CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE
PROMOSSA DAL MINISTERO DELLA DIFESA

LINEAMENTI DIDATTICI

CORSO DI ALTA FORMAZIONE IN

"Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali"

A.A. 2025-2026

ATTO DISPOSITIVO

IL PRESIDENTE
CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE

VISTO il Decreto Legislativo datato 15 marzo 2010, n.66 "Codice dell'Ordinamento Militare";
VISTO il Decreto del Presidente della Repubblica datato 15 marzo 2010, n.90 "Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare";
VISTA La Direttiva SMD n. 109 "Tabelle Ordinative e Organiche del Centro Alti Studi per la Difesa ed 2021 -3^ variante e la Direttiva CASD 001 "Direttiva di funzionamento interno ed. 2021;
VISTA la Direttiva per la formazione interforze del personale SMD-FORM 001 ed. 2022 e la direttiva per la ricerca e la formazione della Difesa SMD-FORM 010 ed. 2022;
VISTO il DM 4 luglio 2024 n. 922 del Ministero dell'Università e della Ricerca che configura il CASD quale Scuola superiore universitaria ad ordinamento speciale di alta qualificazione e di ricerca nel campo delle scienze della difesa e della sicurezza.
VISTO il punto 3 dell'art. 2 della legge 240/2010 c.d. legge Gelmini, "Norme in materia di organizzazione delle università" che prevede che gli istituti di istruzione secondaria a ordinamento speciale adottano proprie modalità di organizzazione nel rispetto dei principi di semplificazione, efficienza, efficacia e trasparenza dell'attività amministrativa;
VISTO "Regolamento in materia di master universitari, corsi di alta formazione e corsi di formazione" del CASD/SSU;
VISTO l'approvazione della proposta di istituzione del Corso di Alta Formazione in *Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali* da parte del Comitato dei Direttori.

APPROVA

I Lineamenti didattici del Corso di Alta Formazione in "Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali" per l'Anno Accademico 2025 - 2026.

Roma, lì 22 SET. 2025

IL PRESIDENTE
(Gen. C.A. Stefano MANNINO)

ATTO DISPOSITIVO

IL PRESIDENTE
CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE

VISTO:	l'art. 1 del Decreto 4 luglio 2024 (G.U. n. 213 del 11.09.2024), che istituisce il Centro Alti Studi Difesa (CASD) quale Scuola Superiore Universitaria a Ordinamento Speciale (SSUOS) di alta qualificazione e di ricerca nel campo delle scienze della difesa e della sicurezza;
VISTO:	lo Statuto del Centro Alti Studi Difesa/Scuola Superiore Universitaria a Ordinamento Speciale (CASD/SSUOS);
VISTO:	il Regolamento Didattico Generale del CASD/SSUOS;
VISTO:	il Regolamento in materia di Master universitari, Corsi di Alta Formazione e Corsi di Formazione.

NOMINA

Il Col. Stefano PANONI quale Direttore del Corso di Alta Formazione in "Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali" per l'Anno Accademico 2025 - 2026.

Roma, lì 22 SET. 2025

IL PRESIDENTE

(Gen. C.A. Stefano MANNINO)

ATTO DISPOSITIVO

IL PRESIDENTE
CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE

VISTO:	l'art. 1 del Decreto 4 luglio 2024 (G.U. n. 213 del 11.09.2024), che istituisce il Centro Alti Studi Difesa (CASD) quale Scuola Superiore Universitaria a Ordinamento Speciale (SSUOS) di alta qualificazione e di ricerca nel campo delle scienze della difesa e della sicurezza;
VISTO:	lo Statuto del Centro Alti Studi Difesa/Scuola Superiore Universitaria a Ordinamento Speciale (CASD/SSUOS);
VISTO:	il Regolamento Didattico Generale del CASD/SSUOS;
VISTO:	il Regolamento in materia di Master universitari, Corsi di Alta Formazione e Corsi di Formazione.

NOMINA

Il Col. Stefano PANONI quale Direttore Scientifico del Corso di Alta Formazione in "Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali" per l'Anno Accademico 2025 – 2026.

Roma, lì 22 SET. 2025

IL PRESIDENTE
(Gen. C.A. Stefano MANNINO)

RIFERIMENTI

a. Concetto Strategico del Capo di Stato Maggiore della Difesa, ed. 2022;

b. Decreto interministeriale del 4 luglio 2024 (G.U. n. 213 del 11.09.2024);

c. Regolamento Didattico Generale del CASD/SSUOS, ed. 2025;

d. SMD-FORM-001 "Direttiva per la formazione interforze del personale", ed. 2022;

e. SMD-FORM-010 "Direttiva per la ricerca e la formazione della Difesa", ed. 2022;

f. SMD-CTM-002 "Procedure per l'ammissione di personale militare straniero ai corsi presso Istituti ed Enti delle Forze Armate Italiane", ed. 2018;

INDICE

ALLEGATI		
A	Schede formative	
B	Cronoprogramma	
C	Piano di impiego del tempo	
D	Piano generale dei costi	

1. GENERALITÀ

Il CASD è un Centro di istruzione universitaria che eroga corsi di formazione dottorale, alta formazione post-laurea e formazione continua nel campo della difesa e della sicurezza nazionale. In particolare, il Centro per la Formazione Logistica Interforze (CeFLI) sviluppa corsi ed indirizza gli studi per istruire il personale dell'intero comparto della Difesa sulle procedure logistiche interforze, nazionali e NATO/UE, nonché sulle più evolute tecniche di ingegneria logistica e gestionale allo scopo di fornire una qualificazione superiore nel settore della Logistica interforze.

2. DENOMINAZIONE DEL CORSO

Corso di Alta Formazione in "Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali".

3. STRUTTURA ACCADEMICA DEL CORSO

a. Struttura accademica proponente
Centro per la Formazione Logistica Interforze (CeFLI).

b. Struttura accademica responsabile per la progettazione didattica
Centro per la Formazione Logistica Interforze (CeFLI).

c. Struttura accademica responsabile per la gestione del corso
Centro per la Formazione Logistica Interforze (CeFLI):
- Direttore del Corso: Col. Stefano PANONI (Capo Dipartimento Studi e Sviluppo Normativa).
- Direttore scientifico: Col. Stefano PANONI.

4. SEDE E PERIODO DI SVOLGIMENTO

a. Sede delle lezioni e periodo didattico
Le lezioni di didattica frontale inizieranno il 10 ottobre 2025 e si concluderanno il 30 gennaio 2026. Le lezioni si svolgeranno in presenza, al Centro per la Formazione Logistica Interforze, sito presso la Caserma Rossetti, viale dell'esercito 86, 00143 Roma, e da remoto con esclusione dei periodi delle festività natalizie, di fine/inizio anno. La data di discussione dell'elaborato finale sarà comunicata durante lo svolgimento del corso.

b. Segreteria studenti
La segreteria studenti è sita presso la sede del Centro Alti Studi Difesa (CASD/SSU) sita in P.zza della Rovere, 83 – 00165 Roma. Le comunicazioni relative alla parte amministrativa dovranno essere indirizzate al seguente indirizzo e-mail: segreteriastudenti@unicasd.it, mentre le comunicazioni inerenti alla didattica del corso dovranno essere indirizzate all'indirizzo e-mail cefli.segreteria@casd.difesa.it.

5. OBIETTIVI FORMATIVI GENERALI DEL CORSO

Il corso è concepito per sviluppare competenze metodologiche, analitiche e strategiche per interpretare e gestire le dinamiche che caratterizzano le organizzazioni complesse e statuali, con particolare attenzione alle catene logistiche che presiedono al settore della sicurezza e difesa. Il corso mira a rafforzare le capacità decisionali e manageriali del personale dirigente, promuovendo una visione olistica e sistemica che valorizzi la funzione logistica come leva fondamentale per la resilienza del sistema Paese.

6. STRUTTURA DIDATTICA DEL CORSO

L'attività formativa corrisponde a n. 15 crediti formativi universitari (CFU) e impegnerà gli iscritti per non meno di n. 98 ore di attività didattica frontale.

Attività formative	SSD	Ore di didattica	CFU
Modulo 1 Il sistema di difesa nazionale	IEGE-01/A GSPS-02/A	23	**All. "C"**
Modulo 2 Caratterizzazione e mitigazione della minaccia	GSPS-02/A GEOS-04/C ECON-07/A GIUR-03/A	20	**All. "C"**
Modulo 3 La funzione logistica per la difesa e la resilienza delle organizzazioni complesse e statuali	ECON-07/A GIUR-03/A IEGE-01/A	55	**All. "C"**
Totale ore di didattica/CFU		98	15

7. ATTIVITÀ FORMATIVE DEL CORSO

a. Attività didattiche
   - Schede formative (**All. "A"**);
   - Cronoprogramma (**All. "B"**);
   - Piano di impiego del tempo (**All. "C"**).

b. Attività integrative
   Non previste.

8. DESTINATARI DEL CORSO

a. Frequentatori
   Il Corso si rivolge a ingegneri, economisti, dottori in scienze politiche, agli Ufficiali delle Forze Armate e personale altamente qualificato adatto a ricoprire ruoli manageriali interessato a cogliere le opportunità e approfondire gli aspetti inerenti la Difesa e resilienza di enti pubblici e privati di rilevanti dimensioni e complessità che richiedono una comprensione integrata dell'ambiente in cui operano sia per gli aspetti tecnici intrinseci volti al miglioramento dei processi decisionali interni, sia in ambito internazionale consolidando o migliorando il proprio vantaggio competitivo.

b. Uditori
   Vedasi para 13, b.

9. REQUISITI DI AMMISSIONE E SELEZIONE

a. Requisiti di ammissione
   Possono partecipare al CAF studenti italiani e stranieri. Per poter essere iscritti al CAF è necessario essere in possesso di uno dei seguenti requisiti:
   - Laurea conseguita secondo gli ordinamenti didattici precedenti il decreto ministeriale del 3 novembre 1999 n. 509;
   - Lauree specialistiche ai sensi del D.M. 509/99 e lauree magistrali ai sensi del D.M.270/2004;
   - titolo accademico conseguito all'estero equiparabile per durata e contenuto al titolo accademico italiano richiesto per l'accesso al CAF. I titoli di studio conseguiti all'estero verranno valutati, ai soli fini dell'iscrizione al CAF, secondo la vigente normativa.

   I requisiti per l'ammissione al CAF dovranno essere posseduti alla data di scadenza del termine utile per la presentazione delle domande di iscrizione.

b. Numero dei posti disponibili

Al CAF possono partecipare a titolo gratuito Ufficiali delle FA e Funzionari/e della Difesa selezionati dalle articolazioni competenti del Ministero della Difesa, nel numero di 15 frequentatori.

Al CAF vengono ammessi inoltre fino ad un massimo di 15 candidati esterni all'Amministrazione Difesa, selezionati tramite concorso basato sulla documentazione presentata dal/dalla candidato/a.

c. Selezione

La selezione dei candidati appartenetti all'AD viene svolta dagli organi d'impiego di FA sulla base dei posti messi a disposizione dal CASD/SSU.

Per i candidati esterni all'AD, la valutazione dei titoli è effettuata da un'apposita Commissione nominata dal Direttore del CeFLI.

I candidati dovranno presentare domanda di ammissione alla selezione corredata di:

- autocertificazione laurea con voto finale ed esami sostenuti,
- curriculum vitae,
- certificazione conoscenza lingua inglese
- lettera sulle motivazioni alla base della scelta di iscriversi al CAF.

La Commissione procederà all'esame dei titoli, attribuendo i punteggi (max. 30 punti) sulla base dei seguenti parametri:

- voto conseguito – max. 4 punti (n. 4 punti per la votazione 110 e lode, n. 3 punti da 110 a 105, n. 2 punti da 104 a 100, n. 1 punto da 99 a 90);
- altri titoli ed esperienze post laurea – max. 20 punti;
- certificazione lingua inglese – da 1 a 6 punti (da A1 a C2).
- Al termine della verifica dei titoli sarà stilata una graduatoria dei soli soggetti considerati idonei alla frequenza del CAF. Il proprio stato personale (ammesso / non ammesso / non idoneo) potrà essere visionato nell'area privata su Esse3.

10. ESIGENZE DI DOCENZA

a. Docenti e formatori

I docenti civili sono stati selezionati sulla base di accordi/convenzioni preesistenti con atenei ed enti nazionali. I formatori militari sono stati individuati tramite ricerca interna alle FA. L'elenco del personale docente/formatore è riportato in **All. "C"**.

b. *Mentor* e *tutor*

N.A.

11. VALUTAZIONE E RICONOSCIMENTO TITOLI

a. Valutazione e conseguimento titoli

Il rilascio del Diploma di CAF in "Strategie di Difesa e Resilienza di Organizzazioni Complesse e Statuali" e la conseguente acquisizione dei n. 15 CFU sono condizionati:

- al pagamento dell'intera quota di iscrizione;
- al raggiungimento della percentuale minima di frequenza delle lezioni, che non deve essere inferiore al 75 % del monte orario complessivo delle attività in presenza;
- al superamento della prova finale, consistente nella redazione di un elaborato di gruppo/individuale e nella discussione orale del predetto elaborato di fronte a una Commissione giudicatrice.

La valutazione della prova finale verrà espressa in centodecimi (110), la Commissione giudicatrice può, all'unanimità, concedere il massimo dei voti con lode, il voto minimo per il superamento della prova è 66/110.

b. Attestati di frequenza
Su richiesta degli interessati sarà rilasciato un attestato di frequenza alle lezioni del corso.

12. PIANO GENERALE DEI COSTI E PROGRAMMAZIONE DELLA SPESA

a. Piano generale dei costi
Vedasi **All. "D"**.

b. Programmazione della spesa
Spesa programmata e finanziata sul capitolo di spesa 2265/6.

13. DISPOSIZIONI MATRICOLARI, AMMINISTRATIVE E LOGISTICHE

a. Documentazione caratteristica per i discenti militari
N.A.

b. Obbligo di frequenza e Cessazione dal corso
La frequenza del CAF è obbligatoria. La percentuale minima di frequenza è stabilita nella misura 75% del monte orario complessivo delle lezioni. Per difetto dei requisiti si potrà disporre in qualsiasi momento, con provvedimento motivato, l'esclusione dal CAF e il riconoscimento del solo attestato di Uditore.

c. Procedura di iscrizione, quota di iscrizione e modalità di pagamento
La domanda di ammissione dovrà essere presentata esclusivamente tramite il sistema informatico Esse3 **dal 9 settembre 2025 al 3 ottobre 2025**, con la seguente modalità on line:
- tramite sito www.unicasd.it accedere alla sezione **"ESSE3"** ed effettuare la registrazione.
- accedere quindi al sistema Esse3con le proprie credenziali, compilare online la domanda di iscrizione.

Durante la procedura di registrazione sul sistema Esse3 dovranno essere caricati i seguenti documenti, esclusivamente in formato .pdf:
- copia di un documento di riconoscimento in corso di validità;
- copia del codice fiscale (solo per i cittadini italiani e gli stranieri che ne sono in possesso);
- autocertificazione del titolo universitario, se conseguito in Italia;
- attestazione livello di conoscenza della lingua inglese;
- curriculum vitae;
- lettera sulle motivazioni alla base della scelta di iscriversi al CAF;
- copia del titolo straniero tradotto, legalizzato e accompagnato dalla Dichiarazione di valore in loco, oppure dall'Attestato di Verifica del titolo da parte di CIMEA o corredato di *Diploma Supplement*, se il titolo è stato conseguito in uno dei Paesi dello Spazio Europeo dell'Istruzione Superiore.

A seguito del superamento della selezione, i soli candidati ammessi al CAF **fra il 4 e il 10 ottobre 2025** dovranno presentare domanda d'immatricolazione su Esse3 e caricare la ricevuta di pagamento.

La quota d'iscrizione al CAF è stabilita in **€ 540,00** (+16 € marca da bollo), da versare all'atto dell'immatricolazione;

La modalità di pagamento è telematica, tramite sistema PAGO PA; saranno fornite le istruzioni di pagamento dalla Segreteria.

Il mancato pagamento dell'intera quota d'iscrizione al CAF precluderà il rilascio del diploma/attestato di partecipazione.

In caso di iscrizione e successiva rinuncia a proseguire il CAF, l'iscritto è tenuto a darne comunicazione scritta al Direttore del CAF e alla Segreteria Studenti. Le quote d'iscrizione eventualmente già pagate non sono rimborsabili.

d. Aspetti logistici
Per l'accesso alla caserma Rossetti, i frequentatori dovranno inviare copia del documento d'identità al seguente indirizzo e-mail: cefli.segreteria@casd.difesa.it. L'accesso in auto è

subordinato alle necessità contingenti del Comando Caserma, per la domanda di accesso è necessario effettuare una richiesta al precedente indirizzo e-mail indicando marca, modello, colore e targa della vettura.

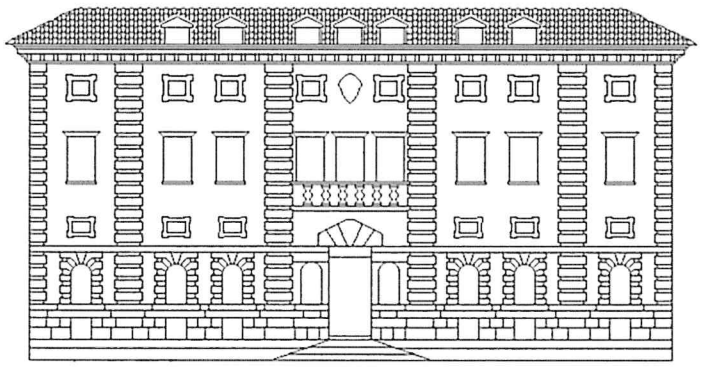
e. Trattamento dei dati personali
Titolare del trattamento dei dati personali forniti è il Centro Alti Studi Difesa - Scuola Superiore Universitaria, con sede legale in Roma, Piazza della Rovere 83, nella persona del Presidente del CASD, contattabile all'indirizzo PEC: difealtistudi@postacert.difesa.it.
Il Referente per la protezione dei dati personali presso il CASD è il Dirigente autorizzato dal Titolare del trattamento, in relazione alle proprie funzioni e competenze, alla protezione dei dati.
I contatti del Responsabile unico della Protezione dei Dati personali della Difesa sono i seguenti:
- indirizzo di posta elettronica: rpd@difesa.it;
- indirizzo di posta elettronica certificata: rpd@postacert.difesa.it.

Il Responsabile per il trattamento dati sul Sistema Esse 3 è Cineca Consorzio Interuniversitario contattabile all'indirizzo e-mail privacy@cineca.it.

f. Responsabile del procedimento concorsuale
Ai sensi di quanto disposto dall'art. 5 della L. 241/90, il responsabile del procedimento concorsuale di cui al presente bando è il Colonnello Alessandro TASSI, Capo Dipartimento Formazione Avanzata del Centro per la Formazione Logistica Interforze (CeFLI) - Centro Alti Studi Difesa - Scuola Superiore Universitaria – caserma Rossetti, Viale dell'esercito 86 – 00143 Roma, e-mail cefli.cadire@casd.difesa.it

14. NORME DI COMPORTAMENTO, PRESCRIZIONI E OBBLIGHI

Prima di accedere alla caserma Rossetti, sede del CeFLI, i frequentatori dovranno prendere visone della schede di pre-accesso che sarà gli fatta pervenire dalla segreteria del Centro alla casella di posta elettronica comunicata all'atto dell'iscrizione al corso. La scheda dovrà essere firmate per presa visione e restituita al mittente, stesso mezzo.
Per i militari è prescritto l'utilizzo dell'uniforme di servizio mentre per il personale civile un abbigliamento consono al luogo.



SCHEDA FORMATIVE

Modulo 1 – Il sistema di difesa nazionale

L'insieme di politiche, strutture, risorse e strategie finalizzate a garantire la sicurezza del territorio, la protezione della sovranità e la difesa contro minacce esterne e interne. Questo sistema è costituito da una serie di elementi che lavorano in sinergia per creare una difesa nazionale solida e capace di rispondere a diverse tipologie di minacce, che spaziano dai conflitti armati alle minacce asimmetriche, come il terrorismo o gli attacchi cibernetici.

Illustrazione delle sue componenti: Forze Armate, Ministero della Difesa, Sevizi di Intelligence, Infrastrutture critiche e Difesa Cibernetica, Difesa e Protezione Civile, Politica delle Alleanza, Logistica e catena di Approvvigionamento.

a. La logistica interforze nel sistema di difesa nazionale. Industria e logistica 5.0.

La logistica interforze si riferisce alla cooperazione tra diverse forze armate (Esercito, Marina, Aeronautica, e altre agenzie di sicurezza) e agenzie governative, per ottimizzare la gestione e distribuzione delle risorse necessarie a supportare operazioni militari e di difesa nazionale.

L'idea di interforze implica che tutte le branche delle forze armate lavorino insieme in modo coordinato per condividere risorse, informazioni e operazioni logistiche, riducendo i costi e migliorando l'efficacia complessiva del sistema di difesa. Le principali aree di applicazione includono:

- Distribuzione delle risorse: Coordinare la distribuzione di equipaggiamenti, rifornimenti, munizioni, carburante e altri beni vitali tra le varie forze.
- Supporto durante operazioni congiunte: In scenari di conflitto o di crisi, dove più branche delle forze armate operano in sinergia, la logistica interforze garantisce che tutte le risorse siano disponibili e correttamente distribuite in tempo reale.
- Gestione dei materiali e delle forniture: La condivisione di magazzini, infrastrutture di trasporto e punti di approvvigionamento tra forze diverse è essenziale per l'efficacia operativa.
- Tecnologia e informatizzazione: I sistemi di monitoraggio, le piattaforme di gestione delle risorse e le soluzioni di *supply chain* digitale permettono una visibilità e un controllo continuo sul flusso di materiali e informazioni.

L'evoluzione della logistica e dell'industria è strettamente legata all'innovazione tecnologica, e l'introduzione del concetto di Industria 5.0 porta con sé nuove sfide e opportunità.

Industria 5.0 si distingue dalle precedenti evoluzioni (Industria 4.0) per l'integrazione di tecnologie avanzate con l'interazione umana. In particolare, l'industria 5.0 mette al centro l'essere umano, in combinazione con la robotica avanzata, l'intelligenza artificiale, la stampa 3D, la realtà aumentata e altre tecnologie emergenti. L'obiettivo è creare un sistema di produzione e logistica in cui macchine e persone lavorano fianco a fianco per ottimizzare la produttività e la personalizzazione dei prodotti, pur mantenendo la flessibilità e l'efficienza.

Nella logistica 5.0, le seguenti tecnologie stanno giocando un ruolo sempre più importante:

- Robotica collaborativa: L'uso di robot e droni per eseguire compiti logistici in modo autonomo ma sotto il controllo umano. I robot sono in grado di lavorare fianco a fianco con gli esseri umani, migliorando l'efficienza senza sostituirli.
- Intelligenza Artificiale e *Big Data*: Le piattaforme di IA analizzano i flussi logistici in tempo reale, ottimizzando la gestione delle risorse, la previsione della domanda e la pianificazione delle rotte di approvvigionamento. L'uso di *Big Data* permette una comprensione approfondita dei processi logistici e dei comportamenti del mercato, migliorando la pianificazione e la risposta alle crisi.
- *Blockchain*: L'adozione della *blockchain* per tracciare ogni movimento di merci in modo sicuro e trasparente. Questo garantisce una gestione più sicura dei materiali e una visibilità a livello globale su tutte le operazioni logistiche.

- *Internet of Things* (IoT): Sensori IoT connessi a piattaforme centralizzate monitorano in tempo reale le condizioni di magazzini, veicoli, merci, ecc., migliorando la gestione delle scorte, la manutenzione predittiva e il monitoraggio delle condizioni di sicurezza.
- Automazione e Digitalizzazione: Magazzini automatizzati, veicoli autonomi, e soluzioni di gestione completamente digitalizzate migliorano l'efficienza e riducono i tempi di risposta.

Il connubio tra logistica interforze e Industria 5.0 potrebbe trasformare radicalmente le operazioni di difesa nazionale. In particolare:

- Le tecnologie avanzate potrebbero essere applicate a scenari di difesa, dove la logistica interforze beneficia della capacità di automatizzare la gestione delle risorse e delle forniture in modo più rapido e preciso.
- L'AI e i Big Data potrebbero consentire una pianificazione e gestione predittiva delle operazioni logistiche, ottimizzando il trasporto e la distribuzione di materiali in scenari complessi.
- L'uso di droni e robot autonomi potrebbe migliorare la logistica sul campo di battaglia, riducendo il rischio per il personale umano e garantendo il rifornimento continuo anche in ambienti ad alta pericolosità.
- L'*Internet of Things* (IoT) e la *Blockchain* garantirebbero un monitoraggio in tempo reale delle risorse, una gestione sicura dei dati e una tracciabilità totale dei materiali e delle forniture, migliorando la sicurezza e l'affidabilità delle operazioni.
- In questo contesto, la capacità di rispondere rapidamente e in modo coordinato a situazioni di emergenza o a conflitti su larga scala potrebbe essere notevolmente migliorata, grazie a una logistica più snodabile, sicura e intelligente.

b. Le Forze Armate nel sistema di difesa nazionale

I processi per una crescente partecipazione della FA al "Sistema Paese", attraverso rapporti operativi e istituzionali. Il concetto di interoperabilità, la capacità della Difesa di proiettare sia *Hard Power* che *Soft Power*, per accrescere il "capitale di credibilità" internazionale e abilitare nuovi spazi di manovra. La logica della struttura organizzativa interforze, le operazioni MDO. La FA integrata e interoperabile in ambito nazionale e internazionale. L'ammodernamento tecnologico e la capacità *dual use* dei mezzi e dei sistemi, l'adeguamento delle infrastrutture, la formazione, il reclutamento. Uno Strumento militare quale autorevole esportatore di sicurezza e moltiplicatore di potenza nel più ampio contesto del Sistema Paese.

c. I centri di comando e controllo unificati

Strutture o sistemi centralizzati utilizzati per coordinare, gestire e monitorare operazioni complesse, in vari settori come la sicurezza, la difesa, la gestione delle emergenze e, più recentemente, anche in ambito industriale o sanitario.

Questi centri combinano diverse tecnologie per garantire che le decisioni vengano prese in modo rapido e informato, utilizzando informazioni in tempo reale. Le caratteristiche principali di un centro di comando e controllo unificato includono:

- Centralizzazione delle informazioni: Tutte le informazioni cruciali vengono raccolte in un'unica piattaforma, permettendo una visione d'insieme delle operazioni.
- Comunicazione immediata e sicura: La comunicazione tra diverse unità operative è fondamentale, e i centri di comando utilizzano tecnologie avanzate per garantire comunicazioni sicure e tempestive.
- Monitoraggio in tempo reale: Grazie a sensori, radar, video-sorveglianza e altre tecnologie, i centri possono monitorare e rispondere a situazioni di crisi o di emergenza in tempo reale.
- Gestione integrata: La possibilità di gestire più flussi di dati provenienti da diverse fonti e di coordinare azioni tra diversi enti o reparti (come forze dell'ordine, sanità, soccorso, etc.) è uno degli aspetti chiave.
- Sistemi decisionali avanzati: Spesso i centri di comando utilizzano algoritmi, intelligenza artificiale e sistemi di supporto alle decisioni per analizzare rapidamente grandi quantità di dati e suggerire risposte ottimali.

Questi centri sono essenziali per la gestione di eventi ad alta complessità, come disastri naturali, attacchi informatici, operazioni di difesa o crisi sanitarie.

d. Il sistema nazionale di difesa civile

Le strategie di prevenzione e pianificazioni mirate al soccorso all'interno di scenari complessi. La minaccia, i possibili scenari, le misure da adottare sul modello DIME (*Diplomatic, Information, Military, and Economic*).

e. Il sistema nazionale di protezione civile e meccanismo unionale

La Commissione interministeriale, le procedure attuative nelle situazioni emergenziali e di crisi sia in ambito nazionale che comunitario (meccanismo unionale). La sicurezza delle infrastrutture critiche, delle risorse materiali, dei servizi, dei sistemi di tecnologia dell'informazione, delle reti e dei beni infrastrutturali, la catena di approvvigionamenti, la salute, la sicurezza e il benessere economico o sociale dello Stato. Le esercitazioni, la loro effettiva funzionalità e la capacità operativa. I nuclei N.B.C.R. il soccorso in caso di pericolo nucleare, batteriologico, chimico e radioattivo.

f. Sistema di informazione per la sicurezza della Repubblica

Il Sistema di Informazione per la Sicurezza della Repubblica (SISR) è un elemento cruciale della sicurezza nazionale italiana. Esso è composto da una serie di agenzie, organi e strutture che lavorano in sinergia per proteggere gli interessi strategici del paese, come quelli politici, militari, economici e industriali, attraverso la raccolta, l'analisi e la gestione delle informazioni relative alla sicurezza. La Legge 124/2007, che disciplina il funzionamento dei servizi di sicurezza e di intelligence in Italia, ed è orientato a prevenire minacce interne ed esterne che potrebbero compromettere la stabilità del paese.

- Le Autorità delegate

  In Italia, la sicurezza nazionale è garantita da un insieme di autorità e organismi che operano a livello istituzionale e che hanno il compito di proteggere il paese da minacce interne ed esterne. La Legge 124/2007 sulla sicurezza nazionale ha definito il quadro normativo e stabilito le competenze di varie autorità in relazione alla gestione della sicurezza e della difesa del paese. Di seguito, esplorerò le principali autorità delegate alla sicurezza nazionale in Italia e i loro compiti. Presidenza del Consiglio dei Ministri. Ministero dell'Interno. Ministero della Difesa. Agenzia per la Cyber Sicurezza nazionale (ACN). Agenzia Nazionale per la Sicurezza delle Infrastrutture Critiche (ANSCI). Consiglio Supremo di Difesa. Servizi di Intelligence (AISI e AISE).

- La funzione di controllo

  l controllo della sicurezza nazionale è una funzione fondamentale per il governo di ogni paese, essenziale per garantire la protezione degli interessi vitali e la stabilità della nazione. In Italia, questa funzione è esercitata da un insieme di istituzioni, organi di coordinamento, e servizi di sicurezza che operano insieme per garantire la sicurezza interna, la difesa nazionale, e la protezione da minacce esterne e interne. Prevenzione delle minacce. Gestione delle crisi e delle emergenze. Protezione delle infrastrutture critiche. Controllo delle armi e della proliferazione. Protezione della sovranità e dei confini. Istituzioni deputate. Strumenti di controllo.

- Sicurezza delle informazioni

  Politiche, pratiche, tecnologie e misure adottate per proteggere le informazioni sensibili da minacce come accessi non autorizzati, furti, manipolazioni e perdita di integrità, disponibilità e confidenzialità dei dati stessi. Aree relative alla sicurezza delle informazioni (confidenzialità, integrità, disponibilità). Minacce e misure di protezione. Normativa. Sicurezza delle informazioni in un contesto nazionale.

- L'Organizzazione Nazionale per la Sicurezza (ONS)

  L'Organizzazione Nazionale per la Sicurezza (ONS) è un'entità centrale che coordina e gestisce la sicurezza nazionale di uno stato, con l'obiettivo di proteggere gli interessi vitali della nazione da minacce interne ed esterne. Sebbene la struttura e le funzioni di un'Organizzazione Nazionale per la Sicurezza possano variare da paese a paese, generalmente l'ONS svolge un ruolo cruciale nella gestione della sicurezza interna e della difesa nazionale, nonché nell'implementazione delle politiche di sicurezza. Funzioni Principali dell'Organizzazione Nazionale per la Sicurezza. Struttura dell'Organizzazione Nazionale per la Sicurezza. Strumenti e Risorse Utilizzati. La Sicurezza Nazionale e la Cooperazione Internazionale.

- Il segreto di stato, la Legge 124/2007 e le garanzie funzionali
  Il segreto di stato e la Legge 124/2007 (nota come Legge sulla sicurezza nazionale) sono aspetti cruciali per la protezione delle informazioni sensibili e per la difesa della sicurezza nazionale in Italia. La Legge 124/2007 è una normativa che ha introdotto importanti disposizioni relative alla protezione delle informazioni riservate, stabilendo le garanzie funzionali per la gestione e la divulgazione delle informazioni classificate, tra cui quelle legate alla sicurezza dello Stato.
- La relazione annuale sulla politica dell'informazione per la sicurezza quale strumento di analisi geopolitica
  La Relazione Annuale sulla Politica dell'Informazione per la Sicurezza è uno strumento fondamentale utilizzato da un paese per fare il punto sulle proprie strategie e politiche di sicurezza informativa, nonché per analizzare e rispondere alle sfide geopolitiche legate alla sicurezza nazionale. Questo documento offre una panoramica completa delle attività e delle operazioni legate alla sicurezza dell'informazione, alle minacce e alle vulnerabilità a livello sia nazionale che internazionale.
  In Italia, la Relazione Annuale sulla Politica dell'Informazione per la Sicurezza viene presentata dal Presidente del Consiglio dei Ministri al Parlamento e al pubblico. Essa serve a dare trasparenza sulle politiche di sicurezza e a orientare le scelte future in relazione alla protezione delle infrastrutture critiche, alla *cybersecurity*, alla difesa delle informazioni sensibili e alla gestione delle minacce globali. La Relazione Annuale sulla Politica dell'Informazione per la Sicurezza ha anche un ruolo di analisi geopolitica strategica (monitoraggio degli sviluppi globali, influenza e *soft power*, rischi economici e strategici delle risorse). Struttura e contenuti della relazione.

Modulo 2 – Caratterizzazione e mitigazione della minaccia

La caratterizzazione e la mitigazione della minaccia sono due passaggi fondamentali nel ciclo di gestione delle minacce, in particolare quando si parla di minacce legate alla sicurezza nazionale, alla difesa e alla stabilità internazionale. Entrambi questi concetti giocano un ruolo cruciale nella protezione degli interessi e dei valori di uno Stato, sia a livello strategico che operativo.

a. Minacce antropiche

Le minacce antropiche sono pericoli derivanti dall'azione umana, e possono essere sia dirette (come guerre, attacchi terroristici, crimine organizzato) che indirette (come i danni ambientali o le pandemie). Sono complesse e interconnesse, e spesso richiedono una risposta globale e coordinata per minimizzare i rischi e limitare i danni. La comprensione e la gestione di queste minacce è essenziale per proteggere la sicurezza, la stabilità e la prosperità delle società moderne. Le minacce derivanti da conflitti armati, terrorismo. Le minacce antropiche possono anche derivare dalle attività industriali, agricole e urbane. Il crimine organizzato e le attività illegali. Minacce sanitarie e pandemiche. Le disuguaglianze sociali, le crisi economiche e i conflitti interni.

b. Criticità naturali

Conoscenze dei fenomeni naturali e delle interazioni con gli ecosistemi, le attività antropiche e le infrastrutture. Previsione, gestione e mitigazione dei rischi. *Data Management* e interoperabilità.

- Le tecniche di previsione, prevenzione e mitigazione dei rischi e loro impatto sull'ambiente, anche in un contesto di cambiamenti globali;
- Il concetto di *Open Data Access*, l'utilizzo dei dati e delle informazioni per la ricerca e il monitoraggio ambientale. Infrastrutture e iniziative multidisciplinari.

c. *Risk Assessment*, metodologie di identificazione, analisi e valutazione del rischio operativo

Il *Risk Assessment* (o Valutazione del Rischio) è un processo cruciale per la gestione della sicurezza, sia in ambito operativo che strategico, e riguarda l'identificazione, l'analisi e la valutazione dei rischi a cui è esposta un'organizzazione, al fine di prendere decisioni informate riguardo le azioni da intraprendere per mitigarli o accettarli.

Nel contesto della sicurezza operativa, il *Risk Assessment* è utilizzato per identificare i rischi che potrebbero compromettere l'efficienza, la sicurezza fisica, la sicurezza informatica e la continuità operativa di un'organizzazione. Il processo è fondamentale per prendere decisioni in ambito cybersecurity, sicurezza fisica, gestione delle crisi e continuity planning.

d. Minacce alla sicurezza nazionale fisiche e cibernetiche

Le sfide legate alla dimensione *cyber*, rilevanza geopolitica e geostrategica, in ragione della peculiare trasversalità di questo dominio, quale potenziale strumento di propagazione e amplificazione degli altri tipi di minaccia. *Big Data*, la sicurezza di una nazione dipende dall'accesso alle informazioni. Il confronto multidimensionale e l'ambiente cognitivo nei moderni conflitti. La competizione tra potenze in ambito tecnologico, il ruolo delle *Emerging & Disruptive Technologies* nei futuri sviluppi strategici, militari e industriali.

e. *Cyber Legad*

Legislazione sulla *cybersicurezza* e sulle normative legali che regolano l'uso e la protezione delle tecnologie digitali e delle informazioni su internet.

f. Il *Cognitive Warfare* (Disinformazione e tecniche di contrasto)

Il *Cognitive Warfare* può essere definito come una strategia di conflitto che mira a influenzare, manipolare o distorcere la percezione della realtà dell'avversario (o della popolazione target) per indurre comportamenti favorevoli agli obiettivi di chi lo conduce, utilizzando tecniche psicologiche, mediatiche e cibernetiche. Le operazioni possono mirare a indurre confusione, seminare discordia, alterare la verità o creare disinformazione con l'intento di minare la coesione sociale, la credibilità politica e la stabilità psicologica di un avversario. Il *Cognitive Warfare* è considerato multidominio perché agisce su più fronti simultaneamente e si intreccia con altre forme di operazioni, come la guerra cibernetica, la guerra dell'informazione e persino il conflitto tradizionale. In effetti, il dominio cognitivo è tanto un obiettivo quanto un campo di battaglia di un conflitto.

La disinformazione è una delle tecniche più potenti e pericolose nel contesto della guerra moderna, delle operazioni psicologiche e delle strategie politiche. Si tratta di informazioni false o ingannevoli diffuse intenzionalmente con lo scopo di manipolare l'opinione pubblica, creare confusione, minare la credibilità di un avversario o alterare il corso degli eventi. Le tecniche di disinformazione sono spesso strettamente collegate alle *Psychological Operations* (PSYOPS), ma si estendono anche all'ambito politico, economico e sociale. Disinformazione intenzionale. *Misinformation. Malinformation.* Le tecniche di contrasto alla disinformazione sono essenziali per proteggere la verità, mantenere la fiducia nelle istituzioni e ridurre gli effetti negativi delle campagne di disinformazione. Verifica dei fatti. Educazione ai media e pensiero critico. Monitoraggio e rimozione dei contenuti. Campagne di contro narrativa. Collaborazione tra enti pubblici e privati. Creazione di piani di comunicazione trasparenti.

g. Digital Service Act

Il *Digital Services Act* (DSA) è una legge europea fondamentale che regola i servizi digitali, ed è stata adottata dalla Commissione Europea per rendere più sicuri, giusti e trasparenti i servizi online nell'Unione Europea. Entrato in vigore nel 2022, il DSA rappresenta un passo importante nella regolazione delle piattaforme digitali e nell'affrontare i rischi legati all'uso di internet, come la disinformazione, i contenuti dannosi, la privacy degli utenti e la sicurezza online.

Il DSA è complementare al *Digital Markets Act* (DMA), che regola la concorrenza nel mercato digitale. Mentre il DMA si concentra sul contrasto alle pratiche anticoncorrenziali e sul rafforzamento della concorrenza nelle piattaforme digitali, il DSA mira a proteggere gli utenti e a garantire un ambiente online sicuro e trasparente.

h. Reputational risk management

Il *Reputational Risk Management* (Gestione del rischio reputazionale) è un processo strategico che le organizzazioni implementano per proteggere e gestire la loro reputazione. La reputazione è un *asset* intangibile ma di grande valore per ogni azienda, istituzione o individuo, poiché influisce direttamente sulla fiducia dei clienti, sul valore del brand e sulla relazione con i partner e le comunità. Gestire il rischio reputazionale significa identificare, prevenire e mitigare i fattori che potrebbero danneggiare l'immagine pubblica o la percezione che il pubblico ha di un'organizzazione. Identificazione del rischio reputazionale. Valutazione del rischio. Prevenzione del rischio reputazionale. Mitigazione del rischio reputazionale. Monitoraggio continuo ed analisi dei risultati. Cultura aziendale e responsabilità sociale. Tecnologia e strumenti di monitoraggio.

Modulo 3 - La funzione logistica per la difesa e la resilienza delle organizzazioni complesse e statuali

La funzione logistica è fondamentale per garantire la difesa e la resilienza delle organizzazioni complesse e degli Stati, specialmente in un contesto di crisi o emergenza. La logistica non è solo una funzione operativa, ma si configura come un elemento strategico che permette alle organizzazioni di rispondere rapidamente a minacce, garantendo la sostenibilità delle loro operazioni e la capacità di adattarsi a situazioni impreviste.

a. ***Risk Management & Business Continuity Management***
   La varietà dei rischi a cui una organizzazione/ente è sottoposta e le principali motivazioni che spingono all'introduzione di un metodo di gestione dei rischi. La valutazione dei rischi alla base di qualsiasi decisione strategica. Le fasi per una corretta implementazione del *Business Continuity Management*: il *Business impact analysis*, la definizione del *Business Continuity Plan*, sviluppo di sessioni di training e awareness per coinvolgere la popolazione aziendale.
   La cultura del *continuous improvement*, azioni periodiche, revisione e verifica delle procedure e degli *asset*.
b. **Direttiva europea 2008/114/CE, individuazione e designazione delle infrastrutture critiche**
   La Direttiva Europea 2008/114/CE riguarda l'individuazione e la designazione delle infrastrutture critiche (*Critical Infrastructure*, CI) nell'Unione Europea, con l'obiettivo di rafforzare la protezione di quelle risorse che sono essenziali per il funzionamento delle economie e delle società. La Direttiva mira a garantire che le infrastrutture chiave siano adeguatamente protette contro rischi che potrebbero compromettere la sicurezza e stabilità di uno Stato membro, specialmente in caso di attacchi terroristici, disastri naturali o altre emergenze. Infrastrutture critiche e loro identificazione.
c. ***Disaster management, Critical Infrastructure Management*, Tecniche di analisi del rischio e competenze multidisciplinari**
   Disaster Management e *Critical Infrastructure Management* sono ambiti strettamente interconnessi, poiché entrambi si concentrano sulla protezione e il ripristino di infrastrutture critiche e servizi essenziali in scenari di crisi, come disastri naturali, attacchi terroristici, guasti tecnologici o emergenze sanitarie. La gestione di questi eventi richiede un approccio multidisciplinare che integri competenze provenienti da vari settori: ingegneria, sicurezza, gestione del rischio, diritto, economia, e altri. Le tecniche di analisi del rischio sono fondamentali per identificare, valutare e mitigare le minacce, mentre la preparazione e il coordinamento tra diverse entità sono essenziali per una risposta efficace (analisi qualitative e quantitativa, *Failure Mode and Effects Analysis*, analisi delle vulnerabilità, simulazioni e stress test).
d. **La pianificazione territoriale e gli eventi incidentali Na-Tech**
   La pianificazione territoriale e la gestione degli eventi incidentali Na-Tech (Naturali e Tecnologici) sono strettamente connesse alla protezione e alla resilienza di un territorio di fronte a emergenze e disastri che coinvolgono sia rischi naturali che tecnologici. La gestione integrata di questi eventi è fondamentale per ridurre i danni e migliorare la capacità di risposta a crisi che coinvolgono le infrastrutture critiche, la salute pubblica, e la sicurezza. Pianificazione Territoriale: Obiettivi e Definizione. Eventi Incidentali Na-Tech (Naturali e Tecnologici) esempi e caratteristiche. Strategie di Pianificazione Territoriale per Gestire gli Eventi Na-Tech.
e. ***Big data* e intelligenza artificiale quale strumento per l'analisi predittiva**
   Big Data e Intelligenza Artificiale (IA) sono due delle tecnologie più potenti e trasformative per l'analisi predittiva, che rappresenta una delle aree più dinamiche nell'ambito della gestione dei dati e della sicurezza nazionale, gestione del rischio, salute pubblica, economia e prevenzione dei disastri.
   L'analisi predittiva si concentra sull'uso di modelli statistici e algoritmi avanzati per analizzare dati storici e correnti, con l'obiettivo di fare previsioni su eventi futuri. Combinando *Big Data* e IA, è possibile migliorare la capacità di previsione e prevenire situazioni critiche prima che accadano. Definizioni e caratteristiche di big data. L'IA per l'analisi predittiva.
f. ***Data literacy* e *Block chain management* quale supporto decisionale e operativo**
   Data literacy e *blockchain management* sono due concetti chiave che stanno emergendo come strumenti fondamentali nel supporto decisionale e operativo in diversi ambiti, dall'economia alla

sicurezza, dalla gestione aziendale alla gestione delle risorse pubbliche. Entrambi, se usati in modo strategico, possono migliorare significativamente l'efficacia delle decisioni e l'efficienza operativa. *Data literacy* è la capacità di leggere, comprendere, creare e comunicare con i dati. In altre parole, si riferisce alla capacità di utilizzare i dati in modo efficace per prendere decisioni informate.

In un mondo sempre più *data-driven*, avere una forza lavoro *data-literate* è cruciale. L'abilità di capire i dati e le informazioni che li accompagnano, e saperli applicare correttamente nel processo decisionale, è diventata un elemento distintivo di organizzazioni di successo, sia nel settore pubblico che in quello privato. La *blockchain* è una tecnologia distribuita che consente di registrare e verificare transazioni in modo sicuro, trasparente e immutabile. In sostanza, si tratta di un registro digitale in cui le informazioni vengono salvate in "blocchi" e collegati tra loro, creando una catena sicura e decentralizzata.

L'applicazione della *blockchain* nel supporto decisionale e operativo si sta espandendo a molti settori, dalla gestione delle risorse finanziarie alla sicurezza nazionale, fino alla gestione delle forniture e dei contratti. Quando data *literacy* e *blockchain* management vengono utilizzati insieme, creano un ambiente in cui i dati sono non solo più facilmente comprensibili, ma anche sicuri, tracciabili e affidabili.

g. **L'intelligenza artificiale a servizio della difesa degli obiettivi sensibili, il monitoraggio e l'analisi predittiva delle criticità**

L'intelligenza artificiale (IA) sta giocando un ruolo sempre più cruciale nel settore della difesa e nella protezione degli obiettivi sensibili, come infrastrutture critiche, dati riservati, e aree strategiche di rilevanza nazionale e internazionale. L'uso dell'IA in questi contesti sta migliorando significativamente le capacità di monitoraggio, analisi predittiva e risposta automatica a minacce emergenti, offrendo nuove opportunità per ottimizzare la sicurezza e la resilienza delle organizzazioni statali e aziendali. La difesa degli obiettivi sensibili richiede una protezione multilivello che comprenda il monitoraggio continuo, la rilevazione di anomalie e la prevenzione di attacchi o intrusioni. L'IA è un elemento chiave in questo processo, poiché è in grado di analizzare grandi quantità di dati in tempo reale, identificando modelli e comportamenti sospetti, e intervenendo rapidamente per mitigare le minacce. L'analisi predittiva è un campo in cui l'IA ha un impatto significativo nella gestione del rischio e nella protezione delle infrastrutture sensibili. Gli algoritmi di *machine learning* possono analizzare enormi volumi di dati storici e in tempo reale per prevedere eventi che potrebbero rappresentare una minaccia o una criticità per la sicurezza.

h. ***Cyber Threat Intelligence* nella difesa delle infrastrutture critiche**

Cyber Threat Intelligence (CTI) è l'attività di raccolta, analisi e diffusione di informazioni relative alle minacce cibernetiche che potrebbero colpire un'organizzazione, un paese o una rete di infrastrutture critiche. Il termine si riferisce a tutte le informazioni utili per identificare, monitorare e rispondere proattivamente a minacce informatiche o a incidenti di sicurezza. L'obiettivo principale del CTI è prevenire, identificare e rispondere a *cyber* attacchi in modo più rapido ed efficace.

i. **Il *Golden Power* quale strumento a tutela degli *asset* strategici del Paese**

Il *Golden Power* è uno strumento giuridico e normativo messo in atto da numerosi Stati per tutelare gli *asset* strategici nazionali in un contesto globale sempre più interconnesso e competitivo. La sua introduzione e applicazione rispondono alla necessità di proteggere settori considerati di interesse cruciale per la sicurezza nazionale, l'economia e la sovranità. Il termine *Golden Power* (o "potere d'oro") si riferisce alla facoltà dello Stato di intervenire, vietare o limitare operazioni economiche o acquisizioni che riguardano determinati settori strategici del paese. Questo potere è volto a prevenire che attori esterni (sia pubblici che privati) acquisiscano il controllo o influiscano sulle risorse o infrastrutture vitali per la sicurezza nazionale.

Il *Golden Power* permette al governo di esercitare un diritto di veto su operazioni di fusione e acquisizione che potrebbero compromettere la sicurezza, la stabilità economica e la sovranità del paese. Settori di applicazione. Decreto legge 21/2012.

j. **I piani di sicurezza secondo lo standard di riferimento BS7799 (ISO/IEC 17799), il ciclo Plan-Do-Check-Act (PDCA)**
Lo standard BS 7799, sviluppato dal *British Standards Institution* (BSI) e successivamente evoluto nell'ISO/IEC 17799 (ora noto come ISO/IEC 27001 per la gestione della sicurezza delle informazioni), fornisce un *framework* completo per gestire la sicurezza delle informazioni in modo sistematico. Questi standard sono stati fondamentali per l'evoluzione della gestione della sicurezza delle informazioni e sono ancora oggi una delle principali linee guida utilizzate dalle organizzazioni per proteggere i propri dati e i sistemi informatici.
Il modello di sicurezza delle informazioni proposto dallo standard si basa sul ciclo di gestione del miglioramento continuo *Plan-Do-Check-Act* (PDCA), che è una metodologia consolidata e ben radicata nella gestione della qualità e nelle pratiche di sicurezza aziendale. Il ciclo *Plan-Do-Check-Act* (PDCA) aiuta le organizzazioni a pianificare, implementare, monitorare e migliorare continuamente le loro politiche e pratiche di sicurezza.

k. ***Due diligence* ambiti e applicazione**
La *due diligence* è un processo fondamentale di verifica e valutazione che viene effettuato in vari ambiti, con l'obiettivo di raccogliere informazioni dettagliate e accurate su un soggetto, un'operazione, o una transazione prima di prendere decisioni significative. Si tratta di una pratica che mira a ridurre i rischi e garantire la conformità a normative e standard aziendali. Il termine *due diligence* è ampiamente utilizzato in contesti legali, finanziari, aziendali e di sicurezza. La *due diligence* è uno strumento essenziale per minimizzare i rischi in qualsiasi tipo di transazione o operazione, che si tratti di acquisizioni aziendali, investimenti, partnership strategiche o operazioni internazionali. Le sue applicazioni sono molto ampie e variano in base all'ambito, ma l'obiettivo centrale rimane sempre quello di garantire una decisione informata, riducendo al minimo i rischi e ottimizzando il valore dell'operazione.
In un contesto di sicurezza nazionale, per esempio, la *due diligence* diventa ancora più cruciale, dato che le infrastrutture critiche devono essere protette da minacce interne ed esterne. La capacità di anticipare rischi e proteggerle proattivamente è fondamentale per la stabilità e la sicurezza di un paese.

l. ***Recovery Fund***
Il *Recovery Fund* è un meccanismo finanziario istituito dall'Unione Europea per sostenere la ripresa economica degli Stati membri, colpiti da eventi straordinari, come la pandemia di COVID-19, con l'obiettivo di stimolare la crescita economica, migliorare la resilienza e promuovere la transizione ecologica e digitale. Il fondo è stato un elemento centrale della risposta europea alla crisi economica, e si inserisce nel più ampio programma *Next Generation* EU, un pacchetto di misure varato nel luglio 2020. Il *Recovery Fund* ha come obiettivo principale quello di recuperare i danni economici causati dalla pandemia e rafforzare la capacità economica e sociale dell'Unione Europea, affrontando in particolare tre sfide cruciali: sostenibilità economica e crescita, transizione ecologica e digitalizzazione. Struttura del *Recovery Fund* (*Next Generation* EU, PNNR). Meccanismo di Assegnazione e Controllo. Impatti attesi.

m. ***Vulnerability Assessment* metodologie per identificare**
Il *Vulnerability Assessment* (Valutazione delle Vulnerabilità) è un processo critico per identificare, analizzare e gestire le vulnerabilità all'interno di un sistema, che siano informatiche, fisiche o organizzative. Questo processo permette di capire quali sono le aree di un'infrastruttura o di un'organizzazione che potrebbero essere soggette a rischi e di adottare misure per mitigarli prima che si verifichino incidenti o danni. Obiettivo del *Vulnerability Assessment*. Metodologie per Identificare le Vulnerabilità. Metodologie di Analisi e Valutazione. Strategie di Mitigazione e Risoluzione.

n. **Le transizioni digitali e ambientali: relazioni interpersonali, logistica e trasporti. Uno studio di *futures studies* su guerra cognitiva e sicurezza nazionale**
Le transizioni digitali e ambientali stanno trasformando radicalmente diversi settori, inclusi quelli della logistica e dei trasporti, con implicazioni significative non solo a livello economico e operativo, ma anche in termini di sicurezza nazionale e guerra cognitiva. Lo studio delle tendenze future, attraverso i *futures studies*, aiuta a comprendere come evolveranno questi settori e quali rischi e opportunità si presenteranno. Le Transizioni Digitali e Ambientali: Impatti su Logistica e

Trasporti. Il futuro della logistica e dei trasporti non riguarda solo le tecnologie fisiche e i processi operativi, ma anche l'evoluzione delle relazioni interpersonali e della sicurezza cognitiva. In un contesto globale sempre più complesso, i rischi legati alla guerra cognitiva e alla sicurezza delle informazioni assumono un'importanza crescente. I *futures studies* sono approcci interdisciplinari che cercano di prevedere e analizzare i possibili scenari futuri in un contesto di incertezze e variabili complesse. Applicati alla logistica e alla sicurezza nazionale, questi studi possono aiutare a identificare le tendenze emergenti, analizzare i rischi e prevedere come le transizioni digitali e ambientali influenzeranno le operazioni future. Gli scenari futuri della logistica e dei trasporti devono integrare non solo la digitalizzazione, ma anche la sostenibilità ambientale. Le politiche di decarbonizzazione impatteranno i settori dei trasporti e della logistica, spingendo verso l'adozione di tecnologie più ecologiche e modelli di business più sostenibili. Tuttavia, la sicurezza rimane un obiettivo centrale. Proteggere le infrastrutture critiche da minacce digitali e fisiche sarà essenziale. La resilienza delle infrastrutture critiche (sistemi di trasporto, logistica, comunicazioni) alle crisi globali e agli attacchi sarà cruciale. Le previsioni future richiedono l'adozione di tecnologie più sicure, come *blockchain* e AI per la gestione delle catene di approvvigionamento, per proteggere le infrastrutture da minacce.

o. ***Positioning Navigation & Timing*: una funzione critica per la logistica**
Positioning, Navigation, and Timing (PNT) è un componente fondamentale delle infrastrutture moderne e svolge un ruolo cruciale nella logistica, nelle operazioni di trasporto e in molte altre applicazioni di sicurezza e gestione delle risorse. La combinazione di posizionamento, navigazione e temporizzazione si riferisce a sistemi che forniscono informazioni geografiche e temporali precise e in tempo reale, essenziali per una vasta gamma di operazioni. PNT: Una Funzione Critica per la Logistica. Rischi e Minacce ai Sistemi PNT.

p. ***Positioning Navigation & Timing*: una funzione critica per la logistica. Infrastrutture critiche e dati geospaziali**
Il PNT è collegato a molte infrastrutture critiche in vari settori, tra cui il trasporto, l'energia, la comunicazione, la sicurezza nazionale e l'economia digitale. L'affidabilità di questi sistemi è fondamentale per il corretto funzionamento della società moderna. Settore energetico. Settore delle comunicazioni. Difesa e sicurezza nazionale. Settore finanziario. I dati geospaziali (o GIS - *Geographic Information Systems*) sono una risorsa strategica in molte operazioni logistiche e gestionali. In particolare, i dati geospaziali svolgono un ruolo fondamentale nel miglioramento dell'efficienza delle infrastrutture critiche, supportando la gestione dei territori e la protezione delle risorse vitali (pianificazione e gestione urbana, analisi delle vulnerabilità, controllo delle catene di approvvigionamento).

q. **Gli "hot topics" della logistica: AI & Digitalizzazione, Intermodalità e Sostenibilità, *Ex Works* e *Supply Chain Disruption***
Gli *hot topics* della logistica si concentrano su alcune delle principali tendenze e sfide che stanno modellando l'industria oggi. L'evoluzione tecnologica, la sostenibilità e l'efficienza operativa sono temi centrali nel contesto della logistica moderna. AI e Digitalizzazione nella Logistica. Intermodalità nella Logistica. Sostenibilità nella Logistica. L'*Ex Works* (EXW) è uno dei termini *incoterms* (*international commercial terms*) più usati nel commercio internazionale, ed è un aspetto fondamentale da considerare nella logistica globale. Esso indica che il venditore mette la merce a disposizione dell'acquirente in un luogo convenuto (ad esempio, il magazzino), ma l'acquirente si assume tutta la responsabilità per il trasporto, la dogana e i rischi legati alla consegna. Le interruzioni della catena di approvvigionamento (*Supply Chain Disruption*) sono eventi che influenzano negativamente il flusso regolare di beni e servizi, causando ritardi, carenze e costi più elevati.

Allegato "B"

DIAGRAMMA TEMPORALE DEL PROGRAMMA FORMATIVO
CAF STRATEGIE DI DIFESA E RESILIENZA DI ORGANIZZAZIONI COMPLESSE E STATUALI A.A. 2025-2026

LUGLIO		AGOSTO		SETTEMBRE		OTTOBRE		NOVEMBRE		DICEMBRE		GENNAIO		FEBBRAIO		MARZO		APRILE		MAGGIO		GIUGNO	
1		1		1		1		1		1		1		1		1		1		1		1	
2		2		2		2		2		2		2		2		2		2		2		2	
3		3		3		3		3		3		3		3		3		3		3		3	
4		4		4		4		4		4		4		4		4		4		4		4	
5		5		5		5		5		5	CMM / FLR	5		5		5		5		5		5	
6		6		6		6		6		6		6		6		6		6		6		6	
7		7		7		7		7	FLR	7		7		7		7		7		7		7	
8		8		8		8		8		8		8		8		8		8		8		8	
9		9		9		9		9		9		9	FLR	9		9		9		9		9	
10		10		10		10	SDN	10		10		10		10		10		10		10		10	
11		11		11		11		11		11		11		11		11		11		11		11	
12		12		12		12		12		12	CMM	12		12		12		12		12		12	
13		13		13		13		13		13		13		13		13		13		13		13	
14		14		14		14		14	SDN	14		14		14		14		14		14		14	
15		15		15		15		15		15		15		15		15		15		15		15	
16		16		16		16		16		16		16		16		16		16		16		16	
17		17		17		17	SDN / CMM	17		17		17		17		17		17		17		17	
18		18		18		18		18		18		18		18		18		18		18		18	
19		19		19		19		19		19	FLR	19		19		19		19		19		19	
20		20		20		20		20		20		20		20		20		20		20		20	
21		21		21		21		21	CMM / FLR	21		21		21		21		21		21		21	
22		22		22		22		22		22		22		22		22		22		22		22	
23		23		23		23		23		23		23	FLR	23		23		23		23		23	
24		24		24		24	CMM / FLR	24		24		24		24		24		24		24		24	
25		25		25		25		25		25		25		25		25		25		25		25	
26		26		26		26		26		26		26		26		26		26		26		26	
27		27		27		27		27		27		27		27		27		27		27		27	
28		28		28		28		28	SDN	28		28		28		28		28		28		28	
29		29		29		29		29		29		29				29		29		29		29	
30		30		30		30		30		30		30	FLR			30		30		30		30	
31		31				31	CMM / FLR			31		31				31				31			

	AREE DISCIPLINARI
SDN	IL SISTEMA DI DIFESA NAZIONALE
CMM	CARATTERIZZAZIONE E MITIGAZIONE DELLA MINACCIA
FLR	LA FUNZIONE LOGISTICA PER LA DIFESA E LA RESILIENZA

Allegato"C"

STRATEGIE DI DIFESA E RESILIENZA DI ORGANIZZAZIONI COMPLESSE E STATUALI - Piano impiego del tempo

OBIETTIVO DEL CORSO:	Sviluppare competenze metodologiche, analitiche e strategiche per interpretare e gestire le dinamiche che caratterizzano le organizzazioni complesse e statuali, con particolare attenzione al settore della sicurezza e difesa. Il corso mira a rafforzare le capacità decisionali e manageriali del personale dirigente, promuovendo una visione olistica e sistemica che valorizzi la funzione logistica come leva fondamentale per la resilienza del sistema Paese.

AREE DISCIPLINARI	ARGOMENTO	SSD	DOCENTE	PERIODI	DATA	ORARIO
Il Sistema di difesa nazionale	La logistica interforze nel sistema di difesa nazionale. Industria e logistica 5.0.	IEGE-01/A	Col. Stefano Panoni - Dott.ssa Hristina MITANOSKA	4	10/10/2025	08.00 - 11.50
Il Sistema di difesa nazionale	Le Forze Armate nel sistema di difesa nazionale.	GSPS-02/A	Col. Roberto FORLANI	2	10/10/2025	12.00 - 12.50/14.00 - 14.50
Il Sistema di difesa nazionale	I centri di Comando e Controllo Unificati.	IEGE-01/A	CV Riccardo RIZZOTTO	1	10/10/2025	15.00 - 15.50
Il Sistema di difesa nazionale	Il sistema nazionale di difesa civile.	GSPS-02/A	VICE PREFETTO Riccardo MATTEI	1	10/10/2025	16.00 - 16.50
Il Sistema di difesa nazionale	Il sistema nazionale di difesa civile.	GSPS-02/A	VICE PREFETTO Riccardo MATTEI	2	17/10/2025	08.00 - 09.50
Caratterizzazione e mitigazione della minaccia	Minacce Antropiche.	GSPS-02/A	Dr. Alessandro Maria PESSOLANO	2	17/10/2025	10.00 - 11.50
Caratterizzazione e mitigazione della minaccia	Criticità naturali.	GEOS-04/C	Dott.ssa Ilaria MAZZINI	4	17/10/2025	12.00 - 12.50/14.00 - 16.50
Caratterizzazione e mitigazione della minaccia	Minacce alla sicurezza nazionale fisiche e cibernetiche.	GSPS-02/A	ACN	2	24/10/2025	08.00 - 09.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Risk Management & Business Continuity Management.	ECON-07/A	Prof. Fabio NONINO	4	24/10/2025	10.00 - 12.50/14.00 - 14.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Direttiva europea 2008/114/CE, individuazione e designazione delle infrastrutture critiche.	GIUR-03/A	Col. Valentina CAPURRO	2	24/10/2025	15.00 - 16.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Disaster management, Critical Infrastructure Management Tecniche di analisi del rischio e competenze multidisciplinari.	ECON-07/A	Prof. PATRIARCA Prof.ssa STEFANA	4	31/10/2025	08.00 - 11.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	La pianificazione territoriale e gli eventi incidentali Na-Tech.	ECON-07/A	Prof.ssa STEFANA	2	31/10/2025	12.00 - 12.50/14.00 - 14.50
Caratterizzazione e mitigazione della minaccia	Cyber Legad.	GSPS-02/A	Col. Valentina CAPURRO	2	31/10/2025	15.00 - 16.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Big data e intelligenza artificiale quale strumento per l'analisi predittiva.	IEGE-01/A	ACN	3	07/11/2025	08.00 - 10.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Data literacy e Block chain management quale supporto decisionale e operativo.	IEGE-01/A	ACN	2	07/11/2025	11.00 - 12.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	L'intelligenza artificiale a servizio della difesa degli obiettivi sensibili, il monitoraggio e l'analisi predittiva delle criticità.	IEGE-01/A	ACN	3	07/11/2025	14.00 - 16.50
Il Sistema di difesa nazionale	Il sistema di informazione per la sicurezza della Repubblica.	GSPS-02/A	Gen. Paolo POLETTI	8	14/11/2025	08.00 - 12.50/14.00 - 16.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	cyber threat intelligence per la difesa delle infrastrutture critiche	ECON-07/A	Ing. Vincenzo VERDE	4	21/11/2025	08.00 - 11.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Il Golden Power quale strumento a tutela degli asset strategici del Paese.	GIUR-03/A	Col. Luca Gennaro CIOFFI	2	21/11/2025	12.00 - 12.50/14.00 - 14.50
Caratterizzazione e mitigazione della minaccia	Risk Assessment, metodologie di identificazione, analisi e valutazione del rischio operativo.	ECON-07/A	Col. Alfredo RUSSO	1	21/11/2025	15.00 - 15.50
Il Sistema di difesa nazionale	Il Sistema nazionale della protezione civile e meccanismo unionale.	GSPS-02/A	DNPC	5	28/11/2025	08.00 - 12.50
Caratterizzazione e mitigazione della minaccia	Il Cognitive Warfare.	GSPS-02/A	Col. Antonio DI LEONARDO	2	05/12/2025	08.00 - 09.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	La norma ISO 27002, il ciclo Plan-Do-Check-Act (PDCA).	GIUR-03/A	ACN	3	05/12/2025	10.00 - 12.50
Caratterizzazione e mitigazione della minaccia	Digital services act.	GIUR-03/A	ACN	1	12/12/2025	09.00 - 09.50
Caratterizzazione e mitigazione della minaccia	Reputational risk management.	ECON-07/A	Community Group	6	12/12/2025	10.00 - 12.50/14.00 - 16.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Due diligence ambiti e applicazione.	ECON-07/A	Community Group	6	19/12/2025	08.00 - 12.50/14.00 - 14.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Recovery Fund.	ECON-07/A	Prof. GIAGNORIO	4	09/01/2026	09.00 - 12.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Vulnerability Assessment metodologie per identificare.	IEGE-01/A	Prof. Pierluigi LOCATELLI	4	23/01/2026	08.00 - 11.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Le transizioni digitali e ambientali: relazioni interpersonali, logistica e trasporti. Uno studio di futures studies su guerra cognitiva e sicurezza nazionale.	IEGE-01/A	Prof. Alessandro STERPA	2	23/01/2026	12.00 - 12.50/14.00 - 14.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Positioning Navigation & Timing: una funzione critica per la logistica.	IEGE-01/A	Col. Marco BELOGI	2	23/01/2026	15.00 - 16.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Positioning Navigation & Timing: una funzione critica per la logistica. Infrastrutture critiche e dati geospaziali.	IEGE-01/A	Col. Marco BELOGI	4	30/01/2026	08.00 - 11.50
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali	Gli "hot topics" della logistica: AI & Digitalizzazione, Intermodalità e Sostenibilità, Ex Works e Supply Chain Disruption.	IEGE-01/A	Prof. Pietro SPADACCINI	4	30/01/2026	12.00 - 12.50/14.00 - 16.50
				98		

ORARIO DELLE LEZIONI

MATTINO **POMERIGGIO**

0800/0850 - 0900/0950 - 1000/1050 - 1100/1150 - 1200/1250 1400/1450 - 1500/1550 - 1600/1650

SSD	Periodi	CFU
ECON-07/A	31	4
GEOS-04/C	4	1
GIUR-03/A	8	1
GSPS-02/A	26	4
IEGE-01/A	29	5
	98	**15**

STRATEGIE DI DIFESA E RESILIENZA DI ORGANIZZAZIONI COMPLESSE E STATUALI					
OBIETTIVO DEL CORSO:	Sviluppare competenze metodologiche, analitiche e strategiche per interpretare e gestire le dinamiche che caratterizzano le organizzazioni complesse e statuali, con particolare attenzione al settore della sicurezza e difesa. Il corso mira a rafforzare le capacità decisionali e manageriali del personale dirigente, promuovendo una visione olistica e sistemica che valorizzi la funzione logistica come leva fondamentale per la resilienza del sistema Paese.				
AREE DISCIPLINARI	**ARGOMENTO**	**SSD**	**DOCENTE**	**PERIODI**	**DATA**
Il Sistema di difesa nazionale (23 periodi)	La logistica interforze nel sistema di difesa nazionale. Industria e logistica 5.0.	IEGE-01/A	Col. Stefano Panoni - Dott.ssa Hristina MITANOSKA	4	10/10/2025
	Le Forze Armate nel sistema di difesa nazionale.	GSPS-02/A	Col. Roberto FORLANI	2	10/10/2025
	I centri di Comando e Controllo Unificati.	IEGE-01/A	CV RIZZOTTO	1	10/10/2025
	Il sistema nazionale di difesa civile.	GSPS-02/A	VICE PREFETTO Riccardo MATTEI	1	10/10/2025
	Il sistema nazionale di difesa civile.	GSPS-02/A	VICE PREFETTO Riccardo MATTEI	2	17/10/2025
	Il sistema di informazione per la sicurezza della Repubblica.	GSPS-02/A	Gen. Paolo POLETTI	8	14/11/2025
	Il Sistema nazionale della protezione civile e meccanismo unionale.	GSPS-02/A	DNPC	5	28/11/2025
Caratterizzazione e mitigazione della minaccia (20 periodi)	Minacce Antropiche.	GSPS-02/A	Dr. Alessandro Maria PESSOLANO	2	17/10/2025
	Criticità naturali.	GEOS-04/C	Dott.ssa Ilaria MAZZINI	4	17/10/2025
	Risk Assessment, metodologie di identificazione, analisi e valutazione del rischio operativo.	ECON-07/A	Col. Alfredo RUSSO	1	21/11/2025
	Minacce alla sicurezza nazionale fisiche e cibernetiche.	GSPS-02/A	ACN	2	24/10/2025
	Cyber Legad.	GSPS-02/A	Col. Valentina CAPURRO	2	31/10/2025
	Il Cognitive Warfare.	GSPS-02/A	Col. Antonio DI LEONARDO	1	05/12/2025
	Il Cognitive Warfare.	GSPS-02/A	Col. Antonio DI LEONARDO	1	12/12/2025
	Digital services act.	GIUR-03/A	ACN	1	12/12/2025
	Reputational risk management.	ECON-07/A	Community Group	6	12/12/2025
La funzione logistica per la difesa e la resilenza delle organizzazioni complesse e statuali (55 periodi)	Risk Management & Business Continuity Management.	ECON-07/A	Prof. Fabio NONINO	4	24/10/2025
	Direttiva europea 2008/114/CE, individuazione e designazione delle infrastrutture critiche.	GIUR-03/A	Col. Valentina CAPURRO	2	24/10/2025
	Disaster management, Critical Infrastructure Management Tecniche di analisi del rischio e competenze multidisciplinari.	ECON-07/A	Prof. PATRIARCA Prof.ssa STEFANA	4	31/10/2025
	La pianificazione territoriale e gli eventi incidentali Na-Tech.	ECON-07/A	Prof.ssa STEFANA	2	31/10/2025
	Big data e intelligenza artificiale quale strumento per l'analisi predittiva.	IEGE-01/A	ACN	3	07/11/2025
	Data literacy e Block chain management quale supporto decisionale e operativo.	IEGE-01/A	ACN	2	07/11/2025
	L'intelligenza artificiale a servizio della difesa degli obiettivi sensibili, il monitoraggio e l'analisi predittiva delle criticità.	IEGE-01/A	ACN	3	07/11/2025
	Cyber threat intelligence per la difesa delle infrastrutture critiche.	ECON-07/A	Ing. Vincenzo VERDE	4	21/11/2025
	Il Golden Power quale strumento a tutela degli asset strategici del Paese.	GIUR-03/A	Col. Luca Gennaro CIOFFI	2	21/11/2025
	La norma ISO 27002, il ciclo Plan-Do-Check-Act (PDCA).	GIUR-03/A	ACN	3	05/12/2025
	Due diligence ambiti e applicazione.	ECON-07/A	Community Group	6	19/12/2025
	Recovery Fund.	ECON-07/A	Prof. GIAGNORIO	4	09/01/2026
	Vulnerability Assessment metodologie per identificare.	IEGE-01/A	Prof. Pierluigi LOCATELLI	4	23/01/2026
	Le transizioni digitali e ambientali: relazioni interpersonali, logistica e trasporti. Uno studio di futures studies su guerra cognitiva e sicurezza nazionale.	IEGE-01/A	Prof. Alessandro STERPA	2	23/01/2026
	Positioning Navigation & Timing: una funzione critica per la logistica.	IEGE-01/A	Col. Marco BELOGI	2	23/01/2026
	Positioning Navigation & Timing: una funzione critica per la logistica. Infrastrutture critiche e dati geospaziali.	IEGE-01/A	Col. Marco BELOGI	4	30/01/2026
	Gli "hot topics" della logistica: AI & Digitalizzazione, Intermodalità e Sostenibilità, Ex Works e Supply Chain Disruption.	IEGE-01/A	Prof. Pietro SPADACCINI	4	30/01/2026
				98	

SSD	Periodi	CFU
ECON-07/A	31	4
GEOS-04/C	4	1
GIUR-03/A	8	1
GSPS-02/A	26	4
IEGE-01/A	29	5
	98	**15**

Allegato "D"

CORSO DI ALTA FORMAZIONE IN STRATEGIE DI DIFESA E RESILIENZA DI ORGANIZZAZIONI COMPLESSE E STATUALI

PIANO GENERALE DEI COSTI

DENOMINAZIONE	DISPONIBILITA'	TARIFFA SALA	NUMERO GIORNATE DI UTILIZZO	TOTALI
	POSTI DISPONIBILI	**€/giorno* a max disponibilità**	**GIORNI**	
SALA VERDE/GIALLA	24	€ 800,00	15	€ 12.000,00

SPESE PER UTILIZZO AULA DIDATTICA

DENOMINAZIONE	VALORE
DOCENZE	€ 3.021,30

COSTI STIMATI PER LE DOCENZE

€ 67,14 costo orario
45 ore a pagamento

DENOMINAZIONE	VALORE LORDO	NUMERO GIORNATE DI UTILIZZO	TOTALE
COSTO STRAORDINARIO PERSONALE Ce.FLI**	€ 97,36	15	1.460

STRAORDINARI PERSONALE A SUPPORTO

* I costi sono stati formulati sulla base del prezzo medio di mercato

** Colonnello, Ten. Col., 1° LGT

verrà impiegato un dirigente (€ 31,77 lordo) e un SU (€ 16,91) per 2 ore pro capite di straordinario in quanto il CAF è concomitante con altre attività previste in svilgimento il venerdì su cui saranno distribuiti gli ulteriori costi di stroridnario.

TOTALE COSTI	€ 16.481,70
PREZZO DI ISCRIZIONE (STIMA SU 30 FREQUENTATORI)	**€ 549,39**