, figure dedicate – ovvero i *Data Manager* – disporranno dell'autorità e della responsabilità di garantire la disponibilità di «dati» qualitativamente validi, gestendoli come un "prodotto".

Questo è un cambiamento radicale nell'erogazione delle soluzioni digitali poiché tali figure dovranno interagire con trasversalità in tutta la Difesa, attraverso i processi di *data management*, affinché i «dati» disponibili rispondano alle caratteristiche richieste dai "*data consumer*" autorizzati (qualità estrinseca). A loro volta, questi dovranno garantire il rispetto delle finalità per le quali i «dati» sono stati forniti e quello della norma di riferimento per le specifiche categorie di «dati» trattati.

Un approccio standardizzato e governato in tutto il comparto Difesa è assicurazione della qualità gestionale, alla base della proficua e tempestiva condivisione e valorizzazione dei «dati».

---

[89] La prima è definita da metriche relative alle dimensioni della qualità mentre la seconda dipende dalla conformità dei «dati» alle aspettative delle esigenze decisionali del contesto.

[90] Come si vedrà nel prosieguo, in conformità al paradigma "*zero trust*".

ABILITANTI PER LA VALORIZZAZIONE DEL «DATO»

I seguenti elementi sono fondamentali per un'efficace gestione dei «dati» e sono principi e standard neutri dal punto di vista sia tecnologico sia della classifica del «dato».

Tecnologia

La tecnologia di riferimento rappresenta gli standard, i principi di progettazione, i modelli e le raccomandazioni tecnologiche per garantire la conformità alla Strategia.

In particolare, si promuove un approccio distribuito, decentralizzato e federabile, orientato al *cloud computing* e all'automazione, pur nel rispetto dei principi di sicurezza e sovranità dei «dati». Una tale architettura migliorerà la resilienza e favorirà l'integrazione delle capacità, consentendo la scalabilità necessaria al soddisfacimento delle crescenti esigenze di «dati» della Difesa e continuando a facilitare il *data exploitation* e l'interoperabilità.

Qualunque sia l'architettura, *on-prem*, *cloud* o *edge,* è necessaria l'implementazione di applicazioni basate su architetture aperte, facilmente gestibili all'interno di contesti *cloud* ibridi e *multicloud* (migrazione "one click"), così da evitare i *lock-in* ed essere agili nell'adattamento rispetto a ogni scenario operativo.

Dovrà favorirsi l'introduzione di standardizzazioni delle tecnologie commerciali esistenti, mantenendo comunque la libertà di scelta e di azione, affidandosi sempre più a tecnologie aperte e affermate come *standard* riconosciuti quali microservizi e la c.d. containerizzazione, tali da consentire agile sviluppo e facile rilocazione all'interno delle moderne info-strutture.

Nel contesto tecnologico, risulta fondamentale la creazione di una *data platform* ossia di uno strumento tecnologico tale da consentire l'esercizio automatizzato del *data management* secondo il modello di *data governance* individuato dalla Difesa.

Un'appropriata *data platform* è un abilitatore strategico, perché:
- rende i «dati» un *asset* condiviso e riutilizzabile invece di lasciarli isolati nei silos applicativi;
- permette di creare servizi digitali più intelligenti (ad esempio applicazioni predittive, automazione, personalizzazione);
- supporta una cultura *data-driven*: le decisioni si basano su evidenze quantitative;
- favorisce scalabilità e agilità, grazie a *cloud* e tecnologie moderne (*data lakehouse* moderni, streaming)[91].

In generale, si dovrà perseguire un equilibrio efficace e soprattutto sostenibile tra soluzioni proprietarie e in outsourcing, comprendendo le esigenze di alta capacità computazionale.

Standardizzazione nazionale e NATO/UE

La standardizzazione nazionale e internazionale consente di gestire e non subire i progressi tecnologici, i mutevoli scenari e i requisiti in continua evoluzione per le attività sui «dati», migliorando interoperabilità e sicurezza.

Talento e cultura

[91] Esempi pratici di *data platform*: Azure Data Platform (Microsoft), Google Cloud BigQuery + Dataflow, AWS Data Lake + Redshift + Glue, soluzioni open source come Apache Hadoop + Spark. In ambito aziendale: piattaforme interne custom integrate con CRM, ERP, IoT

La Difesa deve volgere un'attenzione particolare alla formazione, per disporre di una forza lavoro competente nella gestione e nell'utilizzo dei «dati» con una solida mentalità multidisciplinare e di ottimizzazione dei processi. Ciò al fine di dotare il personale della Difesa delle competenze necessarie per sfruttare con efficacia i «dati» nei rispettivi ruoli.

Per quanto afferente alla crescita del talento e della cultura sarà necessario favorire una formazione inter-dicasteriale e inter-agenzia tale da standardizzare la gestione dei «dati», tramite corsi erogati col supporto del mondo accademico e di esperti del settore industriale. I programmi di formazione e i syllabus dovranno ispirarsi alle linee di indirizzo indicate nella presente Strategia.

In modo esemplificativo e non esaustivo, per l'implementazione dei fattori abilitanti, questa Strategia raccomanda:

- il rafforzamento del partenariato pubblico-privato ovvero relazioni strutturate con industria, mondo accademico e centri di ricerca, a fronte delle complesse dinamiche connesse al reclutamento militare ma anche delle peculiarità dell'innovazione tecnologica, per cui nessuna organizzazione può considerarsi autonoma. Per la crescita di talento e cultura sarà in particolare necessario favorire una formazione interforze, inter-dicasteriale e inter-agenzia, tale da standardizzare la gestione dei «dati», con corsi erogati dal mondo accademico e da esperti del settore industriale, in conformità alle linee di indirizzo indicate nella Strategia;
- la promozione della consapevolezza e il monitoraggio dello stato dell'Organizzazione;
- la condivisione, la capitalizzazione delle informazioni in modo da fornire a tutti i livelli dell'Organizzazione le informazioni necessarie allo svolgimento delle proprie mansioni, armonizzando le lavorazioni caratterizzanti le diverse attività operative;
- l'adozione di strumenti all'avanguardia per prendere decisioni oggettive basate sui «dati» e non sulle percezioni dei singoli o esperienze del passato;
- contromisure di sicurezza appropriate rispetto alla classe d'informazione trattata, scongiurando iniziative sproporzionate e non oggettivamente rispondenti ai principi del «dato» come in atto nel dominio "non-classificato";
- l'aderenza alle normative di categoria sia nazionali sia internazionali (GDPR, STANAG NATO, etc.) e in particolare, la conservazione dei «dati» nel rispetto delle normative NATO o EU;
- il costante confronto con le autorità civili nazionali responsabili nel settore della gestione e della cultura del «dato», anche in riferimento alle normative europee di settore.

STRUMENTI DI DATA-ANALYTICS

Per sostanziare l'approccio decisionale basato sui «dati», questa Strategia sottende la necessità di:

- elaborare *policy* per implementare soluzioni di *data- analytics* e per l'uso incrementale e strutturato dell'IA, in accordo alla relativa dedicata "Strategia" della Difesa;
- abbattere le barriere info-strutturali ostacolanti l'uso dei «dati», con focus specifico al carattere *user friendly* degli applicativi di trattazione del dato "non-classificato" e con visione prospettica, anche di quello "classificato". In sostanza, il «dato» deve essere accessibile a chi lo deve impiegare e solo ciò consente un'appropriata continuità operativa anche e soprattutto nel lavoro quotidiano. Infatti, un «dato» gestito in maniera sproporzionata rispetto alla sua classifica, travisando il principio di sicurezza e distorcendo

la tecnologia a fronte dell'esigenza operativa, non potrà mai fornire il suo ottimale contributo informativo (mancato *need to share*);
- capitalizzare le opportunità offerte dalla tecnologia *cloud-to-edge*, al fine di garantire il *data-exploitation* dove serve e con la massima agilità;
- verificare la coerenza tra la qualità e l'incremento della quantità dei «dati» disponibili per i servizi digitali, consentendo la pronta risposta alle esigenze operative della Difesa;
- garantire una scalabilità selettiva con info-strutture comprovate e abilitate all'uso dell'IA.

La Difesa necessita di funzionalità di analisi e *dashboard* avanzate per la più efficace *situational awareness* ai livelli strategico, operativo e tattico e in qualunque contesto (gestione risorse, logistica, operazioni, ecc.). Al contempo, tali funzionalità si devono caratterizzare per immediatezza di impiego, favorendo la citata connotazione *user-friendly*.

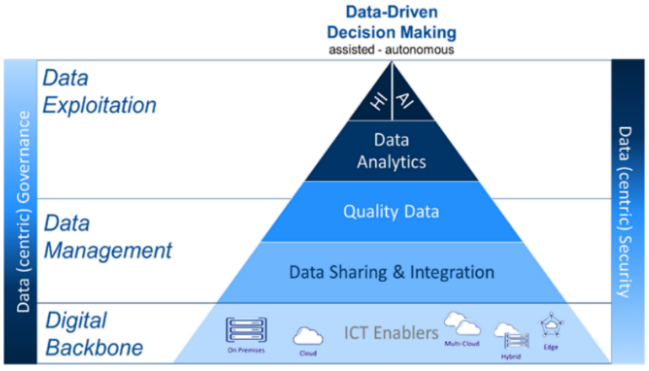
L'analisi avanzata mira a utilizzare il massimo dei «dati» disponibili e offre la capacità di misurare, visualizzare e anche prevedere i fattori alla base di una decisione. Con «dati» di qualità, i *data scientist* – sia militari sia civili – possono realizzare modelli di vantaggio significativo per esplorare le variabili e offrire al "decisore" quadri situazionali rispondenti alle esigenze in divenire.

Strumenti commerciali all'avanguardia sono già in grado di offrire tali capacità ed è necessaria una spinta per un progresso di integrazione condiviso. Un processo decisionale efficace richiede il collegamento tra i «dati», tool analitici per misurare i progressi e l'incremento della trasparenza nell'esecuzione.

Quindi, il percorso discendente dalla Strategia dovrà puntare sullo sfruttamento di *software* innovativi, convertendo il potenziale del «patrimonio informativo» in un vantaggio decisionale. Il risultato sarà l'approccio al *data-driven decision making* e la conseguente definizione di un ambiente favorevole all'approccio multi-dominio nonché la predisposizione al miglioramento continuo, attraverso la razionalizzazione e l'ottimizzazione delle risorse e dei processi.

SERVIZI DI INTELLIGENZA ARTIFICIALE

Per la Difesa, l'IA è uno strumento strategico per cui va seguito un percorso virtuoso, in accordo a specifiche direttive politico-militari, tali da indirizzare le implicazioni di natura etica, operativa, organizzativa e tecnica.



Ciò allo scopo di governare la peculiarità dell'attuale *momentum* digitale, in cui bisogna garantire il coerente uso degli strumenti dell'IA al suo interno, considerando anche le esperienze del personale al di fuori del perimetro professionale (qualsivoglia scostamento e disordine tra le azioni digitali condotte nella sfera personale e professionale è infatti foriero di *deficit* di rendimento e di potenziale nocumento alla sicurezza dell'«informazione»).

Il potenziale dell'IA è enorme e comunque subordinato alla qualità del «dato», precondizione per essere sicura, affidabile e responsabile. L'IA è da considerarsi imprescindibile in tutti i

settori della Difesa[92] ed è questo il motivo per cui è stata elaborata una specifica Strategia per l'IA, cui si rimanda per gli aspetti di dettaglio.

In questa sede, si coglie l'occasione per richiamare come lo sviluppo dell'IA sottenda le seguenti considerazioni.

Acquisizione di conoscenza su una scala e a una velocità senza precedenti

Gli algoritmi di IA possono elaborare grandi quantità di «dati», analizzare modelli e ricavare informazioni, superando le capacità umane. Tuttavia, all'incremento delle conoscenze corrisponde la crescente difficoltà nel gestire queste informazioni in modo efficace. L'enorme volume e la complessità della conoscenza generata dall'IA richiedono sviluppo di solidi *framework* per la verifica, la convalida e l'interpretazione dei modelli.

Complessità dei processi decisionali basati sull'IA

I sistemi di IA diventano sempre più sofisticati, impiegano algoritmi complessi tali da produrre risultati accurati ma potrebbero non fornire motivazioni spiegabili o interpretabili. In alcuni casi, l'IApuò produrre risultati corretti senza poter comprendere appieno come sia arrivata a tali conclusioni. Questa complessità in ambiti critici in cui la trasparenza e la responsabilità sono essenziali solleva preoccupazioni su implicazioni etiche e potenziali conseguenze indesiderate. Ciò presuppone una continua considerazione nel ricercare l'equilibrio tra accuratezza e complessità dei sistemi di IA.

Tendenza ad affidarsi sempre più a sistemi di IA

Poiché gli algoritmi di IA dimostrano crescenti prestazioni e precisione, è ineludibile la tendenza a fare sempre più affidamento sulle loro decisioni. I sistemi di IA possono commettere errori e soprattutto, incontrare scenari al di fuori dei «dati» di addestramento. La sfida sta nel discernere quando l'IA è autorevole e quando dovrebbe prevalere il giudizio umano. È necessario comprendere i limiti dei sistemi di IA, progettare controlli ed equilibri adeguati e stabilire confini chiari per la supervisione e l'intervento umano. Trovare il giusto equilibrio tra giudizio umano e autorità dell'IA è fondamentale per garantire un processo decisionale responsabile.

Capacità di completa autonomia

I sistemi autonomi si riferiscono a macchine o armi alimentate dall'IA in grado di identificare e ingaggiare obiettivi in modo indipendente senza il controllo umano diretto. Lo sviluppo di tali sistemi solleva questioni etiche e legali, poiché foriere di gravi conseguenze. Specifiche politiche e regolamenti dovranno essere finalizzati alla garanzia di aderenza dei sistemi completamente autonomi ai principi etici e ai principi di proporzionalità e distinzione. In particolare, la Difesa è chiamata a rafforzare la sua comprensione del panorama delle soluzioni nonché della maturità e della sicurezza dei servizi di IA, così come dettagliato nella Strategia per l'IA.

a. Sviluppo di applicazioni di IA

Qualunque sia lo sviluppo di nuove applicazioni di IA o l'adattamento di modelli di IA esistenti, lo sfruttamento dei «dati» da loro sviluppati dovrà essere conforme ai principi di uso responsabile per l'IA nella Difesa: *lawfulness, responsibility and accountability,*

[92] Si pensi alle possibili applicazioni a bordo dei mezzi militari nonché nei contesti organizzativi, formativi e logistici.

explainability and traceability, reliability, governability, and bias mitigation [93]. Il mancato rispetto di questi principi potrebbe compromettere l'affidabilità delle applicazioni di IA.

Attese le implicazioni accennate per l'uso dell'IA, lo sviluppo e l'impiego degli algoritmi dovrà comunque essere efficace, sicuro, responsabile e sostenibile. Per lo sviluppo dovranno essere favoriti modelli e algoritmi commerciali aperti in modo da permettere di verificare se la gestione dell'IA sia stata eseguita in modo etico e sicuro nel rispetto dei citati principi di uso responsabile e in assenza di eventuali *bias* AI e allucinazioni note.

Per qualunque modello applicato fin dalla sua istruzione con dati della Difesa e in seguito all'apprendimento come modello istruito, l'impiego del modello di IA dovrà diventare di accesso e uso esclusivo della Difesa.

b. Test, valutazione, verifica e validazione delle applicazioni di IA

A seguito dello sviluppo, dovranno essere messi in atto strumenti e modelli per il *Test, Evaluation, Verification and Validation* (TEV&V) degli algoritmi di IA, così come indicato nella Strategia per l'IA, al fine di certificare le soluzioni IA rispetto a specifici criteri[94].

Altresì, si potranno ricercare sinergie con l'Agenzia per l'Italia digitale, anche per il continuo confronto con le standardizzazioni in corso di definizione per l'uso civile, UNI/CT 533 IA, WD *Risk Management System* (RMS), WD AI *Quality Management System* (QMS) AI, in particolare nel caso di sviluppo e dispiegamento di applicazioni duali.

FASI LOGICHE DEL GOVERNO E GESTIONE DEL «DATO»

a. Individuazione del perimetro di applicazione

Per conseguire l'efficace valorizzazione del «dato» con un coerente impiego di risorse, le funzioni di governo e gestione vanno centrate sui processi *core* della Difesa, che sono:

- **elaborazione *policy* e sviluppo capacitivo** in chiave DOTLMPFI-SPE[95] (compito attestato al livello politico-militare e Stato Maggiore della Difesa);

[93] NATO *Artificial Intelligence Strategy*, 2025. ISO 42001.

[94] Elenco non esaustivo: robustezza degli algoritmi; resilienza agli attacchi avversari; capacità degli esseri umani di comprendere e fidarsi dei risultati del modello (i.e. allucinazioni bias IA); competenza necessaria alla comprensione dei risultati; la conformità ai sei principi di uso responsabile per l'IA.

[95] L'acronimo DOTLMPFI è utilizzato in ambito NATO e difesa nazionale per descrivere l'insieme dei processi e delle aree funzionali da considerare nello sviluppo capacitivo. Esso identifica le otto dimensioni (o "levers") che devono essere affrontate in modo integrato affinché una capacità sia effettivamente realizzata e sostenibile nel tempo: D – *Doctrine*: dottrina, concetti operativi e principi di impiego; O – *Organization*: strutture organizzative necessarie; T – *Training*: addestramento, esercitazioni e programmi formativi; L – *Leadership*: comando, leadership, processi decisionali e responsabilità; M – *Materiel*: equipaggiamenti, infrastrutture e sistemi tecnici; P – *Personnel*: personale in termini di quantità, qualità e specializzazione; F – *Facilities*: installazioni, basi, poligoni, centri di supporto; I – *Interoperability*: standard, procedure e soluzioni per garantire la piena interoperabilità. Recentemente, all'acronimo DOTLMPFI sono stati aggiunti ulteriori tre elementi (S, P, E) che riflettono l'evoluzione dei processi di sviluppo capacitivo e l'allineamento agli standard NATO più recenti: S – *Sustainability*: la sostenibilità complessiva della capacità lungo il ciclo di vita, comprensiva di logistica integrata, manutenzione, catene di fornitura e gestione dei costi operativi; P – *Policy*: il quadro politico-strategico e normativo di riferimento (nazionale, NATO, UE) che indirizza l'adozione e l'impiego della capacità; E – *Economics*: la dimensione economico-finanziaria, con analisi dei costi/benefici,

- ***procurement*** secondo il "codice degli appalti" (compito attestato alla Direzione Nazionale degli Armamenti)
- **pianificazione operativa e impiego delle Forze** (compito attestato al Comando Operativo di Vertice Interforze);
- **organizzazione e approntamento delle Componenti** dello Strumento (compito attestato agli Stati Maggiori di Forza Armata).

Dall'analisi dei processi di *core business* e dalle relazioni interagenti tra loro, si individuano le informazioni trattate e i «dati» usati nelle varie fasi dei processi e sotto processi e chi sia autorizzato a produrre, modificare o solo impiegare un certo «dato», senza poterne alterare l'informazione.

L'identificazione dei processi e di chi li possa trattare comporta la necessità di definire i ruoli abilitati ad accedere all'informazione e il mascheramento dell'informazione verso coloro abilitati a utilizzare i «dati» senza dover necessariamente conoscerne il contenuto, secondo il principio *need to know* e *need to share*.

Tali azioni sono funzionali alla corretta definizione degli standard per l'implementazione della *data platform* e in particolare, delle sue basi dati (quali ad esempio i *data lakehouse*).

b. Individuazione delle informazioni

Le informazioni forniscono la visione della realtà relativa a un determinato contesto, derivando dall'elaborazione di un insieme di «dati». Esse sono necessarie per prendere decisioni consapevoli e favorire la collaborazione tra le parti coinvolte in un processo, con lo scopo di raggiungere gli obiettivi di ogni singola fase in tempi congrui e col miglior rendimento.

A valle dell'identificazione delle aree e dei processi di *core business* è indispensabile individuare le relative «informazioni», quali siano i «dati» costituenti e quali siano le fonti autoritative in grado di fornirli [condizione 1 "accuratezza", condizione 5 "completezza"].

c. Identificazione di "attori e ruoli"

L'identificazione degli attori e dei ruoli nei processi essenziali dell'Organizzazione consente di individuare gli *owner* di quei processi e quindi dei «dati» oltre a fornire chiare indicazioni di chi può fare cosa. Tale informazione è fondamentale per l'implementazione del *need to know* e del *need to share*, attraverso la configurazione dei diritti di accesso e i permessi di lettura, scrittura ed esecuzione dei «dati» [condizione 9 "protezione"].

d. Ristrutturazione e integrazione dei processi

La ristrutturazione e l'integrazione dei processi favorisce la trasformazione digitale ed è fondamentale per l'implementazione dell'approccio multi-dominio, l'automazione delle lavorazioni e il miglioramento dei tempi di risposta lungo tutte le fasi di processo.

e. Classificazione delle «informazioni»

disponibilità di risorse e modelli di finanziamento per assicurare la fattibilità e l'efficienza della capacità. In questo modo, DOTLMPFI + SPE costituisce oggi una matrice più ampia e aggiornata di riferimento per la pianificazione e lo sviluppo capacitivo: non solo centrata su dottrina, organizzazione, personale ed equipaggiamenti, ma anche sulle condizioni di sostenibilità, la cornice politico-strategica e gli aspetti economici indispensabili per l'effettiva realizzazione e perdurante efficacia delle capacità militari.

In accordo alla ISO 27001[96], le informazioni prodotte, modificate e utilizzate per il completamento delle attività devono essere associate a una classe d'informazione. In questo modo, potranno essere disponibili, protette, mascherate, crittografate, preservate, conservate ed eliminate in modo sistematico nonché secondo quanto stabilito dalle norme di legge o dalle necessità dall'Organizzazione.

Il patrimonio informativo della Difesa è in possesso di consolidate e condivise modalità di classificazione militare; nella fattispecie:

- Dominio "classificato": sono le informazioni cui sia stata attribuita una delle classifiche/qualifiche di segretezza previste dalla legge 124/2007[97] e quindi, assoggettate alle relative normative sia nazionali sia delle organizzazioni internazionali di appartenenza (NATO e UE). Trovano corrispondenza con la categorizzazione di «dato» "critico" e "strategico", così come indicato nella "Strategia *cloud* nazionale".
- Dominio "non-classificato" sono le informazioni sprovviste di classica/qualifica di segretezza poiché la loro eventuale diffusione/violazione/compromissione non comporta danno alla sicurezza dello Stato[98]. Non sono soggette alle misure di protezione speciali previste per le informazioni classificate, come il controllo degli accessi, l'autorizzazione NOS, l'accreditamento dei sistemi informativi. Trovano corrispondenza con la categorizzazione di «dato» "ordinario", così come indicato nella "Strategia *cloud* nazionale" [condizione 6 "conformità"].

La classificazione delle informazioni compete all'originatore, in funzione del potenziale "*danno all'integrità della Repubblica, anche in relazione ad accordi internazionali*". Quindi, la valutazione dei rischi in caso di violazione e/o compromissione è funzionale per la definizione delle modalità di protezione dei «dati» e in particolare, per le politiche di accesso alle «informazioni», la gestione delle identità, i tempi e i modi di conservazione, i requisiti info-strutturali e la politica di continuità operativa [condizione 6 "conformità", 9 "protezione"].

Per inciso, ai fini della definizione delle citate modalità, questa Strategia sottende la necessità di riferirsi a un'analisi del rischio a norma di legge – quale è il "segreto di Stato" – per l'attuazione di contromisure e monitoraggi puntuali verso i punti di esposizione derivati da rischi mitigabili e comunque da confrontarsi sempre con l'effettiva esigenza operativa e la coerenza in termini di risorse assegnate e sostenibilità.

f. Identificazione delle "fonti autoritative"

L'identificazione delle fonti autoritative e dei flussi dei «dati» [condizione 13 "tracciabilità" e condizione 11 "sovranità"] oltre a rispondere ai requisiti richiesti per esempio dal GDPR, garantiscono per il «dato»:
- accessibilità
- integrità
- standardizzazione

[96] Standard internazionale dei requisiti per un sistema di gestione della sicurezza delle informazioni (*Information Security Management System* – ISMS). L'obiettivo principale della ISO 27001 è garantire che un'organizzazione possa identificare, gestire e ridurre i rischi associati alla sicurezza delle informazioni, proteggendo così la confidenzialità, l'integrità e la disponibilità dei dati.

[97] Art. 42, comma 3.

[98] PCM-ANS 1/2006 Disposizioni in materia di tutela e gestione dei documenti classificati.

- protezione
- monitoraggio accurato
- razionalizzazione delle fonti
- conservazione

Questo passo [condizione 2 "aggiornamento", condizione 4 "compatibilità tra sistemi", condizione 5 "completezza", condizione 7 "conservazione", condizione 9 "protezione", condizione 12 "standardizzazione", condizione 16 "efficienza energetica e sostenibilità"] è la base per costruire processi trasversali e collaborativi, tali da arricchire e aggiornare l'«informazione», in maniera continua. Infatti, con tale approccio ogni "lavorazione", si sviluppa, capitalizzando il valore del «dato» disponibile nell'ecosistema anziché ricreare – come ora accade – «informazione» *ex novo*. L'identificazione delle fonti autoritative è essenziale per la valorizzazione del patrimonio informativo e l'ottimizzazione dei tempi di risposta del comparto Difesa, instaurando una comunicazione virtuosa e sinergica tra le Forze Armate, alla base dell'approccio multi-dominio.

In sostanza, i «dati» creati dai processi "produttori", diventano servizi messi in "consultazione" di altri processi durante le fasi di lavorazione per produrre la porzione di informazione di cui a loro volta sono identificati proprietari.

Ciò garantisce vantaggi in termini di operatività e di sicurezza, eliminando le duplicazioni e indirizzando le risorse verso le componenti info-strutturali utili ad assicurare la continuità della "missione" e gli algoritmi di IA a supporto delle attività analitiche e predittive [condizione 1 "accuratezza", condizione 3 "analisi", condizione 10 "rilevanza"].

Le architetture applicative in *cloud* e a microservizi permettono di implementare tale approccio in sicurezza nonché a pieno vantaggio della continuità operativa e dell'approccio multi-dominio, incrementando altresì il grado di resilienza passiva dell'Organizzazione.

g. Definizione dell'identità digitale

La definizione di un'identità digitale unica della Difesa da implementare attraverso un sistema di *Identity, Credential e Access Management* (ICAM)[99] e *single sign-on* di tipo *cloud native* è basilare per agevolare la cooperazione delle articolazioni coinvolte nei processi di lavorazione/approvazione e nell'utilizzo di strumenti comuni, atti a produrre «informazioni» e «dati» coerenti e risposte rapide. Inoltre, tale approccio garantisce una maggiore sicurezza delle informazioni in quanto ogni azione è svolta centralmente, in un unico punto di accesso, oltre a essere sempre tracciata e monitorata.

Al riguardo, si pensi ai vantaggi introdotti dallo SPID o dalla CIE, i quali, seppur limitatamente all'identificazione, consentono l'accesso a tanti portali della Pubblica Amministrazione attraverso un'unica identità digitale senza necessità di registrarsi o doversi ricordare numerose *ID* e *Password*. Ciò rappresenta – per il cittadino e nella fattispecie per l'operatore militare – un *game changer* della propria capacità di "lavorazione" ed è facilmente comprensibile il vantaggio garantito su larga scala, all'Organizzazione.

h. Identificazione dei servizi e della loro criticità

[99] Approccio strategico alla gestione delle identità digitali, delle credenziali e del controllo degli accessi in un ambiente digitale. Questo sistema garantisce che solo le persone o entità autorizzate possano accedere alle risorse necessarie, migliorando la sicurezza e l'efficienza.

Per un contesto organizzativo ottimizzato, integrato e interoperabile è indispensabile un piano di continuità operativa basato sull'effettiva "criticità" dei servizi. In tal senso, va definito – in via prioritaria – un catalogo dei servizi, per il censimento delle applicazioni a supporto dei processi – di *core* business e non – delle fonti autoritative e dei flussi di «informazione».

Infatti, un tale censimento porta a una razionalizzazione rilevante dei sistemi, a valle dell'ottimizzazione di processi e «dati», potendo individuare i servizi effettivamente critici, i livelli di servizio da garantire, le modalità di preservazione e i tempi di conservazione degli elementi essenziali per la continuità operativa dell'organizzazione.

i. Adeguamento normativo e di legge

Ove necessario, lo Stato Maggiore Difesa è chiamato a promuovere l'aggiornamento normativo, con modalità coerenti alle azioni previste per l'implementazione della Strategia. In particolare, andranno considerate con attenzione le esigenze connesse alla gestione del «dato» classificato.

j. Modernizzazione delle applicazioni e dei sistemi

La realizzazione di applicazioni in ottica *cloud native* e la modernizzazione dei processi di sviluppo del *software* è un passo da compiere con la fase di ottimizzazione dei processi, delle fonti autoritative e dei flussi di «dati».

Logica conseguenza della modernizzazione delle applicazioni è l'adozione di cicli di sviluppo basati su metodologia *DevSecOps* [100]. Detti cicli favoriscono sviluppi continui e incrementali, rilasci verificati dal punto di vista della sicurezza e installazioni rapide negli ambienti *target*.

Inoltre, la sicurezza delle «informazioni» deve essere garantita in tutte le fasi del ciclo di sviluppo, in special modo nelle fasi di test, di massima eseguite con il supporto di operatori esterni, dove per evitare di accedere ai «dati» sensibili per le verifiche funzionali ed evitare di conoscerne il contenuto reale, si dovranno attuare tecniche di mascheramento per i non autorizzati.

k. Mitigazione dei rischi

Mitigare i rischi di sicurezza, favorendo l'adozione delle citate architetture *zero trust*, in grado di tracciare chi ha avuto accesso e trattato quali «dati» e per quanto tempo (*auditing*).

Inoltre, lo Stato Maggiore Difesa dovrà formalizzare – nell'ambito delle pubblicazioni di competenza – i requisiti/procedure di sicurezza del *software*, tali da mitigare le minacce in essere o potenziali, in accordo alle metodologie e standard di riferimento.

l. Resilienza dei sistemi

Il livello di resilienza dei sistemi dipende dal "piano di continuità operativa", funzionale al contenimento dei tempi risposta e di ripristino degli ambienti in caso di eventi di sicurezza. Inoltre, detto piano deve prevedere lo sfruttamento di info-strutture *cloud* e/o interconnessioni satellitari da parte delle applicazioni, in caso di eventi avversi. Queste

[100] *DevSecOps* significa "Sviluppo, Sicurezza, Operazioni" ed è la pratica di integrazione dei *test* di sicurezza in ogni fase del processo di sviluppo del *software* ovvero l'estensione della metodologia *agile* alle attività, a valle della fase di sviluppo pura.

fattispecie vanno considerate in fase di progettazione insieme agli elementi utili alla realizzazione di sistemi e applicazioni aperte nonché predisposte all'integrazione di sistemi IT/OT/IOT, scalabili, portabili e quindi indipendenti dalle infrastrutture fisiche di supporto [condizione 8 "portabilità tra piattaforme"].

m. Responsabilità e figure organizzative

A complemento del "Modello per il governo e la gestione condivisa e interconnessa dei dati" nell'ambito del Ministero della difesa[101], si individuano le seguenti figure.

Chief Data Officer (CDO)

Il CDO è la figura responsabile della predisposizione e dell'applicazione delle regole, delle procedure e degli standard per il governo e la gestione dei «dati», sulla base delle disposizioni del RUD.

Il CDO si identifica con il Capo del VI Reparto dello Stato Maggiore della Difesa, già Responsabile per la Transizione Digitale (RTD) della Difesa[102].

Il CDO, in particolare:
- presiede il Comitato consultivo interforze per la gestione del «dato»;
- propone al RUD l'evoluzione della "Strategia Digitale" e del modello di *governance* e di *management*, in relazione agli eventuali mutamenti normativi, organizzativi o tecnologici;
- promuove la diffusione della cultura del dato e l'alfabetizzazione digitale nell'organizzazione;
- contribuisce nell'individuazione e nella condivisione con gli EdO competenti, di specifiche esigenze formative e/o addestrative per adeguare le professionalità in materia di gestione dei «dati».

Data Quality Control Manager (DQCM)

È il responsabile delle verifiche di attuazione delle direttive in materia di governo e gestione dei «dati». Il DQCM è identificato nel Vice Capo del VI Reparto dello Stato Maggiore della Difesa per l'area "valorizzazione del dato".

Il DQCM, in particolare:
- svolge azioni di audit semestrali in collaborazione con i *Chief Data Officer* di dominio (CDOd),
- monitora i livelli di qualità dei dati e di efficacia degli impianti di controllo attraverso i relativi KPI;
- supporta i dCDO nelle attività di gestione della qualità dei «dati»;
- presenta gli esiti dei citati audit nell'ambito delle riunioni del Comitato consultivo interforze per la gestione del dato, riportando altresì le eventuali proposte di miglioramento.

Chief Data Officer di dominio (dCDO)

Il *Chief Data Officer* di dominio (dCDO) è la figura di riferimento delegata per l'implementazione delle direttive centrali di governo e di gestione dei «dati», coordinando

[101] Modello che sarà approvato con dedicato Decreto Ministeriale.
[102] Decr. Min. Dif. 18 settembre 2020 «Individuazione, compiti e funzioni del RTD del Dicastero della difesa».

e assicurando l'attuazione delle attività di *data exploitation* all'interno della propria organizzazione.

I dCDO, nell'ambito dei rispettivi Domini Dati:
- assicurano il rispetto degli standard di data governance e *data management* ed eseguono i controlli interni di verifica e misurazione dei KPI interni, riportando i risultati al DQCM durante i citati *audit*;
- promuovono la qualità dei dati e l'efficacia degli impianti di controllo all'interno dei propri domini dati;
- collaborano con il DQCM nelle attività di verifica e *audit* e per la produzione dei relativi KPI
- supportano i *Data Manager* nella gestione dei *data product*;
- supportano le attività di formazione e *literacy* nel proprio dominio dati.

I CDO di dominio hanno dipendenza organica dai Responsabili di Dominio dati e funzionale dal DQCM.

Data Manager

Il *Data Manager* è la figura a supporto di ogni dCDO, responsabile della gestione del ciclo di vita di uno specifico insieme di dati.

Il *Data Manager*:
- cura l'aggiornamento dei contenuti informativi e degli elementi descrittivi dei «dati»;
- supervisiona e prende decisioni relative alla creazione, conservazione, condivisione ed eliminazione dei «dati», in accordo alle direttive del dCDO;
- è responsabile della conformità dei «dati» alle normative applicabili per categoria;
- assicura la qualità e l'integrità dei dati di propria competenza;
- coordina con i *Data Steward* e i *Data Custodian* la gestione operativa dei «dati»;
- supporta il dCDO nelle attività di verifica/audit e nella misurazione dei relativi KPI.

Data Steward

Il *Data Steward* è la figura a supporto di ogni dCDO – esperta nella gestione dei «dati» a livello operativo – incaricata di curare l'implementazione delle politiche di *data management*.

Il *Data Steward*:
- applica le regole di gestione dei dati e garantisce la qualità e l'integrità dei «dati» a livello operativo;
- monitora la conformità dei «dati» alle normative e collabora con altri team per risolvere problemi relativi ai «dati»;
- definisce e mantiene i metadati associati ai «dati» di competenza;
- supporta il dCDO nelle attività di verifica/audit e nella misurazione dei relativi KPI.

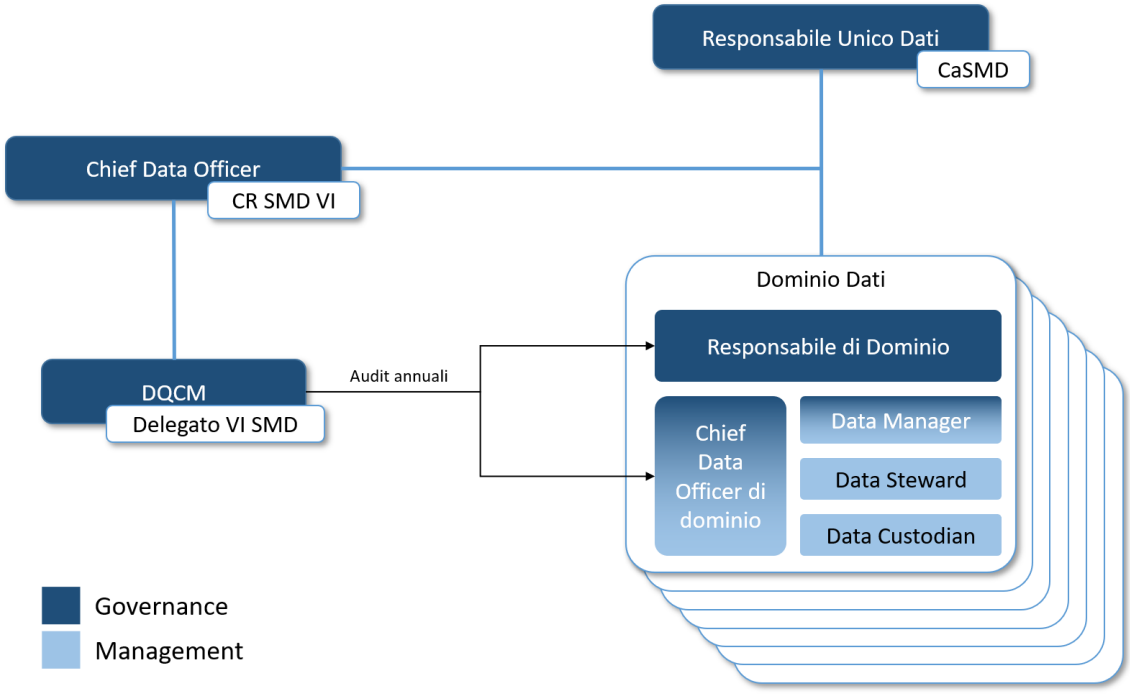
Data Custodian.

Il *Data Custodian* è la figura a supporto di ogni dCDO, responsabile della gestione tecnica dei «dati», custodendoli e garantendone la sicurezza, l'integrità e la disponibilità.

Il *Data Custodian*:
- assicura la manutenzione e l'aggiornamento dei sistemi di archiviazione e gestione dei «dati»;

- implementa e monitora le misure di sicurezza per proteggere i «dati» e gestisce i permessi di accesso ai «dati»;
- esegue il *backup*, la *recovery* e la conservazione dei «dati»;
- collabora con i *Data Manager* e i *Data Steward* per garantire la disponibilità dei «dati».
- supporta il dCDO nelle attività di verifica/audit e nella misurazione dei relativi KPI.

I CDO di dominio, i *Data Owner*, i *Data Steward* e i *Data Custodian* sono nominati dagli RDD di dominio.



Struttura di Governance

n. Formazione

La valorizzazione del «dato» richiede un cambiamento culturale all'interno della Difesa e dev'essere supportato da competenze e professionalità.

In particolare, l'efficace implementazione della Strategia necessita del coinvolgimento di tutto il personale, il quale deve essere formato per il pieno soddisfacimento delle esigenze connesse al nuovo "campo di battaglia", in accordo a quanto indicato per le azioni sottese alla condizione 15 "formazione".

ALLEGATO E - *Key Performance Indicator*

Per misurare qualità, *performance* e sicurezza delle successive fasi del processo di implementazione, si riportano di seguito degli esempi non esaustivi di indicatori da considerare per ciascun pilastro.

VALORIZZAZIONE DEL DATO

I KPI dovranno essere applicati per misurare i seguenti parametri: *data readiness* [103], *data-driven culture* [104], *governance & controls* [105], *data foundations* [106], *data exploitation* [107].

Livello di maturità nella valorizzazione del «dato», secondo il citato *Data Exploitation Maturity Model*.

Livello di qualità dei «dati», misurato in base al tasso di errori e incongruenze corrette e alla tempestività di aggiornamento dei «dati» in accordo alle prescrizioni stabilite in via procedurale

Stato di costituzione dell'organizzazione di *Data Governance*, misurato attraverso l'attivazione dei ruoli chiave, la definizione dei processi di responsabilità sul ciclo di vita del «dato» e l'adozione di modelli di governo conformi agli standard NATO/UE.

Numero delle basi «dati» integrate nel sistema di *data management.*

Tasso di adozione dei modelli analitici predittivi nei processi decisionali, operativi e logistici.

Riduzione dei silos informativi tramite condivisione e riutilizzo dei «dati» tra Forze Armate e organismi della Difesa.

Grado di *cloud readiness* delle applicazioni per la valorizzazione del «dato», misurato come percentuale di applicazioni con livello di maturità 1, 2 o 3 rispetto al modello *cloud-native*[108] e capaci di supportare il riposizionamento flessibile dei «dati» in ambienti *cloud*, *edge* o multi-*cloud*, in funzione di scenari operativi o geopolitici variabili.

Percentuale di adozione di tecnologie *cloud,* distinto tra «dati» non-classificati/bassa classifica (cloud qualificato) e ad alta classifica (cloud sovrano-disconnesso), rappresenta il grado di transizione architetturale verso modelli più agili, scalabili e sostenibili.

Numero di operatori formati su strumenti di *data management* e cultura "*data-driven*".

---

[103] Capacità di raccogliere, preparare e rendere i «dati» disponibili, accessibili, corretti, aggiornati e pronti a essere sfruttati nei processi decisionali, operativi o di analisi

[104] Promozione di una mentalità consapevole e valorizzante la centralità del «dato».

[105] L'implementazione di politiche e processi per garantire la qualità e la sicurezza dei «dati».

[106] La struttura di base, le tecnologie, i processi e le strategie che un'organizzazione implementa per raccogliere, gestire, archiviare, organizzare e utilizzare i propri dati in modo efficace, riferite nello specifico relative alle info-strutture appropriate per gestire grandi quantità di «dati».

[107] L'abilità di utilizzare i «dati» per ottenere vantaggi, in termini operativi, organizzativi, informativi e decisionali.

[108] Un'applicazione *cloud native* implementa il "manifesto" di 12 fattori (https://12factor.net). Il rispetto di questi fattori la rendono idonea allo sfruttamento della tecnologia *cloud* anche indipendente, autoconsistente, in grado di sfruttare qualsiasi tipo di infrastruttura, altamente flessibile e scalabile.

CONNETTIVITÀ AVANZATA

Percentuale di copertura delle reti sicure e resilienti, ossia la misura dell'estensione delle reti Difesa (terrestri, aeree, satellitari) con requisiti di sicurezza, continuità operativa e resilienza, in ambito nazionale e nei teatri operativi.

Riduzione della latenza nelle comunicazioni operative, misurata in millisecondi nei contesti C5ISR e logistici, in condizioni standard e di crisi, per garantire reattività e coordinamento in tempo reale.

Numero di nodi integrati in architetture *software-defined*, indica il grado di transizione dalle reti *legacy* verso reti virtualizzate, scalabili e riconfigurabili, essenziali per operazioni multi-dominio e mobilità.

Grado di interoperabilità con le reti NATO/UE, valutato tramite test tecnici, esercitazioni e validazioni inter-alleate, rappresenta la capacità della Difesa di cooperare efficacemente nei contesti multinazionali e di corrispondere agli obbiettivi indicati dalle citate sei spirali FMN.

Disponibilità media dei servizi di connettività critica, misurata in termini di *uptime* (%), esprime l'affidabilità delle info-strutture a supporto delle missioni, anche in ambienti degradati.

Percentuale di dismissione o riconversione di reti *legacy*, ossia la misura dell'avanzamento nel processo di razionalizzazione infrastrutturale, attraverso l'eliminazione o modernizzazione di sistemi obsoleti a favore di architetture federate e sicure.

CYBER

Incremento della sicurezza e della resilienza nel dominio cibernetico, nella dimensione cognitiva e nello spettro elettromagnetico

Grado di adozione del modello *Zero Trust*
Valutato sulla base della copertura applicativa e infrastrutturale, esprimerà il livello di maturità dell'implementazione del modello su reti sia interforze sia delle Forze Armate.

Percentuale di sistemi aggiornati
Percentuale di *asset* rilevati da strumenti di *discovery* e tempo medio necessario per applicare un aggiornamento correttivo

Grado di condivisione della consapevolezza situazionale cyber interno allo Strumento militare
Automazione nella condivisione situazionale del dominio interno allo Strumento militare, ivi compreso per la c.d. *Cyber Threat Intelligence*

Numero di eventi cyber gestiti
Indicatore quantitativo della capacità di gestione eventi cibernetici e di avvio efficace del ciclo di lezioni apprese al temine

Livello di *cyber awareness* del personale
Indicatore sul livello di consapevolezza acquisito dal personale in materia di rischio *cyber* e impiego sicuro degli *asset* digitali

Capacità di svolgere operazioni *full-spectrum*, sin dal tempo di pace

Numero di esercitazioni *cyber* condotte annualmente

Indicatore su numero di es. da svolgere in ambito nazionale e NATO/UE, per: testare le procedure di risposta a incidenti interni allo Strumento militare; agire quale "Autorità nazionale per la gestione di crisi cibernetiche" su vasta scala; sincronizzare gli effetti di componente nell'approccio MDO

Livello di forze @*readiness* per la funzione e i compiti assegnati allo Strumento militare

Disponibilità di personale da impiegare @*readiness* per i piani militari e i compiti assegnati allo Strumento militare

Livello di *Capability Target* dell'Alleanza raggiunti

Grado di raggiungimento degli obiettivi capacitivi qualitativi e quantitativi individuati in ambito Alleanza.

Coerenza quantitativa e qualitativa degli organici

Percentuale di personale assegnato e qualificato in ruoli cyber critici

Consistenza e professionalizzazione del personale impiegato a supporto delle funzioni specialistiche di dominio cyber, rispetto al fabbisogno dichiarato.

Consolidamento della cooperazione internazionale e della CCB.

Livello di cooperazione cyber con paesi partner internazionali.

Numero di esercitazioni e attività formative congiunte effettuati presso i Paesi *partner*, attraverso *Mobile training team*, e a distanza (es. formazione *online*).

ALLEGATO F - Fattori di rischio

1. Carenze qualitative e quantitative di risorse umane con competenze digitali avanzate

   Il divario tra le esigenze strategiche della trasformazione digitale e le effettive capacità interne, sia tecniche sia gestionali, può compromettere l'attuazione di soluzioni digitali complesse, rallentando l'adozione di tecnologie abilitanti, la protezione del «dato» e lo sviluppo di architetture resilienti.

2. Resistenza al cambiamento culturale e organizzativo

   L'inerzia istituzionale e la limitata diffusione della cultura "*data-driven*" e "*cyber-aware*" possono ostacolare l'adozione di approcci innovativi. In particolare, la tendenza a mantenere silos informativi, a compartimentare i «dati» e a trascurare processi standardizzati compromette l'interoperabilità e la costruzione di un patrimonio informativo comune, essenziale per la transizione al paradigma data-centrico.

3. Frammentazione delle responsabilità e debolezza nel governo del «dato»

   L'assenza di un modello federato di *data governance* può determinare ridondanze, inconsistenze e scarsa *accountability* lungo l'intero ciclo di vita del «dato». La presenza di dati duplicati, obsoleti, non tracciati o non sottoposti a validazione automatizzata compromette la qualità dell'informazione e la capacità di generare analisi affidabili, alimentare modelli predittivi e supportare decisioni tempestive e sicure, con impatti sulla prontezza operativa.

   Tali rischi riguardano anche l'approccio a vincoli normativi, quali il GDPR.

4. Ritardi o mancate scelte strategiche sull'adozione della tecnologia *cloud*

   La mancata, parziale o ritardata implementazione del *cloud* computing – in ambito sia "non classificato" sia "classificato" – limita la valorizzazione del «dato», la scalabilità architetturale e l'efficienza gestionale.

   In un contesto segnato da carenze di personale tecnico, risorse materiali e capacità gestionali, il *cloud* costituisce uno strumento di razionalizzazione. Infatti, consente di dismettere *data centre* obsoleti e liberare risorse da reimpiegare in attività a maggior valore operativo, come la protezione e l'elaborazione dei «dati» classificati.

5. Obsolescenza delle info-strutture ICT e deficit di interoperabilità

   La persistenza di sistemi *legacy* e la lentezza nella transizione verso architetture *software-defined* riducono la flessibilità e la scalabilità delle reti operative. L'insufficiente armonizzazione con gli standard NATO/UE compromette la piena interoperabilità con reti alleate, ostacolando la cooperazione nelle operazioni congiunte, generando colli di bottiglia informativi e duplicazioni di capacità.

6. Insufficiente resilienza delle reti e dei sistemi connessi

   La mancata adozione di architetture *secure-by-design*, l'esposizione a minacce ibride e l'assenza di modelli *zero trust* aumentano la vulnerabilità a compromissioni critiche, pregiudicando la continuità operativa e la protezione del perimetro digitale.

7. Tempi lunghi e rigidità nei processi di *procurement*

Le attuali procedure di acquisizione possono risultare inadatte rispetto alla velocità dell'innovazione digitale, determinando ritardi nella disponibilità di capacità critiche e quindi, un disallineamento eccessivo tra le esigenze operative e il loro soddisfacimento.

8. Limitata sinergia inter-istituzionale e con il comparto industriale

La debole cooperazione tra le componenti militari, civili, industriali, accademiche e della ricerca può impedire la creazione di un efficace «ecosistema digitale» nazionale.

In particolare, un'eventuale inerzia inter-agenzia nei rapporti coi pilastri tecnico-operativi di cybersicurezza rischia di ridurre l'efficacia dello Strumento militare nell'ambito dello spazio cibernetico di interesse nazionale.

9. Bassa capacità di attrazione verso il "talento digitale"

L'elevata competitività del settore privato in termini di carriera, flessibilità e condizioni economiche ostacola l'attrazione e la fidelizzazione di giovani professionisti con elevate competenze digitali.

In assenza di percorsi dedicati, carriere specialistiche e ambienti tecnologicamente stimolanti, la transizione digitale rischia di rallentare per effetto di un *gap* generazionale non colmabile con la sola formazione interna.

10. *Vendor lock-in*

L'adozione di soluzioni proprietarie chiuse o scarsamente modulari può ridurre la capacità della Difesa di adattarsi in tempi congrui, a nuove esigenze operative o standard internazionali.

Ciò limita la flessibilità architetturale, aumenta i costi di transizione e vincola la libertà strategica nel medio-lungo periodo.

11. Mancata acquisizione di capacità di comunicazione satellitare multi-orbita e multi-provider

Il mancato sviluppo o impiego di soluzioni di comunicazione satellitare multi-orbita e multi provider (in particolare, in orbita bassa) limita fortemente la resilienza e la continuità operativa in scenari distribuiti, multi-dominio o privi di copertura terrestre affidabile.

In un contesto operativo sempre più dinamico e interconnesso, la disponibilità della capacità in parola, è essenziale per garantire latenza ridotta, larghezza di banda adeguata e ridondanza strategica nei sistemi di comando e controllo.

ALLEGATO G - Glossario

Artificial Intelligence (AI)

Tecniche e sistemi che consentono a macchine e *software* di svolgere compiti tipici dell'intelligenza umana (apprendimento, analisi, decisione).

Con specifico riferimento all'impiego degli strumenti di IA, si rimanda alla Strategia IA e Difesa.

Alliance Data Sharing Ecosystem (ADSE)

Meccanismo NATO per la condivisione sicura, protetta e interoperabile di «dati» e modelli AI/ML tra Alleati, NATO Enterprise e partner qualificati, basato su *governance* comune e federazione delle fonti.

Chief Data Officer (CDO)

Figura responsabile della strategia, qualità e valorizzazione del patrimonio informativo all'interno dell'organizzazione Difesa.

Chief Information Officer (CIO) – Capo del VI Reparto di SMD

Figura responsabile della strategia ICT e della modernizzazione digitale dell'organizzazione.

Cloud Computing (*Cloud* Sovrano/Qualificato /Pubblico)

Modello di servizio che consente l'accesso remoto a risorse informatiche, distinguendo tra ambienti ad accesso riservato, controllato/qualificato e commerciale.

Cloud Native

Architetture e applicazioni progettate per funzionare in ambienti *cloud* in modo nativo, con livelli di maturità crescenti (da 0 a 3).

Command & Control (C2)

Processi e sistemi attraverso cui i comandanti dirigono le forze militari e coordinano le operazioni.

Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR)

Infrastruttura integrata che unisce comando e controllo con capacità informative e tecnologiche.

Data-Centric Security

Modello di sicurezza che protegge direttamente i «dati», indipendentemente da dove si trovino, applicando controlli di accesso, cifratura e *policy* al «dato» stesso invece che solo alle reti o ai dispositivi.

Data Fabric

Architettura «dati» distribuita che consente di integrare, gestire e accedere in modo uniforme a informazioni provenienti da fonti eterogenee, garantendo interoperabilità, sicurezza e *governance* centralizzata.

Data Exploitation Maturity Model (DEMM)

Modello NATO per valutare il livello di maturità di un'organizzazione nella valorizzazione del dato, dalla raccolta alla generazione di valore informativo.

Data Governance

Insieme di regole, processi e responsabilità per garantire qualità, sicurezza, interoperabilità e uso strategico dei «dati» lungo tutto il loro ciclo di vita.

Data Management

Insieme di processi, metodologie e strumenti per la raccolta, organizzazione, protezione, qualità, archiviazione e utilizzo dei «dati» lungo tutto il loro ciclo di vita. In ambito Difesa, garantisce che i «dati» siano trattati come *asset* strategici, accessibili e affidabili, a supporto della superiorità informativa e delle decisioni multi-dominio.

Data Mesh

Modello decentralizzato di gestione dei dati, in cui ogni *Data Domain Owner* è responsabile del ciclo di vita dei propri dati, in coordinamento con un modello federato centrale.

Defence Innovation Accelerator for the North Atlantic (DIANA)

Iniziativa NATO che mette in rete acceleratori e centri di test per sperimentare tecnologie emergenti e dirompenti in ambito Difesa.

Digital Twin

Rappresentazione digitale di un sistema fisico o di un processo, che consente simulazioni, monitoraggio e ottimizzazione in tempo reale.

Digital Backbone (NATO)

Info-struttura digitale federata e sicura dell'Alleanza, concepita per garantire connettività universale, interoperabilità e accesso persistente ai «dati» e ai servizi ICT tra domini, nazioni e livelli decisionali. Integra reti, *cloud computing* e *data fabric*, con architettura orientata ai servizi, connettendo sensori, effettori e decisori per abilitare le Multi-Domain Operations e il processo decisionale *data-driven*.

European Defence Fund (EDF)

Fondo Europeo per la Difesa: strumento finanziario UE per sostenere progetti collaborativi di ricerca e sviluppo in ambito difesa.

EU *Defence Innovation Scheme* (EUDIS)

Schema europeo di innovazione per la difesa, complementare all'EDF, con focus su PMI e tecnologie disruptive.

Federated Mission Networking (FMN)

Iniziativa NATO per creare reti di missione federate, interoperabili e sicure, a supporto delle operazioni multinazionali.

Identity, Credential and Access Management (ICAM)

Sistema integrato per la gestione delle identità digitali, credenziali e autorizzazioni di accesso ai sistemi informativi.

Intelligence, Surveillance and Reconnaissance (ISR)

Funzione militare tale da integrare raccolta *intelligence*, sorveglianza continuativa e ricognizione mirata per fornire consapevolezza situazionale e supporto decisionale.

Low Earth Orbit (LEO)

Costellazioni satellitari in orbita bassa, utilizzate per garantire comunicazioni resilienti, a bassa latenza e ad alta disponibilità.

Machine Learning (ML)

Branca dell'IA tale da consentire ai sistemi di apprendere dai «dati» ed evolvere le proprie prestazioni senza essere esplicitamente programmati. Utilizza algoritmi statistici e modelli matematici per riconoscere pattern, effettuare previsioni o classificazioni, e supportare processi decisionali automatizzati.

Microservizi

Architettura applicativa la quale suddivide un sistema in piccoli servizi indipendenti, favorendo modularità e manutenzione agile.

Mean Time to Respond (MTTR)

Tempo medio necessario per rispondere a un incidente di sicurezza informatica, dalla rilevazione all'attuazione di misure di contenimento e recupero.

Multi-Domain Operations (MDO)

Concetto operativo il quale integra in modo sinergico azioni nei domini terra, mare, aria, spazio e cyber.

NATO *Innovation Fund* (NIF)

Fondo di investimento NATO a supporto di *start-up* e imprese tecnologiche con soluzioni *dual-use* strategiche per l'Alleanza.

Permanent Structured Cooperation (PESCO)

Cooperazione strutturata permanente tra Stati membri UE per sviluppare capacità comuni in ambito difesa.

Responsabile Unico dei «Dati» (RUD) – Capo di Stato Maggiore della Difesa

Figura prevista nella *governance* federata, responsabile della gestione operativa e della custodia dei «dati» per l'intero comparto Difesa.

Repository

Contenitore logico o fisico di dati, strutturati o non strutturati, gestiti secondo policy di accesso, sicurezza e conservazione. Può assumere forme diverse (*database*, archivi documentali, sistemi *cloud*, ecc.) ed è finalizzato a garantire disponibilità, integrità, reperibilità e condivisione dei dati lungo il loro ciclo di vita.

Data Warehouse

Repository centralizzato, ottimizzato per l'analisi e la reportistica, che conserva dati strutturati e storicizzati provenienti da più fonti, trasformati secondo logiche di qualità e coerenza (schema-*on-write*). Supporta funzioni di business intelligence, indicatori e *decision-making* su dati "puliti" e consolidati.

Data Lake

Repository scalabile che raccoglie dati eterogenei e grezzi (strutturati, semi-strutturati e non strutturati), conservandoli in forma nativa (schema-*on-read*). È organizzato per zone (*raw*/ *bronze*, *curated*/ *silver*, *trusted*/ *gold*) e abilitato da catalogo, metadati, controlli di qualità e sicurezza. Può alimentare sia data *warehouse* sia applicazioni di *advanced analytics*, IA e ML.

Semantica dei dati

Capacità di dare significato e contesto ai dati, mediante metadati, modelli concettuali, ontologie e vocabolari condivisi, per descrivere cosa rappresentano i dati, quali relazioni intrattengono, come vanno interpretati. Abilita interoperabilità, integrazione, *querying* e analisi più comprensibili e affidabili, riducendo ambiguità e aumentando precisione e trasparenza nello sfruttamento del patrimonio informativo.

Security Information and Event Management (SIEM)

Piattaforma per la raccolta, analisi e correlazione in tempo reale dei log e degli eventi di sicurezza generati da infrastrutture IT/OT.

Software Defined Networking (SDN)

Architettura di rete che separa il piano di controllo dal piano dati, permettendo una configurazione dinamica, automatica e centralizzata.

Time to Capability

Intervallo di tempo necessario tra l'avvio di un programma di sviluppo/acquisizione e la piena disponibilità operativa della capacità alle Forze Armate.

Zero Trust

Modello di sicurezza informatica che non assume alcuna fiducia a priori, richiedendo autenticazioni continue e controllo degli accessi basati sul contesto.

PAGINA NON SCRITTA

PAGINA NON SCRITTA

MINISTERO DELLA DIFESA