Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

MINISTERO DELLA DIFESA

Piano Nazionale di Ripresa e Resilienza (PNRR)
Missione 1 – Componente 1 – Asse 1
Investimento 1.5: CYBERSECURITY
CUP: D46G21002310006

PIANO OPERATIVO

MINISTERO DELLA DIFESA

Nuove soluzioni basate su integrazione di sistemi di monitoraggio cibernetico con sistemi C2, potenziamento SCADA e realizzazione Centro di Valutazione della Difesa.

Revisione Maggio 2024

Digitally signed by GIOVANNI GAGLIANO
Date: 2024.05.10 14:18:04 CEST

Sommario

1 Introduzione ... 3
2 Descrizione del progetto ... 3
2.1 Obiettivi ... 3
2.2 Rispetto dei principi trasversali ... 4
3 Modalità operative ... 4
4 Piano progettuale di dettaglio ... 5
4.1 Irrobustimento delle capacità di Cyber Defence della Difesa ... 5
4.1.1 Identificazione Interventi ... 5
4.1.2 Soluzione Tecnologica ... 6
4.2 Integrazione del dominio *cyber* nei sistemi di Comando e Controllo della Difesa ... 8
4.2.1 Identificazione Interventi ... 8
4.2.2 Soluzione Tecnologica ... 8
4.3 Acquisizione di capacità di protezione cyber per dispositivi OT/IoT ... 9
4.3.1 Identificazione Interventi ... 9
4.3.2 Soluzione Tecnologica ... 9
4.4 Acquisizione di una piattaforma di supervisione dedicata ai sistemi SCADA ... 10
4.4.1 Identificazione Interventi ... 10
4.4.2 Soluzione Tecnologica ... 11
4.5 Realizzazione Centro di Valutazione della Difesa ... 11
5 Tempi e costi di realizzazione ... 12
6 Integrazione con altri interventi ... 22

1 INTRODUZIONE

In accordo con le linee guida elaborate dalla Commissione Europea per l'elaborazione del Piano Nazionale di Ripresa e Resilienza (PNRR) della Pubblica Amministrazione, il Ministero della Difesa ha identificato specifiche aree di intervento, ovvero attività e temi correlati, finalizzati a migliorare le predisposizioni di sicurezza informatica e che formano un pacchetto coerente di misure complementari per il potenziamento delle capacità *Cyber Defence*. Le componenti hanno un grado di dettaglio sufficiente ad evidenziare le interconnessioni tra le diverse misure in esse proposte a salvaguardia delle catene del valore e delle infrastrutture critiche, nonché garantire l'accesso alle risorse di importanza strategica e proteggere i sistemi di comunicazione. Il progetto vede come direttrici la piena adesione al Codice dell'Amministrazione Digitale (CAD), alle regole per la semplificazione e la trasparenza, alle Misure Minime di Sicurezza emesse dall'AgID, alla definizione del Perimetro di Sicurezza Nazionale, alla protezione dei dati secondo il GDPR fino alla strategia nazionale cloud. Gli interventi previsti sono orientati alla razionalizzazione, al consolidamento, alla resilienza e alla convergenza dei sistemi informativi e delle infrastrutture di sicurezza in chiave interforze, al monitoraggio delle applicazioni e dei servizi in linea con la frontiera tecnologica, all'adeguamento normativo dei sistemi informativi (es. GDPR, NIST, ecc.), al consolidamento delle capacità di risposta/contenimento agli attacchi cibernetici rivolti verso le infrastrutture critiche strategiche della Difesa.

Si evidenzia che le attività descritte nel seguito sono in linea con le attività previste dal "Piano Operativo PNRR M1C1-I1.5" elaborato dall'Agenzia Cybersecurity Nazionale (ACN) nell'ambito dell'Accordo tra Presidenza del Consiglio dei Ministri-Dipartimento della Transizione Digitale (PCM-DTD) ed ACN stessa. In particolare, le attività dell'AD rientrano nell'ambito delle attività tecniche e nelle tempistiche previste per le Milestone e Target che l'ACN deve rispettare in qualità di soggetto attuatore della misura PNRR M1C-I1.5.

Come evidenziato nell'Accordo ACN-AD i fondi assegnati all'AD per le attività del presente Piano Operativo sono in totale 49.250.000,00 Euro.

2 DESCRIZIONE DEL PROGETTO

2.1 OBIETTIVI

Dal 2012, il Ministero della Difesa ha intrapreso alcune iniziative di consolidamento degli assetti di protezione cyber con interventi finalizzati ad introdurre delle capacità iniziali di contrasto alla minaccia cibernetica e ad affrontare in maniera puntuale le criticità di volta in volta identificate.

Il tema della difesa cibernetica è trattato in diverse parti del documento programmatico pluriennale per la Difesa per il triennio 2019-2021 e ripreso successivamente all'interno delle Linee programmatiche Difesa presentate in audizione congiunta Camera e Senato dal Ministro della Difesa L. Guerini e nel concetto strategico del Capo di Stato Maggiore della Difesa.

Si prevede di utilizzare l'ambiente cibernetico sia per compiti operativi che di

supporto, potenziando le capacità *cyber* difensive, di resilienza, di deterrenza e di risposta/contenimento agli attacchi informatici, al fine di assicurare la libertà di manovra della componente militare nazionale nel dominio e concorrere, con gli altri Dicasteri, alla prevenzione e al contrasto dei possibili attacchi ai sistemi di comunicazione e informazione di rilevanza strategica per gli interessi nazionali e alle infrastrutture critiche.

Il Comando per le Operazioni in Rete (COR), in coordinamento con le componenti specifiche di F.A., dovrà essere in grado di gestire, con visione unitaria e coerente, la condotta tecnico-operativa, lo sviluppo armonico e la protezione delle capacità relative all'*Information Communication Technology* (includendo anche la distribuzione dei servizi di comunicazioni satellitari della Difesa) e di quelle dedicate alle attività operative nel dominio cyber.

2.2 RISPETTO DEI PRINCIPI TRASVERSALI

Le attività del progetto dell'AD, che sono parte dell'Intervento complessivo M1C1-I1.5 dell'ACN, si pongono rispetto ai principi trasversali previsti dal PNRR come segue:

- *Climate and Digital Tagging*: il progetto AD supporterà la creazione di un ecosistema digitale nazionale con elevate garanzie di cybersicurezza.
- Equità di Genere: le iniziative nell'ambito del progetto AD sono tese a valorizzare e fornire nuove opportunità alle donne in ambito cybersicurezza per garantire la parità di genere.
- Valorizzazione e protezione dei giovani: le iniziative nell'ambito del progetto AD sono tese a valorizzare e fornire nuove opportunità ai giovani, quali ad esempio il supporto allo sviluppo di nuove iniziative di innovazione tecnologica in ambito cybersicurezza.
- Riduzione divari territoriali: il progetto AD prevede la creazione di laboratori (Fissi e Mobili) specializzati distribuiti sul territorio che permetteranno la riduzione dei divari territoriali presenti tra le regioni del paese.
- *Do Not Significant Harm* (DNSH): il progetto AD non presenta impatti significativi sull'ambiente. L'acquisizione delle risorse informatiche necessarie alla realizzazione dei laboratori e dei mezzi tattici rispetteranno le garanzie di efficienza energetica indicate dalle normative europee.

3 MODALITÀ OPERATIVE

L'AD intende costituire una struttura tecnica che assicuri un adeguato coordinamento, controllo e monitoraggio di tutte le attività connesse alle progettualità del presente Piano Operativo.

In tale contesto, si prevede di istituire una *governance* di missione, facente capo al Capo di Stato Maggiore della Difesa in qualità di "Soggetto sub-attuatore" nei confronti di ACN e al Sottocapo di Stato Maggiore della Difesa delegato alla firma degli Accordi Attuativi con l'Agenzia di Cybersicurezza Nazionale; tale *governance* di missione è guidata dal VI Reparto dello Stato Maggiore della Difesa (SMD), con il Capo del VI Reparto di SMD/Responsabile per la Transizione al Digitale (RTD) della Difesa, quale

referente, e si concretizza con la costituzione di un apposito Gruppo di Lavoro (GdL) composto da personale designato dalle varie articolazioni competenti a vario titolo sia dell'Area tecnico-operativa, sia dell'Area tecnico-amministrativa. In tale ambito, per garantire una continuità nello sviluppo dei progetti, si valuterà la possibilità di integrare il GdL con risorse mirate e dedicate, con provata esperienza nel settore tecnico e amministrativo, da collocare a presidio delle specifiche attività nelle diverse articolazioni coinvolte anche verificando la possibilità di acquisire un supporto esterno nello sviluppo delle progettualità, soprattutto per rinforzare le dotazioni organiche di natura amministrativa della stazione appaltante (almeno 3 unità), ricorrendo agli accantonamenti di fondi previsti per il Ministero Difesa dall'art. 16 del D.L. 31 maggio 2021, n. 77.

4 PIANO PROGETTUALE DI DETTAGLIO

Le attività del presente Piano Operativo posso essere suddivise nell'ambito delle seguenti 5 macro-aree tematiche di intervento:

- Irrobustimento delle Capacità di Cyber Defence della Difesa
- Integrazione del Dominio Cyber nei Sistemi di Comando e Controllo della Difesa
- Acquisizione di Capacità di Protezione Cyber per Dispositivi OT/IoT
- Acquisizione di una Piattaforma di Supervisione dedicata ii Sistemi SCADA
- Realizzazione Centro di Valutazione Della Difesa

Nel seguito saranno descritti dettagli tecnici delle 5 aree evidenziando i possibili interventi operativi e le soluzioni tecnologiche che si prevede di adottare per realizzare gli interventi stessi.

4.1 IRROBUSTIMENTO DELLE CAPACITÀ DI CYBER DEFENCE DELLA DIFESA

4.1.1 Identificazione Interventi

L'intervento prevede un programma pluriennale di Potenziamento delle capacità di Protezione Cibernetica della Difesa consentendo di perseguire i seguenti obiettivi strategici:

- Potenziare le attuali capacità di *Cyber Defence* garantendo la coerenza e la interoperabilità con i sistemi NATO, innalzando il livello di resilienza e sicurezza delle infrastrutture della Difesa, creando al contempo un ambiente in grado di recuperare velocemente i danni derivanti da attacchi *cyber*. In tale quadro, dovrà essere garantito per l'intero infodominio della Difesa, il rispetto delle Misure Minime di Sicurezza dell'AGID e dei requisiti di sicurezza stabiliti dal DL 105/2019 che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica, per i beni ICT della Difesa che saranno inseriti.
- Supportare il potenziamento della risposta/contenimento e resilienza ad atti *cyber* ostili, mediante l'ampliamento degli strumenti di comando e controllo delle attività operative nel dominio *cyber*. A tale scopo risulta necessario avviare l'acquisizione di strumenti tesi a rafforzare la *Cyber Operational Picture* necessaria alle attività di pianificazione e condotta operativa di attività funzionali a verificare la postura di sicurezza del dominio *cyber* e ad incrementare la *Cyber Situation Awareness*.

- Potenziare le attività di formazione, addestramento e diffusione della "cultura" in ambito cibernetico. Tale potenziamento sarà attuato mediante l'accrescimento qualitativo e quantitativo delle figure professionali interne specializzate, con l'adozione di strumenti avanzati che sfruttino innovative capacità di intelligenza artificiale (*Cyber Range*), e attraverso un programma formativo/addestrativo di *Cyber Security Awareness* (CSA), a favore del personale dell'intero comparto Difesa non impiegato nello specifico settore, finalizzato ad adeguare le conoscenze di base in materia cibernetica all'attuale quadro di minaccia presente sulle reti globali, anche in considerazione della costante evoluzione che caratterizza questa tipologia di minaccia.

4.1.2 Soluzione Tecnologica

Per quanto riguarda il potenziamento delle attuali capacità cyber, gli interventi per potenziare le attuali capacità di *Cyber Defence*, si concretizzeranno in attività di potenziamento/consolidamento di quanto realizzato finora sull'infrastruttura ICT della Difesa, mediante:

- Reingegnerizzazione degli applicativi: incremento di sicurezza, performance, resilienza e "gestibilità" degli applicativi centralizzati della Difesa, utilizzando tecnologie in grado di realizzare gli stessi applicando i principi di *cyber security* by *design*.
- Protezione perimetrale: incremento della protezione dell'infostruttura della Difesa da attacchi esterni e/o minacce di natura cyber;
- Misure di Sicurezza: risoluzione delle criticità delle reti della Difesa emerse dalla valutazione dello stato dell'infrastruttura ICT (*self assessment*);
- Migrazione alla nuova infrastruttura dominio utenti e FF.AA.: migrazione delle utenze (utenti e PdL) in una nuova architettura di Active Directory (AD), che porterà ad una gestione più sicura delle credenziali, degli accessi e dei servizi core erogati in ambito Difesa.

Per quanto riguarda il potenziamento degli strumenti di Comando e Controllo, lo sviluppo delle relative capacità dovrà prevedere l'evoluzione del *software* CyCOP già disponibile presso il Comando per le Operazioni in Rete (COR) nella versione 1.0.

Il progetto, nel suo complesso, mira ad avviare il processo di integrazione di ulteriori funzionalità al citato *software* CyCOP, attraverso l'acquisizione di moduli abilitanti alla resa di una più coerente *Cyber Operational Picture* a favore del Reparto *Cyber Operations* del COR.

Nello specifico si provvederà all'acquisizione dei seguenti moduli:

- modulo CMDB, che costituirà il *repository* contenente i dati sia dell'infrastruttura IT da "analizzare" (istanza RED), sia quelli relativi all'infrastruttura attraverso il quale verranno condotte le suddette azioni di analisi e valutazioni di sicurezza (istanza BLUE). All'interno di tale modulo saranno contenuti i dati caratterizzanti gli *asset* di missione, gli *asset* di rete, le configurazioni operative necessarie, i dati di geolocalizzazione e i sistemi di Comando e Controllo adoperati e sarà

interrogabile dagli altri moduli componenti del *software* CyCOP per reperire dati e informazioni su specifici *asset*;

- modulo di integrazione con il *software* CyCOP deputato a garantire lo scambio bidirezionale di informazioni tra il modulo CMDB e i restanti moduli della piattaforma, al fine di rendere impiegabili i dati contenuti nelle citate due istanze durante lo svolgimento delle attività di verifica;
- interfaccia abilitata all'inserimento dei dati relativi ai citati *asset* che garantisca il popolamento del modulo CMDB in modalità automatica e/o manuale da parte di un operatore.

Relativamente al potenziamento delle attività di formazione, addestramento e diffusione della cultura cibernetica, la Difesa ha avviato nel 2018, nell'ambito del Piano Nazionale di Ricerca Militare (PNRM), il progetto di ricerca tecnologica "UNAVOX", per lo sviluppo di un prototipo di *Cyber Range* presso la Scuola Telecomunicazioni Militari di Chiavari. Il piano di implementazione del progetto, articolato in tre spire successive, è stato ultimato nel 2021 con il rilascio conclusivo di un poligono virtuale.

Nel 2021, SMD, con il progetto *Cyber Range* 1.0, ha conferito a TELEDIFE il mandato di far evolvere il sopracitato poligono potenziandone le capacità operative nei settori della formazione e dell'addestramento *cyber* a favore del personale della Difesa.

Con il presente Piano Operativo, la Difesa intende avviare un'ulteriore fase di consolidamento e potenziamento della capacità previste nel *Cyber Range* 1.0 che ne completi le funzionalità per la simulazione di scenari ed erogazione moduli formativi maggiormente complessi ed il loro facile impiego per le esigenze formative ed addestrative della Difesa.

Tale poligono virtuale consolidato e potenziato potrà essere impiegato anche a favore di altre amministrazioni, ovvero in contesti multinazionali, quali quello dell'iniziativa dell'EU che prevede la federazione dei *Cyber Range* dei Paesi aderenti.

In aggiunta, al fine di accrescere la consapevolezza generale del personale impiegato presso il Dicastero su tematiche di sicurezza cibernetica, addestrandolo al contempo ai corretti comportamenti da adottare in caso di attacchi di *phishing*, verrà acquisita una soluzione di *Cybersecurity Awarness* e *Phishing Simulation* da impiegare presso l'Area di Vertice Interforze e presso le singole F.A.. Verrà quindi strutturato un percorso formativo trasversale sulle principali tematiche di sicurezza cibernetica, erogato in modalità ibrida (sincrona e/o asincrona), con sessioni di valutazione individuale e collettiva, supportato da campagne di *Phishing* simulato e controllato, per il quale saranno resi disponibili appositi documenti di report che potranno essere importati nei sistemi di gestione del personale e della formazione dell'Amministrazione Difesa.

4.2 INTEGRAZIONE DEL DOMINIO *CYBER* NEI SISTEMI DI COMANDO E CONTROLLO DELLA DIFESA

4.2.1 Identificazione Interventi

Per le piattaforme di Comando e Controllo (C2) (sistemi strategici e operativi), i sistemi di combattimento (sistemi tattici) ed i sistemi di comunicazione (compresi quelli satellitari), le Forze Armate sono certamente chiamate, come chiunque utilizzi sistemi digitali per le proprie attività operative, ad analizzare le architetture informatiche abilitanti, per misurarne i livelli di sicurezza e resilienza. Tutti i sistemi militari evolvono verso operazioni in ambienti net-centrici e devono poter mantenere il più possibile inalterate le capacità, ai fini del raggiungimento degli obiettivi di missione. Per soddisfare questa esigenza occorre progettare architetture e sistemi resilienti in ambiente *cyber* ostile.

Inoltre, i sistemi di Comando e Controllo dovranno essere caratterizzati dalla capacità di utilizzare efficacemente l'ambiente cibernetico sia per compiti operativi, che di supporto, potenziando le capacità *cyber* difensive, di resilienza, di deterrenza e di risposta/reazione agli attacchi informatici, al fine di assicurare la libertà di manovra della componente militare nazionale nel dominio *cyber*.

Negli attuali scenari (strategico, operativo e tattico), i sistemi di Comando e Controllo, ad oggi, per gli aspetti relativi alle capacità di sorveglianza e protezione, non includono la dimensione di *Cyber Security* delle piattaforme che includono componenti IT (*Information Technology*) e OT (*Operational Technology*) come, ad esempio, quelle deputate al controllo dei sistemi di automazione delle basi militari o delle navi e dei sistemi *embedded* nell'armamento.

Attualmente le soluzioni di comando e controllo sono consolidate a partire dagli anni 90 e si estendono dal supporto alla decisione umana fino alla gestione automatizzata delle procedure operative. Sono state progettate per operare nel dominio dello spazio cinetico e nel dominio dello spazio elettromagnetico. I nuovi scenari richiedono di dotare i sistemi di C2 con capacità di risposta, robustezza e resilienza alle minacce nel dominio cibernetico, e richiedono necessariamente la capacità di testarli ai fini della resistenza a eventuali attacchi informatici portati dall'avversario.

4.2.2 Soluzione Tecnologica

In tale scenario, attraverso il presente Piano Operativo, la Difesa intende colmare tale gap attraverso due interventi "verticali":

- acquisizione di una capacità di Pianificazione e Condotta Operativa (C2[1]) delle attività *di Red Teaming"* (identificata "*C2Red*") tipica dell'approccio di "*offensive security*" per la verifica della postura di sicurezza del dominio *cyber* della sua Infostruttura. Le capacità che dovranno essere rilasciate attraverso tale soluzione avranno come obiettivo primario la realizzazione di un sistema di valutazione sulla capacità di protezione degli *Asset* interni al Dicastero e, in eventuale aggiunta, potranno essere rese disponibili ad altri Dicasteri/Organizzazioni

[1] Comando e Controllo

(approccio *dual-use*) al fine di verificare la loro postura di sicurezza delle reti e dei sistemi informativi.
Nello specifico quindi, tale soluzione dovrà essere in grado di permettere di assolvere ai compiti di valutazione approfondita della capacità di resilienza dell'infostruttura in esame rispetto ad un attacco *cyber*, sfruttando scenari di emulazione concreta di una minaccia *cyber* realistica.

- Rafforzamento della sicurezza cibernetica sulle comunicazioni satellitari militari, attraverso l'implementazione architetturale di apparati *Modem Transec*[2] sulle tratte di comunicazioni satellitari, abilitati alla funzione di monitoraggio e controllo da remoto. In aggiunta, al fine di garantire il contestuale irrobustimento della sicurezza cibernetica sulle componenti di Comando e Controllo asservite alle comunicazioni satellitari, sarà prevista l'implementazione di una soluzione di gestione centralizzata dei *Log* di sicurezza generati dai citati apparati. La raccolta di tali informazioni verrà resa disponibile alle strutture di *Cyber Defence* della Difesa.

4.3 ACQUISIZIONE DI CAPACITÀ DI PROTEZIONE CYBER PER DISPOSITIVI OT/IOT

4.3.1 Identificazione Interventi

La trasformazione digitale impone la gestione e visibilità della rete, il rilevamento delle minacce e l'insight operativo anche per ambienti OT e IoT, per consentire di affrontare l'*escalation* dei rischi informatici e aiutare a garantire un'elevata resilienza e affidabilità nel monitorare e controllare una varietà di infrastrutture critiche che forniscono servizi critici ed essenziali. La crescente integrazione delle tecnologie informatiche nell'ambito OT/IoT e l'estensione della connettività delle organizzazioni fra sedi remote mediante le reti pubbliche, hanno accresciuto l'esposizione a una sempre più ampia gamma di problemi di sicurezza. Affrontare questi problemi è una grande sfida perché le soluzioni di sicurezza devono rispondere a peculiari vincoli tecnologici e operativi che caratterizzano tale ambito.
La strategia di cybersicurezza Nazionale e le direttive di settore, quali la NIS, stanno affrontando la definizione di prescrizioni volte a porre in sicurezza anche gli ambienti OT/IoT in considerazione del potenziale notevole impatto sul sistema socio-economico in caso di incidente cyber.
Anche in ambito militare, si rende necessaria delle capacità di *cybersecurity* e *defence* per rendere possibile la gestione sicura di ambienti integrati IT e OT/IoT, garantendone resilienza e protezione.

4.3.2 Soluzione Tecnologica

La soluzione tecnologica prevede l'estensione della capacità dei sistemi di monitoraggio della sicurezza, in modo da monitorare e gestire gli ambienti OT/IoT attraverso *agent* e sonde opportunamente inserite nella rete e nei *device/end point*, in modo da avere l'analisi del contesto in tempo reale e permettere la gestione della sicurezza.

[2] *Transmission Security* - processo per impedire che le trasmissioni di dati vengano infiltrate, sfruttate o intercettate da un individuo, un'applicazione o un dispositivo.

A tale fine occorre certificare l'identità dei dispositivi OT/IoT per garantire che ogni oggetto sia realmente quel che dice di essere, sia autorizzato a trovarsi in una data rete e sia legittimato a dialogare con determinate altre macchine, sensori o oggetti connessi.

L'implementazione della sicurezza OT/IoT in ambito Difesa sarà ottenuta mediante i seguenti interventi:

- Integrazione di soluzioni di sicurezza nei dispositivi di tipo "mobile";
- Realizzazione del sistema APN Difesa, mediante la attivazione di una rete virtuale estendibile anche sulle infrastrutture radiomobili dei *provider* commerciali di telefonia mobile, intervento complementare all'iniziativa di *"Realizzazione di un'infrastruttura Radio-Mobile LTE 4G e 5G della Difesa"*, finanziata con risorse Difesa e parte funzionalmente integrante del presente Piano Operativo, in quanto la disponibilità di nodi di comunicazione Radio-Mobile, configurando questi un asse proprietario di connettività, costituisce la infrastruttura di base indispensabile per la necessaria interoperabilità (roaming) con le reti dei differenti provider commerciali.

  La implementazione di un servizio *Access Point Name* di tipo privato consente di rafforzare in modo determinante la sicurezza delle modalità di accesso alla rete INTERNET per mezzo dei *device* di telefonia mobile impiegati dal personale appartenente alla Difesa, ove costoro si connettano alle reti LTE 4G e 5G gestite da *provider* commerciali. L'acceso in parola sarà, infatti, gestito presso il Comando Operazioni di Rete della Difesa assicurando agli utenti Interforze e delle Forze Armate un *gateway* verso la rete INTERNET, controllato e protetto per mezzo delle architetture di sicurezza logica già in esercizio. La possibilità degli utenti della Difesa di accedere alle risorse delle reti dati pubbliche attraverso il servizio APN privato, al fine di perseguire livelli di esercizio sicuri, affidabili e resilienti adeguati, costituisce una finalità operativa imprescindibile in considerazione della diffusione della fruizione di servizi in mobilità.

4.4 ACQUISIZIONE DI UNA PIATTAFORMA DI SUPERVISIONE DEDICATA AI SISTEMI SCADA

4.4.1 Identificazione Interventi

Un moderno Sistema d'arma, dal punto di vista funzionale, va visto come una complessa architettura informatizzata costituita da *software*, *firmware*, *hardware*, non isolata, ma che interagisce pianamente con il mondo circostante attraverso le sue componenti di comunicazione ed i suoi sensori.

Il crescente impiego di tecnologie informatiche nei sistemi d'arma determina, pertanto, l'esigenza di verificare la rispondenza al requisito di *cyber resilience* analizzando la capacità di resistere a tentativi di interdizione, inganno e acquisizione del controllo da parte di possibili avversari.

In tale ottica occorre agire sulle numerose componenti che generalmente compongono tali sistemi complessi:

- Sensoristica (integrata o esterna);
- Componente di Comando e Controllo;

- Componente di Comunicazione;
- Componenti ausiliarie (ad es. Lanciatori, piattaforme di guida dei vettori, strumenti di controllo dei *payload* ecc.).

Infatti, più che in altri Sistemi complessi, nei Sistemi d'arma le vulnerabilità di alcuni componenti possono rompere equilibri compromettendo irrimediabilmente l'intero Sistema.

4.4.2 Soluzione Tecnologica

La soluzione tecnologica da adottare dovrà essere basata su *standard* internazionali di riferimento, architetture consolidate e dovrà considerare aspetti di *Secure by Design*, *Secure by Configuration* e *Secure by Monitoring*.

4.5 Realizzazione Centro di Valutazione della Difesa

A seguito dell'istituzione del Perimetro di Sicurezza Nazionale Cibernetica (Decreto Legge 105/2019, convertito in Legge 133/2019, e atti discendenti), e con la successiva costituzione dell'Agenzia per la Cybersicurezza Nazionale (Decreto Legge 82/2021, convertito in Legge 109/2021), al Ministero della Difesa sono state conferite nuove funzioni e responsabilità nell'ambito del dominio *cyber*.

In particolare il Centro di Valutazione della Difesa:

- con la citata legge 109/2021 è accreditato ed ha una delega generale, in qualità di organismo di valutazione della conformità, alle valutazione ed al rilascio di Certificati Europei di sicurezza cibernetica di livello di affidabilità "elevato" (il massimo tra i 3 livelli previsti) per i sistemi di rispettiva competenza;
- con la legge 133/2019, è stato individuato quale Ente competente per la trattazione delle pratiche del proprio Ministero che coinvolgono beni ICT inseriti a Perimetro. In tale contesto, il Centro di Valutazione della Difesa, per i sistemi di propria competenza e analogamente a quanto previsto per il Centro di Valutazione e Certificazione Nazionale istituito presso l'Agenzia per la Cybersicurezza Nazionale, potrà condurre la fase di Verifiche Preliminari ed imporre test e condizioni da inserirsi come clausole contrattuali nelle procedure di *procurement* e successivamente la fase di Valutazione e conduzione dei test per l'approvazione e l'eventuale imposizione di prescrizioni all'impiego del prodotto individuato durante la procedura di affidamento.

Per quanto precede, il Centro di Valutazione della Difesa dovrà dotarsi, oltre al già esistente laboratorio Class per le valutazioni sotto schema classificato, di una struttura organica e infrastrutturale idonea al funzionamento dei laboratori per lo svolgimento delle attività di cui alle precedenti alinee, accreditati rispettivamente da ACN (laboratorio PNSC) e Accredia (laboratorio di Certificazione Europea). Il laboratorio PNSC, in particolare, dovrà dotarsi di ambienti e strumenti idonei alla verifica e valutazione dei sistemi e servizi afferenti a ciascuna delle 4 categorie incluse nel perimetro, quali: HW/SW per le reti di telecomunicazioni, HW/SW per la sicurezza delle reti di telecomunicazioni, HW/SW di monitoraggio/controllo per reti di telecomunicazioni e sistemi industriali, SW per l'implementazione dei meccanismi di sicurezza. È prevista inoltre la creazione di un sito secondario con funzioni di *Back-Up* per il laboratorio

EUCC. Per il laboratori PSNC, in considerazione delle tempistiche stringenti imposte dalle norme per le attività di Verifica e Valutazione, è previsto che il sito secondario, oltre a garantire funzioni di *Back-Up* e *Disaster Recovery*, possa essere impiegato quale eventuale alternato al laboratorio del Centro.
L'intervento da effettuare dovrà, quindi, rispondere a tutti i requisiti richiesti dalle norme nazionali e europee e agli *standard* internazionali di riferimento e, in particolare, prevedere:

- adeguate predisposizioni infrastrutturali;
- l'allestimento di idonei laboratori;
- l'acquisizione e messa in opera di materiale hardware e software idoneo per la costituzione del sito di *Disaster Recovery*, dedito allo stoccaggio di copie di backup del materiale informativo (*storage*) prodotto durante l'esercizio delle proprie funzioni;
- la creazione del sito secondario, ridondato, teso a garantire *High Availability*, in termini infrastrutturali, dei sistemi tecnologici a supporto e dei sistemi *hardware e software*;
- il potenziamento delle attività di formazione, addestramento e diffusione delle competenze necessarie a sostenere i processi di verifica e valutazione di sicurezza cibernetica, con l'obbiettivo dell'accrescimento sia qualitativo che quantitativo delle figure professionali specializzate coinvolte a tutti i livelli;
- l'accreditamento e la certificazione dei laboratori in linea con i quadri normativi di riferimento.

5 TEMPI E COSTI DI REALIZZAZIONE

I dettagli dei tempi e dei costi stimati per il raggiungimento dei target sono riportati nel diagramma GANNT riportato a seguito. Il grafico è suddiviso nelle 5 macro-aree d'intervento, che a loro volta sono ripartite in workpackage (WP), che rendono evidenti le finalità operative, descrivendo, per ogni intervento, le tempistiche previste definite in coerenza con le esigenze amministrative e di applicabilità tecnica riguardanti le singole imprese. Le attività di ogni WP comprendono il raggiungimento di obiettivi primari (analisi sistemistiche, individuazione delle soluzioni tecnologiche, applicabilità delle stesse e definizione dei requisiti), obiettivi secondari (perfezionamento delle procedure di acquisizione e avvio delle attività), esiti tangibili (conclusione delle forniture, compimento delle assistenze sistemistiche, consegna degli eventuali materiali, raggiungimento della operatività dei sistemi). La stima dei costi evidenziata nel GANTT si basa su valutazioni di pregressi interventi e su giudizio di esperti.
Di seguito al GANTT si trova la tabella con la descrizione di dettaglio degli interventi associati a ciascun workpackage.

Per la rendicontazione delle attività in parola ricorrendo a finanziamenti europei, la Difesa ha istituito una propria struttura organizzativa che prevede, tra l'altro, un funzionario delegato e una contabilità speciale unica per tutti i progetti d'interesse in ambito PNRR.

In termini di pianificazione finanziaria annuale, si riporta di seguito l'articolazione temporale prevista delle erogazioni in base alle previsione di esecuzione dei vari atti amministrativi di prevista stipula nell'ambito delle attività del presente PO.

Anno di riferimento	Erogazione prevista in Euro
2022	4.925.000,00
2023	4.500.000,00
2024	22.765.000,00
2025	10.690.000,00
2026	6.370.000,00
TOTALE	**49.250.000,00**

PNRR - INVESTIMENTO 1.5 CYBERSECURITY PER LA DIFESA (1.5)
"NUOVE SOLUZIONI BASATE SU INTEGRAZIONE DEI SERVIZI DI MONITORAGGIO CIBERNETICO CON SISTEMI C2, POTENZIAMENTO SCADA"
"ATTIVAZIONE DEL CENTRO DI VALUTAZIONE DELLA DIFESA"

TERMINE ACCORDO ACN AD

WORK PACKAGES (WP) OBIETTIVI PRIMARI: DEFINIZIONE REQUISITI, ANALISI COERENZA CON ALTRI WP SECONDARI: AVVIO ITER CONTRATTUALE ED INIZIO ATTIVITA' ESITI TANGIBILI: RAGGIUNGIMENTO RISULTATI OPERATIVI	GOVERNANCE DIFESA		2022				2023				2024				2025				2026				STIMA COSTI
	ITER TECNICO-AMM.VO	ESECUZIONE CONTRATTUALE	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
1 - Project Management	///	///				1,1								1,2			1,3						
IRROBUSTIMENTO DELLE CAPACITA' DI CYBER DEFENCE DELLA DIFESA																							
2 - Reingegnerizzazione Applicativi																							17.200.000,00 €
OBIETTIVO PRIMARIO 2.1	TELEDIFE	TELEDIFE (DDE) COR (ASSISTENTI)				2,1																	
OBIETTIVO SECONDARIO 2.2														2,2									
ESITI TANGIBILI 2.3																				2,3			
3 - Protezione perimetrale																							
OBIETTIVO PRIMARIO 3.1	TELEDIFE	TELEDIFE (DDE) COR / FA (ASSISTENTI)				3,1																	
OBIETTIVO SECONDARIO 3.2													3,2										
ESITI TANGIBILI 3.3																				3,3			
4 - Misure di Sicurezza ICT																							
OBIETTIVO PRIMARIO 4.1	TELEDIFE	TELEDIFE (DDE) FA (ASSISTENTI)				4,1																	
OBIETTIVO SECONDARIO 4.2														4,2									
ESITI TANGIBILI 4.3																				4,3			
5 - Migrazione nuova infrastruttura dominio utenti e FF.AA.																							
OBIETTIVO PRIMARIO 5.1	TELEDIFE	TELEDIFE (DDE) COR / FA (ASSISTENTI)				5,1																	
OBIETTIVO SECONDARIO 5.2											5,2												
ESITI TANGIBILI 5.3																				5,3			
6 - Capacità di pianificazione e condotta nel dominio cyber																							
OBIETTIVO PRIMARIO 6.1	TELEDIFE	TELEDIFE (DDE) COR (ASSISTENTI)				6,1																	
OBIETTIVO SECONDARIO 6.2													6,2										
ESITI TANGIBILI 6.3																				6,3			
7 - Formazione e addestramento cyber																							
OBIETTIVO PRIMARIO 7.1	TELEDIFE	TELEDIFE (DDE) COR (ASSISTENTI)				7,1																	
OBIETTIVO SECONDARIO 7.2													7,2										
ESITI TANGIBILI 7.3																	7,3						
INTEGRAZIONE DEL DOMINIO CYBER NEI SISTEMI DI COMANDO E CONTROLLO DELLA DIFESA																							
8 - Valutazione di sicurezza dei sistemi C2																							10.490.000,00 €
OBIETTIVO PRIMARIO 8.1	TELEDIFE	TELEDIFE (DDE) COR (ASSISTENTI)				8,1																	
OBIETTIVO SECONDARIO 8.2											8,2												
ESITI TANGIBILI 8.3																	8,3						
9 - Sicurezza delle componenti di gestione dei sistemi satellitari																							
OBIETTIVO PRIMARIO 9.1	TELEDIFE	TELEDIFE (DDE) COR / FA (ASSISTENTI)				9,1																	
OBIETTIVO SECONDARIO 9.2														9,2									
ESITI TANGIBILI 9.3																				9,3			
ACQUISIZIONE DI CAPACITA' DI PROTEZIONE CYBER PER I DISPOSITIVI OT/IOT																							
10 - Accesso alla rete e protezione dei dispositivi mobili																							7.520.000,00 €
OBIETTIVO PRIMARIO 10.1	TELEDIFE	TELEDIFE (DDE) COR (ASSISTENTI)				10,1																	
OBIETTIVO SECONDARIO 10.2													10,2										
ESITI TANGIBILI 10.3																				10,3			
11 - Realizzazione sistema APN della Difesa																							
OBIETTIVO PRIMARIO 11.1										11,1													
OBIETTIVO SECONDARIO 11.2														11,2									
ESITI TANGIBILI 11.3																				11,3			
ACQUISIZIONE DI UNA PIATTAFORMA DI SUPERVISIONE DEDICATA AI SISTEMI SCADA																							
12 - Protezione Sistemi di supervisione fisici (SCADA)																							4.790.000,00 €
OBIETTIVO PRIMARIO 12.1	TELEDIFE	TELEDIFE (DDE) COR / FA (ASSISTENTI)				12,1																	
OBIETTIVO SECONDARIO 12.2													12,2										
ESITI TANGIBILI 12.3																				12,3			
REALIZZAZIONE CENTRO DI VALUTAZIONE DELLA DIFESA																							
13 - Realizzazione Centro di Valutazione della Difesa UE						UE																	9.250.000,00 €
MILESTONE UE M1C1.7	TELEDIFE	TELEDIFE (DDE) SMD II/CEVA (ASSISTENTI)																					
MILESTONE UE M1C1.21														UE									
POTENZIAMENTO OPERATIVO INTEGRAZIONE TARGET																				UE			

OBIETTIVO PRIMARIO · OBIETTIVO SECONDARIO · ESITI TANGIBILI · UE MILESTONE UE · UE MILESTONE UE · UE OBIETTIVI POTENZIAMENTO COERENTI CON MILESTONE

TOTALE 49.250.000,00 €

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
1	*Project Management*				
Macro-Area 1: IRROBUSTIMENTO DELLE CAPACITÀ DI CYBER DEFENCE DELLA DIFESA					
2 <u>Reingegnerizzazione degli applicativi</u>	Incremento di sicurezza, performance, resilienza e "gestibilità" degli applicativi centralizzati della Difesa, utilizzando tecnologie in grado di realizzare gli stessi applicando i principi di *cyber security by design*.		**2.1**	Studio del disegno architetturale dei *software* applicativi oggetto di ammodernamento.	
			2.2	Sviluppo/conversione degli applicativi verso architettura a microservizi.	
			2.3	Implementazione sui sistemi in produzione e avvio operativo.	
3 <u>Protezione Perimetrale</u>	a) Predisposizione di una infrastruttura di *Business Continuity* per la federazione dei SIEM della Difesa. b) Predisposizione di una infrastruttura di *Business Continuity* per le sonde di ispezione del traffico		**3.1**	a) Studio architetturale infrastruttura di *Business Continuity* della federazione dei SIEM. b) Studio architetturale infrastruttura di *Business Continuity* della soluzione RSA Netwitness e acquisizione prima trance di materiale. c) Acquisizione prima trance di materiali e licenze per sistema Cortex XSOAR.	

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
	della tecnologia RSA Netwitness dell'A.D.. c) Acquisizione sistema di Security Orchestration, Automation and Response (SOAR) per la Marina Militare.		**3.2**	a) Acquisizione materiale per infrastruttura di *Business Continuity* della federazione dei SIEM. b) Acquisizione materiale per infrastruttura di *Business Continuity* della soluzione RSA Netwitness. c) Completamento equipaggiamento per piattaforma Cortex XSOAR.	
			3.3	a) b) Avvio operativo delle due infrastrutture di *Business Continuity.* c) Implementazione sistema, acquisizione supporto sistemistico e prima installazione piattaforma XSOAR.	
4 Misure di Sicurezza ICT	a) Gestione centralizzata dei *log* con valenza legale, comprensivo di adeguate procedure di *backup.* b) Adeguamento e armonizzazione delle procedure di gestione del rischio.		**4.1**	a) Studio architetturale su tecnologia da implementare per la gestione centralizzata dei *log*. b) Redazione procedura di *Backup* dei *log*. c) *Assessment* e *Gap Analysis* delle procedure da aggiornare. d) Installazione, customizzazione e formazione sulla piattaforma digitale automatizzata per	

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
	c) Acquisizione piattaforma digitale automatizzata per attività *di Risk Assessment & Management* per l'intero Dicastero. d) Miglioramento continuo dei processi del Sistema di Gestione per la Sicurezza dell'Informazione in uso presso il CERT Difesa. e) Implementazione del Web Application Firewall e di una soluzione di isolamento dati critici su rete Intranet AM.			le attività di *Risk Assessment & Management.*	
			4.2	a) Acquisizione materiali necessari alla tecnologia di gestione dei *log*. b) Redazione procedure di *Risk Management* e *Business Impact Analysis.* *c)* Supporto e manutenzione piattaforma digitale per le attività di *Risk Assessment & Management.* d) Acquisizione servizi professionali per miglioramento processi ISO 27001 del Sistema di Gestione per la Sicurezza dell'Informazione del CERT Difesa. e) Acquisizione e implementazione soluzione WAF AM.	
			4.3	a) Implementazione e avvio operativo infrastruttura di gestione centralizzata dei *log*. b) Formazione personale su procedure di *Risk Managemen*t e *Business Impact Analysis*.	

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
				c) Cessione definitiva della piattaforma, licenza perpetua per acquisizione del SW da parte della Difesa. e) Acquisizione e implementazione soluzione isolamento dati critici AM.	
5 Migrazione nuova infrastruttura dominio utenti e FF.AA.	Studio e realizzazione di una nuova infrastruttura di dominio e migrazione degli utenti.		**5.1**	Definizione del perimetro di intervento e studio architetturale.	
			5.2	Acquisizione materiale e servizi professionali per realizzazione e integrazione della nuova infrastruttura.	
			5.3	Migrazione utenti e servizi.	
6 Capacità di pianificazione e condotta nel dominio *cyber*	Acquisizione di moduli funzionali integrativi alla piattaforma CyCOP del COR.		**6.1**	Definizione dei moduli da integrare e progettazione definitiva.	
			6.2	Realizzazione e rilascio operativo dei moduli integrativi.	
			6.3	Completamento delle funzionalità rilascio in produzione della piattaforma comprensiva dei nuovi moduli.	
7 Formazione e addestramento *cyber*	a) Attività di consolidamento e potenziamento del poligono *cyber* della Difesa per il raggiungimento della		**7.1**	a) Studio progettuale e primo rilascio di nuovi contenuti teorici e pratici all'interno del modulo formazione. b) Predisposizione piattaforma e sua configurazione.	
			7.2	a) Implementazione soluzioni tecnologiche.	

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
	sua piena capacità operativa. b) Programma formativo e addestrativo di *Cyber Security Awareness* a favore del personale non di settore della Difesa.			b) Popolamento della piattaforma con gli utenti fruitori dei percorsi formativi.	
			7.3	a) *Full Operational Capability* del Cyber Range della Difesa. b) Avvio operativo ed erogazione del servizio.	
Macro-Area 2: INTEGRAZIONE DEL DOMINIO CYBER NEI SISTEMI DI COMANDO E CONTROLLO DELLA DIFESA					
8 Valutazione di sicurezza dei sistemi C2	Sviluppo di un sistema per la valutazione delle capacità di protezione dei sistemi e delle componenti informatiche della Difesa.		**8.1**	Studio progettuale su architettura da implementare.	
			8.2	Acquisizione materiale e supporti sistemistici tesi alla finalizzazione della architettura.	
			8.3	Avvio operativo e formazione.	
9 Sicurezza delle componenti di gestione dei sistemi satellitari	Acquisizione capacità di protezione cibernetica delle comunicazioni satellitari attraverso l'implementazione di modem *TranSec* e gestione dei *log*.		**9.1**	Avvio acquisizione modem Transec.	
			9.2	Definizioni modalità operative e siti di impiego.	
			9.3	Distribuzione e impiego modem, implementazione modulo di gestione dei Log di sicurezza da connettere ai SIEM della Difesa.	
Macro-Area 3: ACQUISIZIONE DI CAPACITÀ DI PROTEZIONE CYBER PER DISPOSITIVI OT/IOT					
10			**10.1**	*a)* Studio per definizione soluzione architetturale del *Mobile Device Management.*	

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
Accesso alla rete e protezione dei dispositivi mobili	a) Acquisizione di una tecnologia di *Mobile Device Management*. b) Estensione della protezione antivirus ai dispositivi mobili in uso in ambito Difesa.			b) Acquisizione licenze e servizi professionali per protezione dispositivi mobili.	
			10.2	a) Messa in opera e acquisizione prima trance di licenze del *Mobile Device Management* individuato dallo studio. b) Acquisizione licenze, servizi professionali e supporto per soluzione protezione dispositivi mobili.	
			10.3	a) Completamento acquisizione licenze, avvio operativo e formazione su *Mobile Device Management*. b) Acquisizione licenze, servizi professionali e supporto per soluzione protezione dispositivi mobili.	
11 Realizzazione sistema APN della Difesa	Implementazione di un servizio di *Access Point Name* (APN) proprietario nel contesto della capacità LTE 4G/5G della Difesa di prevista integrazione ed interoperablità con reti Radio Mobili gestite da provider commerciali.		**11.1**	Definizione procedure di implementazione accesso privato reti 4G/5G. definizione architetture presso COR-Difesa.	
			11.2	Avvio procedure per la realizzazione del *Core Network* 5G della Difesa e sviluppo e configurazione avanzato di APN privato della Difesa. Avvio acquisizione di capacità autonoma per gestione ed utilizzo nodi LTE 4G/5G da parte di utenti Difesa (fondi Difesa). Avvio acquisizione elementi per APN	
			11.3	Implementazione servizio APN ed attivazione componenti aggiuntive di sicurezza per	

Identificativo Work Package (WP)	Descrizione Work Package	identificativo obiettivo		Deliverable Atteso	note
				connettività ed interoperabilità con reti dati pubbliche.	
Macro-Area 4: ACQUISIZIONE DI UNA PIATTAFORMA DI SUPERVISIONE DEDICATA AI SISTEMI SCADA					
12 Protezione Sistemi di supervisione fisici (SCADA)	Attività di *assessment*, *gap analysis* e *remediation* in ambito di sicurezza cibernetica per la protezione dei sistemi SCADA in uso alla Difesa.		**12.1**	Realizzazione piano di progetto, *Asset inventory*, *report* sulle vulnerabilità identificate e documento su *Use Cases* identificati.	
			12.2	Elaborazione documento architetturale di dettaglio teso alla risoluzione delle vulnerabilità emerse nella fase precedente.	
			12.3	Implementazione soluzioni tecnologiche, acquisizione licenze d'uso e formazione specifica.	
Macro-Area 5: REALIZZAZIONE CENTRO DI VALUTAZIONE DELLA DIFESA					
13 Realizzazione Centro di Valutazione della Difesa	Costituzione del Centro di Valutazione della Difesa in raccordo con il CVCN e in linea con le predisposizioni di legge in materia.		**milestone EU M1C11.7**	Acquisizione materiali per realizzazione 4 nodi tipo per i laboratori.	
			milestone EU M1C11.21	Raggiungimento della *Initial Operational Capability* del Centro di Valutazione della Difesa.	
	Potenziamento e mantenimento operativo capacità del Centro.			Acquisizione assetti ed apparati aggiuntivi per rilevamento sorgenti emissive e *test device*.	

6 INTEGRAZIONE CON ALTRI INTERVENTI

Non si prevedono integrazioni con altri interventi finanziati in ambito PNRR a favore del Ministero della Difesa.