AFCEA

CAPITOLO DI ROMA

2024
8° EDIZIONE

1 anno di attività

www.afcearoma.it

Care amiche e cari amici del Capitolo di Roma di AFCEA International,

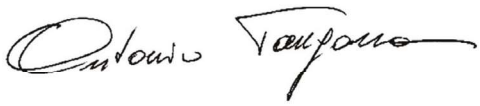
sono lieto di introdurvi anche quest'anno alla nostra rivista annuale, ormai tratto distintivo del nostro Capitolo.

La struttura è rimasta la stessa, ma abbiamo arricchito la sezione dedicata agli articoli, principalmente, dei nostri soci Corporate, ma che ospita anche i contributi esclusivi di illustri amici. Hanno confermato il loro contributo il Presidente e CEO di AFCEA International, il Lt. Gen. Susan Lawrence, USA (Ret.) e il General Manager di AFCEA Europe, il Maj. Gen. Ercih Staudacher, GEAF (Ret.). La novità è costituita dagli articoli scritti dal Direttore di Armaereo, Gen.Isp.Capo Giuseppe Lupoli e dal Capo 6^ Divisione di Terrarm, Col. ing. Mauro Andrea Roddi.
Nella sezione "Eventi" è riportata la sintesi degli eventi organizzati nel 2023, arricchiti dalla presenza di relatori provenienti da diversi settori istituzionali, accademici e industriali a cui va il più sentito apprezzamento e ringraziamento. Sul nostro sito è possibile trovare le presentazioni e i video relativi agli eventi.

Colgo l'occasione per ringraziare tutti coloro che ci seguono e apprezzano a livello istituzionale, accademico e industriale e la cui vicinanza e partecipazione numerosa ai nostri eventi ne testimoniano il successo e costituisco gratificazione per la nostra associazione che, mi piace sottolineare, è no profit e basata esclusivamente su attività volontaria.

Nell'invitarvi a seguirci sempre sul nostro sito e a partecipare ai nostri eventi, rivolgo a tutti l'augurio di una piacevole lettura con un arrivederci alla prossima edizione.

IL PRESIDENTE
Gen.Isp.Capo(r) Antonio TANGORRA



Indice dei contenuti

AFCEA Capitolo di Roma

AFCEA International è un'associazione no profit che si occupa di difesa, intelligence, sicurezza e di tutte le discipline tecnologiche correlate il cui principale obiettivo è promuovere il dialogo tra comunità militari, governative, accademiche e industriali per ampliare la cultura e le conoscenze professionali nei settori delle comunicazioni, del comando e controllo, dell'Information Technology, dell'intelligence, della sicurezza e dello spazio.
Costituita negli Stati Uniti nel 1946 dopo la seconda guerra mondiale per raggruppare i veterani dei "battaglioni SIGNAL", AFCEA International cominciò a includere già nello stesso anno la componente industriale. A partire dal 1979 ha avuto inizio il processo di internazionalizzazione che ha portato alla creazione di Capitoli locali in Canada, Sud America, Europa, Asia, Australia, oltre che negli Stati Uniti per un totale di **140** capitoli in **28** Paesi.

Attraverso i suoi Capitoli, AFCEA International può contare attualmente su oltre **31.000** soci individuali e circa **1.600** soci corporate, costituendo così un vastissimo network i cui valori chiave sono l'etica, la professionalità, l'impegno, la qualità, la formazione e il rispetto delle diversità. Questo ampio network internazionale consente alle comunità coinvolte di cooperare per allineare tecnologie e strategie innovative ai requisiti sempre più sfidanti di coloro che servono le istituzioni. Ogni Capitolo ha una propria organizzazione e svolge le proprie attività in autonomia, in coordinamento con la comunità di AFCEA International e in linea con i suoi principi fondamentali.

Il **Capitolo di Roma** fu costituito nel 1988 e da allora rappresenta un costante e qualificato riferimento per i principali operatori a livello nazionale nei settori dell'Information Technology, Comunicazioni, Difesa, Sicurezza e Spazio, grazie alla capacità di raccogliere e armonizzare contributi provenienti dalle istituzioni, dagli enti di ricerca e università, dalle grandi industrie nonché dalle piccole e medie imprese, con una costante attenzione agli sviluppi tecnologici nei settori trattati.

Il nostro Capitolo partecipa attivamente alla vita di AFCEA International: il Presidente Gen.Isp.Capo(r) Antonio Tangorra è membro del Board of Directors di AFCEA International, inoltre è Vice President per la Regione Mediterranea. La Dott.ssa Fiorella Lamberti fa parte del Board of Directors nonché rappresentante del Capitolo in "Women in AFCEA Outreach Leader " Subcommittee. L'Avv. Alessandra Finocchio e l'Ing. Vincenzo Vitiello sono membri dell'AFCEA International Membership Committee che ha lo scopo di promuovere la crescita del valore dell'appartenenza ad AFCEA, il Dott. Stefano Tangorra è il rappresentante in Young AFCEA in Europe.

L'organizzazione

AFCEA International
www.afcea.org

AFCEA Europe
www.afcea.org/afcea-europe

AFCEA Roma
www.afcearoma.it

Il Capitolo è un'organizzazione molto dinamica e fluida con un continuo ricambio intorno ad un nucleo consolidato e storico. Vi è stata una crescita significativa degli associati ed oggi il Capitolo di Roma può contare su circa **400** soci individuali e **43** corporate. Tutti i soci iscritti al Capitolo costituiscono l'Assemblea che elegge il Presidente, i due Vice Presidenti, il Consiglio Direttivo, il Comitato Tecnico Scientifico e i Proboviri. Il vertice è costituito dal Presidente e due Vice Presidenti eletti annualmente e provenienti singolarmente dai settori rappresentativi dell'Associazione: militare, industriale, accademico. Completano il quadro degli Organi dell'Associazione il Segretario e il Tesoriere, designati dal Presidente, e tre Probiviri, eletti ogni tre anni. Il Consiglio Direttivo, costituito da 15 membri eletti annualmente, definisce ed approva le differenti iniziative, il programma delle attività e le spese relative. Il Comitato Tecnico Scientifico, costituito da 5 membri eletti annualmente, contribuisce ad assicurare che le attività dell'Associazione propongano contenuti tecnico-scientifici adeguati e innovativi, attraverso la selezione di argomenti e tematiche che possano stimolare una divulgazione puntuale e uno scambio culturale tra tutti partecipanti alla vita dell'Associazione.
Inoltre, è attivo il Comitato di Redazione, che ha la responsabilità di tutte le attività Editoriali e di Comunicazione tra cui quelle svolte tramite il sito web.
In linea con le corrispondenti commissioni già istituite da AFCEA International, il Capitolo di Roma ha creato al proprio interno due sezioni dedicate, AFCEA Youth e Women in AFCEA:

- **AFCEA Youth** ha lo scopo di coinvolgere giovani studenti nella vita dell'associazione, anche attraverso la costituzione di Student Club dedicati, per avvicinarli sempre di più al mondo del business nei settori della difesa e della sicurezza, invitandoli a sostenere gli obiettivi tecnico-scientifici dell'associazione con i loro progetti.
- **Women in AFCEA Rome Chapter** è nata per sostenere e valorizzare la presenza delle donne nel mondo istituzionale, accademico e industriale nei settori di interesse dell'Associazione con particolare attenzione all'ambito STEM (Science, Technology, Engineering and Mathematics).

Le attività

L'appartenenza al Capitolo di Roma fornisce l'accesso ad una vasta e qualificata platea per i professionisti del settore pubblico e privato nelle aree delle Comunicazioni, della Cyber, dei Sistemi Informatici, Elettronici e di Comando e Controllo nell'ambito della Difesa, della Sicurezza che opera in tali settori.

A tal fine ogni anno il Capitolo definisce il proprio programma di attività con il contributo dei soci per organizzare riunioni, seminari, conferenze, visite o altre iniziative al fine di mantenere i propri membri aggiornati sulle tematiche d'interesse nei vari settori. La comunicazione degli eventi avviene tramite il sito dell'Associazione e Linkedin, l'accesso ai seminari e conferenze è libero per tutti gli interessati. Il calendario degli eventi è pubblicato anche sul sito di AFCEA International, che riceve i report di ogni evento per la pubblicazione su SIGNAL, rivista ufficiale dell'Associazione, offrendo così anche l'opportunità di presentarsi a una vetrina internazionale.

In particolare le principali attività sono articolate in:

- **Convegni:** sulla base delle principali tematiche scelte ogni anno dal Consiglio Direttivo con il supporto del Comitato Tecnico Scientifico, i convegni hanno l'obiettivo di fare il punto su argomenti di particolare interesse e attualità attraverso la partecipazione delle principali istituzioni coinvolte, del mondo accademico e dell'industrie che operano nei settori di riferimento.

- **Presentazioni aziendali:** ogni socio "corporate" ha la possibilità di effettuare una presentazione su un argomento specifico, giudicato d'interesse dal Consiglio Direttivo con il supporto del Comitato Tecnico Scientifico, per illustrare le problematiche connesse e le proprie proposte e soluzioni, anche utilizzando "case study" con istituzioni e/o mondo accademico.

- **Visite:** AFCEA organizza per i propri soci una serie di visite presso strutture istituzionali, come pure siti d'interesse dal punto di vista culturale e scientifico per incoraggiare la diffusione della conoscenza tecnologica e della cultura tra i propri membri, sia in ambiti prettamente legati alla Difesa e alla Sicurezza sia in ambiti di carattere culturale più generale.

- **Master:** Il Capitolo di Roma sostiene le attività di formazione finanziando da molti anni tre borse per due Master di II livello in: "Ingegneria e Diritto Internazionale dello Spazio nei Sistemi di Comunicazione, Navigazione e Sensing Satellitare" dell'Università di Roma Tor Vergata e "Data Intelligence e Strategie Decisionali" presso l'Università di Roma La Sapienza.

Il sito

Tutte le informazioni sulla storia del Capitolo di Roma, la sua organizzazione, le sue attività, le modalità di associazione, i soci "Corporate" con i rispettivi loghi e profili sono disponibili sul sito web www.afcearoma.it.
In particolare il sito, per ogni evento organizzato, mette a disposizione le presentazioni e le riprese effettuate, nonché un report con una sintesi degli interventi dei vari relatori. In questo modo tutti i soci e i visitatori del sito interessati hanno la possibilità di mantenersi aggiornati e conoscere i contenuti dettagliati.
Tutti i soci hanno anche la possibilità di fare conoscere le proprie attività professionali attraverso la pubblicazione di articoli di elevato contenuto professionale e di notizie di rilevante interesse.
Sul sito sono disponibili, in formato digitale, tutte le edizioni della rivista a numero unico.

Organi dell'Associazione

Presidente:
Gen.Isp.Capo(r) Antonio Tangorra

Vice Presidente (Università):
Prof.ssa Ernestina Cianca

Vice Presidente (Industria):
Ing. Lorenzo D'Onghia

Consiglio Direttivo
Dott.ssa Fiorella Lamberti (socio corporate Leonardo)
Ing. Antonio Gammarota (socio corporate Thales Alenia Space Italia)
Dott.ssa Lucia Di Giambattista (socio corporate Almaviva)
Ing. Paolo Bellofiore (socio corporate Telespazio)
Dott. Stefano Tangorra (socio singolo)
Dott. Marco Braccioli (socio corporate Digital Platforms)
Ing. Vincenzo Vitiello (socio singolo)
Avv. Alessandra Finocchio (socio singolo)
Amm.Isp.Capo(r) Lucio Accardo (socio singolo)
Ing. Roberto De Finis (socio corporate S&A Sistemi e Automazione)
Ing. Andrea Brancaleoni (socio corporate Keysight Technologies)
Gen.C.A.(r) Maurizio Leoni (socio singolo)
Gen.B.A.(r) Alberto Traballesi (socio singolo)
Ing. Piergiorgio Foti (socio singolo)
Col. Gianluca Pedicini (socio singolo)

Comitato Tecnico Scientifico
Ing. Cinzia Crostarosa (socio corporate Larimart)
Dott.ssa Annamaria Nassisi (socio corporate Thales Alenia Space Italia)
Dott. Alessandro Antonini (socio singolo)
Dott. Mirko Leanza (socio corporate Teleconsys)
Ing. Eugenia Finocchiaro (socio corporate Crisel)

Proboviri
B.Gen(r) Aldo Giannatiempo (socio singolo)
Gen.Isp.Capo(r) Pietro Finocchio (socio singolo)
Ing. Ciro Nicolai (socio singolo)

Comitato di Redazione
Gen.Isp.Capo(r) Antonio Tangorra (Managing Editor)
Dott.ssa Fiorella Lamberti (Editor in Chief)
Dott.ssa Lucia Di Giambattista (Editor Team)
Dott. Stefano Tangorra (Editor Team)

Segretario:
B.Gen(r) Aldo Giannatiempo

Tesoriere:
Ing. Vincenzo Vitiello

Membership Officer:
Gen.B. Gianluca Pedicini

Web Officer:
Dott.ssa Lucia Di Giambattista

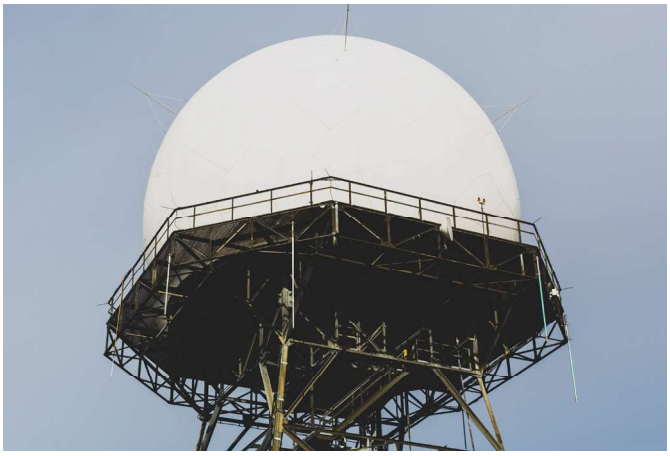
AFCEA HQ Relation Manager
Avv. Alessandra Finocchio
Ing. Vincenzo Vitiello

Gli eventi 2023

INNOVAZIONE E TECNOLOGIE VAISALA PER MISURE METEOROLOGICHE "MISSION CRITICAL"

19 GENNAIO 2023

Il nostro mondo affronta sfide ambientali sempre più pressanti ed è più importante che mai basare le decisioni su dati accurati, affidabili e in tempo reale. In questo contesto, il Capitolo di Roma di AFCEA International e l'associata società finlandese Vaisala, leader mondiale nel settore meteorologico, supportata dal suo Partner in Italia Eurelettronica Icas, hanno organizzato un workshop per presentare tecnologie di misura innovative, progettate per migliorare l'affidabilità ed assicurare operazioni sicure ed efficienti. Fra le tecnologie di osservazione meteorologica per il miglioramento del sistema di allerta, presentate nel corso del workshop, vi è il nuovo radar meteorologico sviluppato da Vaisala, sia in banda X che in banda C; questo utilizza un'innovativa architettura "compatta" e un trasmettitore a stato solido. Sono state presentate anche nuove tecnologie Lidar, fra le quali: il Celiometro Lidar con depolarizzazione, che oltre alla misura degli strati nuvolosi fornisce anche informazioni relative alla caratterizzazione dell'atmosfera; il Doppler Wind Lidar per misure continue del vento a 360°/3D. Infine, è stata presentata la tecnologia del sensore FD70, "tre in uno" che fornisce informazioni sulla visibilità, tempo presente e precipitazioni, che misura con un elevato grado di accuratezza. Per sfruttare al meglio le potenzialità dei radar meteorologici e delle altre moderne apparecchiature e dati di telerilevamento (remote sensing), è stata mostrata la suite software IRIS Focus specifica, di facile utilizzo, web based, che consente agli utenti di accedere e analizzare i dati di telerilevamento in modo rapido e guidato.



Mr Alexis KAVAJA – Vaisala – Innovative technologies for mission critical weather measurements:
Radar Meteorologico con trasmettitore a stato solido in banda X WRS400 e in banda C WRS300;
Profilatore Dial e nuove tecniche di misura

Ing. Alessandro MARCHINI – Eurelettronica ICAS – Wind Lidar Wind Cube

Ing. Martino FANTATO – Vaisala – CL61 Lidar verticale con depolarizzazione del segnale

Mr Tommi LINNA – Vaisala – Forward Scatter Sensor FD70

VEEAM, UN PERCORSO DAL TRADIZIONALE "RESTORE" AD UN COMPLETO "RECOVERY" CONTRO LE MINACCE CYBER

9 MARZO 2023

La Data Protection è un asset fondamentale per assicurare la continuità dei servizi e la protezione da attacchi informatici in ambienti sensibili con infrastrutture strategiche per il Sistema paese.
In ambienti come quello della Difesa, ad una soluzione di Modern Data Protection è richiesto, oltre all'affidabilità, anche la capacità di essere al passo con i tempi e di essere in grado di proteggere architetture applicative e dati in ogni ambito tecnologico presente e futuro.
In particolare, nel corso dell'evento realizzato in collaborazione con Veeam Software Italy sono stati approfonditi temi come:

1. Backup&Recovery;
2. Disaster Recovery;
3. Ransomware e Cyber Security;
4. Inizia ad affacciarsi il tema hybrid cloud (Azure, M365).

C.F. Carlo ROATTA – TELEDIFE – Keynote speach

Dott. Alberto LOZZI – Sales Manager Public Sector Italia, Veeam Software – Veeam in AFCEA, Veeam nella Difesa

Ing. Danilo CHIAVARI – Presales Manager Italia, Veeam Software – Dalla Data Protection alla Availability

Dott. Alessio DI BENEDETTO – Technical Sales Director Southern Europe, Veeam Software – Data Management a sostegno della Cyber Security

Ing. Giuseppe NANTISTA – Enterprise Systems Engineer Italia Veeam Software – Disaster Recovery e Governancein ambienti ibridi e multi-cloud

L'INTELLIGENZA ARTIFICIALE IN AMBITO MILITARE: NUOVE SOLUZIONI ED EVOLUZIONE D'IMPIEGO

3 MAGGIO 2023

A distanza di due anni, AFCEA Capitolo di Roma ha organizzato un nuovo workshop dedicato al tema dell'Intelligenza Artificiale in ambito Difesa, per fare il punto su una tecnologia diventata rapidamente pervasiva in molteplici casi.

Chatbots, Crime Prediction, Face Recognition, Sentiment ed Emotional Analysis Track Recognition, SIGnal/COMmunication INTelligence, IMage/GEO-INTelligence and Advanced Command & Control Systems, Advanced Video Analytics, sono solo alcuni esempi di quanto l'Intelligenza artificiale sia ormai alla base di attività complesse che prevedono la gestione e l'analisi di enormi quantità di dati.

Gli sviluppi recenti nel campo dell'IA stanno rivoluzionando anche le operazioni militari, migliorando l'efficacia e l'efficienza delle missioni grazie sia all'utilizzo di sensori avanzati, sia alle tecniche evolute di elaborazione di grandi basi di dati e di serie temporali, in grado di abilitare per esempio funzioni evolute di manutenzione predittiva fondamentale nell'impiego degli assetti mobili. In questo contesto, grazie agli algoritmi di IA, è possibile migliorare le capacità di prendere decisioni rapide ed efficaci in ambienti operativi complessi, supportando i sistemi di comando e controllo nella selezione di strategie ottimali per l'uso delle risorse disponibili e di possibili procedure di Tasking per rendere più risolutive le Network Centric Operations (NCO Decision Support Systems). Inoltre, l'Intelligenza artificiale può essere impiegata nei sistemi di addestramento delle truppe e nella logistica militare, rendendo più efficiente e sicura la gestione delle risorse e dei materiali con sistemi OBDA (Ontology based Data Management). Le applicazioni possono riguardare la pianificazione strategica e la simulazione di scenari operativi, con un supporto fondamentale per la simulazione delle missioni e l'attuazione operativa seguendo gli schemi già collaudati.

In questo contesto, AFCEA Capitolo di Roma ha riportato l'attenzione sull'Intelligenza artificiale, presentando i progressi compiuti in questi anni, le attività in corso nell'ambito delle Forze Armate, le aziende che operano in questo settore con le proprie soluzioni tecnologiche.

Magg. Francesco CORSO – V Reparto, SEGREDIFESA – Intelligenza Artificiale nella Difesa: le attività di ricerca ed innovazione tecnologica

Col.Fabio ZANICHELLI – Comando Logistico AM – Il nuovo sistema di infologistica AM – principi generali e prospettive future

Dott. Gabriele TONINI – Leonardo – L'intelligenza Artificiale a servizio del Customer Journey

Dott. Nicola GRANDIS – DigitalPlatforms – OSINT e CLOSINT, risorse per valutare e modificare l'approccio all'Intelligence, nell'era dell'Intelligenza Artificiale

Dott. Francesco ORLANDO – Teleconsys – Integrazione dell'Artificial Intelligence in una OSINT Data Platform. "Strappare il velo di Maya" dall'informazione

Ing. Marco BARBINA – Leonardo – Presente e futuro dell'AI in Leonardo

C.F Gianluca Maria MARCILLI – NAVARM – Validazione e collaudo dei sistemi di Intelligenza Artificiale

Dott. Glauco CENCIOTTI, Dott.ssa Angela SEBASTIANELLI – VAR Group Partner IBM – IBM AI@WORK: Le opportunità di un'intelligenza artificiale applicata e "data centrica"

Dott.ssa Silvia M. ANSALDI – INAIL – Tecniche di Intelligenza Artificiale per l'analisi di quasi-incidenti in ambito industriale

IDENTITÀ FISICHE E DIGITALI, SICUREZZA SENZA COMPROMESSI!

La crittografia ed i suoi secret: come gestirli e come renderli inviolabili

6 GIUGNO 2023

La digitalizzazione è un fenomeno pervasivo della nostra società che ci ha reso più vulnerabili; diventa quindi fondamentale assicurare la protezione delle identità fisiche e digitali. In questo contesto il Capitolo di Roma di AFCEA International e l'associata N.I.D.O., hanno organizzato un workshop per presentare soluzioni volte a garantire la sicurezza e l'efficienza delle operazioni, implementando la filosofia "Zero Trust".

N.I.D.O. è un'azienda Italiana con più di 20 anni di esperienza nello sviluppo e commercializzazione di soluzioni personalizzate HW e SW nel settore del Card & Document Management. L'azienda da anni si interfaccia con clienti dagli standard di sicurezza elevati sia per le carte plastiche che per altri documenti, traghettando queste tecnologie verso la digitalizzazione e la loro smaterializzazione. N.I.D.O. è un'azienda in grado di unire alla gestione delle identità fisiche un portafoglio di soluzioni di Cyber Security per tutte le identità digitali, oltre alla gestione e messa in sicurezza dei Secret in ambienti altamente sensibili e complessi. Project Management, Formazione, e Servizi Post Vendita sono erogati da personale certificato al fine di garantire sempre la massima corrispondenza tra quanto proposto e quanto realizzato.

Nel corso del workshop sono stati approfonditi i seguenti argomenti:

1. Attacchi Hackers di tipo BEC (business email compromise) come difenderci in modo efficace;
2. Soluzioni per il management di PKI e certificati SSL. Esiste un orchestratore?
3. La crittografia ed i suoi Secret come proteggerli e come armonizzarne la gestione;
4. Single sign-on e Multi Factor Authentication – Una piattaforma tante applicazioni.

L'evento è stata inoltre l'occasione per condurre riflessioni e considerazioni su:

1. Identità Digitale e Fisica;
2. Personalizzazione di documenti sicuri (Governativi e Bancari);
3. Tecnologie di stampa utilizzabili;
4. Emissione contestuale di documenti fisici e virtuali;
5. Stampanti 3D – un innovativo sistema di stampa che guarda all'infinito.

Dott. Nadia ANGELINI e Dott. Stefano PENNA – N.I.D.O. Group – Attacchi Hackers di tipo BEC (Business e-mail compromise) come difenderci in modo efficace

Dott. Nadia ANGELINI – N.I.D.O. Group – Soluzioni per il Management di PKI e certificati SSL

Ing. Giulio GENNARI – Entrust. La crittografia ed I suoi Secret come proteggerli e come armonizzare la gestione

Dott. Stefano PENNA – N.I.D.O. Group – Single sign-on e Multi Factor Authentication, una piattaforma tante applicazioni

Dott. Giorgio MESTICI – N.I.D.O. Group

- Personalizzazione dei Documenti sicuri-Governativi e bancari
- Tecnologie di stampa utilizzabili
- Emissione contestuale di documenti fisici e virtuali
- Stampanti 3D, un innovativo sistema di stampa che guarda all'infinito

COMUNICAZIONI RESILIENTI PER OPERARE IN UN AMBIENTE MULTI DOMINIO COMPLESSO

22 GIUGNO 2023

Nell'ambito delle attività connesse al 70° Anniversario dell'Arma delle Trasmissioni dell'Esercito Italiano, il Capitolo di Roma di AFCEA ha organizzato presso il Comando Trasmissioni della Cecchignola un evento per presentare lo stato dell'arte e il ruolo cruciale delle nuove tecnologie per garantire la resilienza nelle comunicazioni, indispensabile per operare in un ambiente multi dominio complesso. La robustezza e l'affidabilità delle telecomunicazioni in ambiente multi dominio è un elemento chiave per il successo in operazioni, da conseguire anche con tecnologie mature (ancorché innovative) ed adattabili a scenari operativi sempre più stringenti e in continua "evoluzione", in termini di priorità e di sostenibilità. La capacità di disturbo delle telecomunicazioni, ovvero la loro intercettazione a fini di intelligence tattica, diventano un elemento da tenere in debita considerazione, così come l'utilizzo dello spettro elettromagnetico (e non solo quello fisico) per condurre attacchi cibernetici (c.d. capacità CEMA – Cyber Electro Magnetic Activities). L'utilizzo del 5G in ambito militare prevede la realizzazione di una Infrastruttura Radio Mobile per la Difesa Italiana, introducendo importanti e peculiari funzionalità specifiche per il comparto militare compatibili con la tecnologia 5G civile, ma aggiungendo la sicurezza alla certezza e delle comunicazioni (dati e voce), utilizzabile quindi dalle Forze Armate in Italia e all'estero. All'aggiornamento delle reti di comunicazione su base nazionale si affiancano le tecnologie di supporto alla copertura globale di rete come: i satelliti in orbita bassa per le comunicazioni; il 5G nelle comunicazioni satellitari; l'AI per la gestione delle reti infrastrutturali; ma anche la valorizzazione di applicazioni sempre attuali quali Ponti Radio (HF, VHF, UHF, Link 16 o TADIL-J) o Reti di comunicazioni Troposcatter. Attraverso lo sviluppo di soluzioni ad hoc, si può rispondere ai più severi standard di sicurezza e affidabilità tipici dell'ambiente militare, come soluzioni Mobile Ad-hoc NETwork (MANET), Software Defined Network (SDN), Delay Tolerant Network (DTN), SDR e relativi protocolli e Tactical Data Link militari. Elementi essenziali per lo sviluppo delle reti di comunicazione sicure sono i progetti Europei (i.e. HORIZON 2020 e EDF) in particolare per ciò che riguarda le componenti di sicurezza e di interoperabilità. In questo ambito, l'evento organizzato da AFCEA ha presentato contributi provenienti dal settore militare, istituzionale, accademico e industriale, per mettere a confronto le diverse esigenze operative con le potenzialità offerte dalle nuove tecnologie.

Cap. ing. Stefano PRINCIPE – Comando Trasmissioni E.I. – La continuità delle comunicazioni radio tattiche in situazioni di jamming anti-RCIED

Ing. Giuseppe PRINZIVALLE – IES Srl – Sistema di protezione ed analisi delle waveform nelle comunicazioni tattiche

Ing. Sabrina WAHIB – Thales Alenia Space Italia – LEO small satellites constellation for narrow band and broadband telecommunication applications

CF(AN) Carlo ROATTA – Teledife – Un procurement moderno per telecomunicazioni innovative: il ruolo di Teledife nella Difesa

Ing. Cinzia CROSTAROSA e Ing. Massimo FRANCONE – LARIMART – Sicurezza ed operatività della persona rispetto alle comunicazioni voce ed all'innovazione tecnologica – Equipaggiamenti elettronici LARIMART per comunicazioni semplici, affidabili e resilienti nei domini applicativi

T.Col. Pasquale SILVESTRO – Stato Maggiore Esercito – Il ruolo della componente EW/CEMA per la supremazia dell'ambiente elettromagnetico

Dott. Italo Trisolini LONGOBARDI – INTECS – Solutions L'evoluzione della Tecnica SDR secondo INTECS SOLUTIONS SpA

Ing. Enzo FORTUNATO – Leonardo – Applicazioni 5G nelle reti tattiche – Aspetti di sicurezza. Evoluzione della rete areale, affidabilità e resilienza delle comunicazioni

Ing. Andrea BRANCALEONI e Ing. (PhD) Francesco SPADAFORA – Keysight Technologies – Accelerating Innovations in 5G Non-Terrestrial Networks

Ing. Giovanni GASBARRONE – ANUTEI – Evoluzione delle infrastrutture resilienti di Telecomunicazioni verso il 6G e la Cyber Security quantistica

LE CAPACITÀ CYBER NELLE OPERAZIONI MULTIDOMINIO

11 LUGLIO 2023

L'evoluzione delle tecnologie digitali e l'interconnessione dei domini operativi stanno portando alla necessità di comprendere e sfruttare le capacità cyber nelle operazioni multidominio. Infatti, tali fattori hanno creato nuove opportunità, come pure sfide senza precedenti per le forze militari e le organizzazioni di sicurezza. per garantire un'efficacia ottimale delle operazioni, soprattutto nei nuovi domini come Cyber e Spazio, cruciali per il funzionamento delle società moderne, dalle attività economiche a quelle nel campo della sicurezza e difesa. La protezione delle reti, dei dati sensibili e delle infrastrutture critiche è dunque essenziale per preservare l'integrità, la riservatezza e la disponibilità delle informazioni. A tale scopo, sono in corso processi innovativi per adottare tecnologie all'avanguardia nel rilevamento delle minacce, nell'autenticazione robusta e nella crittografia sicura.

Lo sviluppo delle capacità cyber di prossima generazione sarà cruciale per proteggere le infrastrutture critiche, che includono reti elettriche, reti di approvvigionamento idrico ed i sistemi di trasporto. Lo stesso conflitto in Ucraina ha dimostrato il legame tra dominio spaziale e cyber, nonché la loro importanza per le relative operazioni, evidenziando la vulnerabilità dei sistemi spaziali, da considerarsi ormai una priorità in particolare per le infrastrutture europee. Con questo nuovo convegno, dedicato al mondo cyber, AFCEA ha voluto esplorare le innovazioni che stanno plasmando lo sviluppo della cyber warfare e le ricadute delle tecnologie sviluppate con soluzioni di high availability, crittografia e cyber sicurezza. In particolare, sono state presentate le comunicazioni quantistiche sulle tecnologie QKD (Quantum Key Distribution), e relativi protocolli nel dominio Spazio, le Cyber ElectroMagnetic Activities (CEMA) con tecnologie di high availability e messa in sicurezza delle chiavi di crittografia. Il convegno ha fornito quindi l'occasione per uno scambio di idee e soluzioni da parte dei principali attori nelle istituzioni e nelle industrie del settore, coinvolti nello sviluppo di queste capacità.

Dott. Nicola GRANDIS – Digital Platforms – Scenari Multi-Dominio: Intelligenza Artificiale per difendersi in scenari Multi-Dominio e contrattaccare in modo efficace

Prof. Fulvio RISSO e Ing. Marco MANGIULLI – Aruba – LIQO e ArubaKube, the cloud continuum made real

Col. Carlo MONGELLI – 3^ Divisione Comando Logistico A.M. – Cyber Security in A.M. e approccio alle Operazioni Multidominio

Ing. Andrea CONTI – Leonardo – Situational awareness aumentata e multidominio

C.V. Daniele SANGERMANO – Comando Operazioni in Rete (COR) – Generazione di effetti cyber offensivi in operazioni multidominio

Ing. Paolo CONFORTO – Thales Alenia Space Italia – Distribuzione quantistica di chiavi crittografiche per le telecomunicazioni sicure

Dott. Pietro FELISI – Barracuda Networks – IoT Security: come innalzare il livello della protezione di fronte ai nuovi scenari"

Ing. Daniela PISTOIA – Elettronica – Electronic Warfare and Cyber Warfare: two sides of the same coin

Dott. Stefano PENNA – N.I.D.O. **–** AppSec Synopsis: la sicurezza delle tue applicazioni in una sola soluzione

Dott. Franco BRAUN – Rubrik – Come recuperare in modo rapido, sicuro e certo, mantenendo i dati al sicuro e resilienti

SOSTENIBILITÀ NELLO SPAZIO: UNA NUOVA FRONTIERA

28 SETTEMBRE 2023

Lo spazio è riconosciuto come una risorsa fondamentale per rendere più sostenibile la nostra vita sulla terra. Si pensi ai satelliti per applicazione di osservazione della terra, di telecomunicazione e navigazione, che permettono un monitoraggio e controllo sempre più fine ed accurato e una comunicazione in territori difficilmente raggiungibili da infrastrutture di terra o in casi di disastri. Lo spazio è anche una frontiera tecnologica sviluppata per ambienti ostili e si parla ormai di turismo spaziale, estrazione di risorse e insediamenti umani sulla Luna e successivamente su Marte. Inoltre si sta assistendo a un crescente numero di piccoli satelliti lanciati da numerosi attori non tradizionali come università, aziende private, centri di ricerca e nazioni. Si è quindi passati in pochi anni da un uso governativo dello spazio, a un uso in cui il privato e commerciale hanno un ruolo maggiore con un aumento del numero di lanci e satelliti in orbita.

L'aumento esponenziale del numero dei satelliti in orbita può portare a un degrado dell'ambiente spaziale in ambito LEO e a un amento della quantità di detriti spaziali. Preservare lo spazio è dunque necessario anche per garantire la continuità di quei servizi che servono a terra per uno sviluppo sostenibile. Per tale motivo, le nuove missioni vanno pensate in un'ottica di sostenibilità "by design", facilitando la cooperazione tra satelliti e costellazioni diversi, in modo da permette il riuso di sistemi già in orbita. Inoltre, la veloce evoluzione del settore è stata poco regolamentata, rendendo sempre più cruciale la necessità di un quadro normativo di riferimento per garantire la sostenibilità delle nuove missioni in termini tecnologici, economici e operativi. In tale contesto il Women in AFCEA Committee di AFCEA Capitolo di Roma ha promosso un'iniziativa dedicata al tema della sostenibilità dello spazio. L'evento dal titolo "Sostenibilità nello spazio: una nuova frontiera" si è posto 'obiettivo di sviluppare i vari aspetti della sostenibilità nello spazio, dalla space situation awareness, alle ricadute tecnologiche e all'aspetto normativo, mettendo a confronto scienziate e manager che lavorano in ambito spaziale, per sottolineare come la sostenibilità riguardi anche l'inclusione, soprattutto in un settore che vede crescere la presenza di donne STEM.

Dott.ssa Fiorella LAMBERTI – (Leonardo – Women in AFCEA Rome Chapter) e **Dott.ssa Giuseppina PICCIRILLI** – (ASI – Responsabile Valorizzazione Immagine, Comunicazione e Capo Ufficio Stampa) – Saluti iniziali

Prof.ssa Loredana SANTO – Centro di Ricerca Space Sustainability

Col. Giuseppe GENTILE – SMD UGS – La sostenibilità dell'ambiente spaziale: la prospettiva della Difesa

Ing. Marina RUGGIERI – Università Tor Vergata Dipartimento Ingegneria – Sostenibilità nello spazio: sfide progettuali

Dott.ssa Alessandra DI CECCO – ASI – Progetti ground-based dell'ASI per la sostenibilità delle attività spaziali

Dott.ssa Annamaria NASSISI e Ing. Eleonora MOLTONI – Thales Alenia Space Italia – Azioni di mitigazione per la sostenibilità dello spazio

Dott.ssa. Annamaria DE BIASE – Thales Alenia Space Italia – ECO design: la sostenibilità nello spazio come estensione di quella sulla Terra

Ing. Eugenia FINOCCHIARO – CRISEL – Servizi Orbitali per Space Situational Awareness

Ing. Margherita CARDI – Tyvak International – Space sustainability: Tyvak International solutions

Dott.ssa Francesca LILLO – AVIO S.p.A.- La propulsione spaziale quale pilastro della Space Economy: sviluppi e sostenibilità

Cap. Ing. Veronica VISSICCHIO – SMD SICRAL – Problemi legati al sovraffollamento spaziale e non solo

PRIVATE CLOUD E OPEN SOURCE VIRTUALIZATION: I NUOVI SCENARI

31 OTTOBRE 2023

La continua evoluzione del mondo del Private Cloud è caratterizzata da un lato dalle le migrazioni dei Data Center sui Public Cloud dei tre leader di mercato, dall'altro dall'esigenza di detenere "in casa" una parte dei dati più sensibili che rilancia il ruovo Hybrid Cloud. Inoltre, in una società sempre più interconnessa online ogni pubblicazione di una foto sui canali social di fatto crea un nuovo data center in qualche parte del mondo. Ogni Data Center è formato da migliaia di computer che servono per memorizzare i dati che vengono prodotti giornalmente, sono accesi 24 ore al giorno 7 giorni su 7 e consumano energia elettrica. La Smart City produce milioni di dati anche attraverso gli oggetti interconnessi (sensori, videocamere, ecc..) alla rete, pertanto è fondamentale progettare Data Center sostenibili sia in termini di economicità sia di risparmio energetico. In tale contesto AFCEA Capitolo di Rom ha organizzato con VATES un convegno sul tema: Titolo: Private Cloud e Open Source Virtualization: I nuovi scenari.

VATES è da sempre impegnata a sviluppare sistemi di Virtualizzazione Open Source (il sistema operativo dei Data Center) sostenibili sia in termini di risparmio economico per la Pubbliche Amministrazione e le Aziende private sia in termini di risparmio energetico, contribuendo in ultima analisi agli obiettivi di riduzione del CO_2. Il convegno ha analizzato i nuovi scenari sia tecnologici sia di sostenibilità che richiedono pertanto oggi un nuovo approccio Hybrid/Open che consenta di raggiungere obiettivi di efficienza ed efficacia, riducendo l'impatto ambientale.

Dott. Leandro AGLIERI – Presidente e A.D. Vates Italia – VATES: Open Source Virtualization

Dott. Alessandro MUSUMECI – Capo Segreteria Tecnica del Sottosegretario all'Innovazione presso la Presidenza del Consiglio L'Open Source nella Pubblica Amministrazione

Col. Marco AGABITI – Capo Ufficio Ricerca V Reparto Segredifesa – L'Open Source nella Ricerca e nella Difesa

C.te Cataldo COLIZZI – Comando Operazioni Rete – Il Programma Scipio nel Comando Operazioni Rete Comandante

Dott. Carlo CAVAZZONI – Head of Computational R&D Leonardo Il Progetto di ricerca CertHPCDoc

Mr. Olivier LAMBERT – CEO Vates – VATES: The Open Source Virtualization Company – la roadmap

Mr.Charles SCHULZ – CSOr Vates – VATES: The Open Source Virtualization Company – la strategia di sviluppo

SORVEGLIANZA E DIFESA DELLO SPAZIO AEREO IN ITALIA: L'AERONAUTICA MILITARE AL SERVIZIO DELLA SICUREZZA NAZIONALE

22 NOVEMBRE 2023

In un mondo sempre più complesso e minaccioso, la sicurezza dello spazio aereo è diventata ancor di più una priorità strategica per l'Italia. E l'Aeronautica Militare ha un ruolo cruciale nella salvaguardia dello spazio aereo nazionale, contributo fondamentale alla più ampia Sicurezza Nazionale: ruolo che le è assegnato per legge. In questo contesto il Capitolo di Roma di AFCEA International, nell'anno 2023 che ha celebrato il centenario della fondazione dell'Aeronautica Militare Italiana, ha deciso di organizzare un convegno sulla Sorveglianza e Difesa dello Spazio Aereo in Italia.

Durante l'evento, sono stati evidenziati gli aspetti organizzativi, operativi, tecnologici del sistema di sorveglianza e difesa aerea italiano, mettendo in luce l'expertise e la tecnologia all'avanguardia che caratterizzano l'Aeronautica Militare, nel contesto delle sfide attuali e prospettive future della sorveglianza e della difesa dello spazio aereo, rappresentate dalla digitalizzazione e dalla proliferazione delle minacce, insieme alle opportunità offerte dall'innovazione tecnologica.

In particolare, sono stati esplorati quei sistemi che costituiscono il pilastro della sorveglianza aerea italiana, analizzando come questi mezzi e tecnologie avanzate vengono coordinati dai centri di comando altamente specializzati per individuare e monitorare qualsiasi minaccia potenziale, garantendo così la sicurezza degli spazi aerei italiani.

Nel corso del convegno è stato inoltre illustrato un aspetto che ha caratterizzato sin dagli inizi la Difesa Aerea italiana e cioè lo strettissimo coordinamento quotidiano con il Traffico Civile, evidenziando anche l'importanza della cooperazione internazionale, con un focus sulla collaborazione dell'Aeronautica Militare Italiana con la NATO.

Inoltre, si esamineranno. Il convegno sarà aperto da due keynote speech di due rappresentanti di altissimo livello uno per l'Aeronautica Militare ed uno per Leonardo, azienda leader nella Difesa. Seguiranno interventi del Comando Squadra Aerea, del Comando Logistico, di Teledife, dell'ENAV, e del comparto industriale.

Gen.S.A. Alberto BIAVATI – Comandante Squadra Aerea A.M. – L'Aeronautica Militare: Sorveglianza e Difesa dello Spazio Aereo

Ing. Manlio CUCCARO – Chief Operations, Procurement & Services Office Leonardo – La Difesa Aerea tra nuove minacce e un approccio integrato

Col. Aarnn Filippo MONTI – Comandante 4° Stormo – CSA – Presentazioni NATO and National QRA

Col. Garn Patrizio EMILIANI – Teledife 2^ Divisione - L'Evoluzione della Difesa Aerea Nazionale dal punto di vista Tecnologico

Col. AAran Felice D'ANELLI – Comando Logistico A.M. 1° Reparto – Il sostegno tecnico-operativo alla Difesa Aerea da parte del Comando Logistico 3^ Divisione

Dott. Paolo NASETTI e Ing. A. CAPOLEI ATM System Evolution and Strategic Services Planning – ENAV/Presidente & AD-Technosky – Il contributo del Gruppo ENAV alla Difesa Aerea

Ing. Emanuele BERGAMO e Ing. Giuseppe DE FEDERICIS – MATICMIND – Video Analisi AI Driven a Supporto dei Sistemi di Sicurezza Aerea

Prof.ssa Patrizia LIVRERI – CNIT-Lab RaSS, Pisa/Univ. Di Palermo – Towards a long-range microwave quantum radar

I contributi dei soci

THE KEY TO WINNING IS LEADING THE TRANSFORMATION RACE AGAINST OUR ADVERSARIES

AFCEA INTERNATIONAL LTGEN(R) SUSAN S. LAWRENCE

As cyber and other threats continue to menace our way of life, it's more important than ever that we discuss how the unified global community will lead the transformation race against our adversaries and keep our partnerships strong.

The persistent war in Europe changed things for NATO, the European Union and United States. The Russians have been able to upgrade their electronic warfare to vastly improve their defenses. Ukraine and its allies must be able to do the same. A trusted and verified software acquisition pathway is one step toward getting there, but we also must find ways to always be faster and more advanced than our adversaries.

The modern militaries of the United States and its global allies and partners run on software. We must be able to deploy, change and modernize software quickly and effectively. We must work hand-in-hand to lay the groundwork for monumental modernization of software practices for rapid delivery of new capabilities. The goal is to ultimately field capability into production on-demand as required, which may be in hours or days instead months or years.

Today's conflicts are also cyber wars and this paradigm showcases the need to protect infrastructure. Warfare is as much about protecting data and critical infrastructure as it is about protecting land and human life. Data grows more precious with every advance in next-generation cellular technologies, artificial intelligence, machine learning, unmanned systems and the "Internet of Things" components. It is central to our lives and for global security, and we rely on government, academia and industry together to safeguard this vital resource—regardless of the threat.

Additionally, the recent Volt Typhoon threat from Chinese hackers shows how important it is to work together against a common threat. It is worth noting that the Volt Typhoon warning was issued by several U.S. agencies, along with cyber centers in Australia, Canada, the United Kingdom and New Zealand. China is described as the pacing threat — meaning it is the only country that can threaten the United States economically, technologically, politically and militarily — but Russia, North Korea, Iran and others also pose a danger to our critical networks and infrastructure.

The Maryland Air National Guard partnered with Estonia's Cyber Command to host exercise Baltic Blitz. Photo courtesy Maryland National Guard.

Like links in a chain, every country is stronger when the others hold. Conversely, each country is only as strong as the weakest link in the global cyber chain. The sheer urgency of cyber cooperation needed across nations is challenging, almost terrifying.
A lot of challenges must be overcome to promote faster, more efficient and effective collaboration.

Thankfully, international cooperation has become the norm rather than the exception. That trend must continue. With an eye toward the future, we should strive for fully integrated operations between private and public agencies, organizations and select allies.

Which underscores the importance of the work AFCEA International and its Chapters play on the global security stage. Daily, we display the importance of the power of our association's members and their expertise to address and defeat the challenges. Thank you for your membership and contributions for many safer tomorrows.

I wish you all the best. Continue to go and do good work.

Best wishes,

Susan S. Lawrence

Lt. Gen. Susan S. Lawrence,
USA (Ret.)
President & CEO
AFCEA International

READINESS VS. DISRUPTIVE INNOVATION

Conflicting Goals for the Defence Industrial Base?

AFCEA EUROPE GENERAL MANAGER
MAJGEN ERICH STAUDACHER

In 2024, better than ever conditions exist for the Defence industry?

With the new Strategic Concept, collective defence and deterrence by readiness are back in NATO's – and this means predominantly in Europe's – reality.

With regional defence plans now in place, NATO's military planers are expecting delivery of technologies, equipment and supporting services in a much higher pace than in the era of crisis management that allowed ample time to carefully plan, purchase and predict. Decisions then often were slowed down and dictated by dwindling budgets.

NATO, and not lesser the EU, have undergone unprecedented change at an unprecedented pace in the last couple of years. Member states are substantially ramping up their defence budget, with defence expenditure in average growing by 18% in 2024, the biggest increase in decades, and they are aiming at immediate spending. In addition, the concept of Multidomain Operations (MDO) and its impact on data flow and interoperability between the military services, among Allies, and with all stakeholders in defence becomes an undeniable reality. Fortunately, and in broad scope, the ongoing digitalisation of the Allied Armed Forces experiences a boost, partially due to the new financial opportunities, partially due to new technologies such as Artificial Intelligence. So, all is good, everybody should be happy?!

I am sorry to kill your optimism: The reality still looks different. Military customers complain that "production times are lagging behind, delivery times are moving to the right, and prices are going through the roof" (Past Chair NATO Military Committee, Admiral Bauer). Vice versa, industry is troubled by missing decisions, missing contracts, unclear requirements, slow procurement processes.

Readiness requirements are the dominant factor today

The transformation of NATO and EU into the new era of increased readiness has just started. With a new generation of NATO defence plans in place, preparing the Alliance for high-intensity and multi-domain collective defence, substantial resources are required to equip, train, and support the new high-readiness forces "in a timely manner".

From last year's NATO Summit we kept in mind that "we need a robust and resilient defence industry, able to sustainably meet the need of significantly strengthened collective defence." Words to switch to a "wartime economy" model for the defence industry make its rounds.

Military planners and procurement specialists call for expeditious delivery of equipment to fill capability gaps and ask industry to scale up its production of well-established technology.

But also watch the technological edge in defence!

Supporting the urgent needs is not the only challenge for the defence industry, in particular the industry working in the C4ISR and Cyber domain. NATO for the last decade fervently emphasized the need to keep its technological edge. With the war in Ukraine starting in 2014 this goal has become even more important. As it has been stated in the 2024 Summit declaration: "We are accelerating transformation and the integration of new technologies and innovation, including through a plan to improve technology adoption".

The EU drives forward the creation of a European Defence Industrial Base with many programmes and multi-billion European Defence Fund investments. Realizing, that technological advancement in key defence industries – amongst again many in the C4ISR and Cyber field – not only constitutes the pre-requisite for the Alliance members' sovereignty but also provides information, decision, and effects advantages on the battlefield, indispensable for western forces outnumbered by peer enemies, big investments are undertaken to support the related industrial capacity.

It is obvious that a comprehensive, consistent digitalisation of the Armed Forces with game-changing features is essential for the Western nations to keep the upper hand in future conflicts. Digitalisation of the Armed Forces is a must for the survival on the battlefield, the broad and ethical employment of Artificial Intelligence will be indispensable for decision making processes, intelligence, cyber defence, logistics, military health systems and many more. We should remember V. Putin who warned in 2017 that "the one who becomes the leader in this sphere will be the ruler of the world."

Related activities to unearth disruptive future technologies, mostly based on innovations by start-ups and small and medium enterprises in the fields of surveillance, sensors, micro-biology, quantum, and above all, in artificial intelligence, have been initiated by programmes such as PESCO (EU), DIANA (NATO), and HEDI (EDA) with much fanfare.

From a customer standpoint both demands – support readiness and develop future capabilities – are legitimate and necessary. However, they proof to have some potential for conflicts. Even with increases of annually 2 % and more, following the Defence Investment Pledge, there are defence budgets in most nations that don't allow to fulfil all wishes, even with the big jumps ahead since 2022. Actually, the defence budget allocation for research and development (R&D) in support of basic research in industry and academia has been reduced in some nations.

In addition, the Armed Forces are challenged twice, as rapid investments in existing technologies need to be handled

in parallel to the deep changes happening while preparing for the coming future technologies, disruptive with regard to culture, training, and operational concepts. I can imagine, similar parallel requirements exist in industry and make decisions necessary where to focus in the light of limited number of experts. Beyond finances, human resources are to become the new constraint. E.g., the US Army, aware of such challenges, just recently established a strategy which divides the management and human resources attributed to "C2 Fix" (soldiers can communicate and fight on today's battlefield) and "C2 Next" (a prototyping effort the Army is working on with industry in order to experiment with a "data-centric" C2 system).

…and don't forget steadiness and supply chains

The ongoing global supply chain crisis underlines the necessity of a stronger, sustainable western Defence industrial base. If deterrence through digitalisation shall be credible, the equipment to support increased readiness must be state-of-the-art. Digitalisation at the same time drives changes in hard- and software with unprecedented speed. Development cycles until ready-to-market as short as 6-12 months for software, and 1 to 2 years for computer hardware conflict with procurement cycles of 3-5 years. Against this background, everybody acknowledges the urgency of a procurement reform, but just recently acceleration in procuring C5ISR solutions and services started cautiously with specific test projects and procedural improvements in certain nations and international agencies such as NCIA and NSPA. Of course, acquisition procedures need to be thorough and diligent. But tedious budgetary approval processes and political interference should be kept at a minimum. And a well-considered culture of failure should be accepted and introduced also in the procurement sphere.

This is even the more mandatory when implementing emerging, disruptive technologies into the Armed Forces as described above. Start-ups not only need entrepreneurial assistance, testing facilities, and seed money from venture capital to cross the "valley-of-death", they need the close communication with technological versed end-users in the military and courageous procurement specialist. The whole EDT community wants to see… more courage.

There must be a bridge between the actual urgently requested industrial capacities and acceleration measures, such as described in the Defence Production Action Plan agreed at the NATO Summit last year, and a long-term defence industry build-up, sustainable and reliable, which is capable to deliver and maintain tomorrow's technologies.

So, I am happy to see that "to that end, we (NATO) have today agreed the NATO Industrial Capacity Expansion Pledge" (Summit declaration 2024). The pledge aims to accelerate defence industrial capacity and production across the Alliance and underscores the strategic importance of transatlantic defence cooperation. It includes long-term actions such as developing national plans to strengthen industrial capacity, accelerating multinational procurement, enhancing the implementation of standards to increase interoperability, removing barriers to trade and investment, and securing critical supply chains.

In a similar move the EU established a programme – which is actually in its proposal stage, still to be decided by EU parliament –, the European Defence Industry Programme EDIP. It is intended to bridge the gap between short term measures to ramp up production and a more long-term resilience including the high-level, steady production of defence material according to the EU Defence Industry Strategy. Let's be optimistic that all these measures also affect the industry in the C5ISR domain with its special conditions and requirements!

It's time for a new partnership between government and industry

Such initial steps in reforming procurement to make production times to the point, delivery times not moving to the right, and prices staying under the roof can be the beginning of a new era in the relationship between government and industry. If C5ISR products and services delivered by industry reliably, and continuously developed further in close cooperation between original equipment manufacturer (OEM), system integrator, and user the expected outcome as described is possible. It means new contractual arrangements, constant exchange of information, mutual trust, delegated authority, and flexible terms of cooperation. This idea is not completely new, and in my view it is the only possibility to provide disruptive technologies at the trenches. But the idea has been buried somehow in the past. It doesn't not necessarily mean contractors staying permanently on the battlefield nor does it mean outsourcing of core services to industry, although both options should not be discarded from the outset completely.

And in such a new era the short-term requirements of readiness and the long-term requirements of implementing disruptive innovations could be more easily combined.

AFCEA Europe made its first efforts to discuss the subject at TechNet Europe 2023 in London where NCIA and UK procurement officials provided valuable inputs on the ongoing reform steps. The theme was further discussed at TechNet International 2024 in Brussels when NCIA, NSPA, and NATO ACT provided fresh insights into their consolidated reform packages.

It certainly will stay on AFCEA's agenda for a while because it is of crucial relevance today, and it is a theme that touches government/military, industry and academia equally. Finally, it may serve as a prime example for the ethical exchange of thoughts AFCEA stands for. The discussion will go on…

L'IMPORTANZA DELLA SFIDA IPERSONICA NEGLI SCENARI OPERATIVI ATTUALI E FUTURI

GEN.ISP.CAPO GIUSEPPE LUPOLI DIRETTORE DELLA DIREZIONE DEGLI ARMAMENTI AERONAUTICI E PER L'AERONAVIGABILITÀ

Introduzione

Negli ultimi decenni, l'evoluzione delle tecnologie ha portato a una serie di cambiamenti significativi nelle sfide delle operazioni militari e nelle strategie di difesa in generale, tanto da diventare uno dei fattori chiave per la ridefinizione dei concetti strategici, operativi e tattici delle moderne Forze Armate. Tra le cosiddette *Disruptive Technologies*, lo sviluppo di tecnologie ipersoniche riveste sicuramente carattere di rilievo fondamentale, rappresentando una svolta significativa per le Forze Armate di tutto il mondo: la possibilità di dotarsi di velivoli e armamenti capaci di viaggiare a velocità superiori a Mach 5 apre un alveo di soluzioni militari fino a ieri difficilmente ipotizzabili.

Quest'impegno si sostanzia in una duplice veste: da un lato, la necessità strategica di creare capacità di risposta negli scenari operativi attuali e futuri, mantenendo la propria rilevanza in campo internazionale; dall'altro, la valorizzazione del patrimonio tecnologico e industriale portato avanti dalla tradizione aeronautica nazionale.

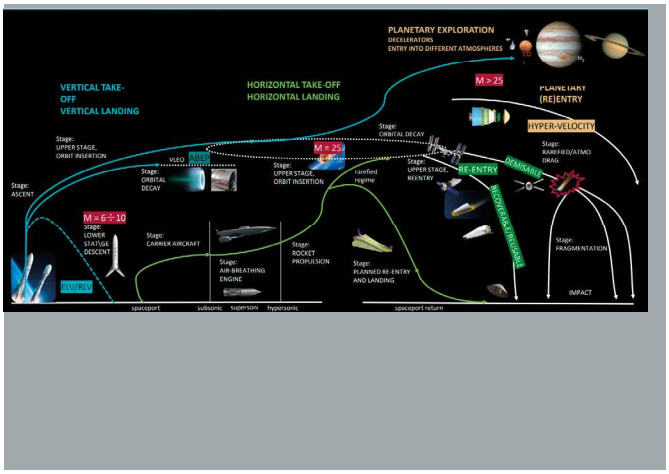
L'impatto che tale tecnologia avrà sulle nostre società e democrazie nei prossimi anni comporta, quindi, la necessità di sostenere gli sforzi nella ricerca, nello sviluppo e nella nuova transizione tecnologica verso sistemi di 6° generazione, affinché tutto il comparto industriale italiano della Difesa possa essere indirizzato verso le soluzioni strategicamente più adatte al ruolo che l'Italia vorrà avere in un panorama internazionale caratterizzato da flessibilità, rapidità d'azione e reattività.

La tecnologia ipersonica

In generale, esistono due principali categorie di tecnologie ipersoniche: i missili ipersonici e i velivoli ipersonici.

I missili ipersonici sono progettati per essere estremamente veloci, mantenendo tuttavia elevate capacità di manovra. Tali caratteristiche rendono più difficoltosa l'intercettazione da parte delle difese schierate permettendo di colpire obiettivi strategici anche a grande distanza in tempi sempre più ristretti, estendendo il proprio campo di azione potenziale anche allo spazio.

L'estrema velocità di azione dei velivoli ipersonici, invece, comporterà una rivoluzione sia in ambito di trasporto strategico, che nelle *Special Operation* e missioni ISTAR (*Intelligence, Surveillance, Target Acquisition and Reconnaissance*), laddove la velocità di esecuzione può fare la differenza tra il successo e il fallimento di un'operazione.



Ovviamente, la sfida tecnologica odierna risiede nello sviluppo di capacità non solo di tipo diretto, e quindi nello sviluppo dei missili e dei velivoli ipersonici, ma anche e soprattutto nel rafforzamento delle difese da minacce esse stesse di tipo ipersonico. In tal senso, è fondamentale lo sviluppo di sistemi di difesa "tradizionali" *ground based*, ma anche dei cosiddetti *glider interceptor*, sistemi balistici avanzati che sono progettati con propulsori di tipo *ramjet* e *scramjet* per l'intercettamento dei missili ipersonici nella loro traiettoria suborbitale.

Come già espresso nell'ultimo Concetto Strategico del 2022 e nel Documento Programmatico Pluriennale della Difesa per il Triennio 2022-2024, tali capacità di difesa potranno essere efficaci solo laddove ci si doti di una difesa integrata in ambito nazionale, inquadrata nella più ampia struttura alleata della NATO.

L'importanza operativa della tecnologia ipersonica

Come tutte le capacità *disruptive*, anche quella ipersonica contribuirà fortemente alla stabilità globale e alla prevenzione dei potenziali conflitti, permettendo di fatto di proteggere i propri interessi nazionali e quelli dei propri alleati in aree geografiche molto distanti. Tale capacità aumenta significativamente il potenziale di deterrenza espresso da un Paese, permettendo una risposta rapida e con impatti strategici significativi alle eventuali minacce di potenziali forze ostili, concetti alla base della definizione stessa di deterrenza.

Negli scenari operativi attuali, diviene quindi sempre più importante affrontare tale sfida per contrastare quella che è la crescente proliferazione di Paesi dotati di capacità offensive con armi di distruzione di massa, che, sfruttando anche le nuove tecnologie ipersoniche, possono costituire una minaccia sempre più pericolosa per il nostro Paese e per i Paesi alleati. Nell'ultimo biennio, Paesi come la Nord Corea e la Russia hanno mostrato di avere a disposizione una capacità di questo tipo, utilizzandola sia a fini dimostrativi che in teatro operativo reale.

Lo scenario attuale rimane denso di una molteplicità di minacce, che vanno dalle organizzazioni terroristiche a Stati con capacità di tipo nucleare. È, quindi, ancora più importante poter agire in maniera flessibile e rapida direttamente sulle basi di lancio o sui siti di Comando e Controllo, riducendo la capacità di risposta ostile, avendo la possibilità di intervenire per neutralizzare le infrastrutture strategiche (come silos di missili nucleari, impianti di produzione di armi chimiche o biologiche e basi aeree e navali) prima che questi possano lanciare un potenziale attacco.

In futuro, oltre agli scenari attuali, si prevede sempre più la possibilità di azioni potenzialmente ostili ad alta intensità con proiezione di forza globale. Gli interessi strategici si concentreranno nei nuovi domini cibernetico e spaziale, laddove la rapidità di intervento offerta dai sistemi ipersonici potrebbe rivelarsi cruciale. Infatti, sistemi integrati di difesa ipersonica potranno incrementare l'attuale capacità di difendere satelliti e le loro stazioni di Comando e Controllo, e di contrastare in tempi brevissimi attacchi di tipo cibernetico. Lo spazio sarà il teatro ideale per svolgere attività di controllo e tracciamento dei vettori missilistici balistici e ipersonici. A maggior ragione, sarà fondamentale garantirne la protezione e la difesa da attacchi nemici.

È chiaro che la sola capacità ipersonica non può essere sufficiente a garantire un corretto funzionamento della macchina della Difesa, laddove non integrata con tutte le altre capacità operative che un Paese come l'Italia possiede e sviluppa continuamente, anche in collaborazione con i suoi partner alleati.

Come tutte le capacità, anche quella ipersonica dovrà pertanto necessariamente innestarsi all'interno di un sistema di Difesa un Sistema di Sistemi il cui funzionamento sarà dettato dalle eventuali necessità che si verranno a delineare. Nessuna capacità è di per sé sufficiente per garantire un contesto di pace e di non belligeranza; purtuttavia, per quanto già detto, quella ipersonica avrà un ruolo determinante in termini di dissuasione, velocità di reazione e potenzialità difensiva.

Risvolti tecnologici e industriali

Lo sviluppo di una tecnologia di nicchia quale quella ipersonica passa attraverso una serie di *gap* tecnologici da colmare. Tali *gap* riguardano diverse discipline, a partire dal settore dell'aerodinamica spinta e della termodinamica, che interessa imprescindibilmente la gestione del calore e resistenza dei materiali di nuova concezione, il settore della propulsione ma anche le sfide dei sistemi avionici di navigazione, controllo, comunicazione e *sensing*, sottoposti a tempi di azione e reazione che richiedono elevatissima precisione dell'*output* fornito.

In tal senso, collaborazioni con Università, centri di ricerca e industrie *high-tech* hanno da sempre un risvolto duale che investe anche gli altri ambiti di interesse puramente civile. A partire dall'aviazione commerciale, che sta esplo-

rando già da tempo le nuove possibilità legate ai viaggi suborbitali e spaziali, all'industria dell'*automotive*, interessata a sistemi di controllo efficaci per i veicoli autonomi, financo a soluzioni impiegabili per il risparmio energetico e l'efficientamento termico delle strutture edili.
Un'altra sfida significativa è rappresentata dall'integrazione di queste tecnologie con i sistemi e con le risorse umane attuali. Ad esempio, l'adattamento delle infrastrutture fisiche (i.e. spazioplani), di quelle tecnologiche (i.e. gallerie del vento ipersoniche) dovrà procedere di pari passo alla costruzione di una rete di condivisione dati tra le diverse comunità scientifiche, industriali e militari di riferimento. Parimenti, sarà fondamentale la formazione continua di personale specializzato non solo nei settori evidentemente più pertinenti al campo ingegneristico. Ad esempio, le implicazioni di carattere medico e fisiologico dovute ai voli ipersonici in regime suborbitale potranno creare fattori di stress rilevanti sul corpo umano, con la necessità di elaborare piani di preparazione fisica, monitoraggio e recupero adattivi.
È quindi evidente che lo sviluppo di tecnologie ipersoniche ha ricadute positive sull'industria nazionale, sullo sviluppo di *know-how* e sulla creazione di posti di lavoro altamente specializzati, in settori notoriamente ad alto valore aggiunto per il Paese.
Un programma di tale respiro tecnologico va, tuttavia, affrontato all'interno di un *framework* internazionale più ampio. L'Italia è da sempre coinvolta in programmi di ricerca e sviluppo con gli alleati della NATO e dell'Unione Europea. Tale coinvolgimento permette la condivisione di risorse, competenze e costi, riducendo il rischio finanziario e tecnologico per ciascun Paese partecipante e facilitando l'interoperabilità tra le varie Forze Armate.
Dal punto di vista industriale, la cooperazione con altri partner internazionali permette altresì una crescita dell'industria nazionale tramite l'accesso a competenze e risorse non sempre disponibili internamente. Tuttavia, nonostante alcuni punti deboli da affrontare in maniera sistematica, il potenziale di ricerca e sviluppo dell'Italia è alla pari con quello dei Paesi più avanzati in ambito militare e tecnologico, creando le condizioni necessarie per proporsi quale *leader* di settore in ambito internazionale. Ciò è particolarmente evidente nei campi come la modellazione aerodinamica, la creazione di nuovi materiali, i vettori di propulsione sostenibili e la sicurezza informatica nelle reti di comunicazione.
Quanto riportato è anche il frutto di iniziative intraprese in ambito Ministero della Difesa, come ad esempio il Convegno tenuto in Accademia Aeronautica a Pozzuoli (NA) nel Novembre del 2023, in cui più di 80 esperti del settore si sono riuniti per dare vita a dei *board* tematici volti ad esaminare gli aspetti fondamentali legati allo sviluppo delle capacità ipersoniche, nel tentativo di contribuire a definire una sempre più moderna strategia di difesa aerea nazionale. È indubbio lo sforzo per il perseguimento di un obiettivo più ampio, che mira a raggiungere la massima qualità ed eccellenza possibile del settore per l'Italia e la sua industria, puntando ad una nuova Economia della Difesa forte e consolidata, che sia il motore trainante della costante innovazione tecnologica del Paese.

Dottrina e normativa

Dal punto di vista operativo, l'adozione di tecnologie ipersoniche richiede una revisione delle dottrine militari esistenti, sia dal punto di vista strategico che tattico, per sfruttare appieno le capacità di rapidità e di penetrazione offerte da questi nuovi sistemi. Tale revisione dovrà tenere conto degli scenari di minaccia attuali e futuri, ma anche del processo di cambiamento tecnologico e umano in atto.
Inoltre, l'utilizzo di sistemi ipersonici solleva questioni etiche e di diritto internazionale, soprattutto in relazione alla loro capacità distruttiva, per cui è fondamentale lavorare da subito allo sviluppo di regole d'ingaggio chiare e in linea con il diritto internazionale.
Dal punto di vista certificativo e di *safety* dei sistemi, la sfida sarà quella di adattare la normativa e i processi attualmente in vigore a questa tecnologia innovativa. Solo per fare un esempio, i sistemi ipersonici si basano su nuovi materiali termoisolanti, dotati di tecnologie di raffreddamento attivo, con capacità di resistenza a elevatissime temperature e a forze aerodinamiche intense, che richiedono uno sforzo non solo puramente tecnico ma anche volto a dimostrarne la rispondenza a standard di sicurezza aeronautica.

Continuare il lavoro di aggiornamento della normativa aeronautica è fondamentale per contemplare tutte le fattispecie legate a questa nuova dimensione tecnologica. Ad esempio, l'adozione di una regolamentazione comune in ambito internazionale sui lanciatori suborbitali si ritiene rappresenti una priorità strategica, sia a livello politico che industriale. L'implementazione di certificazioni appropriate per la sostenibilità e la sicurezza tecnologica incoraggerà il raggiungimento di capacità e promuoverà la *leadership* nel settore aerospaziale di chi si farà promotore di tali iniziative.

Conclusioni

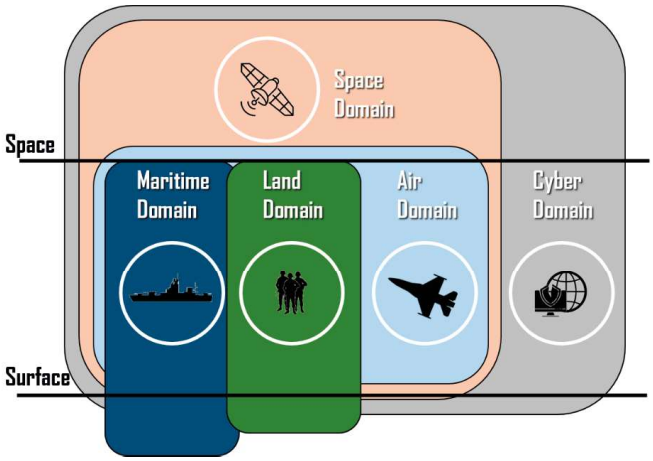
L'adozione e lo sviluppo di tecnologie ipersoniche rappresenta una sfida cruciale e un'opportunità unica per il Paese e il suo comparto industriale. Queste tecnologie offrono vantaggi significativi in termini di superamento delle difese aeree, rapidità nelle operazioni e, quindi, di deterrenza per potenziali azioni ostili, divenendo, negli scenari operativi attuali e futuri, decisive per le sorti nelle situazioni di crisi. Allo stesso tempo, lo sviluppo di tali tecnologie comporta un forte investimento industriale che in proiezione porterà una notevole crescita professionale ed economica di tutto il settore e dell'indotto correlato.

Il percorso verso il raggiungimento di tali capacità è irto di sfide tecnologiche, industriali e operative che richiedono un approccio olistico. Per questo motivo, è essenziale che l'Italia continui l'investimento attualmente in atto in ricerca, sviluppo, formazione e cooperazione internazionale, per assicurarsi il mantenimento di una presenza di rilievo nel panorama delle tecnologie avanzate incluso quella ipersonica.

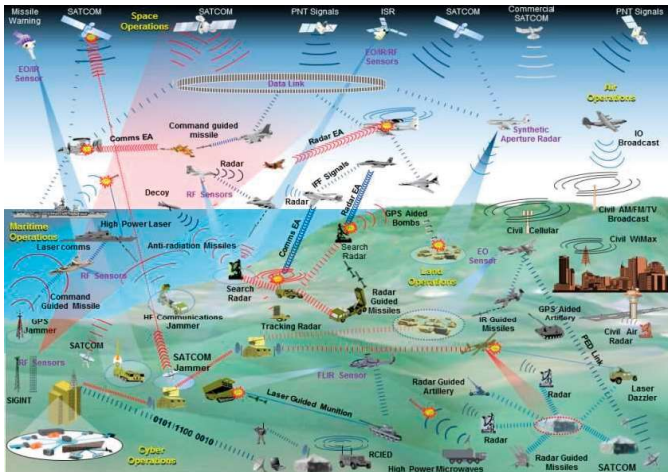
LA GUERRA ELETTRONICA TERRESTRE NELLE OPERAZIONI MULTIDOMINIO

COL. ING. S.SM MAURO ANDREA RODDI
CAPO DELLA 6ª DIVISIONE DELLA
DIREZIONE DEGLI ARMAMENTI TERRESTRI

Le operazioni multidominio rappresentano una frontiera strategica cruciale per la difesa moderna, un approccio olistico che integra e sincronizza le capacità militari attraverso tutti i domini di battaglia: terra, mare, aria, spazio e cibernetico. Quindi multidominio non solo riferito alla classica visione dei cinque domini considerati in modo separato o comunque a *layer* tra loro operativamente collegati ma, secondo una visione molto più moderna e più impattante dal punto di vista operativo, quella che correla domini operativi con le dimensioni di influenza: gli effetti delle attività sui singoli domini possono avere impatti sulla dimensione cognitiva e quindi su quello della percezione in ogni dominio. Questa concezione operativa risponde quindi alla necessità di affrontare una pluralità di situazioni molto diverse tra loro che, di conseguenza, comportano minacce di tipologia e pericolosità sempre più difficili da affrontare.



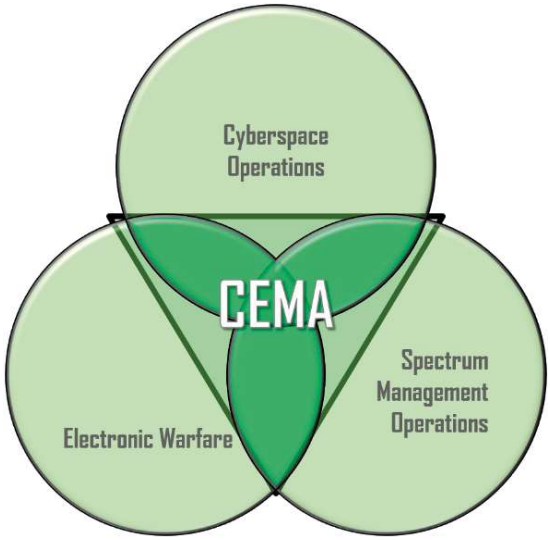
Nel contesto appena delineato, le *Cyber Electromagnetic Activities* (CEMA) e le *Electromagnetic Spectrum Operations* (EMSO) possono influenzare la dimensione cognitiva del campo di battaglia, quale parte integrante dell'ambiente fisico e informativo, influenzando significativamente la capacità dei *decision maker* attraverso la manipolazione delle loro dinamiche cognitive. Di fatto la competizione nella dimensione cognitiva (*Cognitive Warfare* – CW), nella sua dimensione intangibile, prende di mira ideologie, valori e società attraverso un uso sempre più esteso di mezzi di comunicazione e nuove soluzioni tecnologiche. In tal senso la CW si può quindi definire come un'operazione multidominio che impiega mezzi, azioni e strumenti attraverso le connessioni esistenti tra i cinque domini, l'ambiente informativo e lo spettro elettromagnetico per generare effetti nella dimensione cognitiva e influenzare il comportamento umano per ottenere un vantaggio sull'avversario. In questo ambito proprio le CEMA possono quindi essere utilizzate per generare vantaggi strategici, attraverso lo sfruttamento delle vulnerabilità dei sistemi per rendere indisponibili servizi primari, inibire le comunicazioni, disarticolare la catena di comando e controllo delle operazioni, al fine di influenzare e potenzialmente manipolare il comportamento degli avversari. La competizione nella dimensione cognitiva è quindi diventata la componente essenziale dei moderni conflitti, da considerarsi ormai a tutti gli effetti "ibridi", con un confronto tra le parti esteso a nuove aree immateriali, che sfruttano le tecnologie emergenti e le neuroscienze per produrre effetti strategici.



Il contrasto a tali dinamiche, la comprensione e l'elaborazione delle informazioni in tale ambito, richiedono funzioni cognitive avanzate, quali ad esempio l'attenzione selettiva e sostenuta o la memoria di lavoro, al fine di permettere agli operatori di analizzare rapidamente i dati, di adattarsi a situazioni in rapido cambiamento e di prendere decisioni informate in ambienti complessi e spesso stressanti. La formazione e la preparazione in queste aree sono cruciali per sviluppare le competenze necessarie a gestire efficacemente le operazioni CEMA e EMSO, garantendo così il successo delle missioni e la sicurezza delle forze coinvolte.

Dal punto di vista pratico, gli impatti delle *Cyber Electromagnetic Activities* (CEMA) nelle operazioni militari possono essere molteplici e variegati. Ad esempio, le opera-

zioni di guerra elettronica possono includere la diffusione di informazioni false o ingannevoli per confondere o disorientare il nemico, influenzandone così il processo decisionale. Inoltre, le CEMA possono essere impiegate per intercettare o interrompere le comunicazioni nemiche, causando incertezza e ritardi nelle risposte operative. Un altro esempio è l'uso di tecniche di ingegneria sociale attraverso il *cyberspace* per manipolare individui o gruppi, inducendoli a compiere azioni che possono compromettere la sicurezza o rivelare informazioni sensibili. Infine, le PsyOps, o operazioni psicologiche, rappresentano un altro aspetto delle CEMA, dove si utilizzano messaggi mirati per influenzare le percezioni e le emozioni, con l'obiettivo di indebolire il morale o alterare il comportamento delle truppe nemiche. Questi esempi dimostrano come le CEMA possano avere un impatto diretto e significativo sugli aspetti cognitivi, sfruttando la dimensione psicologica della guerra per ottenere vantaggi strategici.



Per la condotta delle operazioni in tale scenario di riferimento, si rende necessario un utilizzo di una componente di *Electronic Warfare* che sia distribuita, coordinata e coerente in tutti i domini. Ciò per la necessità di geolocalizzare e classificare tutti gli emettitori avversari in tempi compatibili con lo svolgimento delle operazioni, possibilmente in *real* time o al più in *near* real time. Ancor di più, devono essere comprese le modalità e le tecniche utilizzate su segnali caratterizzati da crescente sofisticatezza e complessità con l'obiettivo ultimo e come livello di ambizione massimo di eseguire il *fingerprinting* dell'emissione, ovvero, individuare non solo la famiglia e tipologia di emettitore utilizzato ma identificare il singolo dispositivo utilizzato in maniera tale da poterlo riconoscere una volta che verrà di nuovo intercettato e, se del caso, ingaggiarlo.

Tali concetti hanno impatti sull'implementazione tecnologica degli strumenti di *Electronic Warfare* o *Electromagnetic* Warfare, come introdotto in alcune pubblicazioni dottrinali, che dovranno essere caratterizzati da capacità "agili" (*software based*) ovvero in grado di adattarsi rapidamente alle nuove minacce, in tempo reale o in *near real time*. Accanto alla componente *hardware/software* è necessario, in un approccio EW omnicomprensivo, utilizzare anche tecniche ibride, rispetto a quelle classiche, per consentire una individuazione delle emissioni di interesse andando ad integrare altre tecnologie per consentire una maggiore capacità di localizzazione.

L'esperienza maturata negli ultimi due anni nel conflitto Russo-Ucraino ha dimostrato il vasto utilizzo di tecniche di EW allo scopo di impedire le comunicazioni e il C2 nelle operazioni, raccogliere le informazioni attraverso attività *Intelligence Surveillance and Reconnaissance* ISR e disturbare i segnali GPS, attraverso tecniche di diniego e *spoofing*, fattore questo determinante non solo ai fini della localizzazione e navigazione ma anche ai fini della sincronizzazione di tutti gli altri sistemi.

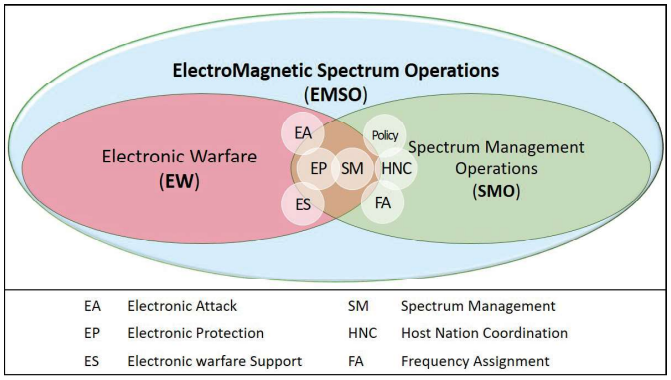
L'esperienza ha quindi dimostrato un ritorno al passato su una disciplina classica che forse per tanti aspetti, eccetto quelli di autoprotezione contro gli ordigni improvvisati (*Radio Controlled - Improvised Explosive Device* - RC-IED), è stata per tanti anni sopita. Accanto alle tecniche di EW classiche, l'elemento di novità è rappresentato dall'introduzione contemporanea delle attività cyber, portando alla sperimentazione pratica del concetto espresso nelle CEMA, con la conseguente dimostrazione del potenziale dell'EW di influenzare l'esito degli scontri senza un'azione cinetica diretta.

Assieme ai suddetti fattori, le recenti esperienze hanno dimostrato l'utilizzo estensivo di droni sia in funzione di sensori, ad esempio con *payload* EW integrato, sia come strumenti cinetici. In tale ambito impedire il funzionamento di questi sistemi amplia ovviamente le attività della guerra elettronica nello spettro elettromagnetico.

Infine, quale ultimo fattore da valutare nell'ambito della pianificazione e sviluppo di attività CEMA, va considerato lo sviluppo di applicazioni di Intelligenza Artificiale, ormai disponibili anche a costi estremamente ridotti e utilizzabili anche senza un elevato grado di formazione: nello scenario descritto, attraverso applicazioni di Intelligenza Artificiale è quindi possibile perpetrare attività offensive

anche senza una esperienza consolidata o una conoscenza approfondita. Ancor di più, l'intelligenza artificiale può essere utilizzata per modificare nel tempo questi tipi di attacchi e quindi rendere mutevole e difficile da contrastare la minaccia; ciò comporta la progettazione di sistemi di contrasto *AI based*.

Quindi, nello scenario sopra illustrato le CEMA, considerate come l'insieme coordinato delle attività di *Cyber Operation* (CO), *Electronic Warfare* (EW) e *Spectrum Management Operations* a disposizione della F.A., dovranno assolvere alla loro funzione essenziale di cogliere, sfruttare e mantenere un vantaggio sugli avversari sia nel *cyberspazio* sia nello spettro elettromagnetico, impendendone l'uso o degradandone le funzionalità e proteggendo al contempo il sistema di comando e controllo della missione.



Come detto, ancorché le operazioni CEMA si svolgano in una dimensione fisica e in quella informativa, esse hanno lo scopo di sostenere gli obiettivi della dimensione cognitiva e per ottenere questo, senza subire l'influenza delle azioni avversarie, è necessario da un lato costruire, gestire e difendere la propria rete e dall'altro condurre azioni tipiche di EW, aggiornate all'evolvere in tutte le nuove sfaccettature che lo scenario operativo ci presenta: solo attraverso tali azioni sarà possibile acquisire la *situation awarness* ed una visione omnicomprensiva dello scenario operativo su un unico sistema, anche attraverso l'integrazione di sensori che oggi sono utilizzati anche per altre attività. Se da un lato le CEMA forniscono quindi un approccio globale comprendenti il cyberspazio e lo spazio elettromagnetico, sussistono ulteriori fattori necessari alla completa riuscita di queste attività che integrano la gestione dello spettro alla EW: le ElectroMagnetic Spectrum Operations (EMSO) che si concentrano specificamente sulla gestione e il controllo dello spettro elettromagnetico. CEMA ed EMSO sono essenziali per raggiungere la superiorità operativa nei moderni ambienti di guerra guidati dalla tecnologia in quanto tramite esse si possono conseguire l'EMS *superiority* e la *dominance* dello spettro nei confronti degli avversari è fondamentale per governare e poter muoversi liberamente in questo ambiente operativo che, ancorché non definito in maniera strutturata, è però determinante per la condotta delle battaglie.

Ovviamente, tale dominio dello spettro elettromagnetico sarà sempre più complicato da ottenere sia per la sua crescente congestione, anche in considerazione della prossima introduzione delle tecnologie 6 G che avranno effetti ancor più dirompenti del 5 G, sia per l'integrazione da parte degli avversari di tecnologie di Intelligenza Artificiale applicate alle comunicazioni che permetteranno una maggiore mutevolezza delle stesse. Ciò richiede che negli sviluppi degli assetti da impiegare sia garantita una capacità di attacco e di difesa nello spettro elettromagnetico che sia adattiva e agile. Ciò richiede delle architetture *software based* ed aperte in grado quindi di modificarsi in tempo reale sul campo di battaglia, anche attraverso l'impiego di tecniche di intelligenza artificiale integrata nei propri sistemi di comando e controllo per contrastare le eventuali minacce avversarie. Tali architetture dovranno necessariamente integrarsi non solo con le componenti tecniche e specialistiche di Forza Armata dei Reparti di Guerra Elettronica, ma con sensori appartenenti ad ulteriori componenti presenti sul campo di battaglia. Assieme alla parte tecnica è necessario altresì garantire la necessaria formazione e l'addestramento al fine di trasferire le capacità tecnologiche di un sistema nei confronti dell'operatore.

In conclusione l'adozione di operazioni multidominio richiede una visione strategica nazionale condivisa e trasversale, che superi le separazioni concettuali rigide e promuova l'integrazione e l'interoperabilità tra sistemi, sensori, processi e attori coinvolti. La rapidità dell'evoluzione tecnologica e la gestione della complessità dello scenario multidominio prefigura l'introduzione e la realizzazione di infrastrutture tecnologiche complesse e comunque vulnerabili che devono essere progettate e implementate con caratteristiche di resilienza e immunità alle azioni avversarie al fine di garantire il vantaggio strategico.

Ciò richiede un costante livello di adeguamento ed innovazione tecnologica che deve essere aiutata anche dalle componenti esterne alla Difesa e quindi centri di eccellenza, università, centri di ricerca ma soprattutto l'industria privata. Tale innovazione, come detto, non potrà

prescindere ovviamente dall'introduzione di strumenti di intelligenza artificiale a "bordo" in grado di esprimere le necessarie capacità di contrasto, ma sempre in un'ottica di ausilio e supporto alla componente umana, che dovrà restare, anche nelle operazioni multidominio, il cuore e l'elemento principale.

Riferimenti:

STATO MAGGIORE DELLA DIFESA – Approccio della Difesa alle Operazioni Multidominio, Ed.2022
NATO – AJP-3.6 -ALLIED JOINT DOCTRINE FOR ELECTRONIC WARFARE Ed. 2020
US Joint Chiefs of Staff – Joint Electromagnetic Spectrum Operations Ed. 2020
US Department of the Army – Field Manual (FM) 3-38 - Cyber Electromagnetic Activities Ed. 2014
STATO MAGGIORE DELLA DIFESA - *Cognitive Warfare* La competizione nella dimensione cognitiva Ed. 2023

UTILIZZO DELLA BLOCKCHAIN PER I DATA LAKE FEDERATI

ALMAVIVA

La tecnologia Blockchain, un tempo sinonimo solo di criptovalute, ha ormai permeato diversi settori, compreso quello della gestione dei dati. In particolar modo, si sono rilevati diversi vantaggi nell'utilizzo della tecnologia blockchain nei Data lake federati per la condivisione dei dati, le differenze tra blockchain pubbliche e private e il concetto di soluzioni Layer 2.

I Data Lake federati consentono la condivisione e la distribuzione dei dati tra diverse organizzazioni. A differenza dei Data Lake tradizionali, che archiviano tutti i dati in un'unica posizione centralizzata, i **Data Lake federati** distribuiscono i dati su più sistemi decentralizzati. Ciò consente alle Organizzazioni di mantenere il controllo sui propri dati, rendendoli comunque accessibili per l'uso condiviso.

La tecnologia blockchain, d'altra parte, è un tipo di tecnologia distribuita: crea una piattaforma decentralizzata in cui tutte le transazioni sono registrate in modo sicuro e trasparente. Ogni transazione viene memorizzata in un blocco e collegata alla precedente, formando una catena. Ciò rende i record immutabili, il che significa che non possono essere modificati o eliminati una volta aggiunti alla blockchain.

Quando i data Lake federati vengono integrati con la tecnologia blockchain, si crea un potente strumento per la condivisione dei dati, con i seguenti requisiti:

1. **Integrità dei dati:** l'immutabilità dei record della blockchain garantisce che, una volta aggiunti, i dati non possano essere modificati o eliminati. Ciò garantisce l'integrità degli stessi, rendendoli una fonte di informazioni affidabile per tutti i partecipanti.
2. **Trasparenza e fiducia:** la natura distribuita della blockchain promuove la trasparenza poiché tutti i partecipanti hanno accesso alle stesse informazioni. Ciò favorisce la fiducia tra i partecipanti, poiché possono verificare i dati in modo indipendente.
3. **Sicurezza:** la struttura decentralizzata della Blockchain e le tecniche crittografiche ad essa associate, forniscono un elevato livello di sicurezza. È quasi impossibile per gli hacker alterare i dati poiché avrebbero bisogno di modificare le informazioni su più della metà dei nodi della rete, il che è computazionalmente impraticabile.
4. **Condivisione efficiente dei dati:** la combinazione di Data Lake federati e Blockchain consente una condivisione efficiente dei dati. È possibile accedere ai dati in tempo reale e l'uso dei cosiddetti **"smart contracts"** può automatizzare il processo di condivisione dei dati, riducendo la necessità di intervento manuale.

Blockchain Pubbliche vs. Blockchain Private

Le blockchain pubbliche consentono a chiunque di unirsi alla rete, partecipare ai processi di consenso e convalidare le transazioni. Le blockchain private, al contrario, limitano l'accesso a un gruppo specifico di partecipanti con ruoli e autorizzazioni definiti, garantendo che solo le entità autorizzate possano partecipare.

Al giorno d'oggi, le blockchain pubbliche stanno passando da meccanismi di consenso ad alta intensità di risorse come **Proof of Work (PoW)** ad alternative più scalabili ed efficienti come **Proof of Stake (PoS)**. La PoS ottiene il consenso selezionando i validatori in base al numero di token che detengono. Le blockchain private spesso utilizzano meccanismi di consenso ancora più efficienti come la **Practical Byzantine Fault Tolerance (PBFT)** o la **Proof of Authority** (anch'essa una soluzione BFT), che sono adatti per ambienti più piccoli e controllati e forniscono conferme delle transazioni più rapide.

Il vantaggio principale delle blockchain pubbliche, sono i numerosi nodi che contribuiscono alla sicurezza e alla decentralizzazione della rete. Reti più grandi rendono più difficile, per ogni singola entità, manipolare la blockchain. Le blockchain private, con le loro dimensioni di rete più piccole, potrebbero avere meno sicurezza e decentralizzazione, rendendole più vulnerabili alla collusione e alla manomissione.

Dall'altra parte, per quanto riguarda la **privacy**, le blockchain pubbliche archiviano e condividono apertamente i dati delle transazioni, rendendoli accessibili a tutti i parteci-

panti alla rete. Questa trasparenza può essere vantaggiosa ma solleva anche problemi di privacy. Al contrario, le blockchain private possono limitare la visibilità dei dati a partecipanti specifici, offrendo maggiore privacy e controllo sulle informazioni sensibili.

Le blockchain pubbliche sono ideali per ambienti "trustless" in cui i partecipanti non hanno bisogno di fidarsi l'uno dell'altro, sapendo che possono semplicemente verificare ogni transazione con la sicurezza fornita dalla tecnologia.

Le blockchain private sono più adatte per situazioni che richiedono una sorta di fiducia tra i partecipanti, come all'interno di consorzi o organizzazioni, consentendo una collaborazione efficiente, la condivisione dei dati e processi semplificati. Gli utenti possono comunque verificare le transazioni, ma a causa delle dimensioni ridotte della rete, non possono essere sicuri che nessuno sia complice nel modificare qualcosa.

La scelta tra blockchain pubbliche e private, per un Data Lake federato, dipende in gran parte dai requisiti specifici del caso d'uso. Se il Data Lake contiene informazioni sensibili che dovrebbero essere accessibili solo a determinate entità, una blockchain privata potrebbe essere più adatta. Tuttavia, una blockchain pubblica potrebbe essere la scelta migliore se sono necessarie piena trasparenza e fiducia.

Sfruttare al meglio entrambe le modalità: il Layer 2

Il **Layer 2** si riferisce a un framework o protocollo secondario costruito su una blockchain esistente. Lo scopo principale di questi protocolli, è risolvere i problemi di scalabilità e di privacy, che affliggono le reti blockchain, senza comprometterne la sicurezza.

Le blockchain private, utilizzate principalmente da aziende e organizzazioni per scopi interni, traggono grandi vantaggi dalle soluzioni Layer 2. Queste soluzioni migliorano la privacy delle transazioni, un requisito fondamentale per le aziende che devono proteggere i dati sensibili. Mantenendo i dati delle transazioni sulla rete privata e registrando solo lo stato finale su una blockchain pubblica, le soluzioni Layer 2 garantiscono che le informazioni private rimangano riservate.

Periodic State Anchoring

Il **Periodic State Anchoring** è un protocollo che prevede la creazione periodica di un'istantanea dello stato della blockchain privata, rappresentata da un "hash" crittografico, a intervalli specifici. Questa istantanea viene quindi registrata su una blockchain pubblica, garantendo una registrazione a prova di manomissione dello stato della blockchain privata in vari momenti nel tempo. In caso di sospetta manomissione, i partecipanti possono verificare l'integrità della blockchain privata confrontando il suo stato attuale con gli snapshot precedentemente ancorati sulla blockchain pubblica. È un protocollo facile da implementare e più economico da utilizzare rispetto ad altre soluzioni.

Uno dei principali avvertimenti, in merito a questo approccio, è la verifica "a posteriori" dello stato della blockchain privata. Ciò significa che la validità dello stato della blockchain privata viene verificata dopo che questa è stata ancorata alla blockchain pubblica. Ciò può rappresentare un problema perché se una transazione dannosa o errata viene inclusa nello stato ancorato, non verrà rilevata fino a dopo il fatto. Nel momento in cui viene scoperto lo stato difettoso, le informazioni errate potrebbero essere già state utilizzate o gestite, portando a potenziali problemi o imprecisioni all'interno della blockchain.

Zero Knowledge Rollup

Gli **Zero Knowledge Rollup** offrono un approccio alternativo al protocollo spiegato sopra, in cui le transazioni vengono verificate prima di essere incluse nello stato blockchain. Ciò si ottiene utilizzando **"prove a conoscenza zero"**, un metodo crittografico che consente a una parte di dimostrare a un'altra che un'affermazione è vera senza fornire alcuna informazione aggiuntiva.

Gli Zero Knowledge Rollup possono impedire in primo luogo l'inclusione di transazioni errate, migliorando così l'integrità della blockchain. Tuttavia, presentano una serie di sfide.

La sfida principale è la complessità delle dimostrazioni a conoscenza zero. Si tratta di una tecnologia relativamente nuova e complessa e la loro corretta implementazione richiede un elevato livello di competenza. Ciò può rendere gli Zero Knowledge Rollup più difficili da implementare rispetto ad altre soluzioni.

Inoltre, i requisiti computazionali per generare e verificare prove a conoscenza zero possono essere significativi. Ciò può limitare i miglioramenti della scalabilità che i rollup Zero-Knowledge possono fornire e può anche comportare costi più elevati.

TECNOLOGIE IA ED EVOLUZIONE DELLE IDENTITÀ DIGITALI

ARUBA.IT

La sinergia tra l'identità digitale e l'intelligenza artificiale rappresenta un terreno fertile per l'innovazione, ma anche una fonte di sfide senza precedenti. Per sfruttare appieno le opportunità introdotte dall'intelligenza artificiale è fondamentale conoscere i rischi e mitigarli, per una vita digitale più sicura.

Ruolo dell'Intelligenza Artificiale nell'Identità Digitale

La trasformazione digitale di beni e servizi si caratterizza di due direttrici di innovazione:

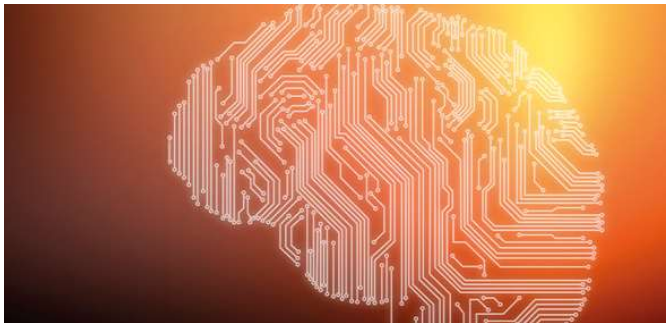
1. **L'affermazione sempre più pervasiva del ruolo dell'identità digitale:** Oggi la nostra identità non è più limitata ai documenti fisici; la nostra identità digitale, rappresentazione virtuale della propria identità reale, è chiave in ogni interazione elettronica nei confronti di persone o di sistemi informatici. Riveste un ruolo fondamentale nel mondo digitale poiché consente l'interazione sicura e fidata tra utenti e servizi online, garantendo che solo gli utenti legittimi possano accedere alle risorse protette. La crescente importanza dell'identità digitale è evidente anche nelle normative odierne, come il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea e il nuovo Digital Identity Framework (eIDAS 2.0), che mirano a standardizzare e proteggere le identità digitali, promuovendo la sicurezza e l'affidabilità nei servizi digitali.
2. **L'introduzione dell'intelligenza artificiale come forza trainante e abilitante l'innovazione tecnologica e di business:** l'IA non è più solo una tecnologia emergente ma si sta affermando come una forza trainante per affrontare il prossimo "salto tecnologico". Dall'automazione dei processi aziendali all'analisi predittiva, fino alla personalizzazione dei servizi, l'IA sta trasformando radicalmente il modo in cui le aziende operano e interagiscono con i clienti.

Una Relazione Sinergica: Opportunità e Rischi

È interessante esplorare quale sarà l'effetto combinato di queste due potenti direttrici. Quali sono le opportunità che ci attendono? E quali i rischi connessi?

Le principali Opportunità:

- **Miglioramento della Sicurezza e della Fiducia:** Combinando l'IA con identità digitali sicure è possibile creare sistemi di autenticazione avanzati che rilevano e prevengono le frodi in tempo reale. Questo non solo protegge gli utenti ma aumenta anche la fiducia nella trasformazione digitale di beni e servizi;



- **Esperienze Personalizzate e Efficienza Operativa:** Con l'IA che analizza le preferenze degli utenti attraverso le loro identità digitali, si possono offrire esperienze altamente personalizzate, migliorando la soddisfazione del cliente e ottimizzando le operazioni;
- **Inclusione Digitale:** l'IA e le identità digitali possono rendere i servizi digitali più accessibili a tutti, indipendentemente dalla loro posizione geografica o dalle loro risorse, promuovendo l'inclusione sociale ed economica.

I principali Rischi:

- **Violazione della Privacy:** l'IA necessita di una grande mole di dati per alimentare i proprio algoritmi; con l'aumento della raccolta di dati personali, la protezione dei dati assume una centralità ulteriore. In aggiunta, l'uso inappropriato dei dati da parte dell'IA può portare a violazioni della privacy;
- **Sicurezza dei dati:** La gestione e la protezione delle identità digitali possono essere compromesse da attacchi informatici sofisticati eventualmente connaturati all'uso dell'IA;
- **Bias e Discriminazione:** Se l'IA viene addestrata con dati distorti o parziali, può perpetuare e amplificare i bias esistenti, causando discriminazioni;
- **Dipendenza Tecnologica:** L'eccessiva dipendenza da tecnologie avanzate può rendere le società vulnerabili alle relative minacce che possono determinare interruzioni tecnologiche o attacchi cibernetici, mettendo a rischio la resilienza dell'ecosistema digitale.

Da tutto ciò si deduce che la sinergia tra l'identità digitale e l'intelligenza artificiale rappresenta un terreno fertile per l'innovazione, ma anche una fonte di sfide senza precedenti. Per sfruttare appieno le opportunità e mitigare i rischi, è fondamentale che aziende, legislatori e sviluppatori tecnologici collaborino strettamente. Solo attraverso un approccio comune etico e responsabile possiamo garantire che queste tecnologie lavorino per il bene comune, creando un futuro digitale sicuro, equo e inclusivo.

In questo articolo, si esplorerà quali **aree di contatto l'IA** sta avendo con i temi dell'identità digitale e come questa può essere utilizzata per **supportare le verifiche dell'identità digitale** prestando particolare attenzione ai principali **rischi** che può introdurre.

Esempi di applicazione dell'IA nelle Identità Digitali

L'applicazione dell'IA nell'ambito delle Identità Digitali si può declinare in diversi contesti ed esempi, tra cui:

1. Riconoscimento Biometrico

La "verifica dell'identità digitale" è un aspetto cruciale per garantire che solo le persone autorizzate abbiano accesso a servizi online, dati particolari o risorse digitali.

L'identificazione biometrica rappresenta una delle evoluzioni più significative nell'ambito dell'identità digitale, offrendo un livello di sicurezza e usabilità senza precedenti. Questa tecnologia sfrutta le caratteristiche uniche e intrinseche degli individui, come il volto, le impronte digitali, la voce e l'iride, per verificare l'identità di una persona. Grazie ai progressi nell'intelligenza artificiale e all'uso di algoritmi avanzati, queste tecniche sono diventate sempre più precise e affidabili, trovando applicazione in vari contesti quotidiani e professionali. I principali metodi di riconoscimento sono:

- **Riconoscimento facciale,** ad esempio, è ampiamente utilizzato per sbloccare dispositivi, nei controlli di sicurezza e per l'accesso ad aree e/o risorse critiche. Questo sistema si basa sull'analisi delle caratteristiche del viso, come la distanza tra gli occhi, la forma del naso e la conformazione della mascella. Le tecnologie alla base del riconoscimento facciale includono algoritmi di deep learning e reti neurali convoluzionali (CNN), che analizzano milioni di immagini per apprendere le caratteristiche distintive dei volti umani. Ad esempio, nei sistemi di sorveglianza urbana, il riconoscimento facciale viene utilizzato per identificare individui sospetti o scomparsi in tempo reale, migliorando notevolmente la sicurezza pubblica;
- **Riconoscimento della voce** sfrutta le caratteristiche vocali uniche di ogni individuo, analizzando parametri come il tono, il timbro, il ritmo e le intonazioni della voce. Gli algoritmi di riconoscimento vocale utilizzano tecniche di machine learning e reti neurali ricorrenti (RNN). Tali tecnologie sono impiegate non solo in assistenti vocali, ma anche in sistemi di autenticazione per l'accesso a servizi bancari, dove gli utenti possono autorizzare operazioni semplicemente parlando. Un esempio pratico è l'uso del riconoscimento vocale per accedere ai conti bancari tramite chiamate telefoniche, dove il sistema verifica l'identità dell'utente attraverso un'analisi della sua voce;
- **Riconoscimento dell'iride e della retina** rappresenta una delle tecniche biometriche più precise, basandosi su caratteristiche oculari uniche e difficilmente replicabili. Algoritmi di matching avanzati, spesso costruiti con strumenti di deep learning, confrontano questi dati con quelli memorizzati per autenticare l'individuo. Queste tecniche sono utilizzate in settori ad alta sicurezza come quello militare e governativo, come nel caso dell'accesso a strutture e/o risorse critiche.

2. Analisi comportamentale e prevenzione delle frodi

L'analisi comportamentale e la prevenzione delle frodi sono diventate priorità cruciali fruizione dei beni e servizi digitali, con la crescente dipendenza dalle tecnologie online e dall'identità digitale.

Due approcci fondamentali in questo ambito sono il rilevamento di comportamenti anomali e l'analisi in tempo reale dei dati.

Il rilevamento di comportamenti anomali si basa sull'identificazione di deviazioni significative dai pattern di comportamento normali. Questo approccio utilizza algoritmi di machine learning per analizzare i dati storici e costruire modelli di comportamento standard per utenti, dispositivi o sistemi. Quando un'attività si discosta significativamente da questo modello, viene segnalata come anomala, potenzialmente indicativa di un'attività fraudolenta o di un attacco informatico. Ad esempio, se un utente accede improvvisamente a un sistema da una posizione geografica insolita o in orari inconsueti, l'algoritmo può identificare questa attività come sospetta. Tecniche comuni utilizzate includono le reti neurali ricorrenti (RNN) e le macchine a supporto vettoriale (SVM). Trova applicazione in diversi contesti come ad esempio nei servizi bancari, ove può essere utilizzata per monitorare le transazioni dei clienti e individuare operazioni sospette; nell'e-commerce per rilevare attività di frode nell'acquisto di beni e servizi.

L'analisi in tempo reale dei dati rappresenta un'altra applicazione nella sicurezza e prevenzione delle frodi. Questa tecnica implica la raccolta, l'elaborazione e l'analisi immediata dei dati man mano che vengono generati. Utilizzando piattaforme di big data, i dati possono essere analizzati in tempo reale per identificare e rispondere rapidamente alle minacce emergenti. Gli algoritmi di apprendimento automatico vengono utilizzati per analizzare i flussi di dati in tempo reale, rilevando modelli sospetti e attivando allarmi o misure di sicurezza automatiche.

Un'applicazione di analisi in tempo reale dei dati è il monitoraggio delle transazioni online. I sistemi possono analizzare ogni transazione in tempo reale per verificare se corrisponde ai comportamenti tipici dell'utente. Se una transazione è atipica, come un acquisto di alto valore da un

luogo insolito, il sistema può bloccare immediatamente la transazione e richiedere una verifica aggiuntiva.

Minacce introdotte dall'IA nelle Identità Digitali

Se da un lato l'IA offre opportunità per migliorare la sicurezza dell'identità digitale, dall'altro introduce nuovi rischi che possono compromettere la privacy e la sicurezza degli utenti. Ecco alcuni esempi:

1. Falsificazione dell'identità e social engineering

Nel contesto dell'IA, due tra i rischi più insidiosi sono rappresentati dalla falsificazione dell'identità, o anche detto *deepfake*, e dal social engineering, entrambi capaci di ingannare sistemi di sicurezza avanzati e compromettere la fiducia nell'autenticazione digitale.

Il deepfake è una tecnica che sfrutta l'intelligenza artificiale, in particolare le reti neurali generative avversarie (GAN), per creare immagini, video o audio falsi che appaiono straordinariamente realistici. Le GAN consistono in due reti neurali che competono tra loro: una genera contenuti falsi (generatore) mentre l'altra cerca di rilevare i falsi (discriminatore). Attraverso questo processo iterativo, il generatore migliora continuamente la qualità dei contenuti falsi fino a renderli quasi indistinguibili da quelli reali. Questo rende il deepfake una minaccia potente, capace di manipolare la percezione visiva e uditiva delle persone. Ad esempio, un attacco di spoofing tramite deepfake può creare un video in cui un individuo appare dire o fare qualcosa che in realtà non ha mai fatto, potenzialmente danneggiando la sua reputazione o utilizzando la sua immagine per accedere a sistemi di sicurezza basati sul riconoscimento facciale.

Per contrastare questi rischi, sono in fase di sviluppo algoritmi di rilevamento dei deepfake, che analizzano dettagli specifici come i movimenti degli occhi, le espressioni facciali e le incongruenze nell'illuminazione per identificare contenuti falsi.

L'ulteriore rischio da non sottovalutare è quello relativo a tecniche di ingegneria sociale che già prima dell'IA avevano un impatto significativo per l'identità digitale, infatti questi attacchi si basano sulla manipolazione psicologica delle persone per indurle a rivelare informazioni riservate o compiere azioni che compromettono la sicurezza. Gli attacchi di ingegneria sociale possono assumere diverse forme, tra cui phishing, spear phishing, pretexting e baiting. Casi più rappresentativi sono l'invio di e-mail fraudolente che sembrano provenire da fonti affidabili, come banche o organizzazioni governative, inducendo gli utenti a fornire le loro credenziali di accesso o altre informazioni sensibili. L'ingegneria sociale può essere potenziata dall'IA per rendere gli attacchi ancora più sofisticati e difficili da rilevare. Gli algoritmi di machine learning possono essere utilizzati per analizzare grandi quantità di dati pubblicamente disponibili sui social media per creare messaggi di phishing altamente personalizzati e credibili. Inoltre, i bot alimentati da IA possono interagire con le vittime in tempo reale, rispondendo alle loro domande e dissipando eventuali sospetti che potrebbero sorgere durante l'attacco.

In questo contesto l'arma migliore contro questa tipologia di rischio sono gli utenti, è fondamentale educare gli utenti sulle tecniche comuni utilizzate dagli attaccanti e implementare misure di sicurezza avanzate, come l'autenticazione a più fattori, che richiede più di un metodo di verifica per accedere ai sistemi. Inoltre, l'uso di algoritmi di rilevamento delle anomalie può aiutare a identificare comportamenti sospetti che potrebbero indicare un tentativo di ingegneria sociale in corso.

2. Bias e monipolazione dei dati

L'alterazione del dataset di addestramento dei modelli di IA, conosciuta anche come *data poisoning*, si verifica quando vengono intenzionalmente introdotti dati falsificati o compromessi. Questo fenomeno diventa sempre più preoccupante con la crescente diffusione di chatbot e assistenti digitali.

Poiché i risultati dei modelli di intelligenza artificiale sono influenzati dai dati utilizzati durante l'addestramento, l'inclusione di dati inaffidabili o malevoli può portare il modello a formare pregiudizi o a prendere decisioni sbagliate.

Ad esempio, in un contesto di riconoscimento facciale, un attaccante potrebbe introdurre immagini alterate nel dataset di addestramento, facendo in modo che il modello non riesca a riconoscere correttamente determinate persone o categorie di persone. Allo stesso modo, dati di transazioni falsificati possono essere inseriti per ingannare un modello di rilevamento delle frodi, facendogli classificare transazioni fraudolente come legittime. Le alterazioni dei dati di addestramento non solo compromettono l'accuratezza del modello, ma possono anche ridurre la sua capacità di generalizzare correttamente su nuovi dati. Un modello di IA utilizzato per la diagnosi medica, se addestrato su dati compromessi, potrebbe fare diagnosi errate, mettendo a rischio la salute dei pazienti.

Per mitigare questi rischi è essenziale implementare robusti meccanismi di verifica e pulizia dei dati, tecniche di outlier detection e anomaly detection che possono aiutare a identificare e rimuovere dati sospetti.

Un altro approccio efficace è l'uso di framework di machine learning federato che consente l'addestramento di modelli su dati distribuiti senza necessità di centralizzare i dati. Questo riduce il rischio di data poisoning, poiché gli attaccanti devono compromettere molteplici nodi indipendenti invece di un singolo dataset centralizzato.

CASO STUDIO – Aruba Remote Digital Onboarding

Per comprendere meglio le implicazioni pratiche dell'interazione tra IA e identità digitali, esaminiamo un caso studio specifico che illustra come queste tecnologie possano essere implementate nel mondo reale. Il caso in questione riguarda un progetto sperimentale di Aruba, che utilizza l'intelligenza artificiale per migliorare i processi di verifica dell'identità digitale. Questo esempio permette di esplorare i benefici derivanti dall'uso dell'IA e come superarne le sfide e le potenziali vulnerabilità.

Creare un'identità digitale sicura è essenziale per ridurre il rischio di frodi e furti di identità, preservare la reputazione online e garantire la privacy dei dati personali. A tal fine, prima di erogare un'identità digitale, è essenziale implementare un sistema di riconoscimento che garantisca i più elevati standard di sicurezza.

Realizzare una soluzione di remote onboarding e identity proofing è un esempio di come l'intelligenza artificiale può essere di supporto ai processi di identificazione e più in generale allo sviluppo dell'identità digitale in Italia.

Aruba, in tale ambito, sta sperimentando un'innovativa soluzione di *remote digital onboarding* basata su tecniche AI con focus sulla implementazione, integrazione e validazione di modelli di intelligenza artificiale, unite alle più canoniche metodologie di sicurezza informatica.

Lo scopo ultimo è quello di creare un processo di identificazione sicuro che possa garantire con maggior precisione possibile le seguenti tre fasi:

1. Certezza della sorgente di acquisizione, mediante l'utilizzo di differenti tecniche atte a determinare l'univocità, la veridicità e l'integrità delle componenti hardware e software con il fine di prevenire metodi di contraffazione come:
   - hijacking dell'hardware del dispositivo: tecnica con la quale si cerca di far credere al dispositivo che delle componenti hardware esterne, come ad esempio delle camere, siano parte del dispositivo stesso, ma in realtà sono sotto pieno controllo dell'attaccante;
   - hijacking del traffico di rete: tecnica usata per cambiare le evidenze raccolte sul dispositivo durante la fase di invio dei dati al fine di inoltrare delle evidenze contraffatte, confezionate ad hoc per lo scopo;
   - reverse engineering del codice applicativo: tecnica usata per capire il funzionamento del software usato in modo da trarne vantaggio;
   - injection and substitution del codice applicativo a runtime: tecnica usata per sfruttare falle software al fine di eseguire del codice malevolo e modificare il comportamenteo del software stesso a proprio vantaggio.
2. Validazione della presenza di un soggetto reale: la sfida maggiore in cui l'IA esercita un ruolo cruciale, grazie alle sue specificità, è quella della "Biometric Presentation Attack Detection (PAD)", ovvero la capacità di individare di essere di fronte ad un artefatto costruito ad hoc per ingannare il sistema. Tali sfide sono normate dall ISO/IEC 30107 e hanno come obiettivo la prevenzione di attacchi ben noti come:
   - print attacks: tentativi di impersonificazione dell'utente finale tramite l'utilizzo di foto stampate e/o digitali;
   - replays attacks: tentativi di impersonificazione dell'utente finale tramite l'utilizzo di video riprodotti su dispositivi esterni;
   - 3D masks attacks: tentativi di impersonificazione dell'utente finale tramite l'uso di maschere 3D fisiche;
   - DeepFake attacks: tentativi di impersonificazione dell'utente finale tramite l'uso di modelli di intelligenza artificale per sostituire all'interno di un video i tratti somatici del soggetto con quelli di cui si intende simularne le fattezze.
3. Identificazione certa del soggetto fisico: dopo aver garantito di non essere di fronte ad un artefatto e/o ad un dispositivo malevolo, è fondamentale assicurarsi che il soggetto in questione sia effettivamente la persona che dichiara di essere. A tal fine è fondamentale che l'utente utilizzi documenti di identità aderenti alle ultime tecnologie e standard internazionali comprovati, più comumentemente denominati e-documents. Questo garantisce di poter sfruttare le caratteristiche digitali del documento per ottenere informazioni già certificate, dall'ente erogatore, in fase di emissione dello stesso. L'analisi di tali documenti, unita all'uso di ulteriori modelli di'intelligenza Artificiale per la validazione degli stessi, garantisce che non ci si trovi davanti ad un caso di clonazione, furto e/o smarrimento del documento stesso.

È chiave per il successo di queste soluzioni rispondere all'aspettativa dei clienti di una interazione immediata ed una user experience agevole in tutte le fasi del processo, già a partire da quella iniziale dell'onboarding. Per questo occorre continuare a sperimentare e fare buon uso di risorse come l'intelligenza artificiale per identificare pattern di comportamento anomali e segnalare potenziali tentativi di registrazione fraudolenta, e al contempo facilitare la verifica dell'identità tramite tecnologie avanzate e potenziare in generale tutte le operazioni.

Un uso consapevole dell'intelligenza artificiale potrà aiutarci a garantire che solo utenti legittimi abbiano accesso ai servizi digitali ed offrire ancora più protezione alle informazioni sensibili durante l'intero processo di onboarding.

GSE IN AEROPORTO: UNA RIVOLUZIONE... INTELLIGENTE

AVIOGEI AIRPORT EQUIPMENT

L'industria dell'aviazione tiene in contatto il mondo con il trasporto di persone e merci.
Con il progredire della tecnologia, un numero sempre maggiore di persone viaggia.
Quest'anno si prevede che il traffico globale di passeggeri raggiunga i 9,4 miliardi. In questo contesto il monitoraggio di tutte le componenti delle operazioni aeroportuali è di vitale importanza al fine di evitare costosi ritardi, che nel caso del trasporto passeggeri comporterebbero anche il verificarsi di un'esperienza negativa di viaggio.
L'impiego dell'intelligenza artificiale (AI) negli aeroporti può aiutare a snellire le operazioni, aumentare l'efficienza e migliorare l'esperienza di viaggio complessiva.
In questo articolo si intende illustrare alcune applicazioni dell'AI nel settore aereo, con particolare attenzione al possibile impiego su mezzi GSE (Ground Support Equipment) aeroportuali, evidenziandone i vantaggi e le sfide che ne deriverebbero.
Diverse tecnologie AI, come l'apprendimento automatico, l'elaborazione del linguaggio naturale (NLP) e la computer vision, stanno trasformando il settore dell'aviazione.
L'apprendimento automatico utilizza algoritmi per la creazione di modelli per l'ottimizzazione dei programmi di volo e dei relativi tempi di consegna e per la previsione dei guasti alle apparecchiature prima che si verifichino.
Il settore del GSE aeroportuale, che include una vasta gamma di attrezzature utilizzate per il supporto a terra degli aerei, come veicoli di servizio, nastri trasportatori, scale passeggeri, rimorchi per bagagli e attrezzature di rifornimento etc.., ha già compreso da tempo la rivoluzione che l'introduzione ed integrazione dell'AI e del machine learning può produrre negli ambiti della "Manutenzione Predittiva" e della Gestione e Geolocalizzazione delle Flotte.
AVIOGEI, leader a livello internazionale nella progettazione, costruzione e certificazione dei GSE, già da tempo ha sperimentato sulle proprie attrezzature modalità di acquisizione di dati operativi destinati alla geolocalizzazione, allo stato dei mezzi e alla gestione "on time" delle attività di manutenzione previste. Tale modalità considera anche l'acquisizione e gestione dati da remoto.
Il successivo sviluppo prevede l'implementazione di sensori IoT (Internet of Things) sui veicoli GSE capaci di raccogliere dati in tempo reale su vari parametri operativi, come temperatura, vibrazioni e pressione, e di sottoporli all'analisi di algoritmi di Machine Learning, per identificare schemi

che precedono i guasti, permettendo così di programmare interventi di manutenzione preventiva.
I risultati attesi per tale implementazione comprendono:

- riduzione del 30% dei guasti imprevisti;
- aumento del 20% della vita utile dei veicoli;
- riduzione del 15% dei costi operativi totali;

Tutte le informazioni ottenute, analizzate e processate dall'AI, possono individuare problemi, snellire i flussi di lavoro e assicurare che le regole di sicurezza siano rispettate.
Nel corso del tempo, questi dati possono aiutare gli aeroporti a migliorare sistematicamente le loro operazioni, portando a processi di movimentazione a terra più fluidi, sicuri e ottimizzati.
Tuttavia, l'implementazione delle applicazioni di AI negli aeroporti può incontrare diversi ostacoli. Alcune delle sfide più note sono legate agli alti costi delle infrastrutture, alla privacy dei dati, alle implicazioni etiche e all'integrazione con i sistemi esistenti.
Analoghe sfide si presentano anche in altri settori, ma nel settore dell'aviazione ci sono sfide specifiche.
L'impiego dell'AI deve soddisfare standard rigorosi e superare numerosi test, perché qualsiasi anomalia potrebbe avere gravi conseguenze.
Un'altra sfida è data dalla difficoltà di adattamento ai diversi ambienti aeroportuali, poiché ogni aeroporto opera con modalità specifiche, con diversi livelli di traffico passeggeri, con l'utilizzo di svariate tipologie di aeromobili. I sistemi di AI devono gestire tutte queste condizioni.
Inoltre, ottenere l'approvazione degli enti normativi e delle parti interessate del settore può essere difficoltoso
I sistemi di AI devono rispettare rigide norme di sicurezza e questo ne può rallentare il processo di sviluppo e distribuzione delle soluzioni. Convincere le compagnie aeree, gli operatori aeroportuali e i passeggeri che l'AI è affidabile e vantaggiosa richiede molti sforzi.
AVIOGEI è fortemente impegnata a sviluppare con specifiche collaborazioni, l'applicazione di queste nuove tecnologie che comprendono, tra l'altro, anche l'implementazione di nuove forme di propulsione delle attrezzature con l'impiego del nuovo vettore energetico idrogeno.

LA NAVIGAZIONE SATELLITARE NELL'ERA MODERNA

Un aggiornamento sul sistema GPS Global Positioning System per i moderni sistemi APR

B.M.A.

Il primo sistema di posizionamento satellitare per impiego professionale e militare è stato il sistema Transit sviluppato dal DOD americano che vide la luce nel 1960 quando il primo satellite, sviluppato su studi della Johns Hopkins University, raggiunse la sua orbita polare ad una altezza di 1.100 km.

Transit

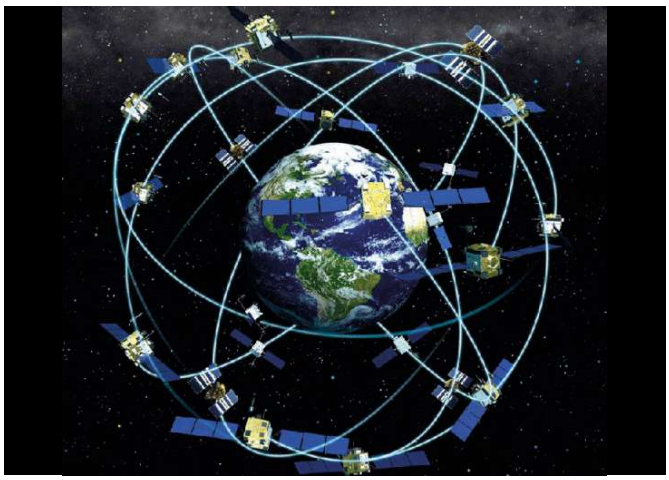
A partire dal luglio 1967 il sistema di navigazione basato su tali satelliti fu reso disponibile all'uso civile. La costellazione di satelliti a bassa quota era organizzata per far transitare un satellite ogni ora circa sulla stessa zona della terra.

La posizione del ricevitore veniva determinata utilizzando il satellite come stazioni multiple nelle diverse posizioni sull'orbita sfruttando l'effetto Doppler del segnale trasmesso per il calcolo del punto.

Il sistema Transit nacque per fornire la posizione molto precisa e correggere l'errore di deriva dei sistemi inerziali dei sottomarini Polaris americani. Conoscendo le effemeridi dei satelliti il ricevitore di bordo calcolava l'orario di passaggio del satellite ed il sottomarino si portava a quota periscopica per sollevare l'antenna e ricevere i dati. Con i dati ricevuti aggiornava la posizione (fix) correggendo l'errore di deriva dei sistemi di navigazione autonoma.

Il sistema Transit andava bene per le piattaforme a bassa dinamica quali navi o veicoli terrestri ma non in campo aeronautico dove era necessario un sistema capace di offrire una capacità di calcolo della posizione, della velocità e del tempo con continuità per le piattaforme aeree ad alta ed altissima dinamica.

Nacque così il GPS NAVSTAR sistema basato su una costellazione iniziale di 24 satelliti in orbita a 10.000 Km dalla terra capace di assicurare una copertura in tutte le aree del mondo di almeno 4 satelliti in vista del ricevitore.



Costellazione GPS

Il ricevitore/processore ricevendo il segnale da ciascun satellite in vista contenente l'informazione di tempo accuratissima e le coordinate del satellite calcola la propria posizione misurando la propria distanza da ciascun satellite. La misura di distanza si effettua correlando il segnale ricevuto dal satellite con una replica dello stesso segnale generata in locale nel ricevitore/processore. La misura dello sfasamento temporale è proporzionale alla distanza antenna ricevente-satellite. Con la misura delle quattro o più distanze si determina la posizione del ricevitore.

Le stazioni a terra (Ground Control Stations) gestiscono i satelliti per mantenerli sulla propria orbita correggono l'errore di tempo dell'orologio di bordo ed aggiornano le effemeridi di ciascuno di essi. I satelliti trasmettono due frequenze L1 ed L2 e le informazioni relative alle posizioni dei satelliti vengono codificate con codici a diverso grado di sicurezza. Un codice C/A (Clear Access) disponibile a tutti, in pratica quello che oggi utilizziamo nei nostri smartphone o navigatori per uso civile ed un codice P preciso e cifrato per l'impiego militare da parte dei Paesi NATO e autorizzati dal Ministero Difesa Americano.

L'esperienza ha dimostrato la straordinaria bontà del sistema di posizionamento globale ed ha avuto un elevatissimo successo tant'è che è stato replicato dall'Europa con il sistema Galileo, dalla Federazione Russa con il GLONASS, dalla Cina con il sistema BeiDou, dall'India con il sistema GAGAN, dal Giappone con il sistema QZSS.

L'utilizzo del sistema GPS nei teatri operativi ha però dimostrato alcune limitazioni perché con la moderna tecnologia sono stati sviluppati sistemi capaci di interferire (jamming) fino ad annullare il segnale utile del GPS o addirittura sostituire il segnale GPS simulando un segnale simile ma con dati ed effemeridi sbagliate (spoofing) cioè capaci di far calcolare una posizione sbagliata all'utente.

Satellite GPS della nuova costellazione

Sulla base di queste esperienze il Ministero Difesa Americano ha iniziato all'inizio degli anni 2000 a studiare e sperimentare segnali con una capacità di resistenza al disturbo molto più potenti e con codici di cifratura capaci di migliorare la sicurezza e la resistenza allo spoofing.

GPS Block III satellites

Satellite	USA designation	SVN	Name	Launch Date (UTC)	Rocket	Launch Site	Status
GPS III-01	USA-289	74	*Vespucci*	23 December 2018, 13:51	Falcon 9 Block 5	CCSFS, SLC-40	In Service
GPS III-02	USA-293	75	*Magellan*	22 August 2019, 13:06	Delta IV M+ (4,2)	CCSFS, SLC-37B	In Service
GPS III-03	USA-304	76	*Matthew Henson*	30 June 2020, 20:10	Falcon 9 Block 5	CCSFS, SLC-40	In Service
GPS III-04	USA-309	77	*Sacagawea*	5 November 2020, 23:24	Falcon 9 Block 5	CCSFS, SLC-40	In Service
GPS III-05	USA-319	78	*Neil Armstrong*	17 June 2021, 16:09	Falcon 9 Block 5	CCSFS, SLC-40	In Service
GPS III-06	USA-343	79	*Amelia Earhart*	18 January 2023, 12:24	Falcon 9 Block 5	CCSFS, SLC-40	In Service

Piano di messa in orbita dei nuovi satelliti GPS e già operativi

Inoltre sono state sperimentate nuove frequenze e nuove modulazioni del segnale migliorando notevolmente la capacità e la sicurezza del sistema. Le novità introdotte sono state sperimentate mantenendo comunque la compatibilità dei nuovi satelliti con i precedenti ricevitori degli utenti.

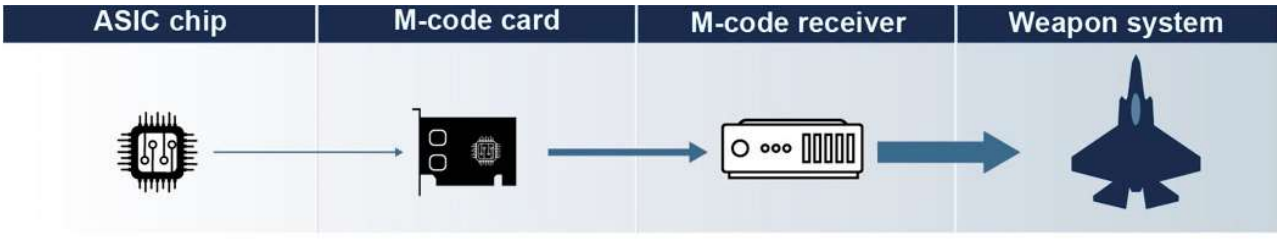
In particolare il nuovo codice M è stato sperimentato per l'impiego sicuro. Esso viene trasmesso dalla nuova costellazione di satelliti GPS che sarà completata per la fine di questo decennio.

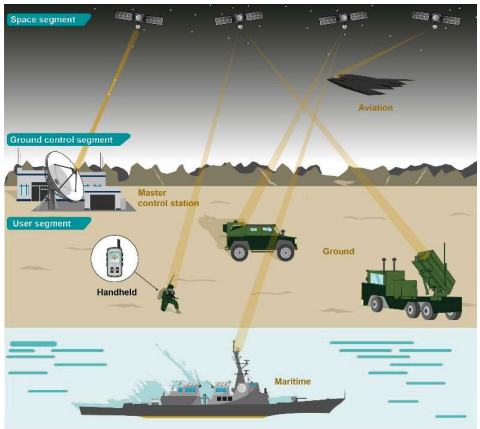
Il codice M è un segnale GPS più forte, criptato e specifico per il settore militare, progettato per soddisfare le esigenze di informazioni PNT (Position, Navigation, Timing) militari. Il codice M permette di superare i tentativi di blocco del segnale GPS, noti come jamming, utilizzando un segnale più potente con una gamma di frequenze più ampia. Inoltre, proteggerà dai falsi segnali GPS, noti come spoofing, criptando il segnale.

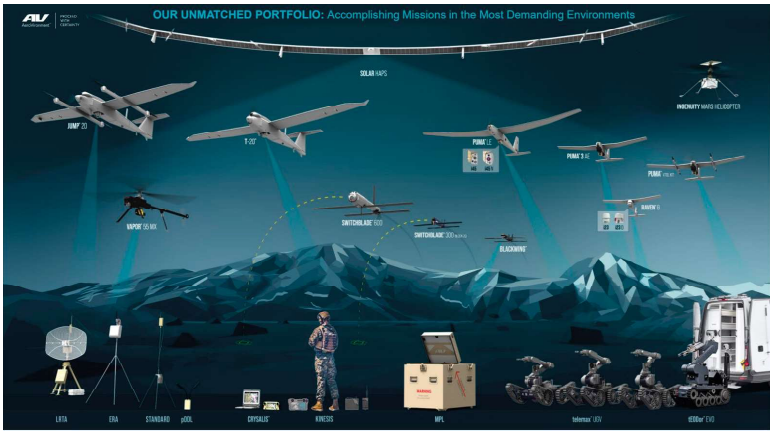
I risultati sperimentali sono stati molto positivi ed è incorso la realizzazione dei chip ASIC (Application Specific Integrated Circuit) che serviranno per realizzare i nuovi terminali utente per le applicazioni terrestri, navali ed aeronautiche.

Una applicazione particolare del codice M sono i ricevitori GPS dei sistemi Aerei a Pilotaggio Remoto che operano in territori maggiormente esposti al rischio di jamming e spoofing. I sistemi APR di produzione della ditta americana **AeroVironment** impiegano ricevitori GPS predisposti per il Codice M e che sono attualmente integrati con sistemi di navigazione autonoma inerziale e Visual ovvero basati su sensori ottici che esaminano il terreno confrontando le misure con i dati memorizzati e determinando la posizione con un'accuratezza sufficiente a svolgere la missione quando il segnale GPS è compromesso.

I sistemi micro **Raven DDL** e **WASP** impiegati dall'Esercito Italiano e dalle Forze Speciali ed i sistemi mini **Puma 3** con lancio manuale e **Puma VTOL** a decollo e atterraggio verticale sono dotati di ricevitore GPS predisposto per essere aggiornato con il codice M.







COMBATTERE IL FUOCO CON IL FUOCO: L'AI PER DIFENDERSI DALLE MINACCE BASATE SU AI

BARRACUDA

L'AI può rendere i cyberattacchi ancora più gravi

L'intelligenza artificiale sta ridefinendo la sicurezza nazionale e i settori a essa collegati. Dai sistemi autonomi di ricognizione e combattimento alla valutazione intelligente dei rischi e all'analisi dei dati, tecnologie come l'AI generativa e il machine learning stanno aumentando velocità, precisione, automazione e raggio d'azione dei sistemi.

Tuttavia, le soluzioni digitali basate su AI ampliano anche la potenziale superficie di attacco esposta alle minacce informatiche, anch'esse rafforzate dall'AI, che può renderle più sofisticate e facilitare l'elusione dei sistemi di rilevamento. Per questo, l'adeguamento delle difese informatiche non può più aspettare.

La guida per i CISO sull'AI nella Cyber Security di Barracuda evidenzia alcuni modi in cui gli hacker possono sfruttare tali tecnologie a loro vantaggio.

1. Sviluppare e lanciare attacchi via e-mail più convincenti. La principale applicazione dell'AI nel phishing, nello spear phishing e nella tattica Business Email Compromise (BEC) consiste nella generazione automatica di contenuti, tra cui messaggi personalizzati e ben contestualizzati. Gli strumenti di AI possono anche aiutare nello spoofing di indirizzi e-mail legittimi, nella ricerca di informazioni pubbliche utili agli attacchi e nell'imitazione di modelli comunicativi reali per ingannare i destinatari. In particolare, l'assenza di errori grammaticali nel testo generato dall'AI complica l'identificazione di messaggi malevoli da parte delle misure di sicurezza tradizionali.

A tal proposito, vale la pena esaminare due modi in cui l'AI può favorire il phishing e le frodi:

a. **Creazione di deepfake**. I video e gli audio deepfake generati dall'AI a partire da contenuti reali sono emersi come potenti strumenti di impersonificazione. Chiunque abbia accesso a filmati e registrazioni audio può utilizzare tool basati su AI per creare imitazioni estremamente realistiche e inserirle nei messaggi di phishing. Ad esempio, le falsificazioni vocali potrebbero simulare personaggi famosi per diffondere truffe o campagne di disinformazione, fino a causare anche perdite finanziarie dirette per le aziende.

b. **Localizzazione dei contenuti.** Gli strumenti di AI consentiranno alle e-mail malevole di essere altamente localizzate e declinate a seconda dei vari contesti linguistici, culturali e settoriali. Ciò si può tradurre in e-mail di phishing multilingue, contenuti con gergo specifico e riferimenti a marchi e istituzioni locali, il tutto per incrementare l'apparente autenticità dei messaggi.

2. Generazione di codice malevolo e adattivo. L'avvento di strumenti malevoli basati su AI come WormGPT e EvilGPT potrebbe permettere ai criminali di automatizzare la ricerca delle vulnerabilità delle vittime, con un conseguente aumento potenziale degli attacchi zero-day. L'AI, inoltre, potrebbe consentire di creare malware adattivi – costituiti da codice malevolo capace di modificare il proprio comportamento per eludere il rilevamento –, o payload dinamici con virus polimorfi, oltre a facilitare l'offuscamento dei contenuti per aggirare gli strumenti di analisi statica.

3. Costruzione di botnet più grandi per attacchi DDoS. Le maggiori capacità di coordinamento e automazione delle reti di bot supportate dall'AI potrebbero amplificare il potenziale di massicci attacchi DDoS. Tali botnet possono evitare sistematicamente gli strumenti CAPTCHA e i meccanismi di proof of work, oltre a evolversi per evitare gli algoritmi tradizionali che si basano su serie storiche di dati per identificare i bot.

4. Furto di credenziali e tentativi di accesso automatizzati su larga scala. Molti attacchi informatici partono dal furto delle credenziali che consentono agli aggressori di accedere a un account e/o a una rete. Gli strumenti di AI possono agevolarli in diversi modi: creando pagine di login false che somigliano a siti web legittimi per raggirare gli utenti; incrementando la quantità dei tentativi di credential stuffing, che testano a ritmi elevatissimi grandi volumi di combinazioni di password e nomi utente ottenute tramite data breach; decrittando le password e neutralizzando i CAPTCHA.

5. Manipolazione dei modelli di addestramento AI. I modelli di AI utilizzati per le applicazioni prevedono l'utilizzo di un'ampia serie di dati per l'addestramento o l'aggiornamento. Se la sicurezza dei dati viene violata e gli hacker riescono a manipolarli e inquinarli, i sistemi basati su tali input grazie all'AI rischiano di fornire risultati imprevedibili e pericolosi, soprattutto per le organizzazioni che si affidano a questa tecnologia per supportare i processi automatizzati.

CINQUE MODI PER RAFFORZARE LE DIFESE INFORMATICHE GRAZIE ALL'AI

BARRACUDA

L'intelligenza artificiale sta trasformando fortemente anche la Cyber Security. Tale tecnologia, infatti, può potenziare le difese informatiche con strumenti avanzati in grado di identificare, interpretare e neutralizzare le minacce. Nonostante questa sembri una novità recente, da diversi anni i principali fornitori di soluzioni di sicurezza, tra cui Barracuda, impiegano l'AI nelle proprie tecnologie. In questo lasso di tempo, l'AI ha dimostrato di poter rivoluzionare la Cyber Security, favorendo lo sviluppo e l'implementazione di sofisticate funzionalità difensive.

Poiché il rischio che i cyberattacchi supportati dall'AI si adattino e imparino dalle difese che incontrano è reale, la costante innovazione nello sviluppo e nell'adozione di misure di protezione è fondamentale. Ad esempio, gli strumenti tradizionali utilizzano blocchi basati sui modelli o sulla firma, meccanismo che può essere appreso e potenzialmente aggirato. Per far sì che ciò non accada, le soluzioni di Cyber Security devono essere sempre un passo avanti nella capacità di rilevare, prevenire e reagire, soprattutto in presenza di minacce nuove ed emergenti. Ecco alcuni aspetti che possono già essere rafforzati grazie all'AI:

1. Sicurezza intelligente delle e-mail

L'intelligenza artificiale non solo è in grado di identificare i modelli di phishing noti, ma anche di rilevare minacce ancora sconosciute, esaminando le anomalie nel comportamento e nelle caratteristiche delle e-mail. L'elaborazione del linguaggio naturale, infatti, analizza il contenuto dei messaggi per determinare il sentiment, il contesto, il tono e l'eventuale intento malevolo. Sfruttando l'AI, le organizzazioni possono migliorare significativamente la protezione delle e-mail, garantendo un rilevamento più accurato ed efficace degli attacchi di phishing personalizzati.

2. Formazione sempre aggiornata e puntuale sulla Cyber Security

I programmi di formazione tradizionali sulla Cyber Security tendono a seguire campagne prestabilite, indipendentemente dai livelli di rischio delle minacce, e prevedono simulazioni o attacchi fittizi, che possono trasformarsi rapidamente in esercizi pro forma con benefici limitati. Barracuda, ad esempio, è all'avanguardia nella formazione "just-in-time" supportata dall'AI, ovvero un approccio che fornisce agli utenti finali una preparazione mirata, personalizzata e puntuale per rispondere in modo dinamico e tempestivo alle potenziali minacce.

3. Sicurezza delle applicazioni

Nella sicurezza delle applicazioni, il ruolo dell'intelligenza artificiale spazia dal rilevamento delle anomalie all'adeguamento dei modelli di machine learning e al contrasto dei tentativi di accesso iniziale e di ricognizione da parte degli hacker. Le soluzioni basate sull'AI possono rilevare i bot malevoli e migliorare l'efficacia complessiva delle misure di sicurezza. Grazie a questi strumenti, le organizzazioni possono così ottimizzare l'individuazione degli attacchi a livello applicativo, riducendo la superficie di attacco.

4. Rilevamento e analisi delle minacce

L'AI può essere impiegata anche per aumentare il volume, la velocità e la qualità del rilevamento delle minacce nonché dei processi di threat intelligence, ovvero di raccolta delle informazioni utili a difendersi dai pericoli informatici. Inoltre, gli algoritmi basati sull'AI possono servire per identificare le irregolarità, analizzare i dati comportamentali, riconoscere gli schemi utilizzati dagli hacker ed effettuare analisi predittive. Tutto ciò consente alle organizzazioni di identificare le minacce emergenti e rispondevi in modo più efficace. Infatti, la capacità dell'intelligenza artificiale di analizzare grandi quantità di dati – sia attuali sia storici – non strutturati provenienti da fonti e formati nativi di vario genere aiuta a stabilire dei punti di riferimento, per poi apprendere e adattarsi in continuazione.

5. Risposta agli incidenti automatizzata e ottimizzata

L'uso dell'AI nella risposta agli incidenti offre ai team di sicurezza la possibilità di rilevare, arginare e neutralizzare gli attacchi in modo rapido e più efficace, riducendo l'errore umano e accelerando la classificazione dei pericoli. Integrando l'AI, i Security Operations Center (SOC) possono migliorare significativamente le piattaforme di rilevamento e risposta alle minacce, creando meccanismi di difesa flessibili contro gli attacchi più avanzati.

Una Cyber Security resiliente grazie all'AI

È importante che le organizzazioni si attrezzino per affrontare un mondo guidato dall'AI, cercando di capire come gli aggressori potrebbero sfruttare tali strumenti e tecnologie per scopi malevoli. In questo modo potranno rafforzare le difese informatiche e adattare opportunamente i propri metodi di rilevamento e protezione, ottenendo un livello di sicurezza generale di gran lunga più elevato. In definitiva, non bisogna temere gli hacker che utilizzano l'AI, bisogna solo essere pronti.

ANTENNA ESA – ELECTRONICALLY STEERABLE ARRAYS DI HAIGH-FARR

CRISEL

Immagina questo scenario, comune a molti test range in tutto il mondo: molteplici contromisure vengono rilasciate simultaneamente da posizioni terrestri e aeree per neutralizzare una minaccia in arrivo. Queste risorse difensive si dirigono verso il bersaglio attaccante per renderlo inoffensivo, provenendo da batterie mobili sparse nei campi di prova e da piattaforme aeree che volano superiormente.
Il compito di un ingegnere durante queste prove è quello di acquisire dati da ogni elemento coinvolto nel test. Tutte queste misurazioni generano dati che vengono inviati ad una destinazione specifica. L'attrezzatura utilizzata per acquisire queste informazioni in modo affidabile, coerente e continuo gioca un ruolo cruciale nel successo complessivo del test, tanto quanto le risorse che attraversano il cielo. Al centro di questo hardware di test ci sono sicuramente le antenne, utilizzate per catturare l'energia RF emessa da tutti questi veicoli. È qui che entra in gioco l'antenna ESA (Electronically Steerable Array) di nuova concezione della Haigh-Farr e proposta sul mercato Italiano da Crisel.
L'impulso alla ricerca e allo sviluppo progettuale della nuova ESA è nato da un'applicazione non dissimile da quella qui descritta: una piattaforma di volo che raccoglie dati provenienti da più assetti aerei. Sul veicolo in volo si acquisiscono i dati che sono integrati a terra con una o più stazioni di telemetria e tracciamento mobili o fisse, simile all'architettura dello scenario di test descritta precedentemente. Indipendentemente dalla piattaforma di ricezione, è possibile utilizzare un'antenna ESA con una delle diverse configurazioni per acquisire i segnali RF in ingresso.

DECENNI DI ESPERIENZA NELLA PROGETTAZIONE E REALIZZAZIONE DI ANTENNE

L'antenna ESA di Haigh-Farr si basa su decenni di comprovata pratica di impiego di array digitali, queste conoscenze sono utilizzate anche nei moderni chipset dell'era digitale 5G. L'Electronically Steerable Array utilizza elementi di antenna facilmente collegabili, modulari, multipli (singola o doppia polarizzazione) per ottenere, con dimensioni adattabili, planari, il multi beam phased array. Questi moduli sono in grado di catturare componenti orizzontali e verticali (nella disposizione a doppia polarizzazione) di qualsiasi segnale RF all'interno della loro gamma di frequenza predeterminata e sintonizzata, all'interno del campo visivo elettrico dell'ESA i segnali RF di ciascun elemento vengono quindi condizionati, filtrati, digitalizzati e infine trasmessi alle schede FPGA e ai processori ARM Cortex che eseguono funzioni matematiche vettoriali complesse personalizzate per eseguire funzionalità di beamforming e di massimizzazione dei fasci coerenti formati come uscite del sistema.
Tali funzionalità sono ottenute attraverso una miscela innovativa di combinatori di reti hardware/software. L'intera architettura consente il beamforming digitale piuttosto che il semplice beamforming RF. Il risultato finale è un'eccellente densità di integrazione RF e digitale in un fattore di forma ridotto che può essere adattato a parametri applicativi specifici e, a sua volta, può essere utilizzato per facilitare l'acquisizione dinamica in auto-tracking di più flussi di dati provenienti da più emettitori RF point-source contemporaneamente.
Mentre queste sorgenti si muovono attraverso la scena del test, l'ESA rimane agganciata ai vari segnali per acquisire quanta più energia possibile per tutta la durata dell'operazione.

CONFIGURAZIONI ANTENNA ESA

La Figura 1a mostra ESA in una configurazione concettualizzata a terra. La configurazione è semplice in quanto un array di antenne multi-modulo è posizionato sopra un treppiede e puntato nella direzione della scena di prova. Orientabile elettronicamente, l'array rimane in una posizione meccanica fissa ma può tracciare le risorse di test spostando elettricamente la copertura del pattern RF mentre gli emettitori RF delle unità in fase di test si spostano.
La Figura 1b fornisce un'immagine del solo pannello ESA visto frontalmente e con una copertura del radome che protegge gli elementi dell'array sotto la pelle. La Figura 1c mostra l'ESA dal retro, inclusi i connettori di interfaccia.
Sotto il radome, e come vista espansa dell'ESA, la figura 2 mostra i vari strati in una configurazione generica.


Fig. 1a

Fig. 1b

Fig. 1c

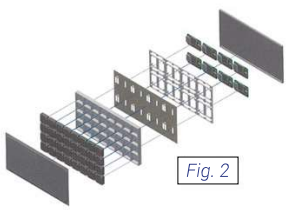


Fig. 2

Un punto chiave da portare a casa per l'antenna mostrata in queste varie viste è il concetto di modularità. L'ESA di Haigh-Farr si basa su un approccio modulare a 8 elementi. Ciò significa che ogni blocco di costruzione ha 8 singoli elementi dell'antenna. Questi moduli possono es-

sere aggiunti o sottratti da un determinato progetto per ottenere il guadagno, la direttività e il rapporto segnale/rumore (SNR) necessari per soddisfare o superare un margine di collegamento precalcolato. Istruttive su quanto possa essere potente l'accoppiamento di questi moduli insieme sono le Figure 3a, 3b e 3c. Iniziamo con la figura 3a e un'antenna a singolo elemento centrata su un gruppo 2 x 2 (l'immagine a sinistra nella figura 3a). Il pattern risultante viene visualizzato a destra, con riferimento a 0° direttamente sopra la testa, 180° direttamente sotto e 90° parallelamente alla superficie terrestre in El e +/-90° riferito al boresight di 0° in Az, tutto come visto da una piattaforma di acquisizione dati in volo. Vengono forniti anche direttività e SNR, e come si può dedurre dalla figura, il modello è sfocato e a basso guadagno.

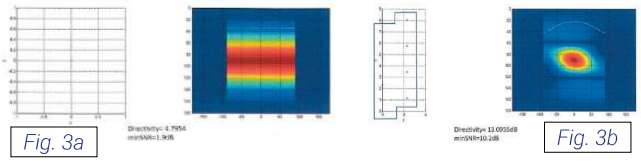


Fig. 3a

Fig. 3b

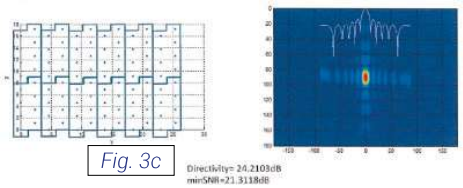


Fig. 3c

La Figura 3b mostra il primo blocco modulare per l'ESA di Haigh-Farr. Gli elementi sono leggermente sfalsati in un assemblaggio di 4 x 9 pollici, i modelli di radiazione stanno iniziando a mostrare la messa a fuoco sull'horizon e il boresight e sia la direttività che l'SNR sono incrementati notevolmente. Questo modulo può ora essere composto in un numero qualsiasi di configurazioni per aumentare il footprint, l'apertura e, soprattutto, le prestazioni elettriche del gruppo ESA. La Figura 3c mostra un esempio di questa crescita se 12 di questi moduli vengono sommati. L'assemblaggio è ora di 20 x 28 pollici, il suo diagramma di radiazione è ben focalizzato e la sua direttività e SNR sono entrambi superiori a 20 dB.

IMPLEMENTAZIONE INIZIALE

Con queste tre immagini e le descrizioni che le accompagnano, è facile immaginare quanto possa diventare potente e flessibile l'ESA. Inoltre, la visione a lungo termine di questa ESA è che sia disponibile in diverse frequenze anche multiple. La fase iniziale è partita con la banda S, focalizzata sulle tradizionali frequenze di trasmissione telemetrica da 2200 MHz a 2290 MHz e alcune bande di frequenza aggiuntive più strette con un'abbondanza di filtraggio per qualsiasi fuori banda.

Come precedentemente detto il design è facilmente adattabile, e può essere portato in banda C o in banda L. La copertura di queste tre bande di frequenza con diverse varianti dell'assieme consentirà la copertura in tutte le principali gamme RF di telemetria utilizzate a livello globale. Inoltre, lavorare dalla banda L fino alla banda C offrirà agli utenti l'opportunità di trovare usi anche diversi per l'ESA Haigh-Farr. Con prestazioni di figura del noise dei singoli elementi inferiori a 2 dB, capacità di limitare di 12 dBm, beam steering dinamico a livello di modulo e cooperativo con tutti gli altri moduli, conversione digitale diretta up/down e gamma dinamica multi-modulo di 100 dB o più a seconda delle dimensioni complessive dell'ESA e del numero di elementi, l'ESA presentata in questo documento è ben posizionata per una varietà di compiti e usi.

Un'ultima considerazione sull'ESA presentata in questo documento su quanto sia appropriata rispetto all'ampiezza dell'applicazione. Lo scenario previsto nell'introduzione è quello di un poligono di prova senza sbocco sul mare con centri di raccolta dati terrestri o aerei: e questo è certamente un caso d'uso reale e valido. Tuttavia, questa scena potrebbe facilmente svolgersi in un oceano aperto, dove l'acquisizione dei dati avviene da uno o più asset marittimi dotati di front-end RF incentrati sull'ESA. Diverse versioni di questa applicazione si sono infatti presentate negli ultimi anni come luoghi praticabili per le ESA che monitorano una varietà di operazioni di test di veicoli multi-avversario/multi-attacco.

Inoltre, le applicazioni per ESA in grado di dirigere attivamente patterns di energia RF potrebbero non avere nulla a che fare con test range o test flight di sorta. I satelliti, ad esempio, sono ottimi candidati per l'utilizzo delle ESA. Sono veicoli sopraelevati e lontani dai centri TT&C a terra. La comunicazione deve avvenire tra lo spazio e la Terra e i fixed-beam array o le antenne a patch singola potrebbero non sempre costituire l'approccio migliore. I sistemi di antenne steerable in grado di fornire copertura RF leading-edge, nadir, or trailing-edge, mentre un veicolo spaziale orbita attorno al globo, modificando gli angoli del fascio di copertura mentre gli angoli di visualizzazione della stazione di terra cambiano dall'orizzonte ascendente all'orizzonte discendente, potrebbero essere il sistema di antenna preferito.

L'antenna ESA è stata progettata anche pensando a questo tipo di utilizzo.

Questo innovativo sistema di antenne array orientabili elettronicamente di Haigh-Farr e Crisel è pronta a supportare le più svariate applicazioni indipendentemente dallo scenario.

DIGITALPLATFORMS: LA DIFESA DELLA SOVRANITÀ DIGITALE ED ELETTROMAGNETICA CON LE ATTIVITÀ CEMA

DIGITALPLATFORMS

L'esito e l'andamento degli ultimi conflitti bellici globali e, soprattutto, il protrarsi della guerra russo-ucraina propagatasi nel cuore dell'Europa a partire dal febbraio 2022, impongono un urgente aggiornamento della dottrina militare e dei modelli di intervento in direzione di un significativo irrobustimento dell'approccio multidominio MDO (Multi Domain Operations.). Nell'attuale scenario di guerra, si assiste sempre più frequentemente al dispiegarsi delle attività **CEMA** (Cyber Electromagnetic Activities) miste alla combinazione di Guerra e Difesa Elettronica (EW), Cyberspace Operations ed Intelligence, in un quadro dove si rendono necessari approfonditi spazi di riflessione e di analisi.
Al riguardo, DigitalPlatforms lavora al fine di incrementare la consapevolezza della necessità di affrontare in maniera innovativa il sempre più complesso scenario operativo, consolidando la convinzione che il Multidominio non può essere confinato al solo campo militare. Al riguardo, diventa urgente, e non solo in ambito militare, la conoscenza e la diffusione della cultura del ***TEMPEST*** *(Telecommunications Electronics Material Protected from Emanating Spurious Transmissions), uno standard di certificazione con cui si identificano le regole, le procedure e gli studi sulle contromisure tecnico-normative e gli strumenti di sicurezza diretti a prevenire o a ridurre lo sfruttamento illegale, tramite tecniche di sorveglianza o intercettazione, delle informazioni sensibili e dei dati rilevabili dalle emanazioni intenzionali dei dispositivi elettronici per comunicazioni.*
Qualsiasi apparecchio con microchip genera un campo elettromagnetico, spesso definito dagli esperti di sicurezza *"emanazione di compromesso"*. Apparecchi e dispositivi elettronici emettono segnali aerei simili a quelli delle stazioni radio e, se non sufficientemente protetti, queste emanazioni possono essere intercettate fino a centinaia di chilometri di distanza e il segnale ricostruito, elaborato ed utilizzato per fini informativi illegali/criminali o compromettenti la sicurezza nazionale e dei sistemi economico-industriali. Apparecchi vulnerabili, oltre ai computer, sono i monitor, gli storage, i cavi di rete, i vivavoce, le stampanti, le macchine dei fax, gli scanner, i dischi drive esterni e diverse altre periferiche a banda larga e ad alta velocità.
Per evitare rischi di intercettazione elettromagnetico, le regole e le procedure del TEMPEST richiedono che i circuiti ed i dispositivi elettronici limitino significativamente le emanazioni e che vengano applicate, a fini di protezione, schermature e messe a terra appropriate.
Le minacce di intercettazione e rilevamento elettromagnetica, sia di provenienza umana (Humint) sia tecnologica (Elint, Sigint, Emsec Infosec) hanno i caratteri dell'imprevedibilità e sono di difficile identificazione e contrasto.
Il rispetto degli standard e delle procedure regolate dal TEMPEST, rappresentano allo stato attuale la protezione massima contro queste minacce. Le postazioni anti-attacco TEMPEST sono generalmente situate sotto camere o tende dotate di una schermatura tale da non permettere alle onde elettromagnetiche di evadere dalla zona di contenimento e dotate di filtri sulla rete elettrica, il tutto gestito dal settore di sicurezza EMSEC[1], che si occupa di questo aspetto nei particolari.
DigitalPlatforms riesce inoltre a garantire l'insieme di operazioni specifiche di configurazione (CEMA: Cyber Electromagnetic Activities) di un dato sistema informatico (e dei suoi relativi componenti) che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano le vulnerabilità dello stesso. Ogni componente erogante il servizio o i servizi (es. sistema operativo, webserver, applicazione web, database, sistema di display, etc..) deve essere oggetto di HARDENING, al fine di ridurre, attraverso l'utilizzo di strumenti, metodi e procedure raccomandati, la superficie di attacco dell'infrastruttura tecnologica, compresi software, sistemi di dati e hardware.
Se le reti sono il substrato comunicativo delle MDO (Multi Domain Operations), è soprattutto nell'IoT (Internet of Things) militare, dove tutti i livelli sono interconnessi attraverso la rete, che diventa indispensabile rafforzare i dispositivi di rete al fine di contrastare accessi non autorizzati alla rete sensibile. La sicurezza dei dispositivi interconnessi con metodologie di rete di livello militare può essere assicurata soltanto applicando la metodologia Hardening, ossia attraverso una serie di linee guida quali una corretta configurazione del firewall con costante aggiornamento delle relative regole di sicurezza, la protezione dei punti di accesso, la disabilitazione di tutte le porte di rete non necessarie, la crittografia del traffico di rete.

[1] La sicurezza delle emissioni (EMSEC) è un'analisi della vulnerabilità di un determinato sistema rispetto all'accesso non autorizzato a seguito di problemi con le emanazioni elettromagnetiche dell'hardware. In genere, la sicurezza delle emissioni viene applicata a sistemi di telecomunicazioni, reti radio, sistemi crittografici o altre installazioni di comunicazione simili. EMSEC si è sviluppato nel tempo come parte fondamentale della protezione dei dati sensibili nelle operazioni governative o aziendali.

ELECTRONIC WARFARE AND CYBER WARFARE: TWO SIDES OF THE SAME COIN

ELETTRONICA

Daniela Pistoia – Corporate Chief Scientist at ELT Group

Traditionally, **Electronic Warfare (EW)** and **Cyber Warfare (CW)** were considered as independent, disparate disciplines: *Cyber-warriors* worked at the bit level, while *Spectrum-warriors* operated below them, targeting ElectroMagnetic Spectrum (EMS).

However, as communications systems have moved to commodity hardware and as radar and navigation systems began to depend on networked operations using commodity network hardware, the boundaries between the two fields have begun blur. Now, Cyber-warriors can provide effects that deny or degrade spectrum and Spectrum-warriors can create effects that allow for the control and exploitation of the network.

Traditionally, **Electronic Warfare (EW)** is any action involving the use of the electromagnetic spectrum (EMS) or directed energy to control the spectrum, attack an opponent or impede opponent assaults via the spectrum: the ultimate purpose of EW is to deny the opponent the advantage of, and ensure friendly unimpeded access to, the EMS. EW can be applied from air, sea, land, and space by manned and unmanned systems, and can target humans, communications, radar, or other assets generally indicated as Spectrum Dependent Systems. For those who are **NOT** familiar with the topic, EW is described as having three major subfields:

- **Electronic Support (ES)**, which involves hostile intercept of opponent transmissions.
- **Electronic Attack (EA)**, in which enemy electronic sensors (radars and communication receivers) are degraded either temporarily or permanently by the transmission of signals designed for that purpose (JAMMING), or cause enemy systems to acquire and track invalid targets (False Targets – DECEPTION).
- **Electronic Protection (EP)**, which is a set of measures designed to protect friendly sensors from enemy electronic attack actions.

On the other side, traditionally, **Cyber Warfare (CW)** involves the use and targeting of computers and networks in warfare to gain a military/economic/competitive advantage by gathering significant information from an enemy or interfering with the enemy's ability to move information over the Internet or other networks or to process information within a computer.
Cyber Warfare involves both offensive and defensive operations pertaining to the threat of cyberattacks, espionage and sabotages conducted by use of malware, which is software whose purpose is to cause harm.

For those who are **NOT** familiar with the topic, CW involves the design, development and deployment of malicious software codes of several types, even if usually clustered in the following major categories:

- **Viruses:** any type of malicious software program that, when executed, replicates itself by modifying other computer programs and inserting its own code and forcing the host computer to do a variety of undesired operations or enter in undesired status. Viruses can also cause undesired information deletion or can modify programs in highly undesirable ways.
- **Worms:** any standalone computer programs that replicates itself in order to spread into other computers. Often, they use a computer network to spread, relying on security failures on the target computer to access it. Worms usually cause some harm to the network, consuming bandwidth by increasing network traffic, where viruses usually corrupt or modify files on a targeted computer.
- **Trojan horses:** any type of malicious software programs, which mislead users of its true intent, for example inducting the user into executing any routine or sub-function disguised to be unsuspicious or drive-by download. Many modern forms act as a backdoor, contacting a controller, which can then have unauthorized access to some functionality of the affected computer or allow to access users' personal information such as passwords or personal identity. Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.
- **Spywares:** any type of software programs that gathers and exports data from a computer for any purpose, for example, they may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge. "Cookies" are a form of spyware requiring special consent, even if the consumer does not know the destination of the data.

There are a number of other terms used to describe various techniques used to attack the ability of a computer to do its job, using the network to gain access to the victim's computer by transferring one of the above-mentioned type of threat.

Both EW and CW aim to perform similar operational functions against the opponent, such as:

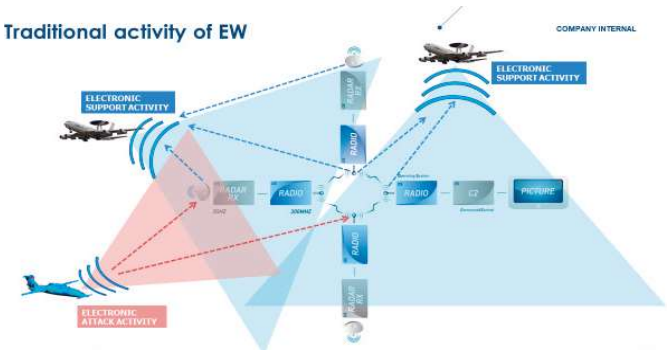
- Collect information from the opponent;
- Interfere with the opponent's operational capability in accessing/using its resources;
- Cause the opponent systems to initiate undesired actions:
- Protect friendly capability from opponent's electronic interference;

The following table reports a comparison between EW and CY in terms of operational functions and how they are perpetrate versus the opponent, showing that each of the EW fields has a parallel technique in Cyber Warfare area.

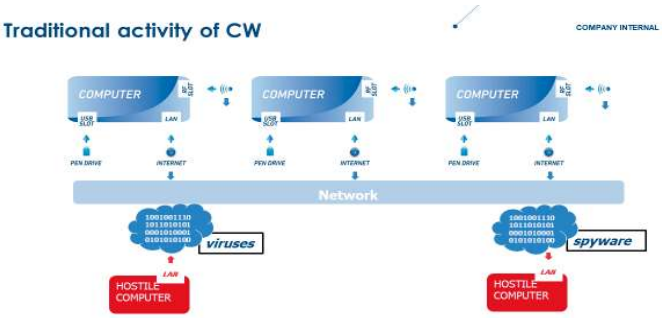
Comparison of Electronic Warfare and Cyber Warfare Functions		
Operational Function	**Electronic Warfare**	**Cyber Warfare**
Collect information from the opponent	**EW Support**, which listens to enemy signals to determine enemy capabilities and operating mode	**Spyware**, which causes information to be exported to a unwanted and hostile location
Interfere with opponent's operational capability	**Electronic Attack – JAMMING**, which either covers received information or causes processing to give inaccurate outputs	**Viruses**, which reduce available operating memory or modify programs to prevent proper processing outputs
Cause opponent systems to initiate undesired actions	**Electronic Attack – DECEPTION (false targets),** that look like credible targets, which are acquired and engaged by missiles or guns	**Trojan horses**, which are hostile software accepted by enemy computers because they appear valid and beneficial
Protect friendly capability from opponent's electronic interference	**Electronic Protection**, which prevents enemy jamming from impacting own operational capability	**Passwords and firewalls**, which prevent malware from penetrating a computer

The traditional difference between EW and CW is how the hostile function is introduced into an opponent's systems.

As shown the following picture, EW enters the enemy systems' functionality electromagnetically: through the Electronic Support functionalities, interception of signals transmitted by an opponent Spectrum Dependent System (a Radar system or a radio) is performed, while through the Electronic Attack functionalities the ability of such systems to access and use the EMS is degraded, negated or spoofed.



As shown in the following picture, traditional cyber-attacks assume the malware entering the victim computer via the network, a USB drive or any other software based support.

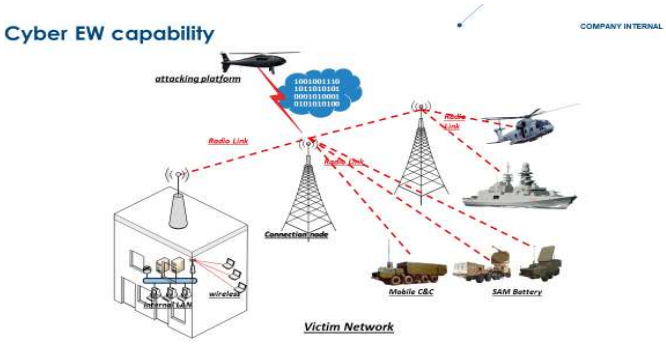


Modern systems (civil, national infrastructures, military) are today increasingly based on communication networks without fixed infrastructure, entering in the categorization of Spectrum Dependent Systems. On the other hand, they are based on the use of computing capability to elaborate data and information, manage their functionalities, and control their status. Following the definition by US DoD, a

computing system is a system whose performed functionalities are mainly implemented and/or are enabled by means of programmable devices, which include DSP, FPGA, CPU, GPU and moreover, in terms of physical components, memory devices, interfaces, operating systems and application logics.
Therefore, a computing system that makes use of wireless interface, provides a vulnerability that can be exploited in order to:

- collect sensitive information, which can be used for any operation within the network;
- force the access to the network, to take advantage of the services of the network itself;
- degrade the performance of the network, up to deny the whole service;
- degrade/modify the performance of one or more node of the network, by introducing dedicated data stream and inserting/activating malicious code in the computing system.

For example, an hypothetical device operating against a cell phone network, for instance, may not just blindly inject energy into the cell phone band, as a traditional jammer might do. Instead, it might selectively jam certain frames destined for particular handsets, causing a directed EW effect at the physical link. It might also inject additional data into the link, causing cyber effects at protocol or user level. For instance, forwarding tables could be updated in a way that partitions some users from the network or additional data could be inserted into a user session, invalidating the information the user gains from the session.
In the following, an unmanned aerial platform performs the attack by injecting the payload into the network through a connection node via EMS. The payload is then propagated through the radio network.



The payload can consist in:

- Viruses;
- Computer worms;
- Trojan horses;
- Spyware;

The payload is activated inside the first networked computer ("n-click") and then bounced back to the other servers and computers/computing systems via the wired and wireless networks.
The nodes of networked systems physically reside in one of the traditional domains of warfare (air, land, sea, space), but the ability to achieve the objectives of an operational mission cannot be separated from the ability to control and to have freedom of action in cyberspace that, in this sense, is transversal to all other domains.
Of course, new challenges arise. The design, development and execution of a Cyber EM operation, needs:

- Detailed knowledge of the target:
  - key to address when attacking the application layer;
  - multidiscipline intelligence.
- Being trusted part of the network:
  - key to inject, manipulate or modify the information transmitted inside a wireless network.
- Crack the COMSEC and TRANSEC network protections:
  - different levels of complexity in term of robustness and resilience;
  - success NOT ensured a-priori;
  - expertise, tools, methodology of REVERSE ENGINEERING.
- Deal with verification and validation issues.

Different wireless or wireless/wired networked systems, both military and civil infrastructures, require different frequencies to operate effectively. They may use standard protocols and routing rules or ad-hoc infrastructures. Finally, the information exchanged can be clear or encrypted. In all the cases, they can be modeled as a network of computing systems. For a number of years, military operations have used electro-magnetic attacks to disrupt enemy radars on the battlefield, but today the access and manipulation of the EMS and/or the data and information carried by EMS let us foresee many additional capabilities.In other words, **EMS is an entryway for cyber**. EW and CW are trying to accomplish similar tasks; they can be used in conjunction and thus may be viewed as two sides of the same coin, which is often indicated as **Cyber EW** or Cyber Electromagnetic Activity (CEMA).

RISERVE DI SPAZIO AEREO: NUOVE TECNOLOGIE E CONCETTI OPERATIVI A SUPPORTO DELL'EFFICIENZA DEI FLUSSI DI TRAFFICO

ENAV

Nell'ambito della gestione dei flussi del traffico aereo (ATFM) in Europa, rappresentano dei ruoli cruciali la figura del National Network Manager - NNM, a livello nazionale, e dei Flow Manager Position -FMP, all'interno dei centri di controllo di area (ACC). Il loro compito principale è bilanciare la domanda di traffico e la capacità dello spazio aereo di accogliere tale domanda, nelle diverse fasi del volo (strategica, pretattica e tattica), partecipando a gruppi di lavoro europei e collaborando con il Network Manager Operations Centre (NMOC) di EUROCONTROL. Per assolvere a questo compito il NNM e gli FMP analizzano i dati di traffico, identificano possibili congestioni e coordinano con il Network Manager europeo – NM, con le compagnie aeree o ancora con gli altri FMP per ottimizzare i flussi di traffico.

Diversi fattori contribuiscono agli squilibri tra domanda e capacità nel contesto della gestione del flusso del traffico aereo. Questi includono:

- Condizioni meteorologiche avverse: fenomeni come temporali, nebbia e forti venti possono ridurre significativamente la capacità dello spazio aereo e degli aeroporti.
- Restrizioni dello spazio aereo: chiusure temporanee o restrizioni dello spazio aereo dovute ad attività militari, eventi speciali o emergenze possono limitare la capacità disponibile.
- Altri fattori, come la disponibilità del personale ATCO, guasti tecnici, disponibilità delle piste, differenze nelle prestazioni degli aeromobili (traffico misto), emergenze, ecc.

Questi fattori devono essere continuamente monitorati e gestiti per ridurre al minimo gli squilibri e garantire il flusso sicuro ed efficiente del traffico aereo. Tale monitoraggio viene eseguito attraverso strumenti software messi a disposizione in Europa da EUROCONTROL; ENAV ha deciso di dotarsi altresì di uno strumento sviluppato all'interno del suo gruppo da IDS AirNav, denominato Local Traffic Load Management Tool (LTLMT). LTLMT monitora il traffico rispetto alla capacità disponibile, stima la complessità delle traiettorie, calcolata considerando il numero e la tipologia (orizzontali, verticali, velocità) di interazioni tra i voli. Per interazioni tra i voli si intende una complessa combinazione fra piani orizzontali, verticali, velocità e intenzioni di volo. Il sistema esegue inoltre analisi "what-if" in termini di:

- configurazione dei settori di controllo: supporta i ruoli ACC nell'identificare la configurazione migliore da applicare, considerando il traffico previsto, i vincoli, il numero di postazioni di lavoro disponibili e il periodo di tempo.
- traffico: vengono eseguite analisi per suggerire azioni sui voli (e.g. Flight Level capping), eventualmente combinate con misure di capacità.

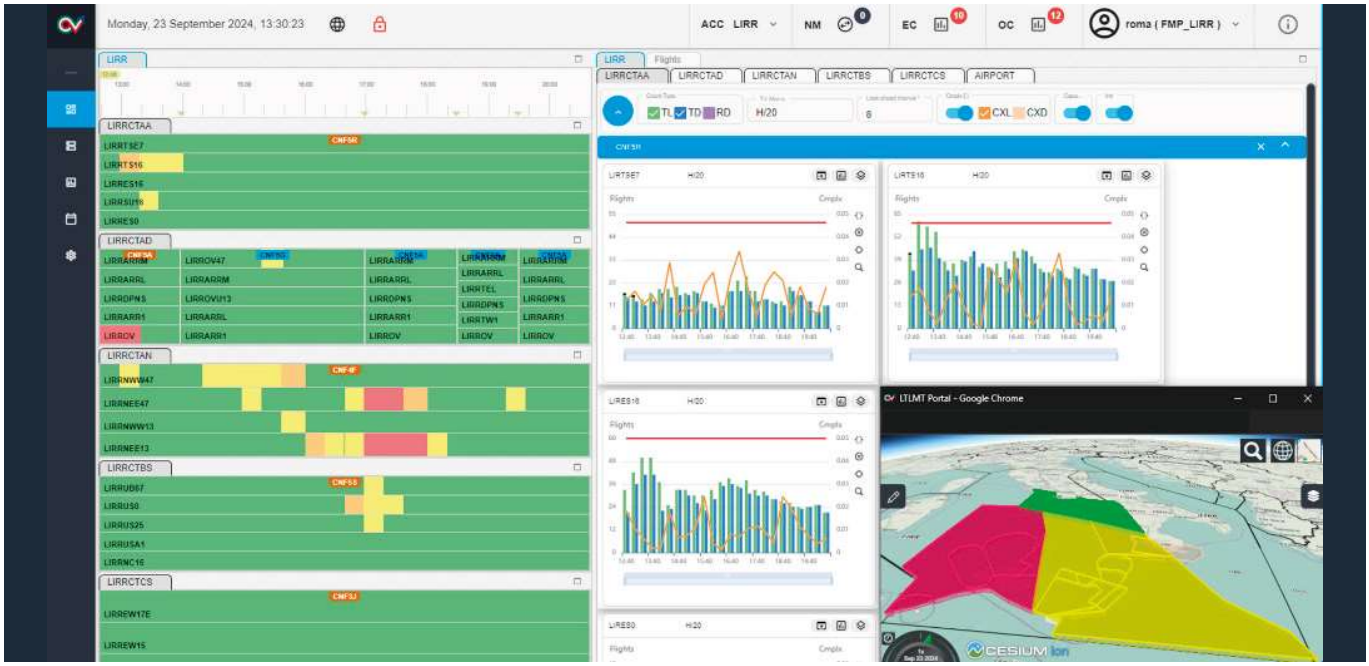


Figura 1. Dashboard di monitoraggio di LTLMT

Nel prossimo futuro, è prevista l'implementazione dell'Advanced Flexible Use of Airspace (AFUA) considerando anche l'applicabilità del concetto di Dynamic Mobile Areas (DMA). Le DMA sono definite come aree mobili di esclusione temporanea dello spazio aereo, il cui scopo è quello di minimizzare l'impatto sulle prestazioni ATFM soddisfacendo al contempo le esigenze degli utenti dello spazio aereo militare. Sono stati identificati tre tipi di DMA, applicabili anche in un contesto operativo di rotte libere (Free Route).
Il programma SESAR (Single European Sky ATM Research) si prefigge di studiare e validare concetti tecnici e operativi a supporto di un sistema evoluto di gestione del traffico aereo per lo spazio aereo europeo. In un Progetto afferente all'ambito SESAR, denominato HARMONIC, ENAV eseguirà delle simulazioni real-time per valutare l'effetto dell'applicazione delle DMA Tipo 1 e di eventi meteorologici, quali l'insorgenza di aree convettive, e come questi eventi possano variare la capacità dei settori ATC.

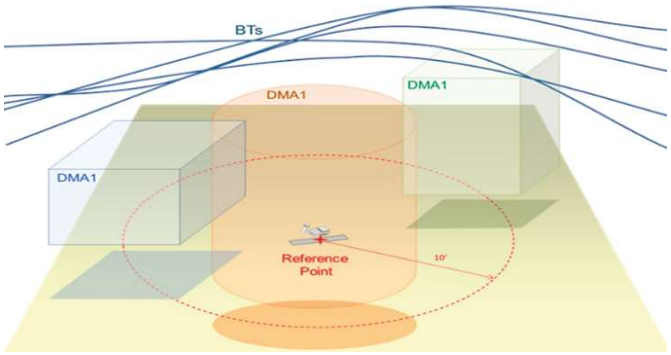


Figura 2. DMA Type 1

Lo scenario operativo delle simulazioni sarà l'ACC di Milano.
L'obiettivo della validazione sarà anche quello di testare un algoritmo avanzato di "Dynamic Airspace Configuration" che permette di presentare al FMP un maggior numero di configurazioni di sala, aumentando l'attuale flessibilità dei settori operativi ATC.
Il fine ultimo è minimizzare eventuali effetti negativi sul traffico aereo civile, derivanti da restrizioni della disponibilità dello spazio aereo, prevedendo ed evitando sbilanciamenti fra domanda e capacità, a salvaguardia di una gestione sicura del traffico aereo.
Con lo sviluppo e l'implementazione di queste tecnologie e procedure operative ENAV si pone all'avanguardia nei concetti di uso flessibile delle sale controllo e dello spazio aereo e conferma il percorso iniziato, fra i primi in Europa, con l'applicazione del "free route".

GEOAI E REALITY MAPPING: NUOVI STRUMENTI A SUPPORTO DELLA DIFESA

ESRI ITALIA

Esri, società leader a livello mondiale nella Location Intelligence, propone un unico sistema geospaziale che supporta a 360 gradi la realizzazione di servizi per la Difesa. La tecnologia Esri è il punto di riferimento per sistemi in grado di recepire e valorizzare le informazioni provenienti da un set di dati e tecnologie sempre più ampio. Inoltre, i sistemi Esri si evolvono rapidamente per adeguarsi alle nuove tecnologie.

Una delle nuove frontiere tecnologiche, che sta acquisendo sempre maggiore importanza, è sicuramente la **GeoAI**. L'intelligenza artificiale geospaziale (GeoAI) è l'applicazione dell'intelligenza artificiale (AI) alle informazioni e all'analisi geospaziale, per accelerare la comprensione nel mondo reale, degli impatti ambientali e dei rischi operativi.

La GeoAI, attraverso la generazione automatizzata di dati e strumenti con algoritmi spaziali, consente di rendere molto più efficienti le operazioni su larga scala.
Con l'intelligenza artificiale geospaziale è possibile, ad esempio automatizzare l'estrazione, la classificazione e il rilevamento delle informazioni da dati di vario tipo come immagini, video, cloud di punti e informazioni testuali.
Anche le analisi predittive beneficiano dell'automatizzazione per creare e trovare modelli, rilevare cluster, calcolare i cambiamenti.

Più in generale gli algoritmi della GeoAI permettono di accelerare la risoluzione dei problemi spaziali.
La GeoAI sta trasformando la velocità con cui è possibile estrarre significato da set di dati complessi, aiutando così a migliorare i processi operativi, e rivoluzionando il modo in cui i dati si trasformano in informazioni, con modelli che si adattano anche quando i dati cambiano.
Il settore della Difesa e dell'Intelligence beneficia notevolmente di queste capacità della GeoAI.

Le organizzazioni militari possono ottimizzare gli sforzi operativi, automatizzando i processi di analisi e recepimento di informazioni e dati provenienti da diverse fonti, come video di droni, image 360, satelliti, sensori, documenti, sistemi di intelligenza artificiale, graph database, processi BIM o complesse matrici multidimensionali.

La GeoAI migliora la qualità, la consistenza e la precisione dei dati, e la potenza dell'automazione permette di aumentare l'efficienza e ridurre i costi.
Rendere più efficiente e veloce la capacità di analisi consente anche tempi di risposta più rapidi e decisioni più consapevoli.

Un altro salto tecnologico che vale la pena menzionare, come strumento a supporto della Difesa e dell'Intelligence, riguarda sicuramente l'accuratezza delle immagini disponibili nella piattaforma Esri, grazie al **Reality Mapping**.
L'esplorazione e la conoscenza dello spazio dove si svolgono le operazioni militari è particolarmente importante, perché fornisce approfondimenti sul territorio e sul posizionamento degli oggetti. Ottenere rapidamente informazioni spaziali è, quindi, molto importante per il successo operativo.

Varie tipologie di immagini come quelle riprese da drone, da aereo e da satellite, attraverso l'uso della tecnologia ArcGIS Reality Studio, vanno a costituire strati informativi che consentono di ricostruire una precisa copia digitale della realtà in 3D per ottenere fedeli ricostruzione di infrastrutture, quartieri e intere città. Queste ricostruzioni rendono il GIS più immersivo, vicino alla realtà e aprono la strada a nuove tipologie di geo-analisi.

Il Reality Mapping ha generato una vera rivoluzione nella gestione dei dati 3D vettoriali superando la visualizzazione delle tradizionali immagini oblique e rendendo l'esperienza utente estremamente fluida e user friendly. Vari strumenti Esri consentono di costruire rappresentazioni di qualsiasi area in modo da poter creare le basi per un **gemello digitale** in **3D** di ambienti naturali o ambienti urbani. Il software fornisce flussi di lavoro di elaborazione automatizzati per aiutare gli utenti ad allineare rapidamente grandi raccolte di immagini e a creare in modo efficiente prodotti di dati fotorealistici e di livello topografico. Gli utenti possono quindi portare questi dati nei propri sistemi GIS per eseguire analisi e visualizzazioni avanzate. Con una esperienza immersiva tridimensionale gli operatori possono per esempio esplorare e camminare virtualmente nella zona delle operazioni militari, anche con l'ausilio dei supporti per la realtà virtuale, come i visori.

Gli scenari ricostruiti hanno un elevato livello di dettaglio e precisione. È possibile simulare diverse ore del giorno e della notte e diversi mesi dell'anno, per sperimentare diverse condizioni dell'ambiente. È possibile inserire nel

modello digitale della realtà informazioni relative a edifici e infrastrutture in corso di progettazione (integrazione BIM e GIS) per verificare la sicurezza dell'area prima e dopo la realizzazione dell'opera. Oppure si può scegliere di dedicare un focus specifico agli edifici strategici che connotano la zona in esame.

Dalla raccolta di dati e immagini all'elaborazione di scenari realistici in 3D, dalla esplorazione virtuale degli ambienti ricostruiti, fino alla creazione di digital twin per analizzare modelli di situational awareness, le tecnologie geospaziali sono, dunque, un valido sostegno per costruire flussi operativi a sostegno delle operazioni militari.

La GeoAI, l'integrazione con i dati BIM e il Reality Mapping rendono ArcGIS un sistema informativo geografico sempre più completo e innovativo, che funziona in un ambiente scalabile con l'ausilio di vari strumenti, dall'automazione dei processi, al deep learning per il rilevamento di oggetti, la classificazione, l'analisi del terreno e il rilevamento dei cambiamenti dalla scala locale a quella globale, fino alla creazione di report, per consentire, più in generale, alle organizzazioni militari di un attuare un processo decisionale più efficace ed efficiente.

FASTWEB, IL CUORE ITALIANO DELL'INTELLIGENZA ARTIFICIALE AL SERVIZIO DEL PAESE

Un modello linguistico nazionale per l'Italia

FASTWEB

La fine del 2022 ha segnato una vera rivoluzione nell'Intelligenza Artificiale (IA) generativa con il lancio di ChatGPT da parte di OpenAI, un sistema in grado di dialogare in modo naturale e generare testi in maniera sempre più umana. L'IA generativa sta rivoluzionando il modo in cui interagiamo con la tecnologia, semplificando e arricchendo la nostra vita quotidiana.

Tuttavia, dietro a questa rivoluzione si nasconde un rischio. Stati Uniti e Cina sono le nazioni che oggi investono di più in Intelligenza Artificiale e la quasi totalità dei modelli linguistici (LLM) su cui si basano questi sistemi è addestrata su dati prevalentemente in lingua inglese o cinese, riflettendo inevitabilmente una visione del mondo polarizzata verso culture estere. Ciò significa che gli LLM che quotidianamente utilizziamo rispondono alle nostre richieste riflettendo una cultura prettamente anglosassone e traducendo poi il risultato in italiano. Questi modelli pertanto non colgono appieno le sfumature e le peculiarità della nostra lingua e del nostro modo di esprimerci.

Ma c'è di più: spesso non è chiaro dove i dati per l'addestramento di questi modelli vengano elaborati e se siano stati raccolti nel rispetto delle norme europee e nazionali, come il GDPR e il diritto d'autore. Una questione di sovranità dei dati che non può essere trascurata.

Seppure in ritardo, l'Europa non è un osservatore passivo: la Francia si è mossa per prima, finanziando progetti nazionali che hanno portato alla realizzazione di LLM performanti (es. Mistral). L'Italia la sta seguendo e ha annunciato investimenti per realizzare LLM sovrani.

È qui che entra in gioco Fastweb, azienda italiana all'avanguardia nella trasformazione digitale del Paese. Fin dal 2019, quando ancora erano poche le realtà nazionali a credere nella potenzialità dell'Intelligenza Artificiale, Fastweb ha intrapreso un percorso innovativo, dotandosi di un proprio Centro di Competenza focalizzato sull'Intelligenza Artificiale e realizzando numerosi progetti interni che hanno migliorato l'efficienza operativa e generato nuove opportunità di business.
Oggi Fastweb alza ulteriormente l'asticella, avviando un progetto ambizioso: la creazione di un LLM italiano al 100%, addestrato su documenti frutto di accordi dedicati con gruppi editoriali italiani, nel pieno rispetto della normativa europea e nazionale. Un modello che sarà in grado di dialogare in modo autentico ed empatico con i cittadini del nostro Paese, cogliendo tutte le sfumature della nostra splendida lingua.

Investendo nella tecnologia NVIDIA DGX SuperPod H100, Fastweb sfrutterà la migliore soluzione disponibile sul mercato per realizzare questo LLM italiano, garantendo al contempo la sovranità dei dati. Il modello sarà infatti installabile nei data center privati dei Clienti o su cloud pubblico, ma il suo utilizzo sul SuperPod di Fastweb, in un data center italiano, massimizzerà le prestazioni e assicurerà una governance dei dati end-to-end gestita direttamente dal personale dell'azienda.

Un passo avanti che non passa inosservato: durante un recente evento globale, NVIDIA stessa ha elogiato il contributo di Fastweb all'adozione dell'Intelligenza Artificiale in Italia. Un motivo di grande orgoglio per un'azienda che, da sempre, si impegna a rendere il nostro Paese un esempio virtuoso di trasformazione digitale, aumentandone la competitività a livello internazionale.
Con questo progetto di LLM italiano, Fastweb dimostra ancora una volta la propria visione pionieristica, ponendosi come un punto di riferimento per l'Intelligenza Artificiale nel nostro Paese, al servizio di aziende, cittadini e della sovranità digitale dell'Italia.

LA RIVOLUZIONE DELLA CYBER SECURITY

FORTINET

La cyber sicurezza è fondamentale in un mondo sempre più digitalizzato, interconesso e automatizzato. Abbiamo impiegato anni per capirlo ma finalmente tutti siamo giunti ad una conclusione: la sicurezza informatica è imprescindibile. Lì dove fallisce la sicurezza informatica fallisce il servizio, può fallire l'intera organizzazione e, ora più che mai, rischia di fallire l'intera nazione. Questo perchè, dato condiviso nei vari report, ad essere prese di mira sono sempre di più le infrastrutture critiche, le pubbliche amministrazioni (che includono anche la sanità in Italia) e la difesa. I dati mostrati dai rapporti Clusit sulla sicurezza ICT in Italia degli ultimi anni, dove Fortinet contribuisce estraendo i dati dai FortiGuard Labs, confermano questo trend. Di seguito gli attacchi individuati nel corso del 2023.

L'Italia nell'ultimo biennio ha fatto ingenti ivenstimenti sulla sicurezza informatica nei settori citati, basti pensare al PNRR, ai finanziamenti ACN (Agenzia per la cyber sicurezza nazionale) e alle convenzioni CONSIP dedicate alla Cyber Security. Sebbene, per la prima volta in assoluto in Italia, i budget pubblici non abbiano costituito una limitazione alle necessità degli enti nazionali di proteggersi, tale impegno non è bastato. Gli attaccanti nel corso del 2023, malgrado gli ingenti investimenti fatti dalle Pubbliche Amministrani e il duro lavoro da parte di tutti gli esperti del settore, ne hanno tratto vantaggio, portando a segno più attacchi dell'anno precedente, con uno sconfortante +65% (rapporto Clusit).
Analizzando le informazioni estratte dai FortiGuard Labs si evince altrisì che circa il 40% delle minacce individuate in Italia e nel mondo, sono collocabili nella fase di Pre-Attacco della Cyber Kill Chain (un modello che descrive le fasi attraverso cui un attaccante deve passare per avere successo nel suo intento). Bisogna ripartire dall'analisi attenta di queste informazioni preziose perché in questa fase nessun sistema di sicurezza tradizionale può aiutare, solo Intelligence e sistemi di Deception possono fare la differenza.

Intelligence e Deception
La Cyber Security moderna richiede non solo la difesa attiva da parte di soluzioni specifiche collocate nelle varie infrastrutture IT/OT/IoT, ma anche l'intelligence proattiva e le tecniche di deception per ingannare e neutralizzare gli attaccanti. Fortinet offre due strumenti avanzati per queste funzioni: FortiRecon e FortiDeceptor.

FortiRecon è una soluzione di intelligence che fornisce una visione completa delle potenziali minacce esterne. Il FortiRecon studia la superficie di attacco esposta e analizza web, dark web e altre fonti per identificare attività sospette e possibili minacce, prima che queste possano colpire l'infrastruttura target. Tale proattività consente alle organizzazioni di prepararsi e proteggersi al meglio dagli attacchi imminenti.

FortiDeceptor, invece, utilizza logiche "honeypot" per creare esche e trappole all'interno della rete, attirando gli attaccanti e raccogliendo informazioni preziose sulle loro strategie. Questa soluzione non solo aiuta a rilevare le minacce avanzate, ormai interne all'organizzazione, ma fornisce anche dati cruciali per migliorare le difese aziendali. La cooperazione delle due soluzioni risulta essenziale per studiare in profondità i propri cyber nemici.

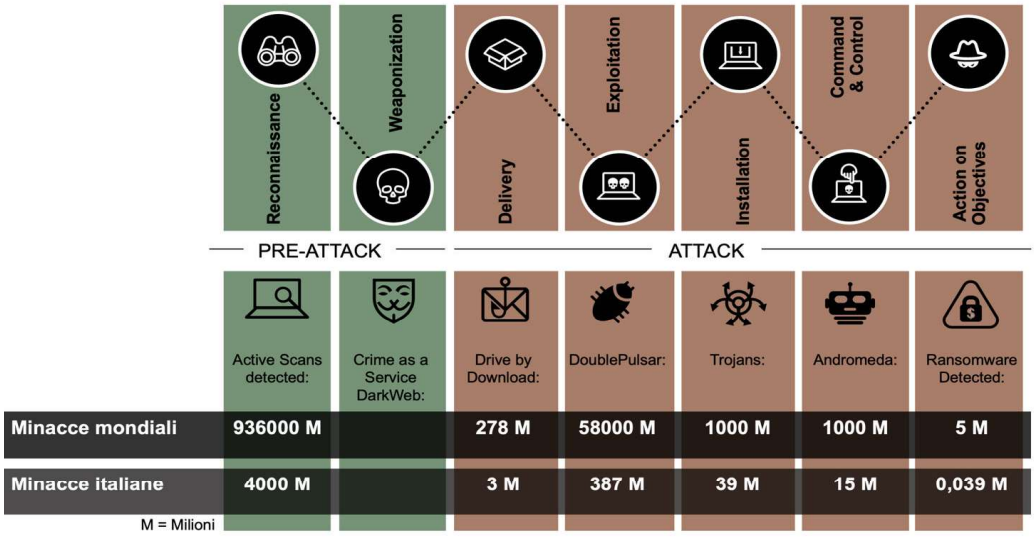
SecOps evolute e basate su IA generativa
La crescente adozione e combinazione di ambienti Cloud, 5G, infrastrutture OT (Operation Technology) e Industrial IoT, insieme alla conseguente evanescenza del tradizionale perimetro di sicurezza, hanno generato un panorama delle minacce più complesso ed esteso, incrementando di molto la superficie esposta ad attacchi. Gli analisti di sicurezza faticano a tenere il passo e il personale qualificato scarseggia. L'approccio attuale delle Security Operations (SecOps) non sempre riesce a fornire adeguato supporto agli Analisti: c'è costantemente la tendenza a concentrarsi sulla tecnologia a discapito di quello che dovrebbe essere l'elemento umano nella Cyber Security. Questo paradigma ha portato alla progettazione di SOC costituiti da decine di strumenti, il più delle volte non integrati tra loro, che nella quotidianità rappresentano "silos" estremamente dispendiosi da governare sia in termini di tempo che di risorse.
Un SOC "unificato" di nuova generazione o Cyber Fusion Center (CFC), si basa su automazione, orchestrazione ed integrazione delle informazioni interne (CyberSec, IT, OT, NOC). Un moderno CFC è costituito, senza alcun dubbio, da SIEM e SOAR moderni e cooperanti. Le soluzioni FortiSIEM e FortiSOAR, oltre ad offrire funzionalità state-of-art,

aggiungono la più moderna esperienza di utilizzo, basata su Intelligenza Artificiale Generativa, che consente agli analisti di sicurezza di ridurre al contempo i tempi di analisi delle minacce e delle azioni di remediation.

La complessità da sempre ostacola il lavoro degli esperti di sicurezza informatica e, mai come in questi anni in cui le organizzazioni gestiscono venti o trenta soluzioni di sicurezza informatica differenti, questo fattore è determinate. Fortinet fornisce una gamma completa di sistemi, cooperanti e basate sui più moderni algoritmi di IA (Machine Learning, Deep Neural Network, Generative AI) che unisco a FortiSOAR, FortiSIEM, FortiDeceptor, FortiRecon le soluzioni NGFW, SDWAN, ZTNA, SASE, Secure WIFI e Networking, NAC, EDR, WAF, Email security e moltro altro ancora.

Aldo Di Mattia
Senior Manager Systems Engineering Public Administrations, Defense and Critical Infrastructures Italy

Minacce individuate in Italia nel 2023 dai FortiGuard Labs e crescita rispetto l'anno precedente



Minacce individuate in Italia e nel mondo nel 2023 dai FortiGuard Labs e collocate nella Cyber Kill Chain

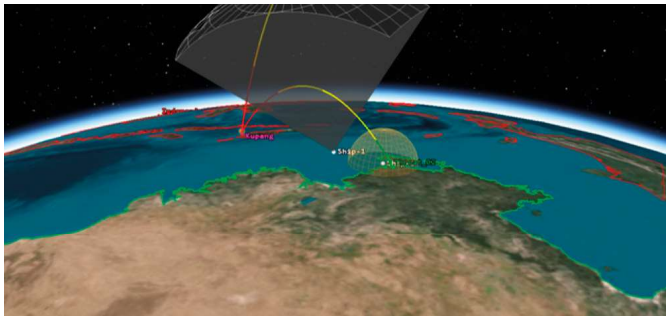
STRATEGIE AVANZATE: LA POTENZA DEL MODELING E SIMULATION NELLE OPERAZIONI MULTIDOMINIO

GMSPAZIO

La capacità di simulare e modellare scenari complessi che coinvolgono vari domini – marittimo, terrestre, aereo e spaziale – è diventata essenziale per la gestione delle operazioni civili e militari. Il Modeling e Simulation fornisce strumenti avanzati per l'analisi e la pianificazione, permettendo di prevedere e gestire situazioni complesse in ambienti multidominio.
Il M&S trova applicazione in numerosi settori, dall'ottimizzazione della navigazione marittima alla gestione delle emergenze urbane, dalla pianificazione delle operazioni aeree alla protezione dei satelliti. L'obiettivo è creare modelli realistici che permettano di testare strategie e prendere decisioni informate. Ad esempio, nel dominio marittimo, le simulazioni possono ottimizzare le rotte delle flotte, ridurre i consumi di carburante e migliorare la sicurezza, pianificare esercitazioni di difesa antisommergibile, creando scenari di combattimento per l'addestramento delle forze navali.

Nel dominio terrestre, il M&S supporta la gestione delle emergenze, la pianificazione urbana e le operazioni militari. Si utilizzano simulazioni per gestire il traffico e ottimizzare l'uso delle risorse, mentre le truppe militari si addestrano in scenari virtuali che replicano condizioni reali. Un esempio concreto è l'uso di M&S per simulare operazioni di guerra urbana, migliorando l'addestramento e la preparazione delle forze armate.

Nel dominio aereo, il M&S è cruciale per l'addestramento dei piloti, la gestione del traffico aereo e la pianificazione delle operazioni. Le simulazioni di volo avanzate permettono ai piloti di addestrarsi in situazioni di emergenza senza rischi reali. In ambito militare, aiutano a pianificare missioni aeree complesse, come le operazioni di supporto aereo ravvicinato, dove l'accuratezza e la tempestività sono fondamentali.
Nel dominio spaziale, supporta la pianificazione delle missioni, la gestione dei satelliti e la previsione degli eventi spaziali. Le simulazioni sono utilizzate per testare sistemi satellitari prima del lancio e prevedere le traiettorie orbitali, riducendo il rischio di collisioni con detriti spaziali. In ambito militare, il M&S aiuta a proteggere i satelliti da minacce come le armi antisatellite e i cyberattacchi.



Le minacce elettromagnetiche rappresentano un pericolo significativo per le operazioni multidominio. Eventi come le tempeste solari possono causare gravi danni ai satelliti e alle infrastrutture, interrompendo le comunicazioni e i sistemi di navigazione. Un'altra minaccia cruciale proviene dagli attacchi elettromagnetici nemici, che possono essere intenzionalmente diretti contro le strutture critiche per paralizzare le operazioni. Il M&S permette di prevedere e mitigare gli effetti di queste minacce attraverso la simulazione di scenari di interferenza elettromagnetica: modelli avanzati possono simulare l'impatto di un impulso elettromagnetico su una rete elettrica, permettendo di sviluppare strategie di difesa e di risposta rapida.
Immaginiamo un attacco nemico coordinato in cui un avversario lancia un attacco simultaneo su più fronti: una flotta navale si avvicina alla costa, unità terrestri si infiltrano nelle città, droni aerei minacciano infrastrutture critiche e satelliti nemici interferiscono con le comunicazioni. Utilizzando il M&S, i pianificatori militari possono creare un modello di questo scenario, simulando le risposte coordinate di tutte le forze coinvolte.

Le navi da guerra possono essere indirizzate verso posizioni strategiche per intercettare la flotta nemica, mentre le truppe di terra vengono mobilitate per difendere le città e neutralizzare le unità infiltrate. I piloti addestrati attraverso simulazioni avanzate possono lanciare contrattacchi per neutralizzare i droni nemici, mentre i sistemi di difesa satellitare lavorano per proteggere le comunicazioni critiche e interrompere le operazioni satellitari avversarie. Grazie alla previsione delle minacce elettromagnetiche, i pianificatori possono anticipare e mitigare gli effetti delle interferenze nemiche, garantendo la continuità operativa delle proprie forze.
Il M&S permette di testare queste strategie in un ambiente controllato, identificando punti deboli e migliorando le risposte prima che l'attacco reale si verifichi. L'integrazione di modelli realistici di tutti i domini coinvolti consente una visione olistica delle operazioni, migliorando il coordinamento e l'efficacia della risposta.

SPACE DOMAIN AWARENESS: L'INNOVAZIONE TECNOLOGICA NELLA DIFESA AEROSPAZIALE

GMSPAZIO

L'industria aerospaziale e della difesa si trova al crocevia di una trasformazione senza precedenti, guidata dall'innovazione tecnologica e dalla crescente dipendenza dalle risorse spaziali. La protezione degli asset strategici spaziali emerge come una priorità cruciale, sia per le applicazioni civili che militari. Diventa, quindi, evidente come la sicurezza spaziale rappresenti un pilastro fondamentale per la società e per le operazioni militari.
Gli asset spaziali, come satelliti per le comunicazioni, il monitoraggio ambientale, la navigazione e l'intelligence, sono indispensabili per la nostra vita quotidiana: non solo supportano le operazioni militari, ma influenzano settori come le telecomunicazioni, la meteorologia, la gestione delle emergenze e la ricerca scientifica. L'integrità di questi sistemi garantisce la continuità operativa e la sicurezza nazionale.
Per quanto riguarda le applicazioni militari, i satelliti ISR (Intelligence, Sorveglianza e Ricognizione) forniscono informazioni critiche sulle attività nemiche, consentendo alle forze armate di prendere decisioni informate e tempestive. La sorveglianza continua delle aree di interesse strategico è basilare per la sicurezza nazionale. I sistemi di comunicazione satellitare militari garantiscono la trasmissione sicura di informazioni sensibili tra unità operative, comandanti e centri di controllo. La resilienza delle comunicazioni satellitari è cruciale durante i conflitti, quando le reti terrestri possono essere compromesse. Inoltre, i sistemi di navigazione satellitare permettono il posizionamento esatto delle forze e il coordinamento delle operazioni. La precisione nei sistemi d'arma guidati, dipende dalla disponibilità e dall'affidabilità dei dati di navigazione satellitare.

La protezione degli asset deve affrontare diverse sfide. Gli space debris rappresentano una minaccia crescente per i satelliti operativi, aumentando il rischio di collisioni. La gestione e la mitigazione dei debris sono essenziali per preservare l'integrità degli asset. Inoltre, sono vulnerabili a cyberattacchi che possono compromettere le loro funzionalità o raccogliere informazioni sensibili. La Cyber Security nello spazio è una priorità per proteggere le comunicazioni e i dati trasmessi. Le armi antisatellite, poi, rappresentano una minaccia diretta, in grado di distruggere o disabilitare i satelliti critici. Lo sviluppo di tecnologie difensive è fondamentale per prevenire l'uso di tali armi.
Gli eventi meteorologici spaziali, come le tempeste solari, possono influenzare negativamente i satelliti, causando danni fisici ed elettromagnetici. Le particelle cariche emesse dalle tempeste solari possono danneggiare i componenti elettronici, interrompere le comunicazioni e degradare le orbite. La previsione e la gestione degli eventi meteorologici spaziali sono essenziali per minimizzare i danni e garantire la continuità operativa.
In questo contesto, l'uso dei digital twin e dell'AI emerge come una soluzione cruciale per affrontare e risolvere queste sfide.

L'applicazione dei digital twin consente di creare repliche digitali di satelliti e altri asset spaziali, monitorandone costantemente le condizioni e prevedendo possibili problemi grazie ai dati raccolti in tempo reale. Questi modelli virtuali possono aiutare a gestire e mitigare i detriti spaziali, prevedere collisioni e ottimizzare le rotte di navigazione. Inoltre, i digital twin possono essere utilizzati per simulare cyberattacchi, permettendo lo sviluppo di strategie di difesa efficaci e l'implementazione di misure di sicurezza avanzate.
L'intelligenza artificiale gioca un ruolo fondamentale nel migliorare le capacità dei digital twin. L'AI può analizzare enormi quantità di dati in tempo reale, identificando pattern e anomalie che potrebbero indicare potenziali problemi. Può monitorare le condizioni dei satelliti per rilevare guasti imminenti o prevedere gli effetti degli eventi meteorologici spaziali, permettendo di prendere misure preventive per proteggere gli asset. Inoltre, può essere utilizzata per ottimizzare le comunicazioni satellitari, garantendo una trasmissione sicura e affidabile delle informazioni sensibili anche durante situazioni di conflitto.
L'uso dei digital twin e dell'AI rappresenta una componente essenziale per la protezione degli asset strategici spaziali. Queste tecnologie non solo migliorano la capacità di monitoraggio e previsione, ma offrono anche strumenti potenti per l'analisi e la risposta alle minacce, garantendo la resilienza e la sicurezza delle operazioni spaziali in un contesto sempre più complesso.

LE TECNOLOGIE ESPONENZIALI PER LA DIFESA TRA VALORE E AFFIDABILITÀ

IBM ITALIA

Prevedere il futuro è probabilmente un'arte da film di fantascienza. Tuttavia, nonostante l'impossibilità di conoscere il domani con certezza, possiamo affermare, con sicurezza, che l'Intelligenza Artificiale (AI) sarà una protagonista indiscussa del nostro avvenire. Questo approccio verso una AI protagonista del nostro futuro lo si ritrova in diversi segmenti di industria e della società compreso il mondo della Difesa. Nonostante le sfide che temi come la AI pone, i leader della difesa rimangono ottimisti sul suo potenziale di aumentare la superiorità tattica, migliorare l'efficacia operativa e aumentare la preparazione dell'intero apparato difensivo. Una recente ricerca di IBM Institute for Business Value1 rileva che le organizzazioni di difesa di tutto il mondo stanno dando priorità all'AI, aumentando gli investimenti in questa tecnologia rivoluzionaria e riconoscendone il potenziale per ottenere un vantaggio strategico.

Dall'invenzione della polvere da sparo nel primo millennio all'avvento dell'aviazione, dei carri armati, dei radar e dei sottomarini nel XX secolo, le organizzazioni di difesa hanno sempre cercato di ottenere un vantaggio strategico attraverso i progressi tecnologici. Oggi, in risposta alle sfide geopolitiche la domanda di maggiori capacità è sbilanciata dalla mancanza di personale in organico e questo impone ai responsabili del mondo della difesa di rivolgersi all'intelligenza artificiale come strumento chiave per mantenere e incrementare l'eccellenza operativa. Con meno persone incaricate di svolgere più compiti in un ambiente operativo sempre più complesso, l'AI rappresenta un'opportunità senza precedenti per affiancare l'uomo a ogni livello nel processo decisionale.

Mentre nel 2023 le tre principali applicazioni hanno riguardato l'incorporazione dell'AI in veicoli autonomi e semi-autonomi e nella fornitura di servizi medici e sanitari, nei prossimi tre anni le organizzazioni della difesa prevedono di fare passi da gigante nell'adozione di AI in altre aree applicative, in particolare nei settori dell'intelligence, della sorveglianza e della ricognizione, del comando e del controllo.
Tuttavia, questa crescita dell'AI nella difesa è rallentata da considerazioni tecniche ed etiche, tra cui fiducia, controllo dei pregiudizi, trasparenza, responsabilità, robustezza dei modelli e gestione dei sistemi autonomi e automatizzati. In particolare, la robustezza dei modelli agli attacchi informatici è un tema sentito per le organizzazioni, che quindi sono impegnate a costruire difese tecniche e organizzative per garantire che le informazioni sensibili e classificate utilizzate nell'AI siano ben protette contro hacking e uso improprio. In questo panorama evolutivo si inserisce la proposta IBM di una intelligenza artificiale aperta, adattabile e soprattutto affidabile. Affidabilità che si declina con un modello di protezione e governo che attraversa l'intera genesi di un modello AI dalla sua creazione a partire dai dati, alla sua erogazione. Ogni fase del ciclo di vita è protetta da strumenti informatici quali quelli per proteggere i dati, API security per poteggere l'accesso ai modelli in esecuzione fino al confidential computing per la protezione dei prompt di invocazione dei modelli quando in uso. Alla protezione fisica di modelli e dati si affianca il governo semantico dei modelli con soluzione di governance che aiutano a verificare l'aderenza della AI alle regole come la EU AI Act, l'assenza di scostamenti dei modelli dalla realtà e prevenire allucinazioni.

Solo con quest'approccio di una AI affidabile e governata in tutti i suoi aspetti il mondo della difesa potrà trarre vantaggio dell'enorme potenzialità che questa tecnologia sta creando.

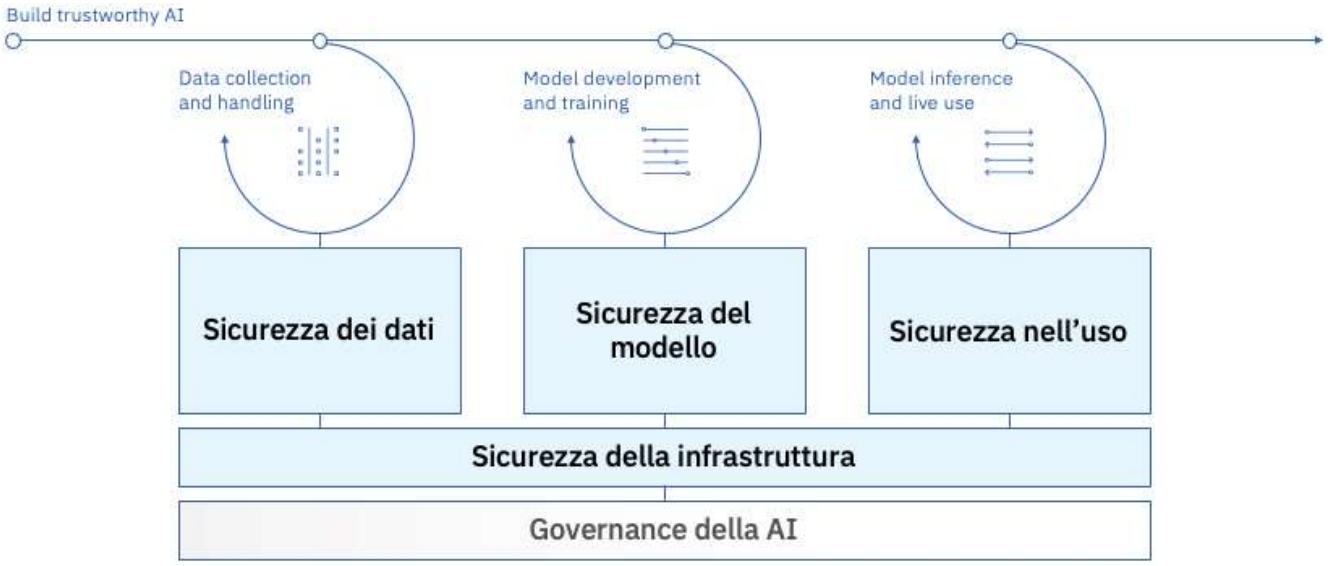


Figura 1. La protezione e governo dei modelli di intelligenza artificiale

Al fianco dell'intelligenza artificiale, una nuova tecnologia si sta sviluppando e promette di rivoluzionare l'informatica nei prossimi anni; si tratta della computazione quantistica.

I computer quantistici sono nuovi tipi di calcolatori basati sulle leggi della meccanica quantistica, la branca della fisica che regola i movimenti delle particelle a scala nucleare. Questa tecnologia permetterà di eseguire calcoli impossibili per i computer tradizionali.

I computer quantistici, la cui teoria di funzionamento è nota fin dagli anni 80 del secolo scorso e che hanno avuto le prime realizzazioni accessibili via cloud nel 2016, non sostituiranno però i computer tradizionali, ma si affiancheranno ai sistemi di super computing e ai motori di intelligenza artificiale per ampliare il numero di problemi risolvibili con l'informatica.
Per ottenere i vantaggi dei computer quantistici però bisognerà ripensare le attuali applicazioni e gli algoritmi che sono alla base di esse. È per questo motivo che, nonostante ancora non esistano computer quantistici abbastanza potenti per dare un reale vantaggio, molte istituzioni e aziende in tutto il mondo hanno promosso programmi di collaborazione con i produttori di questi nuovi hardware per formare una classe di professionisti in grado di usarli e per rivedere le applicazioni in versione quantistica. Chi riuscirà per primo a usare questi strumenti avrà un enorme vantaggio rispetto a chi sarà rimasto in attesa che la tecnologia maturi.

Esistono oggi vari modi per costruire computer quantistici, alcuni basati su fotoni, altri su atomi, altri su di superconduttori, e non si è ancora imposta una tecnologia rispetto alle altre. Secondo il report 2023 di IDC dei provider di hardware quantistico in cloud il leader risulta essere IBM che produce computer quantistici a superconduttori e ha sviluppato il linguaggio di programmazione quantistico Qiskit, usato da quasi il 70% dei programmatori. Questo framework è utilizzabile tramite Phyton ed è un asset open-source.

Lo scorso anno l'IBM ha rilasciato il primo processore con oltre 1000 qubit (le unità computazionali dei computer quantistici) e mette a disposizione via cloud processori da oltre 100 qubit per la ricerca e l'uso aziendale. Questo ha permesso di creare una comunità di utenti di oltre mezzo milione e un gruppo più ristretto di quasi 300 aziende e istituzioni che collaborano direttamente con IBM per lo sviluppo della computazione quantistica.

Gli ambiti in cui questo nuovo tipo di tecnologia porterà i risultati più rilevanti sono:

- Applicazioni nell'ambito dell'intelligenza artificiale e del machine learning; per esempio, nella categorizzazione e processamento delle immagini. Questo potrà avere ricadute nella pianificazione operativa e nella manutenzione predittiva di alcuni veicoli e infrastrutture;
- I problemi di ottimizzazione, che sono molto usati in vari ambiti, tra cui quello logistico e di gestione delle reti di comunicazioni:

- Le simulazioni dei sistemi naturali, che includono lo studio di nuovi materiali e l'analisi di reazioni chimiche oggi non esplorabili con i computer attuali.

I computer quantistici permetteranno però di risolvere anche problemi che oggi vengono utilizzati per i sistemi crittografici, in particolare quelli a chiave asimmetrica, mettendo a repentaglio sistemi di autenticazione, firme digitali e codifica di dati archiviati. In particolare, in questo ultimo caso alcuni agenti malevoli già stanno copiando dati criptati oggi per poterli decifrare non appena saranno disponibili computer quantistici abbastanza potenti; una pratica che passa sotto il nome di "*harvest now, decrypt later*".

L'ente certificatore statunitense NIST nel 2022 ha già identificato 4 nuovi algoritmi resistenti ad attacchi quantistici e a fine del 2024 è previsto il rilascio degli standard di utilizzo in produzione.
Il giorno in cui saranno disponibili computer quantistici abbastanza potenti per rompere gli schemi crittografici sembra ancora lontano. Tuttavia, per poter cambiare gli algoritmi di crittografia sarà però necessario un percorso di preparazione che si profila essere molto lungo.

Sarà prima di tutto necessario fare un inventario dettagliato di tutti gli algoritmi attualmente in uso e dove essi sono utilizzati. Sarà poi necessario costruire dei processi di crypto agility che permettano di cambiare gli schemi crittografici in tempi certi. Queste attività sono già state richieste dal presidente degli Stati Uniti in un memorandum del 2022 alle agenzie governative e anche alcuni paesi europei si stanno muovendo in questa direzione.

L'intelligenza artificiale e il quantum computing sembrano aprire grandi opportunità per chi sarà sfruttarli per primo, ma sono sicuramente una significativa minaccia per chi si farà trovare impreparato.

AI decision advantage for defense, IBM Institute for Business Value, 2024

UN NUOVO SISTEMA PER LA RISOLUZIONE DEL PROBLEMA DEI DETRITI SPAZIALI 'SPACE DEBRIS'

La deorbitazione satellitare e gli scenari futuri

IES

Dal primo lancio dello Sputnik nel 1957 l'umanità ha messo in orbita attorno alla Terra innumerevoli satelliti. Oggi però meno del 10% degli oggetti tracciabili in orbita sono operativi. Il resto è semplicemente spazzatura, identificata con il nome di detriti spaziali o 'space debris'.
Ad oggi, secondo la US Space Surveillance Network, sono circa 35.000 gli oggetti spaziali rivelabili con dimensioni maggiori di 10 cm per una massa totale di circa 8.500 tonnellate.
Vi si aggiungono oggetti piccolissimi (≥1 mm) per un totale di 130 milioni di elementi di massa totale pari a 8.610 tonnellate.
Il rischio di collisioni tra detriti e satelliti attivi c'è, con danni ingenti e con la prospettiva di ulteriori collisioni, che condizionerebbero l'esplorazione spaziale e l'uso di satelliti artificiali.
Vi è poi anche un rischio legato ai detriti che rientrano in atmosfera e che, per loro dimensione, possono costituire un pericolo per gli aerei e non solo.
Le soluzioni sono essenzialmente due: raccogliere i detriti in orbita, con costi, come immaginabile, enormi, oppure intervenire a livello progettuale sui satelliti di prossima generazione, tenendo presente che questi dovranno essere smaltiti, o rimossi dall'orbita, una volta terminato il proprio ciclo vitale.
La IES, in collaborazione con partner tecnologici di settore e centri di ricerca universitari, ha ideato un prodotto utile e pratico, integrabile in un satellite, per la rimozione automatica e certa dello stesso dalla propria orbita al termine del ciclo di vita. Pensato specificatamente per equipaggiare Cubesat (ma con una metodologia applicabile anche a satelliti di grandi dimensioni) tale sistema, denominato DEOS (sistema per la DEOrbitazione dei Satelliti – DEOrbiting system for Satellites), si basa su due componenti fondamentali:
1) un dispositivo di controllo programmabile ad alta affidabilità e resilienza, in grado di eseguire un monitoraggio attivo del nano-microsatellite, e gestire l'attivazione del dispositivo di deorbitazione, controllando la corretta esecuzione della procedura di rimozione/spostamento dall'orbita;
2) un dispositivo di deorbitazione in grado di determinare l'uscita del nano-microsatellite dall'orbita causando la ricaduta nell'atmosfera e la sua conseguente distruzione.

Poiché questo sistema deve poter intervenire alla fine della vita del satellite, esso deve essere più robusto e affidabile del satellite stesso.
Anzi, proprio le radiazioni presenti nello Spazio sono causa dei guasti all'elettronica del satellite, rendendolo un oggetto inanimato e non più controllabile, ovvero un rifiuto spaziale. Nelle identiche condizioni si trova ad operare il sistema DEOS, il quale quindi è concepito con tecnologie o criteri per far sì che non subisca analoghi guasti e si mantenga operativo, così da espletare la procedura di deorbitazione del satellite.
Questo dispositivo di controllo attivo è un sistema microcontrollore ad alta affidabilità e tollerante ai guasti specificatamente sviluppato per impieghi spaziali, denominato Rempro, progettato e realizzato dalla società IES e sufficientemente testato per deciderne l'impiego nel sistema DEOS.
Il processore tollerante ai guasti svolge anche il compito di FDIR al fine di incrementare l'affidabilità di funzionamento del satellite stesso.
L'altro sottosistema fondamentale per il sistema DEOS è quello che fisicamente provoca l'uscita dall'orbita del satellite. In DEOS sono previsti due tipi di dispositivi:

- a vela, che si spiega per aumentare la resistenza aerodinamica sufficientemente per far scendere di quota il satellite (leggero e più adatto a nanosatelliti);
- mediante motore magnetico (più adatto a microsatelliti).

Ecco che organismi internazionali come la statunitense Federal Communication Commission (FCC) stanno promuovendo l'introduzione di una nuova norma per il "deorbiting" (five years rule) che imporrebbe di deorbitare il satellite quanto prima dopo il termine della missione, non oltre 5 anni. Questa, imponendo ai satelliti una permanenza in orbita ben 5 volte inferiore alla norma attuale (che è 25 anni), richiede lo sviluppo di sistemi di rientro atmosferico da installare sul velivolo spaziale.
Come sulla terra vengono stabilite leggi e regole per le persone al fine di garantire il benessere della società, così anche nello spazio, per la presenza antropica che muta l'ambiente, gli organismi di governo stabiliscono nuove regole e norme e nuovi sistemi e dispositivi vengono sviluppati per migliorare la vita di tutti.

LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE SOTTOMARINE: UNA SFIDA CRUCIALE PER LA SICUREZZA E LA STABILITÀ

INTECS SOLUTIONS

Nell'era digitale e nell'economia globale, le infrastrutture sottomarine svolgono un ruolo fondamentale. Questi sistemi di comunicazione e trasporto si estendono per migliaia di chilometri sotto gli oceani, collegando continenti e consentendo la trasmissione di dati, energia e risorse vitali. Tuttavia, la loro vastità e complessità presentano sfide significative per la sicurezza e la protezione.

La vulnerabilità delle infrastrutture sottomarine

I cavi sottomarini, attraverso cui transita la maggior parte del traffico internet mondiale, sono essenziali per il funzionamento delle economie moderne. La loro posizione sott'acqua li rende vulnerabili a danni accidentali, per esempio derivanti da attività di pesca, e a minacce intenzionali, come attacchi terroristici o sabotaggi. Proteggere queste infrastrutture è un compito arduo che richiede una combinazione di tecnologie avanzate, collaborazione internazionale e strategie di difesa efficaci.

La protezione delle infrastrutture critiche sottomarine è un tema cruciale per i paesi tecnologicamente avanzati poiché la compromissione di questi cavi potrebbe causare danni incalcolabili alle economie globali, rendendo la loro sicurezza una priorità strategica. In questo contesto, l'Europa, la NATO e i governi nazionali stanno collaborando per sviluppare soluzioni tecniche capaci di mitigare i rischi attuali e futuri.

L'impegno dell'Italia e dell'Europa

L'Italia è in prima linea nella definizione delle politiche di sicurezza per le infrastrutture critiche sottomarine: a confermarlo il suo ruolo di Coordinator nel progetto di Difesa Europea nell'ambito della Cooperazione Strutturata Permanente (PESCO), denominato "Critical Seabed Infrastructure Protection" (CSIP), che ne è una testimonianza. Questo progetto mira a sviluppare soluzioni congiunte per proteggere le infrastrutture sottomarine e garantire la loro integrità e sicurezza, promuovendo al contempo la cooperazione tra paesi europei.

Le industrie tecnologiche italiane, come Intecs, svolgono un ruolo fondamentale in questo scenario. La loro esperienza e competenza nel settore sono indispensabili per sviluppare soluzioni innovative che possano affrontare le sfide attuali. Intecs, in particolare, è in grado di posizionarsi come un attore chiave nel mercato grazie alla sua conoscenza del dominio e alle sue competenze tecnologiche, acquisiti in oltre 50 anni di esperienza.

L'azienda è impegnata nello sviluppo di sistemi avanzati per la protezione delle infrastrutture sottomarine, contribuendo a migliorare la sicurezza e la resilienza delle reti globali.

Le sfide tecnologiche e le soluzioni innovative

La protezione delle infrastrutture sottomarine richiede l'impiego di tecnologie avanzate e soluzioni innovative. Un elemento chiave è l'utilizzo di veicoli a guida autonoma sottomarini (Unmanned Underwater Vehicles – UUV), che possono aumentare la capacità di consapevolezza situazionale (Situation Awareness) nei fondali marini. Questi sistemi rappresentano una sfida tecnologica complessa, poiché il dominio sottomarino è altamente articolato e richiede l'impiego di molteplici sensori a bordo di piattaforme compatte e dotate di elevata autonomia operativa. In tale settore la Intecs opera mettendo a disposizione di società di primaria importanza le competenze derivanti dal Centro di Intelligenza Artificiale e dal Laboratorio Hardware con soluzioni innovative per la messa appunto di sensori anche quantistici sviluppati con partner industriali ed enti di ricerca.

Le industrie saranno sempre più chiamate a trovare forme di aggregazione e collaborazione per sviluppare soluzioni congiunte. La sinergia tra le diverse parti interessate è essenziale per affrontare efficacemente le sfide poste dalla protezione delle infrastrutture critiche sottomarine. In questo contesto, la collaborazione tra settori pubblico e privato è fondamentale per sviluppare tecnologie avanzate e strategie di difesa innovative.

Una sfida globale

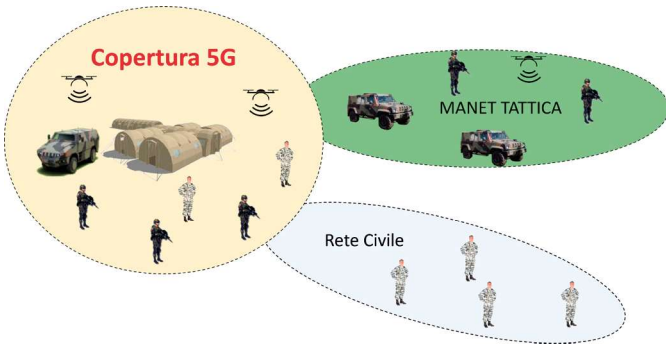
La protezione delle infrastrutture critiche sottomarine richiede una sinergia tra paesi, organizzazioni e industrie. Solo attraverso una cooperazione globale possiamo affrontare efficacemente questa complessa sfida. Garantire la sicurezza delle comunicazioni globali, l'approvvigionamento energetico e la resilienza delle reti è essenziale per il benessere e la stabilità delle società moderne. In conclusione, la protezione delle infrastrutture critiche sottomarine è una sfida cruciale che richiede un impegno collettivo e una collaborazione internazionale. Con il progresso delle tecnologie e l'aumento delle minacce, è ormai necessario sviluppare strategie innovative e soluzioni avanzate per garantire la sicurezza e la stabilità delle reti sottomarine, essenziali per il funzionamento delle nostre società e il benessere delle future generazioni. L'adozione di approcci integrati e la promozione della cooperazione internazionale sono la chiave per affrontare questa sfida e garantire un futuro sicuro per tutti.

5G PER APPLICAZIONI MIL

LEONARDO

Oggi un utente della telefonia radio mobile può guardare un video ad altissima qualità passeggiando mentre controlla la posta e regola la temperatura del proprio appartamento, accendendone alla domotica Tutto questo è possibile grazie alle tecnologie impiegate dalle reti radio mobili degli Operatori che sono in grado di fornire questi e altri servizi a milioni di utenti contemporaneamente.

Una rete 5G oggi si costruisce attraverso 3 macro elementi: RAN (accesso radio), Core e MEC, dove si "programma la rete" e su cui possono essere installati vari applicativi Questi elementi integrati hanno permesso al 5G di essere quello che è oggi: una tecnologia capace di garantire connessioni in tempo reale (con una latenza caratterizzante inferiore a 1ms), altamente configurabile in base alle esigenze dell'utilizzatore e con la capacità di garantire un elevato numero di utenti connessi, garantendo le medesime prestazioni. Proprio per queste caratteristiche, il 5G è diventato d' interesse per applicazioni militari, anche se risulta evidente che non può essere impiegato "as it is" e non solo per una questione di "dato classificato". Lo studio della sua applicazione all'interno dello strumento militare è affrontato oggi a livello NATO ed Europeo a partire dalla identificazione di casi d'uso – veri e propri scenari di impiego operativi – che vanno dallo strategico, all'operativo, al tattico. Un esempio concreto può essere l'applicazione del 5G all'interno di una base militare, di un posto comando o una FOB fino ad arrivare all'area "Combat" propria del campo di battaglia, dove si studiano sia task force navali sia scenari veicolari come il "Mounted and Dismouted Combat" e l'impiego di UxV nelle operazioni terrestri.



Nel progetto EDF 5G COMPAD, Leonardo, in stretta collaborazione con Ericsson, progetta soluzioni che permettano di avere un 5G sicuro militarmente per questi casi d'uso. In particolare, tale progetto ha lo scopo di facilitare l'uso del 5G per la Difesa e abilitare l'interoperabilità tra reti di comunicazioni della difesa e reti pubbliche negli Stati Membri della EU. La sfida è quella di realizzare un sistema 5G **sicuro militarmente** per le future forze armate europee che garantisca:

- Il supporto delle forze di coalizione (Federated Mission Networking);
- L'interoperabilità tra Nazioni;
- L'Utilizzo della rete 5G Commerciale nazionale.

In particolare, Leonardo, come System Integrator della tecnologia 5G nei propri sistemi, si sta occupando di costruire una rete sicura (anche con capacità TRANSEC) che garantisca il passaggio sicuro di dati classificati (COMSEC) e l'isolamento delle applicazioni Mil e delle reti Mil dalla rete 5G attraverso un Gateway dedicato. In altre parole, potremmo definirlo come un livello di sicurezza aggiuntivo, da utilizzarsi quando la sicurezza standard 5G non è considerata sufficiente, come nel trasferimento di informazioni classificate.
Insieme con Ericsson, Leonardo sta lavorando in EDF 5G COMPAD agli aspetti di Cyber e Jamming a cui la RAN può essere esposta. Soprattutto questi due ultimi aspetti fanno la differenza tra un impiego di tecnologia 5G in uso civile rispetto ad un dominio militare. La tecnologia radio delle reti 5G commerciali infatti è uno standard pubblico non concepito per essere robusto alle minacce elettromagnetiche involontarie e volontarie (jamming). La complessità del software necessaria alla sua realizzazione la rende esposta alle minacce cyber che possono colpire la catena di approvvigionamento. Per questo da una parte si studiano tecniche per l'individuazione dei jammer e i loro impatti sulle prestazioni delle RAN, definendo anche e soprattutto tecniche di mitigazione (riconfigurazioni dinamiche) che li minimizzino.
Nel progetto Leonardo ed Ericsson stanno anche definendo tecniche avanzate di Cyber Proactive Deception, una difesa informatica proattiva che comporta la creazione deliberata di informazioni fuorvianti o sistemi esca all'interno di una rete, per fuorviare e confondere potenziali aggressori preservando le risorse radio delle RAN.
Affinché i dispositivi militari futuri, elettro-ottici, radar, comunicazioni possano essere connessi mediante tecnologia 5G si prevede che lo scambio dati avvenga su frequenze dedicate della difesa, utilizzando una rete resiliente e robusta agli attacchi di Jamming e Cyber e sicura militarmente, ossia che garantisca il trasferimento sicuro delle informazioni al suo interno e in isolamento dalle altre reti Mil e civili, pur essendo con quest'ultime interoperabile.

IL PROGETTO JEY-CUAS ALLA BASE DEL FUTURO SISTEMA C-UAS EUROPEO

LEONARDO

Leonardo partecipa attivamente ai programmi finanziati dall'Unione Europea per la Difesa, prima nell'European Defence Industrial Development Programme (EDIDP) e, negli ultimi anni, nell' European Defence Fund (EDF). Un'ampia rete di collaborazioni internazionali, il coinvolgimento delle PMI, la sinergia con la Difesa italiana sono gli elementi principali alla base di questo successo, che ha visto Leonardo aggiudicarsi 13 progetti su un totale di 54 nel 2023, risultando il secondo player europeo.

Il progetto EDIDP JEY-CUAS, uno dei primi progetti acquisiti, si è concluso nel maggio 2024 con la Preliminary Design Review (PDR), svoltasi a Roma con la partecipazione della Commissione Europea e degli End Users.

JEY-CUAS, con un consorzio industriale a guida Leonardo composto da 40 partner provenienti da 14 Stati Membri, ha l'obiettivo di definire le specifiche e la progettazione preliminare di una capacità C-UAS completa (rilevamento, tracciamento, classificazione, identificazione, valutazione del rischio e neutralizzazione), concentrandosi su micro e mini-droni sempre più utilizzati per scopi di difesa e affrontando unità UAS singole o multiple, operanti in squadra o come un unico sistema (sciame).

JEY-CUAS ha specificato e progettato una nuova generazione di sistemi C-UAS basati su architettura plug & play, modulare e flessibile, da utilizzare in diversi contesti supportando gli obiettivi chiave di questa tipologia di sistemi:

- servizi centralizzati e distribuiti per garantire la capacità di crescita del sistema e la personalizzazione dell'interfaccia uomo-macchina;
- *containers* (blocchi logici software) per migliorare la resilienza del sistema;
- funzionalità plug'n'play per consentire una facile installazione di nuovi sensori ed effettori;
- *micro-services* che permettono di strutturare il sistema JEY C-UAS come una raccolta di servizi più piccoli, liberamente accoppiati e distribuibili in modo indipendente.

L'architettura concepita mira ad affrontare la sfida posta dai micro e mini-UAV., per migliorare la *situational awareness* e contrastare la crescente resilienza degli UAS alla prima generazione di C-UAS, rispondendo alle nuove minacce LSS (Low, Small, Slow) e riducendo i tempi di reazione.

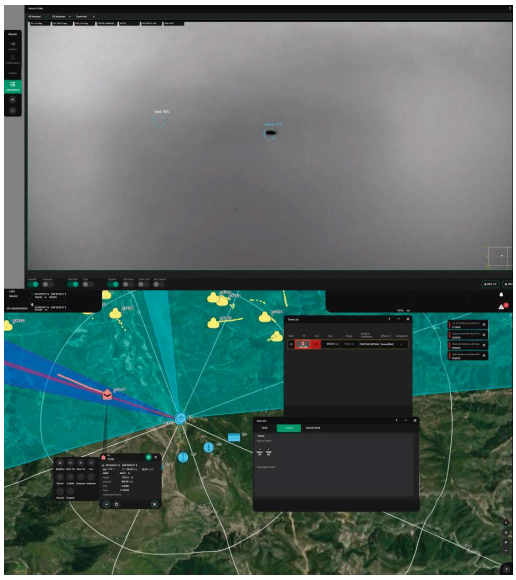
L'architettura e le capability del sistema JEY-CUAS sono state validate attraverso una dimostrazione di sistema, che ha integrato una serie di tecnologie selezionate tra i numerosi sensori, sottosistemi C2 ed effettori, studiati e progettati durante il progetto.

Con l'esercizio dimostrativo sono stati raggiunti i seguenti risultati:

- Integrazione di un sistema complesso con un numero elevato di sottosistemi: 7 sensori, 5 effettori e 3 sottosistemi C2 con approccio plug&play, funzionamento continuo e coordinato.
- CUAS C2 gerarchico multiruolo (sorveglianza, assegnazione effettore, C2 mobili).
- Validazione dell'intera catena di ingaggio CUAS.
- Utilizzo del protocollo SAPIENT per l'integrazione di un drone di sorveglianza, laser, lanciamissili. Sorveglianza completa eseguita con drone di sorveglianza.
- Integrazione tra sottosistemi C2: distribuzione della Common Operating Picture (COP) e dell'assegnazione degli effettori (Weapon Assignment, WA), comando e controllo, C2 mobile.
- Gestione di streaming video EOSS multipli su C2 per supportare la completa consapevolezza della situazione e il processo decisionale.

Oltre al coordinamento del consorzio, Leonardo ha svolto un ruolo chiave nel progetto in quanto responsabile per la realizzazione delle specifiche e dell'architettura di sistema, dell'adattamento e integrazione del suo sistema di Comando e Controllo e del radar TMMR nonché del coordinamento della dimostrazione conclusiva tenutasi al PISQ, Perdasdefogu, Sardegna nell' Aprile 2024.

JEY-CUAS ha aperto la strada al progetto successivo, E-CUAS, un progetto EDF assegnato a un consorzio europeo guidato da Leonardo, che comprende la maggior parte dei partner JEY-CUAS. L'obiettivo di E-CUAS è progettare e validare una soluzione completa anti-drone nei tre scenari, fisso, mobile e deployable, attraverso la realizzazione di un dimostratore tecnologico.



Co-funded by the European Union

Questa pubblicazione è co-finanziata dall'Unione Europea. Il suo contenuto è responsabilità di Leonardo e non riflette necessariamente il punto di vista dell'Unione Europea

JEY-CUAS è co-finanziato dall'Unione Europea nell'ambito del programma European Defence Industrial Development Programme (EDIDP) 2020, attraverso il Grant Agreement EDIDP-CUAS-2020-78-JEY-CUAS.

EFFICIENTAMENTO ENERGETICO DELLE AZIENDE: COME L'INTELLIGENZA ARTIFICIALE PUÒ FARE LA DIFFERENZA

MATICMIND

Piattaforme IoT evolute, quali sono i vantaggi.

Investimenti nel controllo dell'efficientamento energetico sono sempre più strategici per le aziende. Grazie ad essi, infatti, è possibile migliorare le proprie performance e aumentare la competitività sui mercati, riducendo il consumo di energia e le emissioni di CO_2.

Adottare strategie e soluzioni di efficientamento energetico con le quali ottimizzare i costi, migliorare l'efficienza e garantire la sostenibilità dell'energia, consente alle aziende di affrontare le sfide e cogliere le opportunità dell'attuale mercato energetico che, sempre più caratterizzato da importanti trasformazioni, sta mettendo a dura prova il mondo produttivo.

L'intelligenza artificiale (AI) gioca un ruolo chiave nell'efficientamento energetico delle aziende: dall'**ottimizzazione dei consumi** e della **produzione** alla possibilità di attuare un **miglioramento energetico continuo**, dalla capacità analitica di **identificazione dei trend di consumo** alla **manutenzione predittiva** degli impianti, sono innumerevoli le opportunità di risparmio con le quali l'AI potrà aiutare le imprese ad affrontare in maniera efficace il nuovo contesto e a raggiungere l'efficienza energetica.

Efficientamento energetico e AI: vantaggi misurabili

I benefici dell'applicazione di algoritmi di intelligenza artificiale sono concreti e misurabili. Nelle grandi aziende, così come nelle PMI, grazie **all'ottimizzazione dei Building energy management systems**, i risparmi negli edifici variano dal 10 al 20%, mentre salgono intorno al 30% con la **pianificazione ottimizzata di tutte le fasi produttive**.

Le tecnologie basate sull'intelligenza artificiale consentono una **riduzione dei consumi** interagendo e interfacciandosi con gli impianti esistenti, migliorando i processi giornalieri e fornendo risultati esaustivi, precisi e frequenti, con i quali creare dei **modelli affidabili e duraturi per generare valore** e assumere decisioni più efficaci e sicure nel tempo. Si tratta di soluzioni e sistemi di AI la cui importanza è destinata a crescere.

Nei prossimi anni, infatti, l'intelligenza artificiale avrà un ruolo sempre più strategico per le aziende italiane, come rivela un **recente studio dell'Osservatorio Artificial Intelligence della School of Management del Politecnico di Milano:** nel 2023 le imprese italiane hanno investito **760 milioni di euro** nelle **tecnologie per l'intelligenza artificiale**, con un balzo del 52% rispetto al 2022 e una crescita complessiva del mercato pari a +262% negli ultimi 5 anni.

Come l'AI sta rivoluzionando le soluzioni di efficientamento energetico per le aziende

La digitalizzazione dei processi produttivi consente alle aziende la raccolta di **enormi moli di dati** connessi a diversi ambiti, compresi quelli relativi ai consumi e ai vari fattori che li determinano.

Le **piattaforme IoT più evolute** sono in grado di **analizzare le informazioni** acquisite sul campo e di restituire una fotografia dettagliata sul **funzionamento dell'impianto**, costruendo delle **serie storiche di dati**, sulla base delle quali è possibile analizzare il comportamento del sistema in un determinato intervallo temporale. In termini di efficientamento energetico, la disponibilità di dati storicizzati apre a opportunità mai immaginate prima.

Imparando dai dati storici e replicando quanto appreso grazie a soluzioni di Intelligenza Artificiale (AI) e Machine Learning (ML), oggi, le **piattaforme IoT** hanno **capacità di auto apprendimento del contesto** che, oltre ad **analisi comparative sui periodi**, al **monitoraggio di eventuali cambiamenti tra serie di dati e alla creazione delle baseline di dati del cliente**, consente loro di **effettuare previsioni** a supporto dei processi decisionali a carico dell'energy manager dell'azienda. Questo processo di auto apprendimento diventa più efficace quanti più dati si forniscono.

Incentrandosi sui dati reali, gli algoritmi di AI e ML, capaci di apprendere sulla base dell'esperienze e di scoprire

le vere correlazioni tra i dati, conferiscono ad una piattaforma IoT quella **consapevolezza** e **proattività** che la rendono **"evoluta" rispetto all'obiettivo**, cioè in grado di perseguire **l'efficientamento del processo produttivo**, assumendo **decisioni autonome** per il raggiungimento degli obiettivi di business con minori consumi energetici e maggiori risparmi di risorse.
I vantaggi di una **piattaforma IoT evoluta**, quindi, possono essere sempre declinati in termini di **efficientamento energetico**, ovvero di capacità di conseguire gli stessi obiettivi finali, oppure anche più ambiziosi, impiegando un minor quantitativo di risorse.

IoTMind software proprietario di gestione e controllo per soddisfare tutte le esigenze IoT

Oggi l'azienda dispone anche di una propria piattaforma, **IoTMind**: si tratta di un software proprietario di gestione e controllo pensato per soddisfare tutte le esigenze IoT del Cliente.
La nostra offerta si sviluppa su 7 aree tecnologiche (networking, data center, digital workplace, Cyber Security, enterprise application, cloud e IoT) e su un portafoglio completo di servizi professionali (consulenza, progettazione, ingegneria, installazione, configurazione, manutenzione, supporto, servizi gestiti). Disponiamo di competenze specialistiche di alto livello, con oltre 2.000 certificazioni individuali. Maticmind ha instaurato partnership con più di 70 tra i principali fornitori di tecnologia. Con le ultime acquisizioni, il gruppo sviluppa circa 450 milioni di ricavi annui e ha raggiunto i 1.500 dipendenti, distribuiti su tutto il territorio nazionale.
Un'azienda come la nostra, tecnologica e con competenze da system integrator, ha le caratteristiche giuste per affermarsi con successo in questo mercato, per gestire al meglio l'integrazione dei sistemi IT (informatici) con quelli OT (impiantistici), considerando fra questi ultimi sia quelli classici sia quelli più evoluti. Maticmind si serve anche di risorse provenienti dal mondo dell'automazione. Mettere assieme competenze di ingegneria e progettazione con quelle di automazione, legate al mondo delle infrastrutture informatiche, è ciò che rende possibile a Maticmind la realizzazione di progetti complessi.

IDENTIFICAZIONE E LOCALIZZAZIONE DELLE INTERFERENZE NELLE RETI MOBILI: LE SFIDE E LE SOLUZIONI

M.P.G. INSTRUMENTS
Fabio Bianchi Martina

Identificare e correggere le problematiche legate alle interferenti nelle reti radio e cellulari è sfidante ma necessario per la loro criticità. Gli utenti in prossimità di una sorgente di interferenza subiranno una diminuzione delle percentuali di successo delle chiamate, una riduzione della durata della batteria, una scarsa qualità della voce e del throughput dati. Il rilevamento, la localizzazione e quindi l'eliminazione delle fonti di interferenza RF è un'attività essenziale per gli operatori di reti mobili per garantire il servizio offerto.

Lo spettro radio (ovvero la gamma di frequenze da 3 kHz a 300 GHz) è una risorsa limitata e la proliferazione di applicazioni e servizi wireless ha aumentato la necessità di utilizzarlo sempre più. Maggiore è il numero di trasmettitori radio operanti, maggiore è anche il potenziale di interferenze RF. L'interferenza RF può essere definita come l'effetto di una energia indesiderata dovuta ad una combinazione di emissioni, radiazioni, conduzioni o induzioni alla ricezione in un sistema di comunicazione radio e manifestata da un qualsiasi degrado delle prestazioni, da interpretazioni errati o da perdita delle informazioni.

Con l'introduzione del 5G, sono stati rese disponibili nuove e molto più ampie bande nelle gamme delle onde millimetriche e medie. Sebbene la probabilità di interferenza sia relativamente bassa per le caratteristiche dello spettro e per l'utilizzo belle bande sopra indicate, possono comunque manifestarsi interferenze se non vengono eseguite adeguate attività di pianificazione, installazione e manutenzione della rete. Per garantire una strategia di prevenzione ed analisi approfondita, è utile comprenderne le cause, le caratteristiche, gli effetti e quindi come possono essere identificate e mitigate.

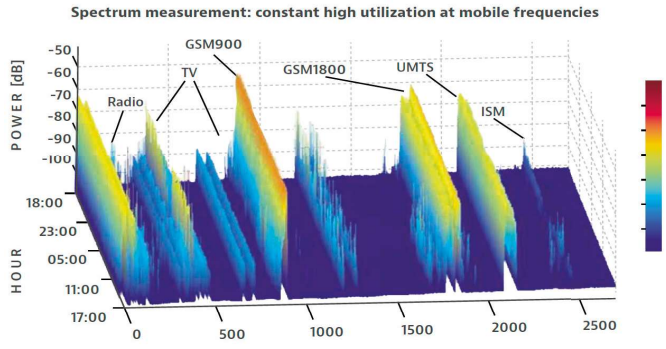


Figura 1. Lo Spettro RF da 0 a 2.5 GHz

Una utile classificazione delle interferenze è quella che le divide tra generatori intenzionali o non intenzionali. I generatori RF non intenzionali sono dispositivi che hanno lo scopo di generare energia RF per l'uso all'interno del dispositivo stesso, ma che consentono a parte di tale energia di essere irradiata o "dispersa" all'esterno. Un esempio di radiazione non intenzionale è la radiofrequenza emessa dagli oscillatori di clock all'interno di un computer portatile o di un tablet.

I generatori intenzionali sono invece dispositivi progettati per generare ed emettere energia RF. Un esempio di generatore intenzionale è un router Wi-Fi.

Fondamentalmente, qualsiasi aumento del rumore di fondo di un ricevitore a un livello in cui la comunicazione prevista può essere interrotta è definito come interferenza.

Partendo da questa definizione, si possono identificare quattro categorie di rumore RF:

1. Rumore naturale, come quello prodotto da fulmini (rumore atmosferico o "statico") o da oggetti celesti (rumore cosmico).
2. Rumore artificiale, prodotto da generatori non intenzionali o accidentali (come definito sopra) da elementi come alimentatori switching ed alcuni tipi di lampade.
3. Rumore aggregato, prodotto intenzionalmente dall'uomo ed emessi da molti dispositivi con o senza licenza che generano emissioni fuori banda, armoniche e altri segnali spuri.
4. Oltre a queste tre categorie di rumore esterno, i ricevitori generano anche un proprio rumore RF interno (rumore "strumentale" o "termico").

Nelle comunicazioni, il noise floor è la misura del segnale creato dalla somma dei rumori RF appartenenti a queste quattro categorie più l'interferenza proveniente da sorgenti intenzionali identificabili. Include quindi tutti i segnali diversi da quello desiderato. Il rumore di fondo è un parametro critico nella progettazione di un sistema di comunicazione perché la capacità (misurata in bit al secondo) di un canale dipende fortemente dal rapporto tra il livello del segnale desiderato e quello generato da queste fonti di rumore e di interferenza.

L'interferenza complessiva proveniente da più sorgenti tende inoltre ad essere simile al rumore e quindi risulta difficile da distinguere dalle sorgenti naturali di rumore e da quello prodotto all'interno del ricevitore. Ciò può causare un aumento netto del noise floor con conseguenze negative per le prestazioni del sistema wireless ed influire sull'uso efficiente ed efficace dello spettro elettromagnetico.

L'interferenza RF (che chiameremo RFI) nelle reti cellulari è uno dei problemi più comuni nelle Radio Access Network (RAN). Diversi sistemi e servizi come comunicazioni mobili, radio mobili, reti locali wireless e trasmissioni video

utilizzano uno spettro assegnato specifico per evitare di trasmettere servizi diversi alla stessa frequenza, che causerebbero collisioni o interferenze del segnale. Tuttavia, in alcuni casi queste e altre unità generano involontariamente emissioni che possono aumentare il rumore di fondo di altri dispositivi, causando problemi di interferenza.

Gli strumenti per la caccia all'interferenza

Il processo di ricerca e risoluzione dei fenomeni di interferenza è complicato e richiede un certo livello di competenza in radiofrequenza, oltre a diversi strumenti a seconda dello scenario e dello specifico caso operativo. Alcuni tools sono più efficienti in determinate circostanze rispetto ad altri.

I due strumenti più comunemente usati per la ricerca delle interferenze sul campo sono gli scanner RF e gli analizzatori di spettro.

Gli scanner sono utilizzati principalmente per l'ottimizzazione della rete e sono utili anche per identificare un'area di interferenza generica, oltre che per misurare e calcolare i parametri RF di dettaglio. Sebbene questi strumenti siano utili per rilevare e identificare le interferenti, hanno una capacità limitata di isolare e localizzare le loro fonti. Alcune unità più recenti offrono la funzionalità di analisi dello spettro ma richiedono comunque una configurazione manuale.

Oltre ad altre funzioni, gli analizzatori di spettro sono invece molto utili per identificare la presenza di segnali spuri o indesiderati in uno spettro RF. Per identificare le anomalie RF vengono utilizzati due tipi di analizzatori di spettro: analizzatori tradizionali Sweep-Tuned e analizzatori in tempo reale (RTSA).

Così come gli analizzatori Sweep-Tuned, i Real Time Spectrum Analyzer (RTSA) utilizzano il calcolo FFT, ma con la maggiore potenza di elaborazione di cui sono dotati è possibile memorizzare l'evoluzione del segnale nel tempo. Quando si utilizza un analizzatore RTSA, gli eventi transitori o i rapidi cambi del segnale RF potenzialmente di interesse vengono sempre catturati. Gli analizzatori di spettro sono generalmente utilizzati con antenne omni e direzionali per la localizzazione delle sorgenti di interferenza. Alcuni offrono funzionalità intelligenti con applicazioni e moduli software aggiuntivi per identificare autonomamente le fonti di interferenza.

Lo spettrogramma (o spectrum waterfall) è un'altra funzionalità offerta su alcuni analizzatori di spettro. Questa funzione è particolarmente utile quando si tenta di identificare segnali periodici o intermittenti poiché cattura lo spettro elettromagnetico nel tempo e utilizza vari colori per differenziare i livelli di potenza delle singole frequenze. Quando viene utilizzata un'antenna direzionale, il tecnico vedrà un cambiamento nell'ampiezza del segnale tracciato; quando cambia la direzione dell'antenna, noterà un cambiamento nei colori dello spettrogramma. La sorgente del segnale si trova nella direzione corrispondente alla massima potenza del segnale.

Figura 2. VIAVI OneAdvisor800 con funzionalità RTSA/Spettrogramma

Figura 3. Misura dello spettro quadrupla per una ricerca di dettaglio

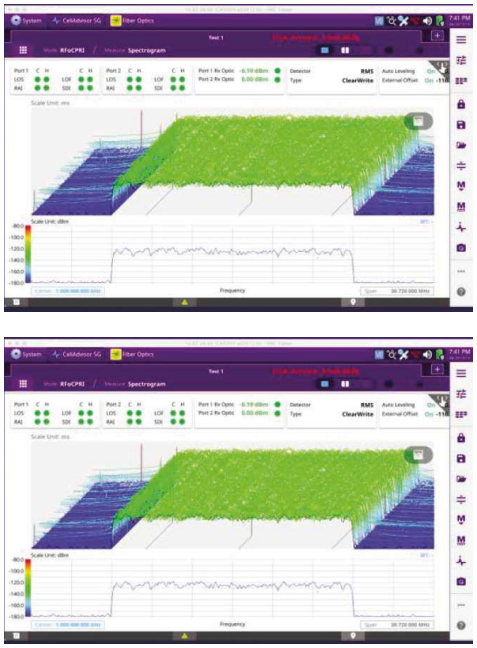


Figura 4. Modalità spettrogramma sul OneAdvisor800

I Realtime Spectrum Analyzer e la ricerca delle Interferenze nel 5G e nelle comunicazioni di nuova generazione (Interference Hunting).

Il 5G New Radio (NR) continua a utilizzare il multiplexing a divisione di frequenza ortogonale (OFDM); tuttavia, le opzioni duplex supportate in NR includono il Frequency Division Duplex (FDD), il Time Division Duplex (TDD) con configurazione semistatica UL/DL e il TDD dinamico. Nello schema TDD, sia il Down-Link (DL) che l'Up-Link (UL) utilizzano la stessa frequenza ma sono assegnati intervalli di tempo diversi per la trasmissione e la ricezione. In tale scenario, l'identificazione di un segnale interferente è estremamente difficile quando la stazione base trasmette il segnale in DL. Per superare questa problematica, viene utilizzata la funzionalità gated sweep che misura solo i segnali durante il periodo di trasmissione UL; la funzionalità di sweep con gate è quindi essenziale per isolare i segnali di interferenza nell'UL. Tuttavia, poiché 5G NR introduce il TDD dinamico in cui le trasmissioni UL e DL possono essere modificate dinamicamente, questa funzione non sarà più efficace. Un analizzatore di spettro in tempo reale (RTSA) può superare questa limitazione, in quanto può rilevare il livello e la frequenza di occorrenza di segnali interferenti in rapida evoluzione sovrapposti al segnale 5G NR. Inoltre, un RTSA può acquisire segnali transitori in modo più efficace.

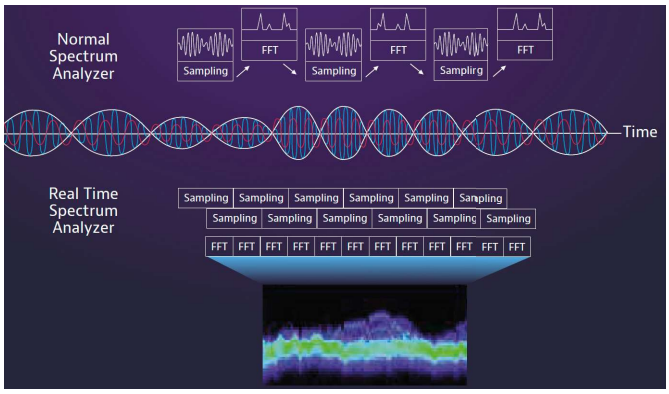


Figura 5. Tecnica di sovrapposizione dell'elaborazione sugli analizzatori RTSA

Un analizzatore di spettro in tempo reale può infatti elaborare da migliaia di spettri al secondo, ma la velocità di aggiornamento dello schermo visivamente percettibile è di 30 fotogrammi al secondo. Per superare questa limitazione lo strumento utilizza una modalità di visualizzazione chiamata persistenza, che presenta a monitor le centinaia o migliaia di dati dello spettro con un colore o una luminosità diversa in funzione della frequenza di occorrenza in modo da determinare la probabilità con cui i segnali compaiono piuttosto che la sola informazione della loro

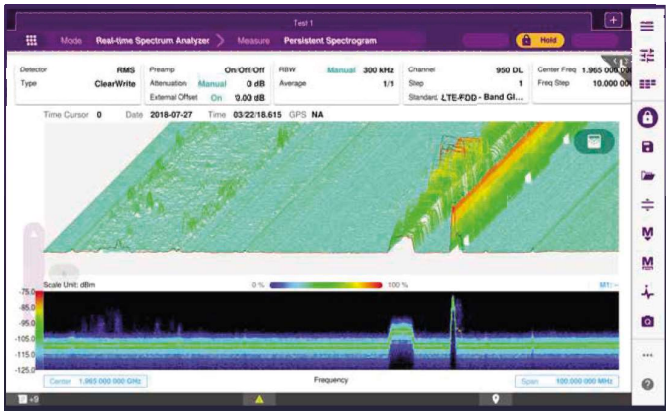


Figura 6. Visualizzazione a persistenza di interferenze a 2.4 GHz

Localizzazione delle Sorgenti Interferenti

Tradizionalmente, isolare le sorgenti di interferenza è un processo molto dispendioso in termini di risorse e costoso. Dopo aver identificato la presenza di interferenza in un'area gestita da una rete a scarse prestazioni, un ingegnere esperto eseguirà numerose misurazioni in diversi punti utilizzando un'antenna direzionale. Utilizzando la tecnica della triangolazione e dopo aver eliminato eventuali anomalie nelle misurazioni, identificherà un'area molto più piccola che dopo alcune iterazioni sarà sempre più ridotta fino a identificare la sorgente dell'interferente. Questa tecnica richiede pazienza, tempo e abilità. Sfortunatamente, per tutto il tempo necessario per completare la ricerca, gli utenti continueranno a subire gli effetti negativi delle interferenze sul servizio radio. VIAVI collabora con gli operatori di reti cellulari e private per migliorare il processo di ricerca delle interferenti. La soluzione completamente automatizzata di VIAVI è facile da configurare ed utilizzare, oltre che intuitiva. Un tecnico RF può infatti identificare e localizzare rapidamente la sorgente interferente semplicemente seguendo un messaggio vocale sfruttando il VIAVI InterferenceAdvisor™, composto dal software EagleEye™ in esecuzione su un tablet Android in accoppiata con il nostro analizzatore di spettro collegato ad un'antenna omnidirezionale. Gli ingegneri non devono quindi più guidare, fermarsi per controllare la direzione e muoversi di nuovo per trovare le aree sospette di interferenza: con VIAVI il processo è completamente automatizzato. I passaggi che prima richiedevano giorni possono ora essere completati in poche ore:Analizzare l'area di rete/sito(i) cellulare con le prestazioni peggiori.

1. Identificare il sito/i settori che subiscono il maggiore impatto
2. Dopo la verifica in loco della presenza di interferenti, muoversi nell'area utilizzando l'InterferenceAdvisor™, la

soluzione di tracking facile da configurare e utilizzare
3. Seguendo le istruzioni, il tool VIAVI identificherà la possibile area di origine dell'interferenza con una indicazione visiva sulla mappa
4. Parcheggiare il veicolo e individuare l'interferenza

Figura 7. Processo di caccia alle sorgenti di interferenza

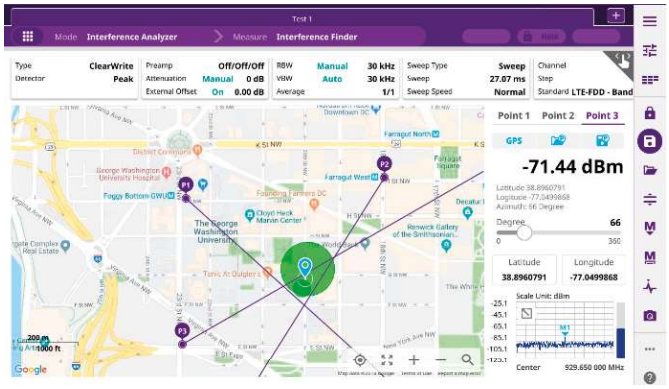


Figura 8. Processo di triangolazione per la localizzazione delle sorgenti di interferenza

Esempio applicativo di Interference Hunting

L'interferenza può essere generata da sorgenti RF intenzionali o non intenzionali, esterne alla rete o interne all'apparato stesso (come, per esempio, le intermodulazioni passive); può inoltre essere una sorgente RF costante o intermittente. Ognuno di questi può potenzialmente compromettere il ricevitore causando un degrado delle prestazioni. In questa sezione esaminiamo un case study che descrive come gli ingegneri utilizzano una varietà di soluzioni per rilevare, identificare e isolare una fonte di interferenza seguendo un processo graduale di ricerca. Alcuni degli strumenti utilizzati ne hanno migliorato il processo generale di ricerca e ridotto l'area di ricerca del bersaglio, nonché il tempo per individuare la potenziale fonte del segnale indesiderato.

Case Study: Identificazione di una Interferente Pirata

Un operatore di reti telefoniche statunitense stava sperimentando un disservizio nella sua rete a causa dell'improvvisa comparsa di una interferente sconosciuta. Diverse macrocelle posizionate nel centro di Nashville, intorno alla Bridgestone Arena, hanno infatti improvvisamente iniziato a segnalare un rapporto segnale/rumore (S/N) pessimo. Utilizzando i dati del Sistema di Supporto Operativo (OSS), la squadra ha identificato le celle ed i settori interessati dall'interferente ma non è stata in grado di determinare con precisione la direzione della sorgente. Il segnale è apparso anche su tutti e tre i settori di un sito all'incirca con stesso livello di potenza, il che non ha sorpreso i tecnici a causa del fitto ambiente urbano e della riflessione del segnale RF sugli edifici. Come hanno risolto il problema delle interferenze? La prima attività è stata quella di restringere l'area di interesse utilizzando il software VIAVI InterferenceAdvisor™ e EagleEye™.

In meno di un'ora di guida con InterferenceAdvisor™ attivo, il gruppo ha ristretto l'area all'isolato di fronte alla Bridgestone Arena stessa, con il segnale interferente misurato ad una potenza di circa -50 dBm. Quindi è stato il momento di individuare la fonte a piedi utilizzando AntennaAdvisor™.

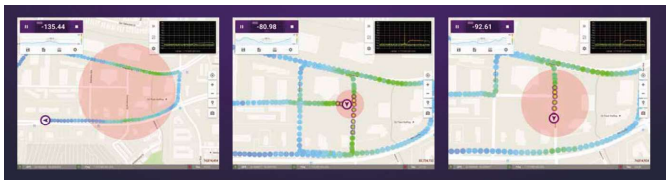


Figura 9. Ricerca dell'area di interesse

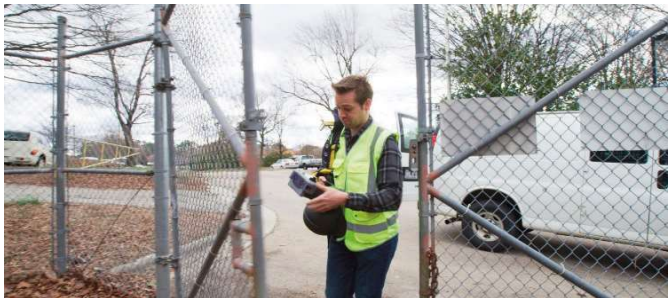


Figura 10. Tecnico nelle vicinanze della sorgente dell'interferenza

Usando l'antenna direzionale con l'opzione Radar Chart, la squadra è stata indirizzata verso un edificio di mattoni a due piani. Quando il team si è avvicinato all'edificio, la potenza del segnale è diventata sempre più elevata, fino a -10 dBm. La parete dell'edificio era tutta in mattoni, senza finestre visibili. Inoltre, non erano presenti antenne visibili sul tetto o sui lati dell'edificio. Solo alcune videocamere di sicurezza erano sono state montate tra il primo e il secondo piano e puntate verso il vicolo sul retro. Entrata nell'edificio la squadra investigativa ha parlato con il responsabile IT, che ha confermato di avere recentemente installato un ripetitore Wi-Fi acquistato online per espandere l'area di copertura della rete. Dopo aver spento il ripetitore, i tecnici hanno quindi utilizzato il OneAdvisor800™ per verificare che il segnale non autorizzato fosse stato eliminato. In meno di due ore, utilizzando VIAVI InterferenceAdvisor™ e AntennaAdvisor™, l'operatore **è stato in grado di isolare** e quindi eliminare un interferente non autorizzato e prevenire il degrado delle prestazioni di una rete cellulare di livello 1.

SPACEDGE™ SERVIZI OPERATIVI IN TEMPO QUASI REALE

Un ecosistema spaziale sicuro, integrato e scalare

PLANETEK

La forte instabilità internazionale e le recenti crisi regionali hanno reso evidente come l'attuale modello di sviluppo dei servizi non consenta di accedere allo sfruttamento dei dati con il rigore e la necessaria tempestività. Alcuni limiti costituiti da informazioni incomplete dei dati osservati (nano satelliti a limitate potenze, larghezza di banda e manovrabilità), scarsa manovrabilità, estrema dipendenza dal fattore umano, sono alcuni delle caratteristiche che affliggono le infrastrutture terrestri e spaziali dei fornitori di servizi e degli utenti finali. Quasi tutti questi problemi possono essere affrontati oggi grazie alla crescente disponibilità di potenza di calcolo a bordo e a tecniche e soluzioni algoritmiche avanzate, come l'intelligenza artificiale, che consentono operazioni autonome. In particolare, le funzionalità avanzate basate sul rilevamento, l'estrazione e lo sfruttamento del contenuto informativo dei dati saranno i punti di valore fondamentali di questo cambiamento di paradigma, spostando l'attenzione oltre i dati "grezzi". L'ottimizzazione dei processi automatizzati e strutturati consente un abbattimento dei tempi di elaborazione e reazione, permettendo ai sistemi di rispondere quasi in tempo reale, costituendo nuovi task per migliorare le acquisizioni EO, allo scopo di rispondere alle nuove esigenze rilevate. **SpacEdge™** offre una soluzione integrata (HW/SW *framework)* per il software di volo (FSW), potenziato dall'intelligenza artificiale (**AI**) e progettato per rivoluzionare il mercato dell'osservazione terrestre (EO) tramite un nuovo concetto di elaborazione dati dei *payload*. Integrato con il ***core Flight System*** (cFS) della **NASA**, SpacEdge™ è in grado di adattarsi a costellazioni già operative, come ponte tra costellazioni di sistemi differenti e come segmento terrestre e spaziale autonomo, in accordo a specifiche esigenze dell'operatore richiedente. Il framework offre un'infrastruttura *onboard* capace di eseguire flussi di lavoro complessi tramite la composizione di funzioni basilari in una struttura a grafi. Fornisce agli utenti un ambiente di sviluppo integrato (IDE) semplificato con un editor per comporre grafi e generare, validare a terra e distribuire in orbita il codice risultante per l'esecuzione a bordo. Spacedge™ consente agli utenti dei vari settori (EO, AI, FSW) di sviluppare e testare soluzioni pronte per il volo con un minimo sforzo, migliorando progressivamente l'implementazione anche senza competenze avanzate di programmazione. L'architettura *software* a bordo, grazie alla modularità del cFS, consente l'interconnessione delle tecnologie costituenti di SpacEdge™ e la gestione dei dati, trasformando i nodi dei *payload* da semplici ricevitori di comandi in nodi attivi capaci di richiedere dati e orchestrare operazioni complesse. Questa modularità permette di caricare ed eseguire applicazioni classiche o basate su reti neurali per l'elaborazione dati EO, senza interferire con altre applicazioni. SpacEdge™ offre così un continuum di elaborazione dati potenziato dall'AI, fornendo risorse in orbita per trasformare i dati grezzi in conoscenza applicabile. Il *layer* della sicurezza delle comunicazioni, offre l'opportunità di gestire sia da un punto di vista hardware che da un punto di vita software, l'integrità delle trasmissioni bordo-bordo, bordo terra, per mezzo della piena adattabilità a sistemi standardizzati o proprietari. L'impiego di sistemi **DLT** (*Distributed Ledgers Technology*) per il protocollo delle trasmissioni delinea un impiego mirato ed ottimizzato della tecnologia ***blockchain*** per assicurare il traffico delle comunicazioni in maniera rapida e sicura. Un esempio di sfruttamento di SpacEdge™ è il monitoraggio satellitare (EO) globale di eventi di rilievo, come una attività cinetica su un'area di interesse (strike) o lo spostamento di mezzi da combattimento (fig. 1). L'osservazione persistente di sensori a grande scala (GSD 20-250 mt.), stabile, giornaliera e a diversi orari, può autonomamente attivare una elaborazione *onboard* che determini, per mezzo degli algoritmi già disponibili e testati, una anomalia sull'area. L'esito dell'elaborazione, è comunicato alla stazione a terra in *near real time* (NRT), tra pochi secondi e meno di 3 minuti, per mezzo dei sistemi di *publishing* o *messaging* e costituisce elemento di *tasking* autonomo ad un ulteriore sensore di altra costellazione (non solo nello spettro *imaging*) con maggiore risoluzione spaziale o ad un insieme di sensori terrestri complementari. Una costellazione proprietaria ad alta risoluzione, grazie all'AI addestrata allo scopo, può iniziare rapidamente i processi di segmentazione e/o riconoscimento automatico dell'evento di interesse, soddisfacendo precisi requisiti informativi, precedentemente forniti ai sistemi di bordo grazie all'interfaccia web di comunicazione. Grazie all'interconnessione satellitare gestita da SpacEdge™, l'esito dell'elaborazione *onboard* e i dati elaborati sono tempestivamente inviati all'utente finale (***Analytics***) per le necessarie valutazioni.

La nuova serie di tecnologie fondate su capacità sempre maggiori di *Blockchain*, *Deep Learning* e AI, unitamente all'innovazione introdotta dai nuovi payload (*CubeSat*) sempre più performanti, apre lo spazio a nuove definizioni, a dimensioni che superano i limiti precedentemente posti. I flussi di lavoro così implementati danno origine ad un nuovo termine: ***SpaceStream. Lo SpaceStream è*** un flusso di lavoro che elabora i dati dove è più conveniente, e "SpacEdge™" è la sua spina dorsale: un nuovo ecosistema per cogliere le opportunità che lo **spazio** offre.

WIRELESS TECHNOLOGY MADE IN ITALY: INNOVAZIONE E QUALITÀ DA OLTRE 25 ANNI

POLOMARCONI.IT

La nostra eccellenza nel settore delle telecomunicazioni
Da oltre venticinque anni, POLOMARCONI.IT S.p.A. rappresenta un punto di riferimento nel mercato internazionale delle comunicazioni wireless, sia civili che militari. Con una solida esperienza nella progettazione, produzione e vendita di componenti per apparecchiature radio, l'azienda italiana ha saputo conquistare una posizione di leadership grazie a un mix vincente di cultura finanziaria, controllo dei costi di gestione e innovazione tecnologica.
Un portafoglio prodotti diversificato e all'avanguardia
POLOMARCONI.IT offre una gamma completa di soluzioni per diverse applicazioni, tra cui:

- ANTENNE: Progettazione e produzione di antenne per una vasta gamma di utilizzi, assicurando sempre alte prestazioni e affidabilità.
- FILTRI: Sviluppo di filtri per migliorare la qualità del segnale e ridurre le interferenze, indispensabili in ambienti complessi.
- SISTEMI DI COMBINAZIONE: Soluzioni avanzate per la gestione e la combinazione di segnali radio in diverse applicazioni.

Settori di applicazione
L'azienda si distingue per la sua capacità di operare in diversi settori, rispondendo alle esigenze specifiche di ciascuno:

- LAND & NAVAL: Le antenne e i filtri per questo mercato garantiscono i più alti livelli di prestazioni RF per tutte le comunicazioni tattiche. I prodotti di POLOMARCONI.IT garantiscono le comunicazioni più affidabili tra basi militari e offshore, tra navi, truppe di terra e altri veicoli militari impegnati sul campo;
- ATC: Ground-to-Air Communications: Antenne, filtri e combinatori per sistemi di comunicazione terra-bordo-terra utilizzati per il controllo del traffico aereo, in ambito civile e militare;
- PMR "Private Mobile Radio": Antenne e filtri per reti radiomobili DMR e TETRA per destinati ai servizi di emergenza;
- TRANSPORT: Grazie a un'ampia gamma di antenne e filtri, è possibile soddisfare tutte le esigenze dei sistemi di bordo, DMR, TETRA, GSM-R (VOCE/DATI), ETCS, ERTMS, M2M, PIS, REMOTE CONTROL, EVENT RECORDER, INTERNET ON BOARD, INFOTAIMENT.

Un modello di successo basato su solide fondamenta
Il successo di POLOMARCONI.IT si basa su due pilastri fondamentali: la cultura finanziaria e il controllo dei costi di gestione. Questi elementi permettono all'azienda di mantenere un'elevata competitività sul mercato, investendo continuamente in ricerca e sviluppo per anticipare le tendenze e le esigenze future del settore delle telecomunicazioni.

Innovazione e proprietà intellettuale: un asset strategico
POLOMARCONI.IT vanta una serie di marchi e brevetti che rappresentano un vero e proprio asset economico-finanziario. La protezione della proprietà intellettuale è considerata un elemento chiave per sostenere la crescita e l'innovazione continua.

Know-how Made in Italy e certificazioni
Il know-how dell'azienda è interamente Made in Italy, un valore aggiunto che si riflette nella qualità dei prodotti e nelle soluzioni offerte. L'azienda è inoltre certificata e in possesso di tutte le licenze necessarie per operare nei diversi mercati di riferimento.

Un futuro di crescita e innovazione
Guardando al futuro, POLOMARCONI.IT continua a investire in ricerca e sviluppo, con particolare attenzione alle tecnologie emergenti nel settore delle telecomunicazioni.
In conclusione, POLOMARCONI.IT S.p.A. è un esempio di come la combinazione di tradizione, innovazione e gestione oculata possa portare a successi duraturi e a una posizione di leadership nel mercato globale delle telecomunicazioni.

POLOMARCONI.IT: Un Omaggio a Guglielmo Marconi
Nel celebrare il 150° anniversario della nascita di Guglielmo Marconi, POLOMARCONI.IT SpA**, con il proprio marchio registrato in tutto il mondo**, si sente particolarmente legata a questa figura storica. La nostra azienda, con il suo nome che rende omaggio al grande inventore, si impegna a portare avanti la sua eredità attraverso l'innovazione continua nel campo delle comunicazioni wireless.
Il nostro lavoro nella progettazione, produzione e vendita di componenti per apparecchiature radio, come antenne, filtri e sistemi di combinazione, è profondamente ispirato dalle scoperte di Marconi. Crediamo fermamente che la dedizione alla ricerca e allo sviluppo, insieme a una solida cultura finanziaria e al controllo dei costi, siano la chiave per mantenere l'eccellenza e la competitività nel mercato globale.

Un Futuro Basato su Innovazione e Tradizione

Mentre celebriamo questo importante anniversario, guardiamo al futuro con ottimismo e determinazione. La nostra missione è continuare a esplorare nuove tecnologie e soluzioni che possano migliorare le comunicazioni globali, mantenendo sempre vivi i valori e l'eredità di Guglielmo Marconi.

Siamo convinti che l'innovazione debba andare di pari passo con il rispetto per la tradizione e la storia. Per questo motivo, POLOMARCONI.IT si impegna a mantenere vivo lo spirito pionieristico di Marconi, esplorando nuove frontiere e cercando sempre nuove sfide da affrontare.

Conclusione

Il 150° anniversario della nascita di Guglielmo Marconi è un momento di grande importanza per riflettere sull'impatto duraturo delle sue scoperte e sull'importanza di continuare a innovare nel campo delle telecomunicazioni. POLOMARCONI.IT S.p.A. è orgogliosa di fare parte di questa eredità, contribuendo con passione e dedizione al progresso delle comunicazioni wireless, in Italia e nel mondo.

In onore di Guglielmo Marconi, continueremo a lavorare con l'obiettivo di raggiungere nuove vette di eccellenza tecnologica, consapevoli del fatto che ogni nostra innovazione è un tributo al suo genio e alla sua visione.

PURE STORAGE PER L'AI: MASSIMA EFFICIENZA E AFFIDABILITÀ

Soluzioni avanzate per l'AI enterprise

PURE STORAGE

L'intelligenza artificiale (AI) sta ridefinendo il modo in cui le aziende operano e innovano. In questo contesto, Pure Storage® si distingue come leader nel fornire soluzioni avanzate di data storage che accelerano l'adozione dell'AI enterprise. Grazie alla collaborazione strategica con NVIDIA, Pure Storage ha sviluppato una serie di nuove reference architecture convalidate, pronte per l'implementazione di casi d'uso basati sull'AI generativa.

Le soluzioni di Pure Storage rispondono alla crescente domanda di infrastrutture AI efficienti e performanti, fornendo un framework robusto per gestire i requisiti di dati e calcolo ad alte prestazioni. Questo è particolarmente importante per settori come la difesa, dove l'innovazione tecnologica è cruciale. Un esempio significativo è rappresentato dalla trasformazione digitale dell'esercito britannico, che ha adottato tecnologie avanzate per migliorare operatività e capacità decisionale. L'integrazione dell'AI è fondamentale per consentire alle forze armate di prendere decisioni più rapidamente dei loro avversari, ambito in cui le soluzioni di Pure Storage possono fare una notevole differenza.

Pure Storage e NVIDIA

La sinergia tra Pure Storage e NVIDIA crea una potenza innovativa nel panorama dell'AI enterprise. Le tecnologie di NVIDIA, leader nel campo delle GPU e delle piattaforme AI, si integrano perfettamente con l'infrastruttura di Pure Storage, offrendo soluzioni che superano la somma delle loro parti. Questa partnership consente alle aziende di beneficiare di un'infrastruttura ottimizzata, capace di gestire carichi di lavoro AI complessi con efficienza e affidabilità. Mike Leone, Principal Analyst di ESG, afferma: "Le reference architecture convalidate da NVIDIA e le proof-of-concept annunciati da Pure Storage forniscono alle aziende di ogni settore una scorciatoia verso il successo nell'AI. Anziché dover investire tempo e risorse nel creare un'architettura AI da zero, i collaudati framework di Pure non solo riducono i rischi di costosi ritardi nei progetti, ma garantiscono anche un ROI elevato per le spese richieste dai team AI come le GPU."

Pure Storage ha riconosciuto subito la crescente richiesta di AI, proponendo una piattaforma efficiente, affidabile e ad alte prestazioni per i deployment AI più avanzati. Le reference architecture convalidate e le proof-of-concept di Pure promuovono l'innovazione AI, fornendo alle aziende gli strumenti necessari per aprire nuove possibilità e ottenere risultati trasformativi. L'infrastruttura dati semplice e robusta di Pure Storage, combinata con le capacità di calcolo avanzato di NVIDIA, crea soluzioni complete per affrontare le sfide dell'AI, della data analytics e del computing avanzato.

Caratteristiche Principali

- Pipeline Retrieval Augmented Generation (RAG) per l'inferenza AI: Pure Storage ha sviluppato una pipeline RAG che sfrutta i microservizi NVIDIA NeMo Retriever e le GPU NVIDIA, abbinati allo storage enterprise all-flash di Pure Storage. Questa soluzione migliora la precisione, l'attualità e la rilevanza delle funzionalità di inferenza per i Large Language Model (LLM), accelerando il time-to-insight delle aziende che utilizzano i propri dati interni per l'addestramento dell'AI.
- Reference architecture certificata NVIDIA OVX Server Storage: Pure Storage ha ottenuto la convalida OVX Server Storage, offrendo architetture storage flessibili convalidate rispetto a importanti benchmark. Questa soluzione fornisce solide fondamenta infrastrutturali per soluzioni AI ottimizzate in termini di costi e prestazioni, affiancandosi alla certificazione ottenuta su NVIDIA DGX BasePOD.
- Sviluppo di RAG verticali: Pure Storage sta creando specifiche RAG dedicate in collaborazione con NVIDIA per accelerare l'adozione dell'AI in settori verticali come i servizi finanziari, la sanità e la pubblica amministrazione. Queste soluzioni permettono di ottenere insight più rapidi e precisi, migliorando l'efficienza operativa.

L'adozione dell'AI enterprise è una sfida complessa che richiede soluzioni innovative e partnership strategiche. Pure Storage, in collaborazione con NVIDIA, offre alle aziende gli strumenti necessari per superare queste sfide e ottenere risultati trasformativi. La loro combinazione di infrastruttura storage avanzata e competenze AI rappresenta un punto di svolta per le aziende che cercano di integrare l'AI nelle loro operazioni, garantendo efficienza, affidabilità e prestazioni superiori.

RIVOLUZIONE CLOUD-NATIVE NELLA DIFESA: SCALABILITÀ E INNOVAZIONE

Sicurezza delle applicazioni mission-critical

PURE STORAGE

Nel panorama tecnologico odierno, l'adozione di piattaforme cloud-native sta diventando sempre più diffusa per accelerare il delivery delle applicazioni business-critical. Le aziende stanno spostando le loro applicazioni all'interno di container per rendere più rapido e scalabile il deployment. Tuttavia, esiste ancora un significativo impegno verso le applicazioni tradizionali residenti in VM, che richiedono un supporto continuo. Gestire entrambe le piattaforme è complesso e costoso, spesso richiedendo la riarchitettura delle applicazioni VM per renderle compatibili con i framework moderni. Secondo un recente sondaggio, l'81% degli stakeholder nel data management prevede di modernizzare o migrare i workload VM verso ambienti cloud-native, principalmente per la semplicità operativa.

In un contesto caratterizzato da minacce in rapida evoluzione e da una crescente complessità nelle operazioni di difesa, l'agilità e la sicurezza dei dati diventano priorità assolute. Portworx by Pure Storage si propone come una soluzione strategica, offrendo una piattaforma completa per i servizi dati Kubernetes, rispondendo efficacemente a queste esigenze nel settore della difesa.

La Soluzione Portworx: Caratteristiche e Vantaggi

La piattaforma Portworx fornisce storage persistente, protezione dei dati, disaster recovery, sicurezza dei dati, migrazioni cross-cloud e gestione automatizzata della capacità per applicazioni basate su Kubernetes. Queste funzionalità sono cruciali per le organizzazioni di difesa che necessitano di sistemi altamente resilienti e in grado di adattarsi rapidamente a scenari operativi in continua evoluzione.

- Storage persistente: Portworx garantisce che i dati delle applicazioni Kubernetes siano sempre disponibili e resistenti a qualsiasi tipo di guasto.
- Protezione dei dati e Disaster Recovery: Offre soluzioni robuste per la protezione dei dati e il ripristino in caso di disastro, assicurando che i dati critici siano sempre al sicuro.
- Sicurezza dei dati: Implementa avanzate misure di sicurezza per proteggere i dati sensibili da minacce esterne, come attacchi ransomware.

- Migrazioni Cross-Cloud: Facilita il trasferimento delle applicazioni e dei dati tra diversi ambienti cloud, migliorando la flessibilità e l'efficienza operativa.
- Gestione automatica della capacità: Ottimizza l'uso delle risorse storage in modo automatizzato, riducendo i costi e migliorando le prestazioni.

Collaborazioni Strategiche

L'integrazione con partner strategici come AWS, Red Hat, IBM e MongoDB amplifica ulteriormente il valore di Portworx, permettendo alle aziende di sfruttare al meglio le loro infrastrutture cloud e on-premise. La collaborazione con questi partner evidenzia la versatilità e l'adattabilità di Portworx a vari ecosistemi tecnologici, rendendolo una soluzione ideale per le aziende che cercano di ottimizzare la gestione dei dati e delle applicazioni.

L'Impatto nel Settore della Difesa

L'adozione di Portworx consente di superare le sfide legate alla velocità di mercato senza compromettere le prestazioni, la sicurezza, la scalabilità e la protezione dei dati. La capacità di Portworx di supportare ambienti Kubernetes in modo sicuro e scalabile facilita la gestione dei carichi di lavoro critici e la protezione dei dati sensibili, offrendo una risposta concreta alle crescenti minacce di sicurezza, come gli attacchi ransomware.

L'integrazione di Portworx nel settore della difesa rappresenta quindi un passo avanti significativo verso la realizzazione di infrastrutture IT agili, sicure e pronte a rispondere efficacemente alle esigenze operative e strategiche.

Conclusione

Portworx rappresenta un passo avanti significativo verso infrastrutture IT agili e sicure, supportando le esigenze operative e strategiche delle organizzazioni modernizzate. Con un focus crescente sull'innovazione e sulla sicurezza dei dati, Portworx si conferma come un partner ideale per le organizzazioni che cercano di mantenere un vantaggio competitivo in un ambiente IT sempre più complesso e dinamico.

TRASFORMARE LA SICUREZZA NELLA SANITÀ: IL JOURNEY DI ARIA CON RUBRIK

RUBRIK

Sfide:

- Oltre 40 istituzioni sanitarie che necessitano di una solida protezione dei dati;
- Il settore sanitario è sempre più un target degli attacchiransomware;
- Esigenza critica di un rapido ripristino operativo e di conformità normativa.

Risultati:

- 5 PB di dati resilienti alle minacce informatiche;
- 10 milioni di dati sensibili dei cittadini protetti e messi in sicurezza;
- 15 istituzioni sanitarie protette con Rubrik Security Cloud in < 3 mesi.

Prodotti presentati:

- Enterprise Edition.

La missione di ARIA S.p.A è gestire e proteggere i dati sanitari critici di 10 milioni di cittadini e oltre 40 istituzioni sanitarie a Milano, Italia. Le organizzazioni sanitarie affrontano attacchi costanti e qualsiasi interruzione può influire direttamente su chi cerca cure critiche. Per affrontare questa sfida, ARIA ha scelto Rubrik Enterprise Edition per una completa risoluzione del ransomware per proteggere e gestire questi ospedali. Con una velocità di implementazione impressionante di soli tre mesi, hanno già implementato Rubrik in 15 ospedali e sono sulla buona strada per distribuire EE in oltre 30 entro la fine del 2024.

La Regione Lombardia, cuore pulsante dell'economia italiana, ha la grande responsabilità di mantenere al sicuro i dati sanitari sensibili di oltre 10 milioni di cittadini. ARIA S.p.A. deve infatti proteggere e gestire i servizi di informazione, comunicazione e tecnologia relativi ai dati governativi e sanitari della regione.
Responsabile per le attività di oltre 40 istituzioni sanitarie, ARIA si è trovata al centro di uno scenario di Cyber Security in rapida evoluzione. La forte crescita degli attacchi ransomware, in particolare quelli rivolti al settore sanitario, ha aumentato i rischi per le attività di ARIA e per il benessere dei cittadini serviti dall'azienda.

Scegliere le capacità di resilienza informatica all'avanguardia di Rubrik

Preso atto di quanto fosse rischiosa la situazione, ARIA ha avviato una ricerca approfondita di un partner affidabile e in grado di rafforzare le sue difese contro gli attacchi informatici. Al termine di un rigoroso processo di selezione, Rubrik si è rivelato il miglior partner possibile, grazie a una suite completa di soluzioni su misura per gli specifici requisiti di ARIA.

Rafforzare un polo sanitario regionale

La partnership con ARIA ha portato risultati notevoli, consolidando la posizione di Rubrik come azienda in prima linea nella sicurezza dei dati sanitari. ARIA è stata la prima amministrazione pubblica italiana ad adottare una soluzione così completa, stabilendo un precedente sulla tutela dei dati sensibili dei cittadini ad un livello senza precedenti. Il continuo impegno di ARIA per la sicurezza dei dati, testimoniato dalla protezione di oltre 5 PB di dati in rapida crescita, è valso all'azienda il prestigioso Cyber Resilience Award di Rubrik – il Transformer – per le notevoli attività di trasformazione dimostrate dall'azienda.

Rubrik (NYSE: RBRK) ha la missione di proteggere i dati del mondo. Con Zero Trust Data Security™, aiutiamo le organizzazioni a raggiungere la resilienza aziendale contro gli attacchi informatici, gli insider malevoli e le interruzioni operative. Rubrik Security Cloud, alimentato dall'apprendimento automatico, protegge i dati nelle applicazioni aziendali, cloud e SaaS. Aiutiamo le organizzazioni a mantenere l'integrità dei dati, garantire la disponibilità dei dati che resiste a condizioni avverse, monitorare continuamente i rischi e le minacce ai dati e ripristinare le attività con i loro dati quando l'infrastruttura viene attaccata.
For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

LA COMPRENSIONE E L'INGANNO: IL RUOLO DELLA SOCIAL NETWORK ANALYSIS NELLO SVILUPPO DEL PENSIERO (A)CRITICO

SISTEMI & AUTOMAZIONE

Nel mondo iperconnesso di oggi, definito "Infosfera" dal filosofo Luciano Floridi, siamo costantemente bersagliati da informazioni, vere e false, provenienti da molteplici fonti eterogenee. In uno scenario in continuo mutamento, la grande sfida che si presenta – da un punto di vista sociale, psicologico, etico, educativo e democratico – è rappresentata dalla capacità di selezionare le informazioni rilevanti che ci avvicinano alla realtà, sottraendoci alle manipolazioni a cui siamo continuamente esposti e che ci rendono particolarmente vulnerabili. Lo sviluppo di un pensiero critico e un uso responsabile delle risorse informative disponibili, sono oggi competenze sempre più necessarie e cruciali. In questo scenario, le tecniche della ***Social Network Analysis*** (**SNA**) offrono una prospettiva unica per interpretare e valutare l'informazione come essenza, e la sua conseguente trasformazione in conoscenza utile (nonché *vera*).

La *Social Network Analysis*: Uno strumento fondamentale

La Social Network Analysis è un approccio metodologico che studia le strutture sociali attraverso l'uso di reti e grafici, consentendo la mappatura e la misurazione delle relazioni e dei flussi esistenti tra gruppi eterogenei di entità. L'approccio è particolarmente utile per **esaminare e comprendere più facilmente le relazioni complesse e le interdipendenze** presenti **in sistemi vasti e interdipendenti, come le società moderne,** mediante il calcolo effettuato attraverso delle metriche matematiche. Questi parametri costituiscono strumenti analitici essenziali nel coadiuvare la mente umana nella lotta al bias, favorendo una visione coerente con la realtà, anche di eventi altamente complessi (scenari geopolitici multilaterali, campagne di disinformazione, interdipendenze infrastrutturali nelle aree di conflitto territoriale).

Mente Umana e *Critical Thinking (Pensiero Critico)*

Il cervello umano è un organo complesso e potente, sostanzialmente ancora ignoto, capace di elaborare informazioni, fare inferenze, generare soluzioni e prendere decisioni. Tuttavia, è notoriamente soggetto e vittima di bias cognitivi e influenze sociali. Lo sviluppo dello spirito critico è cruciale per navigare attraverso il mare di informazioni e disinformazioni che ci circondano. In questo contesto, la citazione attribuita a Voltaire (oggi fortemente rivendicata in 'The Friends of Voltaire' di Evelyn Beatrice Hall), "Non condivido le tue idee, ma per le tue idee morirei", assume un significato profondo. Essa rappresenta il culmine dello spirito critico, dove il rispetto per le opinioni altrui e la ricerca della verità prevalgono sugli individualismi e le divisioni rendendo la collettiva più resiliente.
Valutare criticamente le informazioni usando strumenti come la SNA per distinguere fatti, opinioni e manipolazioni; rispettare la diversità di pensiero, accettando che opinioni diverse possano arricchire il proprio punto di vista; e sfidare le proprie convinzioni, permettono una analisi chiara ed una previsione più affidabile (obiettivo e cardine del processo di Intelligence).

Comprendere per Decidere, Combattendo l'Inganno

L'applicazione della Social Network Analysis, con i tool S&A POLARIS© e STEED© permettono di mappare e analizzare le dinamiche delle informazioni nelle reti sociali, rendendo visibili pattern nascosti. Questa tecnologia – discostandosi nel calcolo dal giudizio umano – diviene quindi cruciale per esaminare un pensiero critico in diverse aree: aiuta a identificare fonti affidabili, riconoscere bias informativi e determinare l'influenza relativa dei diversi nodi. La SNA consente di individuare nodi centrali e influenti, rivelare fonti di potenziali inganni, bilanciare le informazioni ricevute riconoscendo i bias, e valutare l'impatto e l'affidabilità delle informazioni diffuse da nodi influenti.

S&A POLARIS©, tramite la SNA, è quindi uno strumento potente per comprendere e rappresentare l'invisibile nell'infosfera, essenziale in un'epoca in cui verità e inganno si mescolano facilmente e frequentemente. Sviluppare uno spirito critico attraverso la SNA arricchisce la nostra capacità di discernimento e potenzia la nostra abilità decisionale, garantendo scelte informate e aderenti alla realtà. Governare lo spirito critico, come intuì Voltaire, permette di rispettare e difendere le idee altrui e quelle più giuste per tutti, creando una società consapevole e capace di evolvere. Tuttavia, la SNA deve essere integrata con la Scienza della Cognizione per essere veramente efficace. Questa integrazione è il campo di applicazione portato avanti dalla Sistemi & Automazione S.p.A. con il prodotto S&A GUIDE©.

Conclusioni Resilienza alla Guerra Cognitiva

In una società sempre più digitale e interconnessa, cresce l'incertezza e la vulnerabilità, con una crisi di fiducia nelle istituzioni e nei media. La guerra cognitiva sfrutta queste debolezze umane, amplifica le capacità di attacchi Cyber e interviene in un conflitto potentemente.

Senza il confronto ed un riscontro, non possiamo definire la nostra realtà, sottolineando l'importanza della fiducia e della comunicazione efficace per contrastare la manipolazione cognitiva. La disinformazione è una delle principali armi nella guerra cognitiva.

Identificare prontamente e confutare la disinformazione con informazioni accurate è fondamentale, soprattutto in ambito Cyber, così come promuovere la verifica delle fonti. Il supporto di strumenti come la SNA, costruita con il confronto e analisi su più riscontri, insieme con una leadership empatica sono chiavi per una società più resiliente e meno vulnerabile.

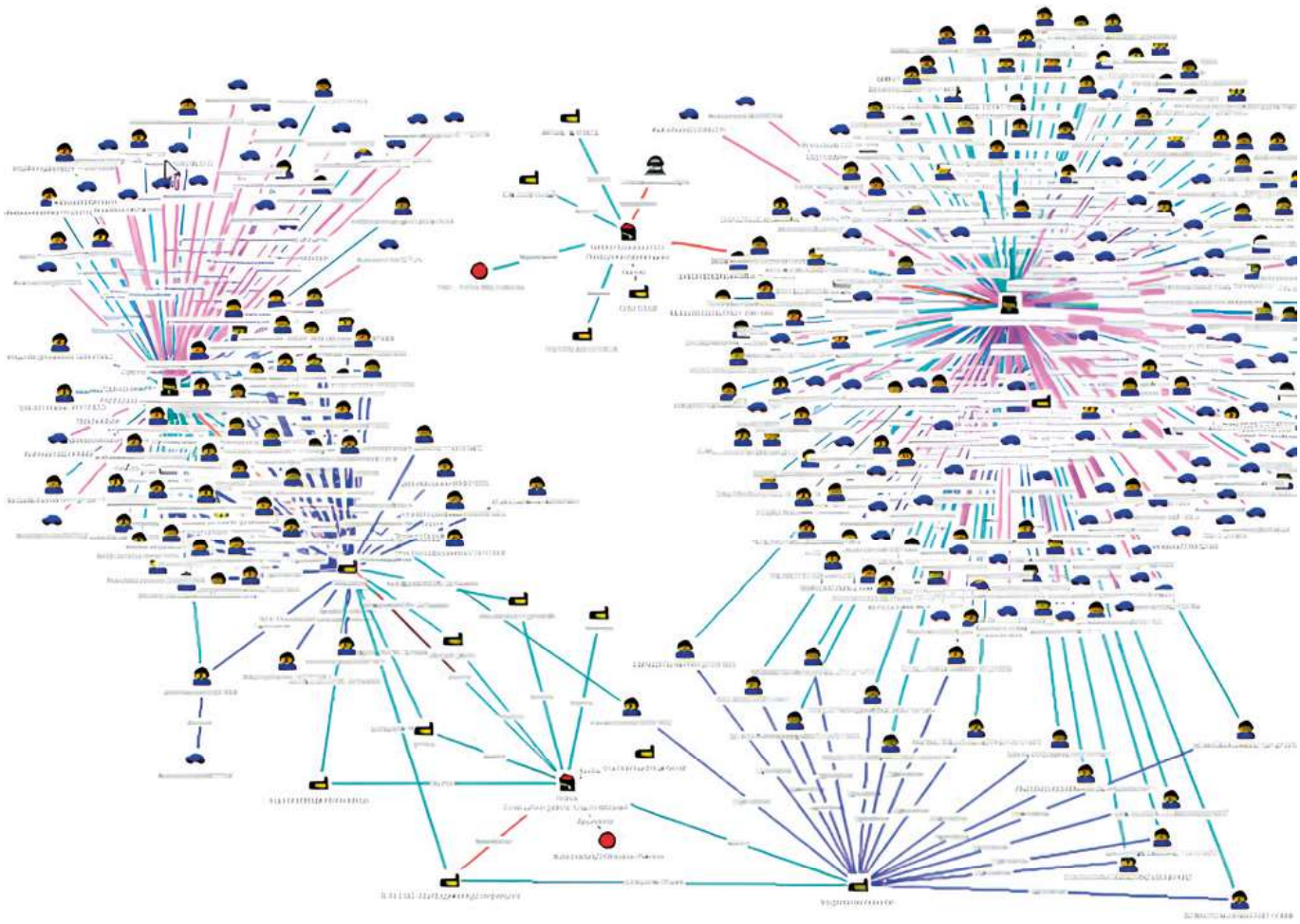


Figura 1. Association Chart con S&A POLARIS ©

STORMSHIELD ENDPOINT SECURITY EVOLUTION

La soluzione EDR nata da un progetto militare

STORMSHIELD

Nato dietro specifica commissione per un **progetto militare internazionale** che doveva rispettare stringenti requisiti e necessità, come quella di dover essere estremamente efficace anche in ambienti air-gap, **completamente trasparente per gli utenti finali, Stormshield Endpoint Security Evolution è la soluzione EDR multi-layer affidabile che, prima di tutto, protegge l'azienda.** L'innovativa tecnologia signatureless blocca proattivamente le minacce più critiche e le azioni di remediation sostenibili contribuiscono ad aumentare il livello di sicurezza dando al team di sicurezza la tranquillità e la cyber-serenità sulla sicurezza dell'infrastruttura.

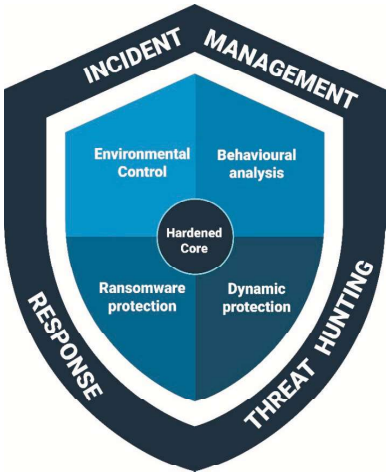
La soluzione EDR che protegge prima di tutto l'azienda

Con il tema della sicurezza informatica ancora regolarmente sotto i riflettori, i criminali informatici cercano di raggiungere i loro obiettivi in modo furtivo. Questo obiettivo li porta ad adattare costantemente le loro tecniche di attacco. Sfruttano, così, le loro vaste conoscenze per sviluppare strumenti dannosi in grado di battere le soluzioni di Cyber Security presenti sulle postazioni di lavoro dei dipendenti.

Le soluzioni antivirus convenzionali e gli altri sistemi di rilevamento, in particolare quelli basati esclusivamente sulle firme, sembrano essere stati superati da tecniche complesse, come il hijacking di applicazioni legittime e l'escalation dei privilegi, oltre che da malware evasivi. Di conseguenza, le soluzioni che si concentrano sul rilevamento e sulla prevenzione degli attacchi noti stanno diventando insufficienti per affrontare questa nuova generazione di cyberattacchi sofisticati e sconosciuti.

Le organizzazioni che intendono proteggersi da questo tipo di attacchi informatici devono implementare soluzioni **EDR** (Endpoint Detection and Response) in grado di rilevarli e garantire una risposta efficiente. Oltre a questo rilevamento, devono anche essere in grado di bloccare gli attacchi cyber sofisticati e sconosciuti in modo proattivo, automatico e in tempo reale, per garantire una continuità aziendale il più possibile fluida. *Questo approccio proattivo risponde al problema che un analista informatico si pone quando gestisce un incidente di sicurezza*.

Immaginate come possa sentirsi non appena ha ricevuto un avviso dalla sua soluzione EDR mentre la sua infrastruttura è probabilmente a rischio. Sa che dovrà fare un enorme lavoro di analisi: **tutti gli eventi di sicurezza e gli indicatori di compromissione, correlare questi eventi e**



prendere la decisione giusta per bloccare l'attacco e rimediare all'incidente.

Tra l'altro, queste notifiche di incidenti sono all'origine dell'aumento della pressione sul team di sicurezza, che ha la responsabilità di gestirli. Si scatena una corsa contro il tempo per analizzare gli eventi, rintracciare l'origine, identificare gli endpoint colpiti e decidere prontamente la risposta da mettere in pratica. L'obiettivo è bloccare la diffusione del malware e limitare l'impatto sull'azienda.

La cronaca ci mostra che le organizzazioni criminali informatiche sono improbabili e troppo spesso vincitrici di questa corsa contro il tempo. Le risposte agli incidenti sono solitamente pertinenti e di grande aiuto per l'analista informatico, che però deve ancora controllare e verificare le informazioni prima di poterle gestire; questa perdita di tempo può nuocere quando si tratta delle minacce più critiche.

Stormshield Endpoint Security Evolution, a new generation of endpoint protection

La soluzione che prima di tutto protegge l'infrastruttura mira a risolvere questo problema. Grazie al suo approccio proattivo, il team di sicurezza sarà meno stressato perché saprà di essere al sicuro. Grazie alle sue innovative capacità di rilevamento, il team può vincere la corsa contro il tempo **bloccando le minacce più critiche in tempo reale**.

Queste funzionalità si basano su una **tecnologia signatureless** che riconosce le tecniche di attacco utilizzate dagli hacker per sfruttare le vulnerabilità degli endpoint. L'intelligenza incorporata nell'agente garantisce un processo **completamente autonomo** che ha dimostrato la sua efficacia contro i malware più sofisticati, compresi gli attacchi persistenti senza file.

Ad esempio, la protezione contro i ransomware avviene identificandone il loro comportamento anomalo. Vengono bloccati anche se sono sconosciuti alla comunità informatica. Stormshield Endpoint Security Evolution verifica innanzitutto l'esistenza di una politica di backup dei dati sulla

workstation e, se non esiste, forza un backup dei dati al giorno. Quindi rileva i comportamenti sospetti o i processi di crittografia dannosi e li blocca non appena individuati. Inoltre, la soluzione blocca i tipi più sofisticati di ransomware che tentano di eliminare i dati di backup. Grazie a queste funzionalità, **Stormshield Endpoint Security Evolution è in grado di rilevare e bloccare le minacce delle principali famiglie di ransomware**.

Incident management and sustainable remediation

In caso di attacco informatico, il team di sicurezza può gestire serenamente l'incidente, poiché le azioni dannose più critiche sono già state bloccate. Quindi, dopo aver ricevuto l'avviso via e-mail, un analista informatico inizia la sua analisi collegandosi alla console che mostra in una dashboard gli incidenti di sicurezza. Dopo aver selezionato l'evento, può raccogliere informazioni contestuali per analizzare le azioni che hanno portato all'allarme. Inoltre, grazie al grafico dell'attacco, l'analista informatico sarà in grado di condurre un processo di threat hunting per identificare tutti gli indicatori di compromissione legati all'attacco. Tali indicatori, come testo sospetto, informazioni di rete, hash, tecniche di aggiramento del rilevamento EDR e così via, sono continuamente generati dall'agente e corrispondono a tutti gli eventi che si sono verificati sulla macchina prima dell'attacco. Le informazioni dettagliate includono i tag MITRE ATT&CK, un modello comune che tenta di classificare sistematicamente il comportamento degli avversari e, quindi, aiuta a classificare gli eventi identificando la fase dell'attacco. Quest'analisi contestuale dell'attacco fornisce all'analista informatico informazioni dettagliate sul processo e lo aiuta a comprendere meglio la natura dell'attacco analizzando gli eventi precedenti. Una volta identificati gli eventi legati all'attacco, l'analista può avviare azioni di remediation per ciascuno di essi. A tal fine, **Stormshield Endpoint Security Evolution suggerisce anche le azioni più appropriate da eseguire**. In questo modo, possono essere avviate più rapidamente azioni di remediation predefinite o personalizzate e tornare a una situazione normale. Ad esempio, è possibile filtrare le connessioni di rete, isolare o ripulire la workstation. Infine, l'analista può concludere la sua indagine eseguendo una scansione all'interno della sua infrastruttura per verificare la presenza di uno degli indicatori di compromissione raccolti su altri computer. Le operazioni di scansione sono particolarmente efficaci contro le minacce latenti. Se individuate, si potranno avviare le stesse azioni di remediation eseguite in precedenza sulla prima workstation.

Una volta che la situazione sarà tornata alla normalità, potranno essere messe in atto alcune azioni di prevenzione. Questo permetterà di agire proattivamente ed eviterà di trovarsi ad affrontare sempre gli stessi incidenti di sicurezza. L'analista di sicurezza è in grado di aggiungere nuovi criteri di sicurezza tramite il pannello di controllo, aggiungendo nuove regole relative agli indicatori di compromissione scoperti durante la sua indagine. Bloccandoli, ha consegnato di fatto le minacce scoperte oggi alla storia aumentando il livello di sicurezza dell'azienda ed evitando che lo stesso incidente si ripeta in futuro**.**

Fully adaptative solution

La gestione dei criteri di sicurezza di Stormshield Endpoint Security Evolution offre ai team di sicurezza un elevato livello di granularità. Possono aggiornare i criteri di sicurezza predefiniti e adattare i livelli di rilevamento e risposta in base ai requisiti di sicurezza dell'azienda.

Inoltre, oltre all'aggiunta di regole che aiutano a effettuare una bonifica sostenibile e ad aumentare il livello di sicurezza, il team può organizzare le proprie policy in base al livello di criticità degli asset. **Questa organizzazione per gruppi di asset è molto utile durante le fasi di implementazione iniziale o di aggiornamento**. Il team di sicurezza può testare le nuove regole o la nuova versione del software su un piccolo gruppo di agenti, per evitare che eventuali errori di configurazione si diffondano interamente all'interno dell'azienda e creino probabili interruzioni.

Combinando i criteri di sicurezza con le funzionalità di controllo dei dispositivi, **la soluzione può adattare dinamicamente il livello di protezione all'ambiente**. Ad esempio, in caso di connessione Wi-Fi pubblica, Stormshield Endpoint Security Evolution è in grado di cambiare il contesto della policy e di adottare operazioni di sicurezza più robuste in questa situazione rischiosa di mobilità, garantendo così la protezione dei dispositivi mobili che possono creare un potenziale rischio per l'infrastruttura.

Le funzionalità di controllo dei dispositivi vanno oltre la connessione alla rete, offrendo un controllo completo sull'uso delle unità USB in azienda. Oltre a bloccare tali dispositivi, il team di sicurezza può anche limitarne l'uso alle sole unità decontaminate. Solo quelle approvate dalla soluzione possono essere connesse alle workstations.

A trusted solution

La solidità della soluzione è garanzia di fiducia e la fiducia è una questione chiave nelle soluzioni di Cyber Security. Stormshield Endpoint Security Evolution è stato riconosciuto attraverso processi di qualificazione e certificazione di sicurezza con le autorità europee competenti, come Producto Aprobado e Producto Cualificado dal CCN-LINCE e CSPN dall'autorità francese ANSSI.

ZEUS: LA PIATTAFORMA PER L'ASSESSMENT IN AMBITO CYBERSICUREZZA

TELECONSYS

L'evoluzione tecnologica ha portato numerosi vantaggi e progressi nella nostra vita quotidiana, ma **ha anche esteso la superficie di attacco IT**, cioè l'insieme dei sistemi esposti in una rete, i punti di ingresso e le vulnerabilità che potrebbero essere sfruttate da un potenziale attaccante**.**

Se in precedenza la rete aziendale veniva considerata il perimetro all'interno del quale tutto era sicuro e quindi autorizzato, con la diffusione dei servizi in cloud, del fenomeno BYOD (Bring Your Own Device) e del lavoro da remoto, spesso connettendosi a reti intrinsecamente insicure, il perimetro aziendale si è dissolto, l'obiettivo delle minacce è diventato l'utente e la superficie d'attacco è divenuta, virtualmente, infinita.

Per rispondere alle nuove minacce, l'Unione europea ha emanato la Direttiva Ue 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni (Direttiva NIS 2) che abroga la precedente Direttiva del 2016 e stabilisce importanti novità e adempimenti per i soggetti essenziali ed importanti.

La NIS2, estendendo l'ambito di applicazione delle norme in materia di cybersicurezza a nuovi settori e entità, migliora ulteriormente la resilienza e le capacità di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'UE nel suo complesso.

In particolare, al **Considerando 89**, la Direttiva afferma che i soggetti essenziali e importanti dovrebbero adottare un'ampia gamma di pratiche di igiene informatica di base, come ad esempio i principi del modello **Zero Trust**.

LA PIATTAFORMA

Teleconsys, per supportare le organizzazioni nella compliance rispetto ai requisiti e agli obblighi introdotti dalla NIS2 e nel percorso di adozione del paradigma Zero Trust, ha sviluppato la piattaforma web ZEUS che digitalizza il processo di **valutazione della compliance e della postura di sicurezza** delle organizzazioni.

L'applicazione, costituita da due moduli semplici ed intuitivi, **guida l'utente step by step nell'esecuzione dell'assessment** e nella compilazione dei controlli, selezionati e studiati per verificare l'adozione di determinate misure di sicurezza, di strumenti tecnologici e di soluzioni di governance da parte della realtà esaminata.

Concluso l'assessment, è possibile **visualizzare graficamente** il livello di maturità rilevato e **confrontarlo** con eventuali assessment precedenti, con un livello target o con quello di ambiti similari per dimensione, settore, normative, ecc.

La piattaforma consente, inoltre, di generare una **roadmap degli interventi** sulla base delle priorità emerse e di effettuare **analisi di tipo what-if** sull'evoluzione della postura.

Attraverso ZEUS è possibile creare **template di assessment personalizzati** a seconda delle specificità e degli obiettivi dell'organizzazione.

IL MODULO ASSESSMENT NIS 2

Teleconsys, al fine di supportare gli enti e le organizzazioni interessate dall'adempimento degli obblighi previsti dalla Direttiva NIS2, ha elaborato un **framework** composto da una selezione di controlli di tipo **sia tecnico sia organizzativo**.

Tali controlli sono stati importati da standard, norme e framework internazionali di settore (es.: FNCS, CSF NIST 2.0, ISO 27001, ISO 31000, CIS, …) e organizzati in **9 contesti** volti a valutare il livello di compliance dell'organizzazione rispetto alla Direttiva.

Nello specifico, i contesti identificati nel framework derivano dai seguenti articoli della Direttiva:

- art. 20: governance;
- art. 21: misure di gestione dei rischi di cibersicurezza;
- art. 22: valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche;
- art. 23: obblighi di segnalazione;
- art. 30: notifica volontaria di informazioni pertinenti;
- art. 32: misure di vigilanza e di esecuzione relative a soggetti essenziali.

Figura 1. Modello NIS2

MODULO ASSESSMENT ZERO TRUST

Secondo il paradigma Zero Trust nessun utente può essere considerato affidabile a priori e ogni richiesta di accesso alle risorse deve essere verificata.

Teleconsys, ispirandosi allo **Zero Trust Maturity Model del CISA** e ai principi del NIST, **ha ideato un modello** costituito da **6 Pillar** e da **2 Capability**, trasversali e applicate a ciascun Pillar. A questi sono associati una serie di controlli il cui stato di implementazione, opportunamente pesato, permette di valutare il **livello di maturità** dell'organizzazione rispetto al modello ZT. Per la definizione degli algoritmi di valutazione, Teleconsys si è avvalsa del supporto scientifico dell'**Università Campus Bio-Medico di Roma** e del contributo di **CISO** di importanti realtà.

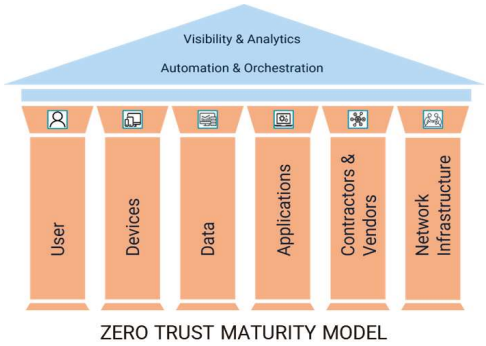


Figura 2. Zero Trust Maturity Model

ELEMENTI DISTINTIVI DELLA PIATTAFORMA

- Semplifica la **governance** della compliance alla Direttiva NIS2 e dell'adozione del modello Zero Trust dell'organizzazione;
- **Monitora** la **postura di sicurezza** in maniera continua e proattiva;
- **Supporta il processo decisionale** nella definizione e implementazione di strategie di sicurezza;
- **Rileva gli interventi prioritari**, assicurando proattivamente la sicurezza delle informazioni;
- Fornisce una **visibilità granulare** sui sistemi e le applicazioni di sicurezza dell'organizzazione;
- **Struttura gli assessment** riducendone i tempi di esecuzione;
- Sfrutta **algoritmi di AI** per le valutazioni;
- Può **notarizzare su un registro distribuito** i risultati;
- È un **prodotto "made in Italy" innovativo**, unico sul mercato.

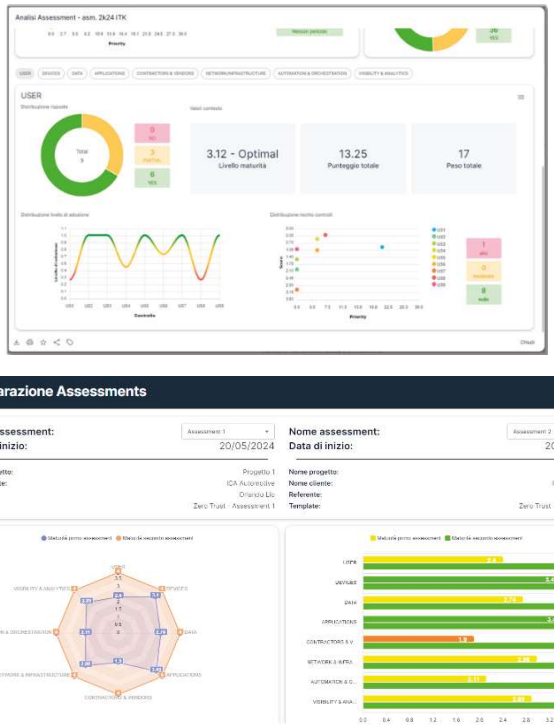


Figura 3. Piattaforma ZEUS

IL VALORE DEL REPORT GENERATO

- Dà una visione chiara (no Excel/Power Point) della compliance alla NIS2 e della postura di sicurezza rispetto al paradigma Zero Trust;
- È utile per la pianificazione degli interventi di remediation;
- È fondamentale ai decisori per giustificare il budget investimenti;
- Certifica la progressione dei miglioramenti nel tempo.

LA CONSULENZA

Teleconsys supporta i clienti nell'utilizzo della piattaforma ZEUS fornendo il servizio di consulenza che si avvale di professionisti certificati e specializzati su ciascun contesto di analisi. Il team guida il cliente nell'esecuzione dell'Assessment, la definizione del Remediation Plan sulla base del Gap identificato e per la strutturazione della Roadmap attuativa degli interventi sulla base delle priorità definite, seguendo lo schema di seguito illustrato.

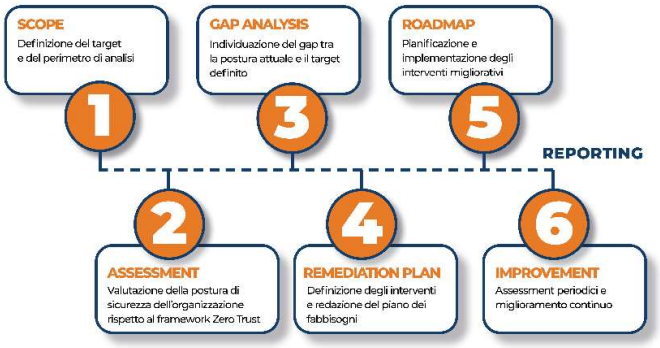


Figura 4. Servizio di consulenza

COMPANY PROFILE

Teleconsys S.p.A., PMI innovativa, è una **Digital Innovation Company** la cui missione è supportare le organizzazioni pubbliche e private nel loro viaggio di scoperta, adozione, trasformazione ed evoluzione digitale, facendo leva sull'innovazione aperta e sulla sostenibilità.

Il nostro **purpose** è quello di generare profitto offrendo i benefici di un'**innovazione etica**, sostenibile e condivisa ("sharing innovation"), per creare un impatto positivo sull'ambiente e la collettività. La digitalizzazione, se sostenibile ed inclusiva, può, infatti, migliorare la qualità della vita e **preservare il pianeta** per le generazioni future.

Per tale motivo, già dal 2021, Teleconsys redige il **Bilancio di Sostenibilità** e dal 2023 è entrata a far parte della **Fondazione per la sostenibilità digitale**.

Con oltre vent'anni di esperienza in settori ad alta intensità tecnologica e in costante trasformazione, siamo il **partner di grandi imprese e pubbliche amministrazioni** nel loro percorso verso la digitalizzazione.

Teleconsys è tra i soci del **Competence Center Cyber 4.0.**

SOLUZIONI CONNETTIVITÀ SATELLITARE FONIA E DATI, SICURE E RESILIENTI, IN AMBIENTI DI TIPO DUAL USE

TELESPAZIO

Telespazio lavora per avvicinare lo Spazio alla Terra a vantaggio di cittadini, istituzioni ed aziende, in settori che vanno dalla progettazione e sviluppo di sistemi spaziali, alla gestione dei servizi di lancio e controllo in orbita dei satelliti, dai servizi di osservazione della Terra, comunicazioni integrate, navigazione e localizzazione satellitare, fino ai programmi scientifici.

Grazie ad un approccio di open innovation, alla contaminazione fra i diversi domini operativi e alla grande e costante attenzione ai temi della sostenibilità ambientale, Telespazio opera già oggi in settori, che nei prossimi anni assumeranno sempre più rilevanza: dai servizi di comunicazione e posizionamento sulla Luna (**Moonlight**) alla gestione e il monitoraggio di satelliti e altri oggetti orbitanti (**Space Domain Awareness**), dalla creazione di avanzati servizi in orbita fino alla gestione via satellite di droni e veicoli unmanned.

In particolare, Telespazio si sta posizionando in alcuni mercati come l'**Advanced Air Mobility** (AAM), dove assumono un ruolo fondamentale la resilienza e la sicurezza delle comunicazioni.

Le soluzioni chiavi in mano di Telespazio rispondono al mercato dell'AAM per supportare l'agricoltura, l'ispezione e il monitoraggio di aree e infrastrutture e la consegna di merci (compresi materiali medici). Grazie al suo ruolo nel mercato dei servizi satellitari, Telespazio è in grado di garantire la comunicazione delle piattaforme digitali a terra e in volo. Inoltre, grazie allo sviluppo di piattaforme di comunicazione proprietarie (TPZ Air100) che permettono la comunicazione nel mondo dei veicoli unmanned in **BRLOS**/**BVLOS**, Telespazio apre scenari innovativi per determinare, insieme all'ente regolamentatore, le direttive per lo sviluppo di nuovi servizi.

Nell'ambito delle comunicazioni satellitari istituzionali, Telespazio partecipa con un ruolo strategico ai programmi governativi ed offre soluzioni innovative con applicazioni e servizi nel campo della protezione civile, della sicurezza e dell'e-government. Infine, i centri spaziali di Telespazio, tra cui Fucino e Scanzano, ospitano il segmento di terra di sistemi di telecomunicazioni satellitari gestiti dai più importanti operatori internazionali (ad esempio: **Inmarsat**, **Eutelsat**, **OneWeb**). L'obiettivo è quello di offrire servizi satellitari commerciali ed istituzionali garantendo un elevato livello di sicurezza e resilienza delle comunicazioni. L'elemento distintivo per utilizzare tali servizi da parte del mondo della difesa è la presenza, presso i teleporti di Telespazio, dell'integrazione con la rete in fibra ottica nazionale (**RIFON**).

Grazie agli accordi con Starlink ed Eutelsat, Telespazio si pone sul mercato come uno dei pochissimi operatori al mondo in grado di offrire servizi su costellazioni LEO (**Starlink** e **OneWeb**) e su costellazioni GEO di ultima generazione (**Intelsat Epic** e **Konnect VHTS**).

Telespazio si pone, quindi, come il partner ideale sia per missioni istituzionali di alto profilo, che per start up e aziende, che si affacciano attualmente al mondo New Space e che necessitano di un approccio service-oriented.

Nel momento storico attuale Telespazio sta supportando le Campagne Navali intorno al mondo, fornendo una connettività come provider di riferimento globale.

In particolare, nel campo delle comunicazioni militari satellitari (**Milsatcom**), Telespazio offre, avvalendosi anche della partecipazione al *programma della Difesa italiana* **SICRAL**, i servizi di telecomunicazioni alle forze armate nazionali e dei Paesi della **NATO.**

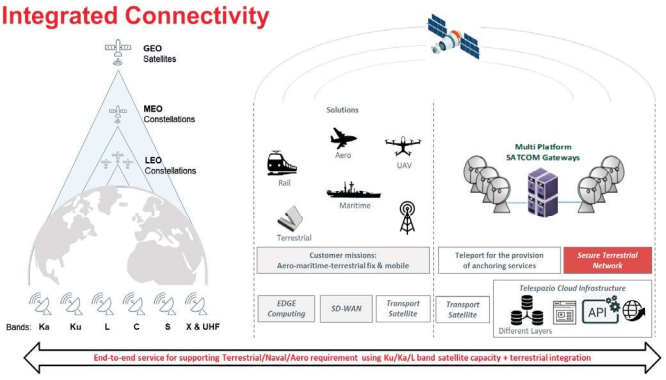
Telespazio inoltre può fornire servizi di connettività in ambito internazionale, in quanto coinvolta nei programmi Alliance Long Lines Activity (**ALLA**) e NATO Alliance Long Lines Activity (**NALLA**), per scopi NATO e di difesa nazionale, che vengono elaborati dalla NALLA stessa.

Gli esperti di Telespazio sono attivi 24 ore su 24, 7 giorni su 7, per controllare tutte le fasi della vita operativa dei satelliti: dalla LEOP (Launch and Early Orbit Phase) alla gestione degli stessi fino al deorbiting. Nel corso degli anni si è sviluppata una vasta esperienza nella gestione dei satelliti nelle diverse orbite (**LEO**, **MEO** e **GEO**).

COMUNICAZIONI IBRIDE: ANYWHERE, ANYTIME

TELESPAZIO

Per le nuove, ma già attuali, **reti di telecomunicazioni di tipo "ibrido"**, in cui è fondamentale l'integrazione di diverse tipologie di connettività (fibra ottica, 5G, 6G, Lte, WiMAX, Broadband Wireless Access, comunicazioni satellitari nelle orbite GEO, MEO, LEO), Telespazio sta studiando e sviluppando in modo innovativo anche sistemi, che integrano tecnologie come **QKD** (Quantum Key Distribution), in funzione del collegamento trattato, nell'ottica di garantire la sicurezza anche nei confronti dell'eventuale potere dei computer quantistici, che potrebbero scardinare gli attuali sistemi di sicurezza improntati verso chiavi di tipo pubblico o privato.
La tecnologia **QKI** (**Quantum Key Infrastructure**) sfrutta la combinazione di una condivisione di protocolli riservati e crittografia One-Time-Pad utilizzando chiavi di generazione quantistica e funge da strato indipendente dal protocollo e si integra nell'infrastruttura IT esistente.
I classici Alice e Bob non hanno le chiavi di cifratura, ma le possono ricostruire con i loro dispositivi tramite le informazioni in possesso delle **Quantum Certificate Authorities** (**QCAs**), perché il modello del QKI (Quantum Key Infrastructure) sfrutta la combinazione di chiavi generate quatisticamente, ossia applica lo «share degli stati entaglement», con tecniche One-Time-Pad, basandosi sulle teorie del calcolo delle probabilità, che è governata dai processi stocastici.
Quando Alice e Bob vogliono comunicare, i QCAs concedono loro tramite canali pubblici le informazioni necessarie per ricostruire una chiave privata. Ogni singolo QCA non ha accesso alla chiave privata e qualsiasi intercettatore, che raccoglie tutti i dati inviati dai QCAs verso Alice e Bob, non accede a nessuna informazione della chiave privata. Le serie casuali inviate dai QCAs possono essere tradotte in una chiave significativa solo combinando i dati con i dispositivi in possesso di Alice e Bob, utilizzando gli stessi QCAs. Quindi Alice e Bob condividono una chiave privata, che può essere utilizzata con un codice OTP per gestire comunicazioni sicure per il trasferimento dei dati. Successivamente, i dati possono essere permanentemente eliminati dagli QCAs oppure archiviati nelle memorie QCAs locali. Ipotizzando che un Hacker potrebbe accedere alle informazioni di dati crittografati con algoritmi commerciali standard, come RSA o AES256, con l'arrivo di un computer quantistico l'Hacker potrebbe sviluppare un nuovo algoritmo per decifrare tali dati. Poiché molti dati segreti devono essere mantenuti per più di cinque anni, questi dati sono già attualmente a rischio. Quindi una valida soluzione potrebbe essere la crittografia post-quantistica (**PQC**), che lavora con algoritmi per la distribuzione di chiavi quantistiche, basati su protocolli ***Quantum Key Distribution*** (**QKD**). In alternativa la tecnologia **PQC** è simile per natura, ma non uguale, alla corrente dei protocolli di crittografia standard, come RSA o AES256, e quindi tale tecnologia post -quantum si basa su problemi matematici, che sono ritenuti molto difficili da risolvere, anche per un computer quantistico.
Nel futuro ci potrebbe essere la necessità di progetti di ricerca scientifica in ambito di crittografia quantistica per possibili scenari applicativi: building istituzionali sicuri cablati in fibra, sale situazione su natanti di grandi dimensioni cablati in fibra per missioni speciali, smart display sui veicoli speciali oppure UAV con applicazioni di Intelligenza Artificiale per grandi moli di Dati (i.e. riconoscimento facciale), che vanno protetti con crittografia quantistica.
La sicurezza online di oggi si basa principalmente sull'infrastruttura a chiave pubblica (i.e. RSA oppure VPN). Il ***Pubblic Key Infrastructure*** (**PKI**) è un insieme di ruoli, politiche, hardware, software e procedure necessari per creare, gestire, distribuire, utilizzare, archiviare e revocare la certificazione digitale; quindi, si sta analizzando la cifratura dei dati, che viaggiano via Internet, anche con Satellite Communications, non di crypto, ossia della cifratura delle radio analogiche con tecniche binarie (0,1).
I progetti di ricerca principali di Telespazio anche in collaborazione con Thales Alenia Space Italia sono SAGA e QUID, inoltre Telespazio Iberica ha avviato un nuovo progetto sulla tecnologia QKD, integrando i segmenti terra e spazio, grazie ai fondi del PNRR, realizzando un sistema di validazione E2E per sistemi QKD, che include lo spazio ed il segmento terrestre.
Per il progetto di ricerca europeo **SAGA** la Fase B1X dell'ESA è da completare con il Concept of Operations di Telespazio ed il servizio di gestione delle chiavi.
Per il progetto di ricerca europeo **QUID,** Telespazio ha proposto due casi d'uso e relativi siti, uno a Roma ed un altro al Fucino come nodi sicuri.



COSTELLAZIONI SATELLITARI IBRIDE MULTI-ORBITA: NUOVE FRONTIERE PER LA DIFESA

Connessione sicura/resiliente per missioni militari

THALES ALENIA SPACE

M. Gargiulo, N. Lamorgese, R. D'Ascenzo, S. Wahib, P. Conforto, M. Petrone, A. Pisano

Gli scenari operativi di interesse militare richiedono la disponibilità di una varietà di informazioni ottenibili per mezzo di sistemi di comunicazione, monitoraggio e osservazione delle aree di intervento, utilizzando strumenti per la gestione dell'informazione di tipo multi-missione. Nel prossimo futuro gli scenari operativi saranno sempre più densamente popolati da una varietà di sensori, attuatori, sorgenti di informazione utilizzati per una molteplicità di applicazioni. La modalità di fruizione del servizio riguarda ad esempio applicazioni come controllo di confini, supporto alla logistica, assistenza al soldato e monitoraggio del suo stato di salute. Tali dispositivi di piccole dimensioni e con prestazioni a radio-frequenza (RF), appartenenti alla classe dei terminali personali, hanno la necessità di scambiare dati con centri di comando e controllo e sono dislocati nella maggior parte dei casi in aree remote, in teatri di battaglia, in aree marittime, dunque in aree in cui reti di comunicazioni terrestri non sono disponibili o non sono sotto il controllo nazionale.

D'altronde, emerge sempre più l'esigenza di stabilire comunicazioni senza vincoli in aree tattiche e di una connessione resiliente, flessibile e disponibile in ogni momento anche per gli scenari post-crisi, nei quali la rete terrestre potrebbe subire critici danneggiamenti. Infatti, un accesso dedicato alla rete satellitare renderebbe l'Amministrazione Difesa (AD) immune da attacchi mirati alle infrastrutture di telecomunicazione o da eventi catastrofici naturali che comprometterebbero differenti elementi della rete terrestre.

Tuttavia, anche in scenari ordinari (non crisi), le reti terrestri non sono in grado di assicurare l'accesso a un servizio di connettività affidabile e onnipresente e di raggiungere aree remote. Diventa quindi fondamentale l'esigenza di integrazione con una infrastruttura di comunicazione satellitare sotto il completo controllo nazionale per il soddisfacimento di diversi requisiti: alta velocità e bassa latenza nello scambio dati (adatta ai tipi di servizi *real-time* e *near real-time*), alta disponibilità, elevato *throughput*, accessibilità continua alla rete per diversi tipi di terminali (personali, mobili, fissi, trasportabili, ecc.), copertura su aree non altrimenti servite.

Figura 1. Futura costellazione multi-missione, ibrida e multi-orbita per applicazioni militari

Inoltre, il monitoraggio delle aree di intervento è effettuato attualmente collezionando immagini da satellite, con un intervallo di tempo necessario per l'acquisizione dell'informazione che dipende dai tempi di rivisita sulla stazione di terra. Le esigenze operative emergenti richiedono però che tale latenza sia la più bassa possibile e tale requisito può essere soddisfatto tramite sistemi di *data relay* per i satelliti di Osservazione della Terra di futura generazione, permettendo così di aumentare i tempi di contatto con le stazioni di terra.

Una soluzione innovativa per rispondere a queste esigenze è rappresentata dalle costellazioni multi-missione, ibride e multi-orbita di satelliti di telecomunicazioni di classe piccola e media in orbita bassa, media e geostazionaria (LEO, MEO, GEO). L'integrazione di satelliti in orbite più basse con i tradizionali satelliti geostazionari, migliora l'efficienza e la sicurezza delle comunicazioni militari.

Uno dei principali vantaggi apportati da un sistema integrato come quello proposto, è la bassa latenza nel trasferimento dei dati. Questa riduzione del ritardo di propagazione del segnale elettromagnetico è fondamentale per applicazioni che richiedono risposte rapide e coordinamento in tempo reale. Inoltre, queste costellazioni di satelliti offrono migliori analisi di *link budget*, facilitando l'uso di terminali meno performanti, e garantiscono una copertura globale, comprese le regioni polari e altre aree

non servite dai soli già dispiegati satelliti GEO.
In particolare, le costellazioni LEO, con i loro numerosi satelliti in orbita bassa, sono in grado di fornire una copertura continua e ridondante. Questo significa che se un satellite termina la sua operatività, altri satelliti possono rapidamente prendere il suo posto, assicurando la continuità del servizio. Le costellazioni MEO, situate a un'altitudine intermedia, combinano alcuni dei vantaggi dei satelliti GEO e LEO, offrendo una copertura più ampia rispetto ai LEO e una latenza inferiore rispetto ai GEO.

Inoltre, per poter dispiegare una costellazione, un requisito fondamentale per i satelliti è quello di avere una bassa massa e un ridotto volume, per poter accomodare in un singolo lancio il massimo numero di satelliti e ridurre i costi. Tra le piattaforme di piccola classe candidate emerge anche una soluzione sviluppata da Thales Alenia Space Italia, che presenta aspetti fondamentali in grado di renderla estremamente versatile, quali un design modulare per una rapida integrazione e test e la compatibilità con una vasta gamma di carichi utili e lanciatori.

Le tecnologie abilitanti includono, oltre all'uso di piattaforme satellitari di piccole dimensioni, carichi utili riconfigurabili in volo con processori digitali di bordo basati su *Software Defined Radio* (SDR) e collegamenti ottici inter-satellitari (O-ISL).
Questi carichi utili hanno lo stesso nucleo digitale riconfigurabile e consentono di concentrare in un unico satellite di dimensioni ridotte la possibilità di supportare diverse tipologie di servizi e missioni. Ciò è ottenuto grazie alla configurabilità a bordo del software mediante un approccio SDR che prevede sia la capacità di memorizzare a bordo le funzioni da attivare sia la capacità di caricare nuovi applicativi dalle stazioni del segmento di terra. Queste tecnologie insieme migliorano l'agilità e la sicurezza del sistema, permettendo una rapida adattabilità ai requisiti di missione e agli ambienti operativi in evoluzione.

La soluzione proposta da Thales Alenia Space Italia prevede una costellazione in cui ogni satellite diventa un vero e proprio nodo di una rete di telecomunicazione capace di prendere decisioni sull'instradamento del traffico. Per soddisfare le diverse tipologie di missione si pensa ad una soluzione in cui i satelliti della costellazione abbiano differenti capacità di *processing* e capacità in termini di CPU, memoria e consumi e che quindi possano lavorare a diversi livelli dello *stack* protocollare e possano gestire o meno funzionalità di livello superiore allo strato fisico, in modo che l'architettura proposta sia ottimizzata proprio per il soddisfacimento dei diversi requisiti delle applicazioni da supportare.

In sintesi, le costellazioni satellitari multi-missione, ibride e multi-orbita rappresentano una soluzione avanzata per le esigenze di telecomunicazione della Difesa, offrendo una copertura estesa, una bassa latenza e una resilienza elevata, la possibilità di usare dispositivi più semplici e meno costosi (*handheld*) grazie ai *link budget* favorevoli, fondamentali per operazioni sicure ed efficaci in scenari complessi. Investire in queste tecnologie significa garantire che le forze armate possano operare con maggiore efficienza, sicurezza e flessibilità in un mondo sempre più interconnesso e dinamico.

INFRASTRUTTURE, TECNOLOGIE E PROTOCOLLI PER LA COMUNICAZIONE QUANTISTICA SATELLITARE

Gli sviluppi di Thales Alenia Space Italia verso la realizzazione di reti di comunicazioni quantistiche globali

THALES ALENIA SPACE

M. Valeri, A. Geraldi, G. Riccardi, E. Cerqueti, M. Ottavi, P. Conforto

Con l'avvento dei computer e tecnologie quantistiche stanno emergendo nuove minacce, ma anche straordinarie opportunità di sviluppo tecnologico, che danno accesso a dei livelli di cyber-security senza precedenti e abilitano innovative applicazioni. La seconda rivoluzione quantistica sta facendo passare le tecnologie quantistiche dalla ricerca accademica alle applicazioni reali sempre più velocemente. Queste tecnologie permettono la realizzazione di protocolli di comunicazione avanzati, noti come *comunicazione quantistica*, che risultano particolarmente rilevanti per applicazioni militari e strategiche. Specifici protocolli infatti, noti come protocolli di *Quantum Key Distribution (QKD)*, garantiscono livelli di sicurezza nella trasmissione di informazioni senza precedenti, garantendo una sicurezza insuperabile nelle telecomunicazioni e nelle conseguenti applicazioni. La garanzia di tali livelli di sicurezza informatica è un requisito ormai fondamentale per molte infrastrutture critiche, in linea con i principi fondamentali di riservatezza, integrità e disponibilità delle informazioni *(CIA: Confidentiality, Integrity, Availability)*. Oltre la comunicazione quantistica sicura, interessanti sviluppi vanno anche nella direzione di condividere risorse quantistiche al fine di abilitare la connessione remota di computer e sensori quantistici. Questi sviluppi trovano campi di applicabilità nell'industria, nella finanza e nella fornitura di servizi strategici, quali la navigazione e il controllo di infrastrutture critiche. Questi campi vedono nello sviluppo di tali tecnologie la possibilità di risolvere problemi di ottimizzazione relativi al loro settore di attività, o migliorare l'accuratezza di stima di quantità fisiche di interesse.

I protocolli per le comunicazioni quantistiche richiedono un intenso lavoro di progettazione e la realizzazione di una nuova infrastruttura territoriale, il cosiddetto *quantum network*, al fine di integrare tali protocolli e tecnologie dando vita ad un più generale *quantum internet*. In questo contesto, lo spazio gioca un ruolo fondamentale per

Figura 1. SPQR Lab sito nell'edificio di Thales Alenia Space Italia a Roma adibito ad esperimenti di comunicazione ottica e quantistica.

il raggiungimento di distanze intercontinentali, come provato da vari studi e da alcune dimostrative missioni internazionali. Infatti, le reti quantistiche metropolitani *(MAN: Metropolitan Area Network),* realizzate a livello terrestre in fibra ottica, riescono a coprire solo distanze limitate a poche centinaia di chilometri. Solo l'integrazione dei MAN terrestri con reti di larga scala *(WAN: Wide Area Network)* satellitari permette alla distribuzione di risorse quantistiche di superare tali limiti.

Numerose iniziative stanno prendendo piede a livello internazionale, europeo e nazionale per la progettazione e sviluppo di sistemi satellitari per comunicazioni quantistiche. L'Europa sta avanzando con la creazione di una rete di comunicazione quantistica, la *European Quantum Communication Infrastructure (EuroQCI)*, che colleghi i 27 Sati Membri. Il progetto, finanziato dalla Commissione Europea (CE) prevede un segmento spazio in fase di sviluppo nell'ambito del progetto *Secure and Cryptographyc system (SAGA)* finanziato dall'Agenzia Spaziale Europea (ESA). Il progetto SAGA condotto Thales Alenia Space Italia con il ruolo di *prime contractor*, si trova attualmente nella fase B1. Un'altra iniziativa Europea per lo sviluppo di un sistema satellitare per QKD è il progetto Eagle-1. Mentre Eagle-1 rappresenta solo un dimostratore tecnologico, SAGA sarà la prima vera missione ad offrire un servizio di comunicazione sicura che tenga in considerazione e rispetti i più stringenti requisiti di sicurezza. Parallelamente, TerrQCI punta a sviluppare l'analogo segmento terrestre sulla breve distanza. Anche a livello nazionale, in Italia, la *quantum backbone* pre-esistente punta a integrare ulteriori sviluppi tramite progetti finanziati dalla CE, e tramite i fondi nazionali PNRR, che uniscono i maggiori attori italiani per lo sviluppo di questa rete quantistica.
Thales Alenia Space Italia è in prima linea in queste inizia-

tive, mettendo a disposizione oltre 40 anni di conoscenze ed esperienze diversificate nel campo delle telecomunicazioni satellitari e coinvolgendo e federando la filiera industriale (spesso formata da piccole e medie imprese) e accademica nazionale permettendo di raggiungere obiettivi altrimenti impossibili. Diversi progetti vedono Thales Alenia Space Italia guidare gli sviluppi spazio necessari alla rivoluzione quantistica, avvalendosi della filiera sia europea che nazionale. In particolare, a livello europeo progetti come LaiQa e QUDICE sono dedicati allo sviluppo di tecnologie quantistiche per lo spazio mentre a livello nazionale, la collaborazione attiva di Thales Alenia Space Italia con altri attori del settore, come Leonardo e CNR, o con startup italiane nel campo quantistico, come ThinkQuantum, permette la realizzazione dei progetti NQSTI e QUID, per lo sviluppo della rete quantistica italiana e la progettazione di future reti quantistiche su larga scala.

Una delle principali tecnologie quantistiche il cui sviluppo è guidato da Thales Alenia Space Italia consiste nel *processore QKD*, il quale controlla il funzionamento end-to-end (E2E) del sistema QKD, gestisce le diverse fasi del protocollo e implementa algoritmi di pre e post-processing dei dati necessari alla generazione di chiavi crittografiche sicure. Inoltre, importanti sviluppi sono in corso su tecniche di sincronizzazione temporale E2E a bassa latenza, che permettono di ridurre i requisiti di memoria a bordo del satellite (progetto SYNQ), su sorgenti quantistiche robuste in grado di operare in ambienti spaziali (progetto RES) e sulle tecnologie abilitanti la comunicazione ottica come i telescopi di bordo e di terra (progetto OPTIMA).
Tali progetti sono portati avanti non solo tramite uno studio di ingegneria di sistema, ma anche attraverso la realizzazione e il test di tecnologie e protocolli all'interno del laboratorio R&D di ottica classica e quantistica in Thales Alenia Space Italia, lo *Space Photonic and Quantum Research Laboratory (SPQR Lab)*. Nel laboratorio è dedicato alla realizzazione di testbed per emulazione di fenomeni critici su collegamenti ottici di comunicazione quantistica e classica come l'effetto Doppler dovuto al movimento relativo tra satellite e terra, la deformazione del fronte d'onda del fascio ottico dovuto al passaggio attraverso l'atmosfera, e l'effetto del fading del segnale dovuto alla turbolenza atmosferica. Questi sviluppi puntano a integrare e incrementare i risultati ottenuti in precedenti progetti durante cui è stata realizzata con successo la prima rete di comunicazione quantistica nell'area metropolitana di Roma, grazie alla quale è stata testata la trasmissione di bit quantistici sia tramite collegamenti in fibra, su link di lunghezza di circa 15km, che in aria, su link di circa 3km di lunghezza.

Thales Alenia Space Italia continua ad investire nel laboratorio di ricerca che si evolve sempre più diventando una risorsa essenziale per l'azienda oltre che un punto di attrazione per nuove risorse interessate al campo delle tecnologie quantistiche satellitari, ospitando diversi lavori di tesi e *internship* universitarie europee da campi quali matematica, ingegneria e fisica.

COME BEDROCK STREAMING È MIGRATO DA VMWARE A VATES

Una della tante storie di successo dei clienti Vates

VATES

Marc Pezin & Charles-H. Schulz

Le cose stanno cambiando nel campo della virtualizzazione. Nel 2021, l'azienda ha scelto di migrare la propria infrastruttura on-premise da VMware a XCP-ng. Una volta completata la migrazione, Bedrock ha accettato di rispondere ad alcune nostre domande.

Chi è Vates?

Vates è un fornitore di software con sede a Grenoble che sviluppa soluzioni Open Source sicure e chiavi in mano per la gestione dell'infrastruttura ICT e la virtualizzazione. In particolare, sviluppa il prodotto **Xen Orchestra**, la sua soluzione di backup e gestione dell'infrastruttura ICT e **XCP-ng**, il suo hypervisor basato su **Xen**.

Nell'ambito della dinamica di crescita internazionale sarà Leandro Aglieri a guidare lo startup e lo sviluppo della filiale italiana di VATES, che annovera già tra i suoi clienti realtà importanti come Generali Operation Services Platform, Starhotels, Ever (Gruppo Esseco) e Camozzi Group.

"Ho lavorato con VATES per più di un anno in Italia – dichiara Leandro Aglieri – e abbiamo compreso le enormi potenzialità della società e delle tecnologie open source di virtualizzazione che propone. Sono certo potrà essere attore strategico nel mondo della Difesa e della Cyber Security in Italia".

Chi è Bedrock Streaming ?

Bedrock Streaming è una società francese che sviluppa una piattaforma di video streaming. Questa piattaforma è venduta in white label ad altri clienti, principalmente emittenti europee. In Francia, la piattaforma è utilizzata da 6play (M6) e Salto.

Bedrock ha più di 45 milioni di utenti in 5 paesi diversi e più di 12 anni di esperienza nel campo.

Vincent Gallissot – Lead Cloud Architect @Bedrock, Senior Site Reliability Engineer – spiega perché parte della loro infrastruttura è nel cloud mentre altri server rimangono in sede.

"L'elasticità del cloud soddisfa le nostre esigenze aziendali, il che ci consente di adattare i nostri costi all'utilizzo effettivo. Per altre esigenze, come strumenti interni (Git, metriche, log), la nostra CDN, apparecchiature video o gateway dedicati con ISP francesi, continuiamo a utilizzare i nostri datacenter di Parigi. Riduciamo i costi gestendo noi stessi alcuni servizi che non necessitano della scalabilità del cloud. D'altra parte, per strumenti critici (come il nostro Git), essere nel cloud ci bloccherebbe troppo ed è importante per noi non mettere tutte le uova nello stesso paniere."

Prima del 2021 e della loro transizione alla nostra soluzione di virtualizzazione XCP-ng, l'intera infrastruttura Bedrock, sia nel cloud che nei loro data center, era gestita con VMware, una situazione che non si adattava a Vincent.

"Siamo un piccolo cliente (non abbiamo 5.000 hypervisor) e i nostri ticket di supporto o richieste di funzionalità non sono stati ricevuti con la serietà che ci aspettavamo. Inoltre, avevamo vSphere 6.x e dovevamo migrare a 7.x, che era un grande progetto su cui dovevamo investire molto tempo. Nella fase precedente al trasferimento del nostro datacenter, abbiamo colto l'occasione per cambiare la nostra soluzione di hypervisor e scegliere un player francese disposto a supportarci. Amiamo la mentalità e la serietà del team Vates, la scelta dell'Open Source e la grande trasparenza delle decisioni."

La loro infrastruttura in loco è destinata agli ambienti di produzione utilizzati dai clienti che utilizzano le loro piattaforme o dai team interni. Per Bedrock Streaming, la cosa più importante è la stabilità della piattaforma.

"Da qualche anno seguiamo l'evoluzione di Vates, così come il progetto Xen Orchestra. Non abbiamo testato altri 200 prodotti, abbiamo provato XCP-NG + Xen Orchestra e l'abbiamo adottato! L'idea era di utilizzare tools che consumano molte risorse (Virtual Machine di grandi dimensioni), ma anche con prestazioni molto buone (come i nostri Network Load Balancer) e con un'esperienza utente UX intuitiva (lavoriamo principalmente sul cloud, l'obiettivo è non spendere 2 ore per poter spostare una VM). Il resto delle funzionalità era piuttosto standard nell'azienda: autenticazione SAML, backup incrementali, alta disponibilità delle VM (failover automatico a caldo), tagging delle VLAN, supporto NFS, ecc."

A Vincent è stato chiesto quali fossero i principali vantaggi di XCP-ng per loro:

"Fa quello che vogliamo, che è già un grande vantaggio!"

"È efficiente, ne abbiamo visibilità (a causa dell'aspetto Open Source, non è una scatola nera), è affidabile e le nostre domande hanno una risposta rapida. Le nostre richieste di funzionalità vengono prese sul serio così come le nostre segnalazioni di bug e la frequenza di rilascio è sorprendente. Infine, gli aggiornamenti sono semplici: non c'è bisogno di fare 200 domande prima di installarli."

Abbiamo chiesto a Vincent come si sentiva riguardo alla nostra assistenza durante la migrazione:

"Ottima, abbiamo spiegato il nostro contesto, che stavamo per installare i nostri hypervisor uno dopo l'altro piuttosto che acquistare un'intera batteria di server nuovi: era quindi necessario fare un doppio giro e andare abbastanza velocemente. Il team di Vates ha subito colpito nel segno offrendoci uno script e strumenti per aiutarci con la migrazione. Abbiamo reinstallato il nostro primo hypervisor sotto XCP-NG, abbiamo configurato Xen Orchestra come volevamo e meno di un mese dopo la migrazione della prima VM, l'intero parco è stato migrato, tutti gli hypervisor giravano sotto XCP-NG, tutto questo è andato in produzione senza tempi di inattività."

"Grazie allo script di importazione delle VM in formato ovf lo abbiamo utilizzato per creare un altro script che esportasse la VM sul lato VMware, mappasse le interfacce di rete e disco e infine importasse la VM. Quindi il processo di migrazione è stato completamente automatizzato. Le piccole VM sono state migrate e rimesse in produzione in pochi minuti."

"La gestione e la configurazione per la produzione di XO/XCP-NG è stata eseguita da due persone ed è durata alcuni giorni, compresi i test di importazione VM. Aggiungiamo 1 mese in più a 6 per migrare poco più di 200 VM."

Alla Vates, siamo molto felici di esserci uniti a Bedrock nell'avventura di Xen e di essere stati scelti per sostituire VMWare.

Questa migrazione dei sistemi di produzione del nostro Cliente senza tempi di fermo è per noi un'opportunità per dimostrare che è molto semplice migrare da altre soluzioni di virtualizzazione.

VATES Italy Board (Charles Schulz – CSO, Nithida Vialle – CFO, Olivier Lambert – CEO, Leandro Aglieri – CEO Vates Italy)

INTELLIGENZA ARTIFICIALE E RANSOMWARE: COME ESSERE PREPARATI

VEEAM
Rick Vanover, VP Product Strategy

L'intelligenza artificiale (IA) potrebbe diventare uno dei grandi paradossi del 2024: siamo stanchi di sentirne parlare eppure continuiamo a parlarne. È una tecnologia che non scomparirà, quindi è meglio abituarsi. L'IA sta rivoluzionando la maggior parte dei settori digitali e il crimine informatico non fa certo eccezione. È quindi ora di passare ai fatti. Si è parlato molto del potenziale impatto dell'IA sulla minaccia globale del ransomware: come sta cambiando il panorama di questa tipologia di attacchi?

Poliziotti e criminali nell'era dell'IA

Sebbene il potenziale futuro dell'IA, sulla criminalità informatica e sulla società in generale, sia immenso (e un po' spaventoso), è più utile concentrarsi sul presente. Attualmente, l'IA è solo un altro strumento a disposizione dei criminali informatici, utilizzato per semplificare un attacco. Il National Cyber Security Centre del Regno Unito ha recentemente avvertito che l'IA aumenterà la minaccia del ransomware: l'utilizzo dell'IA per scopi criminali è quindi già una realtà.

Anche se si tratta solo di sistemare del codice non funzionante o di rispondere a domande specifiche più velocemente di Google, l'IA supporta il lavoro di un hacker tanto quanto quello di sviluppatori onesti: il risultato non è pero garantito: il prodotto finale potrebbe essere comunque di bassa qualità.

Tuttavia, i casi d'uso attuali sono più significativi. Gli algoritmi di intelligenza artificiale possono scansionare reti o ambienti per mappare l'architettura e gli endpoint e, cosa fondamentale, individuare le vulnerabilità. I criminali lo fanno già manualmente, ma l'intelligenza artificiale lo renderà molto più semplice ed efficace. L'intelligenza artificiale può essere utilizzata anche per automatizzare la raccolta di informazioni per attacchi più mirati. Questi strumenti possono analizzare Internet (in particolare i social media) per raccogliere quante più informazioni possibili su un obiettivo per il phishing e il social engineering.

Descrivere l'IA soltanto come "supporto al phishing" è probabilmente riduttivo. Nella sua forma più elementare, anche gli strumenti di intelligenza artificiale più facilmente disponibili possono essere utilizzati per creare e-mail di phishing migliori, colmando la barriera linguistica che spesso rende

queste truffe individuabili. Questo è un altro esempio di utilizzo dell'IA che migliora un'attività dannosa già esistente. Infine, la clonazione vocale (deepfakes), combinata con la raccolta automatica di informazioni, migliorerà ancor di più gli attacchi di social engineering.

Cosa significa per la sicurezza

Non sono solo i criminali informatici ad avere a disposizione un maggior numero di strumenti: anche i team di sicurezza hanno accesso a questi strumenti. Il settore del ransomware è stato valutato a 14 miliardi di dollari nel 2022, mentre quello della sicurezza globale circa 222 miliardi di dollari.

Sul fronte della sicurezza, l'intelligenza artificiale può essere utilizzata per l'analisi comportamentale, il rilevamento delle minacce e la scansione delle vulnerabilità per individuare attività e rischi dannosi. Inoltre, può essere impiegata sia per scansionare le vulnerabilità e i punti di accesso, sia per analizzare comportamenti degli utenti e dati. La sicurezza abilitata dall'intelligenza artificiale mira a prevedere e gestire le minacce prima che diventino violazioni, rendendo la difesa più efficiente ed efficace.

L'utilità dei principi base della security

Una *digital hygiene* e un approccio *zero trust* sono fondamentali. Disporre di copie dei dati diventa più che mai fondamentale. Quando tutto il resto fallisce, l'unica certezza è il backup e la possibilità di ripristinare i servizi. È necessario disporre di più copie dei dati, una offline e una off-site. È inoltre necessaria una strategia di ripristino ben collaudata, che comprenda la scansione dei backup per verificare l'assenza di errori e l'impostazione di un ambiente di ripristino pronto all'uso.

È più semplice di quanto possa sembrare. L'IA non sta cambiando le regole del gioco e i principi base della security sono fondamentali: best practice e una strategia efficace per il backup sono la soluzione quando tutto il resto fallisce.

Soci
Corporate

ALMAVIVA, Gruppo leader italiano nell'Information & Communication Technology, sinonimo di innovazione digitale, Almaviva accompagna i processi di crescita del Paese raccogliendo la sfida che le realtà enterprise devono affrontare per rimanere competitive nell'epoca del digitale, innovando il proprio modello di business, la propria organizzazione, la cultura aziendale e l'ICT. A partire da solide competenze made in Italy, Almaviva ha dato vita a un network globale con 45.000 persone e 1.185 milioni di euro di fatturato nel 2023, che conta 30 aziende e 79 sedi, in Italia e all'estero, con un'importante presenza in LATAM (Brasile, Colombia, Repubblica Dominicana), oltre che negli Stati Uniti, in Belgio, Spagna, Finlandia, Russia, Arabia Saudita, Emirati Arabi Uniti, Egitto, Tunisia".
www.almaviva.it

Ansys. Se hai mai visto il lancio di un razzo, volato su un aereo, guidato un'auto, utilizzato un computer, toccato un dispositivo mobile, attraversato un ponte o indossato una tecnologia indossabile, è probabile che tu abbia utilizzato un prodotto in cui il software Ansys ha svolto un ruolo fondamentale nella sua creazione. Ansys è il leader globale nella simulazione ingegneristica. Attraverso la nostra strategia di Pervasive Engineering Simulation, aiutiamo le aziende più innovative del mondo a fornire prodotti radicalmente migliori ai loro clienti. Offrendo il portafoglio migliore e più ampio di software di simulazione ingegneristica, li aiutiamo a risolvere le sfide di progettazione più complesse e a creare prodotti limitati solo dall'immaginazione.
www.ansys.com

Aruba S.p.A., fondata nel 1994, è il principale provider italiano di servizi cloud, data center, hosting, e-mail, registrazione domini e PEC. La società, con un capitale interamente italiano, conta 16 milioni di utenti e gestisce una vasta infrastruttura distribuita su 7 Data Center che ospita oltre 2,7 milioni di domini registrati, 9,8 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti. Aruba PEC e Actalis sono le due Certification Authority del gruppo, accreditate presso AgID (Agenzia per l'Italia Digitale) per la fornitura di servizi qualificati. L'infrastruttura Aruba è inoltre qualificata da ACN per trattare i dati ordinari, critici e anche strategici della PA. In 30 anni di attività, Aruba ha sviluppato un'ampia esperienza nella progettazione e nella gestione di data center ad alta tecnologia, di proprietà e distribuiti su tutto il territorio italiano. Il più grande si trova a Ponte San Pietro (BG) ed è caratterizzato da infrastrutture e impianti green-by-design conformi ai più elevati standard di sicurezza del settore (Rating 4 ANSI/TIA-942, ISO 22237), a cui si aggiunge l'Hyper Cloud Data Center a Roma, che si estende in un'area di 74.000 m² presso il Tecnopolo Tiburtino e a pieno regime comprenderà 5 data center indipendenti. Aruba implementa soluzioni di efficienza energetica nei suoi data center, dimostrando il suo impegno per la sostenibilità e, inoltre, produce energia pulita attraverso impianti fotovoltaici e centrali idroelettriche. Il network delle infrastrutture si estende anche in Europa, con un data center di proprietà in Repubblica Ceca e strutture partner situate in Francia, Germania, Polonia e Regno Unito.
www.aruba.it

Aviogei, fondata nel 1970, è il principale produttore italiano di attrezzature dedicate all'assistenza aeroportuale. Progetta, assembla, certifica e distribuisce un'ampia gamma di prodotti per la movimentazione e il trasporto di passeggeri e merci, sia per uso civile che militare.
È oggi presente in più di 180 aeroporti ed in 110 paesi nel mondo.
Ha sempre prestato una particolare attenzione alla transizione energetica e alla mobilità sostenibile, a promuovere lo sviluppo della tecnologia in ambito automazione e controllo, collaborando con Enti di Ricerca e Università. Offre da anni attrezzature con batterie a litio di ultima generazione e forte è l'interesse dell'azienda a creare partenariati per realizzare soluzioni innovative. La produzione di Aviogei è rivolta anche alle macchine per la logistica aeronautica militare, alla quale è dedicato lo stabilimento di Dallas in USA per la progettazione dei mezzi elettrici.
www.aviogei.com

B.M.A. nasce nel 1991 e fornisce supporto logistico ai reparti operativi delle Forze Armate, Polizia, Difesa Civile e SAR. Rappresenta in esclusiva in Italia società europee ed americane leader nel settore NVG e CBRN e fornisce consulenza ad aziende e gruppi aziendali sulle migliori strategie commerciali tramite: azioni di marketing, supporto pre e post vendita, partecipazione a gare e procedure pubbliche, realizzazione di corsi di formazione, traduzioni, gestione della codifica NATO, supporto in conferenze, incontri, meeting e seminari con stand, rappresentanza diretta e show-room di prodotti. Possiede la licenza T.U.L.P.S., art. 28 ed è certificata ISO 9001:2800.
www.bma-srl.it

Barracuda. Barracuda Networks sviluppa soluzioni di sicurezza informatica di tipo enterprise, con un focus relativo sia a implementazioni on-premise che cloud-based.
Più di 200000 clienti, a livello globale, hanno adottato soluzioni Barracuda per la salvaguardia dei propri impiegati, dei propri dati e delle proprie applicazioni, da una vasta pletora di attacchi informatici. Barracuda Networks fornisce ai propri clienti delle soluzioni semplici, complete ed economicamente sostenibili per la Protezione della Posta Elettronica, la Protezione delle Applicazioni, la Protezione delle Reti Aziendali e la Protezione dei Dati. Innoviamo continuamente le nostre soluzioni per proporre, oggi, ai nostri clienti, le soluzioni che saranno all'avanguardia domani.
Lavoriamo insieme a più di 5000 partner a livello globale. Il Partner Program di Barracuda Networks comprende un elevato numero di offerte, benefici e servizi per aiutare i nostri partner ad incrementare il proprio business tramite un portfolio di soluzioni potente e semplice da utilizzare.
Insieme ai nostri partner, siamo alla costante ricerca di un miglioramento dei nostri prodotti, dei nostri servizi e del nostro supporto.
www.barracuda.com

Crisel srl fondata nel 1993, è una società leader nella commercializzazione di tecnologie, strumenti, apparati ad alto contenuto tecnologico per svariati ambiti: Spazio, Aerospazio, Difesa, Intelligence, Geospatial e GIS, Automotive e Ferroviario. Grazie alle competenze interne e alle rappresentanze internazionali è in grado di guidare il cliente verso la soluzione più adatta alle richieste di produzione e di ricerca. La nostra offerta si compone: Consulenza Tecnico Scientifica, System Design, Testing, Training, Distribuzione, Produzione, Vendita, Manutenzione e Postvendita. Soluzioni per Telemetria di bordo, Stazioni di terra e antenne telemetriche, Spazio, Geospatial Indoor e Outdoor, GNSS, Simulazione GNSS.
www.crisel.it

CrowdStrike leader globale della Cyber Security, sta ridefinendo la sicurezza nell'era del cloud grazie alla sua piattaforma di protezione degli endpoint creata per bloccare le compromissioni. L'architettura basata su un unico agent a basso impatto della piattaforma CrowdStrike Falcon® applica l'AI a livello del cloud per offrire protezione e visibilità sull'azienda e prevenire gli attacchi agli endpoint ed ai workload sia all'interno che all'esterno della rete aziendale. Sfruttando la tecnologia proprietaria di CrowdStrike Threat Graph®, ogni settimana CrowdStrike Falcon correla oltre 4 migliaia di miliardi di eventi legati agli endpoint provenienti da tutto il mondo, alimentando una delle piattaforme di sicurezza più avanzate mai esistite. Con CrowdStrike, i clienti ottengono una protezione migliore, prestazioni più elevate e un time-to-value immediato.
www.crowdstrike.com/it

Dassault Systèmes, the 3DEXPERIENCE Company, è catalizzatrice del progresso umano; mette ambienti virtuali in 3D collaborativi a disposizione di aziende e persone per concepire innovazioni sostenibili. Utilizzando la Piattaforma 3DEXPERIENCE ed i suoi applicativi per creare gemelli virtuali delle esperienze del mondo reale, i suoi clienti allargano i confini dell'innovazione, dell'apprendimento e della produzione. Dassault Systèmes genera valore per oltre 270.000 clienti di tutte le dimensioni e in tutti i settori industriali, in più di 140 Paesi.

www.3ds.com

Deimos Engineering si occupa dal 1996 di fornire servizi e software alle pubbliche amministrazioni e alle aziende private. Ha maturato dapprima una solida esperienza nella gestione ed elaborazione di dati geografici raster e vettoriali per poi sviluppare importanti competenze nella gestione, elaborazione ed analisi dei dati aziendali, nella creazione di sistemi evoluti di Business Intelligence e nella predisposizione di modelli previsionali avanzati basati sulle tecniche di Machine Learning. Deimos Engineering vanta importanti collaborazioni tecnologiche con la piattaforma per la Business Intelligence Tableau e con Rulex Inc, la più innovativa soluzione di Machine Learning sul mercato.
www.e-deimos.it

DigitalPlatforms S.p.A. (DP) è un gruppo interamente italiano nato nel 2018 con la missione di fornire soluzioni end-to-end e tecnologie Internet of Things e Cyber alla Difesa, alla Pubblica Amministrazione e alle principali aziende che gestiscono le infrastrutture critiche nei settori energia/utilities, trasporti, telecomunicazioni.
Il Gruppo DP è attualmente composto da una capogruppo e sette aziende controllate ed impiega 460 risorse, tra ingegneri, programmatori, consulenti informatici, tecnici di laboratorio, ricercatori, operanti da sedici uffici o fabbriche tutti basati in Italia.
In possesso delle principali autorizzazioni di sicurezza, DP collabora con tutti i grandi Integratori e fornitori di piattaforme della Difesa Italiana ed è Azienda federata AIAD (Associazione Italiana Aziende Difesa). È inoltre vendor certificato presso il Consiglio d'Europa e presso la Nato.
www.platforms.it

Eles nasce nel 1987 ed opera nel settore dell'elettronica e microelettronica applicata a diversi settori high-end e mission critical. In particolare nella progettazione e fornitura di soluzioni di ingegneria e sistemi per la qualifica ed il controllo affidabilità e qualità dei semiconduttori. In quest'ambito fornisce player come STm, Infineon, Qualcomm, Microchip e molti altri. Con la BU Industria & Difesa, sviluppa ed integra sub-moduli di alimentazione impiegati nel settore avionico e navale con offerta qualificata su programmi europei tipo EuroDASS, Horizon e FREMM, fornendo aziende Europee main contractor di sistemi EWS. Eles è orientata alla qualità ed alla soddisfazione del cliente.
www.eles.com

Elt Group, as a European leader in Defence & Security, has been on the cutting edge of Electronic Warfare for more than 70 years, supplying Governments of 30 Countries with more than 3000 high technology systems. The company boasts a strong list of successful national and international collaborations on major programs like the Tornado fighter, the Eurofighter Typhoon combat aircraft, the NH-90 helicopter, the Italian offshore patrol vessel and the Franco-Italian Horizon and FREMM warships. Today the company is involved in the Global Combact Air Program (GCAP), as EW national champion in the Isanke & ICS domain.
Thanks to innovative management of the electromagnetic spectrum, achieved through proprietary and integrated technologies, today the brand is an international Group, named ELT Group, with a multi-domain approach that also covers Cyber, Space and Biodefense.
ELT Group is headquartered in Italy, but has a presence in 11 countries located on 3 continents through sales offices and companies of strategic importance and local law in Germany and Saudi Arabia. Also part of the ELT Group are CY4GATE, which specializes in Cyber security and Cyber Intelligence, and E4Life, Italy's first Biodefense company with a revolutionary technology E4Shield to neutralize the respiratory viruses, including Covid. The Group's mission is based on four pillars: excellence, innovation, proprietary technologies and tradition, allowing it to maintain over the years its excellent niche status in the Italian and international scene. It's controlled by Benigni's family, with Leonardo and Thales in the shareholders structure.
s a global leader in the management of EMSO Electromagnetic Spectrum Operation with a complete portfolio of state-of-the-art solutions to satisfy the most challenging requirements of modern operational scenarios.
ELT's Defence systems are deployed for a variety of key operational missions, from Strategic Surveillance, to Self Protection, Sigint, Electronic Defence and Operational Support for airborne, naval and ground applications, with a focus on cyber security and cyber resilience.
Recently the Group achieved new important target in Space domain: last April the first 'Scorpio' payload was taken into LEO orbit and is conducting its mission to collect unclassified maritime data to intercept possible illicit activities. The company has thus demonstrated that its technologies can also be used in Space, where a more articulated roadmap for intelligence and protection activities is planned.
www.eltgroup.net

ENAV S.p.A. Provider ATC quotato in Borsa, gestisce il controllo del traffico aereo civile in Italia, garantendo sicurezza e puntualità. La Società controlla oltre 2 milioni di voli l'anno attraverso le Torri di controllo di 45 aeroporti e 4 Centri di Controllo d'Area. Appartengono al Gruppo ENAV la società IDS AirNav che fornisce servizi commerciali, sistemi e software d'eccellenza, relativi alla navigazione aerea, la società Techno Sky, che assicura l'efficienza operativa degli impianti, dei sistemi e dei software sul territorio nazionale e la società D-flight, destinata allo sviluppo della piattaforma U-space dedicata ai servizi del Advanced Air Mobility (droni). Le aree di eccellenza comprendono servizi e software all'avanguardia destinati alla progettazione dello spazio aereo, al settore metereologico, alle radiomisure e alle attività di Training.
www.enav.it

Esri Italia, Official Distributor di Esri per il mercato italiano, è l'azienda di riferimento nelle soluzioni geospaziali, nella geolocalizzazione e nei Sistemi Informativi Geografici, con sedi a Roma, Milano, Ferrara, Trento e Cagliari. La società è parte integrante della Esri One Company, un sistema di oltre 80 aziende a livello internazionale che opera in network in oltre 200 paesi. Esri Italia offre sistemi e soluzioni in tutti gli ambiti applicativi dove la localizzazione dei dati risulta cruciale. Attraverso la sua offerta di prodotti e servizi, supporta enti e aziende nella trasformazione digitale, permettendogli di cogliere le opportunità offerte dalla "The Science of Where".
I nostri punti di forza:
- fornire ai clienti la capacità di effettuare analisi geospaziali complesse sui propri dati;
- supportare enti e aziende nell'integrazione della componente geografica con le proprie piattaforme Enterprise;
- diffondere all'interno delle organizzazioni la potenza della lettura geografica delle informazioni.

www.esriitalia.it

Eurelettronica Icas S.r.l., fondata nel 1961, è un'azienda di progettazione, integrazione, installazione, vendita, consulenza e formazione nel campo della meteorologia. È il rappresentante unico di VAISALA in Italia, sin dal 1979, per tutte le applicazioni di Meteorologia. Dal 2011 è anche Partner Tecnico Certificato VAISALA e dispone di personale tecnico addestrato e specializzato.
EURELETTRONICA ICAS distribuisce in Italia anche altre aziende internazionali quali KIPP&ZONEN, MILLARD TOWERS e TOTEX CORPORATION.
www.eurelettronicaicas.com

Fastweb Con 3,3 milioni di clienti su rete fissa e 3,6 milioni su rete mobile Fastweb è uno dei principali operatori di telecomunicazioni in Italia. L'azienda promuove la trasformazione digitale della collettività per costruire un futuro sempre più connesso, inclusivo ed ecosostenibile. Dalla sua creazione nel 1999, la società ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultralarga e favorire la digitalizzazione dei cittadini e del Paese.
Per aiutare tutti a costruire il proprio futuro con fiducia, l'azienda investe continuamente in reti performanti a velocità Gigabit e in servizi innovativi, incoraggia la più ampia diffusione tra la popolazione delle competenze digitali, promuove una cultura inclusiva, coltivando la crescita dei talenti, e sostiene la lotta ai cambiamenti climatici. Dal 2015 la società acquista il 100% dell'energia da fonti rinnovabili e nel 2020 ha fissato ambiziosi obiettivi di riduzione delle emissioni approvati da Science Based Targets iniziative. Già Carbon Neutral per le emissioni dirette e per quelle derivanti dall'erogazione e dall'utilizzo del servizio da parte dei propri clienti, Fastweb ha definito l'ambizioso obiettivo di diventare completamente Carbon Neutral entro il 2025. Premiata con il secondo posto della classifica Europe's Climate Leaders 2021 del Financial Times Fastweb ha ricevuto da Standard Ethics il rating di sostenibilità di lungo periodo "EE+" (Very Strong). Dal gennaio 2022 Fastweb è società Benefit.
www.fastweb.it

Forescout Technologies è il leader nelle attività di Device Visibility e Control.
La nostra piattaforma di sicurezza unificata permette alle aziende e alle agenzie governative di ottenere una conoscenza completa e legata al contesto dell'ambiente relativo alla extended enterprise, includendo gli ambienti Campus, Data Center, Cloud, IoT e OT.
Permette inoltre di coordinare le attività e le azioni dei sistemi di cybersecurity di terze parti presenti nell'infrastruttura aziendale al fine di ridurre i rischi operativi legati all'ambiente informatico e industriale.
I prodotti di Forescout Technologies possono essere istallati velocemente e permettono una operatività sia di tipo agentless che di tipo agent-based, e operano sia in modalità attiva che in modalità passiva a seconda delle esigenze e delle caratteristiche della infrastruttura di rete aziendale.
Essi consentono, in tempo reale, la scoperta di ogni apparato connesso in modalità IP sull'infrastruttura di rete estesa, la classificazione intelligente e granulare degli stessi nonché la analisi posturale e lo stato dell'apparato individuato.
www.forescout.com

Fortinet rende possibile un mondo digitale di cui possiamo sempre fidarci attraverso la sua missione di proteggere persone, dispositivi e dati ovunque. Ecco perché le più grandi imprese, service provider e organizzazioni governative del mondo scelgono Fortinet per accelerare in modo sicuro il loro viaggio digitale. La piattaforma Fortinet Security Fabric offre protezione ampia, integrata e automatizzata sull'intera superficie di attacco digitale, proteggendo dispositivi, dati, applicazioni e connessioni critici dal data center al cloud fino all'home office. Al primo posto nella classifica delle appliance di sicurezza più vendute in tutto il mondo, oltre 755.000 clienti si affidano a Fortinet per proteggere le proprie attività. E il Fortinet NSE Training Institute, un'iniziativa della Training Advancement Agenda (TAA) di Fortinet, offre uno dei programmi di formazione più grandi e ampi del settore per rendere disponibili a tutti la formazione informatica e nuove opportunità di carriera.
www.fortinet.com

GMSPAZIO è attiva dal 2005 al servizio dei mercati dell'aerospazio, della difesa, della sicurezza nazionale e dell'ICT, con soluzioni tecnologiche di elevato livello focalizzate sulla gestione di scenari sintetici 4Ds (Spazio + Tempo) a supporto dei clienti per gestire: Scenari complessi di simulazione, Sorveglianza e Monitoraggio del traffico spaziale e Space Situational Awareness, Attività di Sorveglianza delle frontiere marittime, Modellazione delle reti di difesa missilistica, progetti di telerilevamento satellitare e attività di sorveglianza tramite UAV, offrendo prodotti, servizi e formazione per lo sviluppo di sistemi informativi integrati e personalizzati sulla base delle specifiche richieste degli utenti.
www.gmspazio.com

I&C International Consulting S.r.l. è una società di ingegneria di Roma focalizzata sulla fornitura di servizi professionali per le organizzazioni che operano nell'ambito del Ministero della Difesa e della NATO. I servizi d'ingegneria coprono tutte le fasi del progetto, studi di fattibilità, progettazione, direzione lavori e collaudo nonché il supporto alla certificazione di infrastrutture con elevati requisiti di sicurezza. Le aree di competenza riguardano tutte le categorie di opere collegate alla Difesa, i sistemi di telecomunicazione e radiocomunicazione, gli impianti elettrici, meccanici e di sicurezza fisica e le opere architettoniche e di ingegneria civile, incluse le strutture. La I&C opera in conformità alle norme: 9001:2015, ISO 45001:2018, ISO 27001:2022 e NATO AQAP 2110.
www.intconsulting.it

IBM. Con più di 110 anni di storia, IBM è leader nell'Innovazione al servizio di imprese e istituzioni in tutto il mondo. Opera in oltre 175 paesi. L'azienda – una open hybrid cloud and AI platform company – offre alle organizzazioni di ogni settore l'accesso alle tecnologie esponenziali e ai servizi di consulenza per la trasformazione digitale e la modernizzazione dei modelli di business.
Cloud ibrido, IA, sistemi HW quali mainframe, power e storage, soluzioni SW, cybersecurity e quantum computing: queste le aree in cui IBM è riconosciuta come leader a livello globale e come brand dal forte impegno etico nei confronti del mercato e del contesto sociale in cui opera.
Grande è l'impegno per creare e rafforzare nuove competenze professionali. IBM Research guarda continuamente al "What's Next in Computing" per risolvere le grandi sfide del mondo (scienza del clima, nella scoperta dei materiali, nella sanità e altro ancora). Ulteriori approfondimenti:
ibm.com/annualreport - ibm.com/it - it.newsroom.ibm.com

IES, fondata nel 1990, è composta da un team di esperti nel campo dei sistemi di telecomunicazione per applicazioni civili e militari, negli ambiti terrestri, avionici, navali e ferroviari. La professionalità, la competenza e l'esperienza del proprio staff fanno della IES un interlocutore di primo piano, che la rendono fortemente competitiva nei settori strategici di prestigiosi enti pubblici, privati ed internazionali (NATO). Le attività principali riguardano: progettazione e realizzazione di innumerevoli prodotti (amplificatori RF, matrici Audio/RF, filtri, antenne), installazione e manutenzione di sistemi di comunicazione, con particolare attenzione allo sviluppo di specifici progetti per infrastrutture critiche ad alto livello di sicurezza.
www.iessrl.it

INTECS S.p.A. è un'azienda ingegneristica tutta italiana fondata nel 1974, che offre la più innovativa tecnologia software & hardware, servizi di Ingegneria Informatica e prodotti per sistemi elettronici safey- critical e mission-critical affidabili. Intecs progetta e sviluppa applicazioni, strumenti, software, componenti hardware e prodotti per i settori Aerospazio, Difesa, Trasporti (Automotive & Ferroviario), Telecomunicazioni, Smart Systems, Fintech e AI anche in collaborazione con le principali Industrie,
Organizzazioni, Università e Centri di Ricerca europei ed italiani. L'azienda pone infatti da sempre grande attenzione ed impegno nella Ricerca e Sviluppo, per lo studio e la sperimentazione di tecnologie high tech, al fine di implementare il suo livello di know How ed offrire ai Clienti un supporto sempre all'avanguardia.
www.intecs.it

Keysight Technologies, Inc. (NYSE: KEYS) è un'azienda leader nel settore tecnologico che aiuta ad accelerare l'innovazione e connettere il mondo in modo sicuro. La dedizione di Keysight alla velocità ed alla precisione si estende anche alle analisi sul software che consentono l'introduzione di nuovi prodotti e sistemi elettronici sul mercato più rapidamente, con un'offerta che copre l'intero ciclo di vita del prodotto dalla simulazione progettuale alla validazione dei prototipi, al collaudo produttivo, fino ai test di performance e visibility delle reti e degli ambienti cloud. Le nostre applicazioni vengono utilizzate in ogni settore di mercato delle comunicazioni e dell'ecosistema industriale, nel settore aerospaziale e della difesa, automobilistico, energetico, dei semiconduttori e dell'elettronica generale. Nell'esercizio fiscale 2021, Keysight ha realizzato un fatturato di 4,9 miliardi di dollari. Maggiori informazioni sull'azienda sono disponibili all'indirizzo www.keysight.com, nella newsroom https://www.keysight.com/go/news e su Facebook, LinkedIn, Twitter e YouTube.
www.keysight.com

LARIMART S.p.A., società controllata da LEONARDO SpA, è un punto di riferimento pluridecennale nella progettazione e realizzazione di soluzioni e apparati in ambito Difesa, Sicurezza ed Emergenza.
LARIMART opera da sempre nel rispetto delle linee guida prioritarie per i nostri End-User:

- Realizzare Soluzioni Elettroniche e di Protezione Personale per le specifiche esigenze tecnico-operative, nei contesti di impiego Difesa e Sicurezza;
- Affiancare costantemente gli "End-User" per assicurare un efficace supporto tecnico/sistemistico;
- Sviluppare prodotti/sistemi caratterizzati da affidabilità nei "servizi base" ed aperti all'evoluzione delle prestazioni;
- Assicurare l'evoluzione delle prestazioni combinando l'innovazione tecnologica delle componenti COTS con le specifiche soluzioni idonee ai particolari contesti d'impiego.

I principali settori in cui opera sono: Sistema Soldato, Sistemi elettronici per Mezzi Tattici Terrestri, Applicazioni Navali, Posti Comando e Sale Operative.
www.larimart.it

Leonardo è un gruppo industriale internazionale, tra le principali realtà mondiali nell'Aerospazio, Difesa e Sicurezza che realizza capacità tecnologiche multidominio in ambito Elicotteri, Velivoli, Aerostrutture, Elettronica, Cyber Security e Spazio. Con oltre 53.000 dipendenti nel mondo, l'azienda ha una solida presenza industriale in Italia, Regno Unito, Polonia, Stati Uniti, e opera in 150 paesi anche attraverso aziende controllate, joint venture e partecipazioni. Protagonista dei principali programmi strategici a livello globale, è partner tecnologico e industriale di Governi, Amministrazioni della Difesa, Istituzioni e imprese. Nel 2023 Leonardo ha registrato ricavi consolidati pari a € 15,3 mld, nuovi ordini per € 17,9 mld, e ha investito € 2,2 mld in attività di R&S. Innovazione, ricerca continua, industria digitale e sostenibilità sono i pilastri del suo business nel mondo.
www.leonardo.com

Maticmind è un System Integrator italiano operante nel settore ICT che si propone come Digital Provider in grado di progettare, integrare e gestire soluzioni tecnologiche innovative, grazie a competenze specialistiche in ambito Networking, Cybersecurity, Digital Workplace, Datacenter & Cloud, Application Services, UBB & 5G, IoT e Managed Services.
Lo scenario di riferimento di Maticmind è quello di garantire soluzioni integrate di Networking, Cybersecurity, Data Center, Digital Workplace, Application, Cloud, UBB & 5G e IoT arrivando a soluzioni sempre più orientate alle applicazioni ed ai servizi a valore aggiunto, assicurando una profonda interazione tra le piattaforme infrastrutturali e quelle applicative.
Attraverso la partnership con i maggiori Vendor mondiali, Maticmind ha acquisito un ruolo predominante come partner tecnologico per le più importanti realtà italiane impegnate nella trasformazione digitale delle proprie infrastrutture (operatori di telecomunicazioni, aziende, pubblica amministrazione centrale e locale), posizionandosi saldamente ai vertici del mercato della System Integration.
www.maticmind.it

M.P.G. Instruments S.r.l. fin dal 1984 ha improntato la sua attività nella commercializzazione della strumentazione elettronica di test, curandone la personalizzazione e la manutenzione in accordo ai requisiti dei nostri clienti.
M.P.G. Instruments S.r.l. è strutturata per poter garantire ai propri clienti prodotti e servizi al fine di assicurare:

- innovazione tecnologica costante
- assistenza tecnica tempestiva
- servizi di manutenzione e taratura accurati

Tra le poche in Italia ad avere le certificazioni di qualità EN9100/9110/9120, la sua organizzazione ha reso possibile il consolidamento di partnership con aziende nazionali ed internazionali operanti nel settore.
Lo scopo principale di M.P.G. Instruments è di creare eccellenza e innovazione di prodotto offrendo sistemi integrati, strumentazioni per test in campo avionico e servizi di assistenza allineati con il progredire dell'evoluzione tecnologia odierna.
www.maticmind.it

NI., divisione Test and Measurement di Emerson, continua ad essere leader nei sistemi di test e misura automatizzati attraverso una piattaforma aperta basata sul software, mantenendo il focus sull'innovazione per migliorare il mondo in cui viviamo e superare le complessità delle sfide tecnologiche. Da oltre 40 anni NI serve l'industria dell'Aerospazio e Difesa, e si impegna a fornire tecnologie di test automatizzato dalle elevate performance - sia nell'ambito della costruzione e della manutenzione dei sistemi di test per supportare programmi a lungo ciclo di vita, sia nell'ambito della progettazione di sistemi radar e di guerra elettronica di nuova generazione, sia nell'ambito dell'implementazione di iniziative di trasformazione digitale.
www.ni.com

Planetek Italia, da oltre 25 anni nel settore spaziale, partecipa ai principali programmi di osservazione della Terra e a numerose attività per la Difesa e la Sicurezza dell'Unione Europea. Le tecnologie sviluppate da Planetek sono state utilizzate nell'ambito di missioni spaziali duali, quali COSMO-SkyMed e COSMO-SkyMed Second Generation. Specifiche applicazioni di ultima generazione sono state sviluppate in partnership con la Hexagon Geospatial a supporto di IMINT e GeoINT per le FF.AA. Italiane, nell'ambito del programma nazionale di ricerca della Difesa, dimostrando il ruolo fondamentale delle tecnologie geospaziali in molte applicazioni, quali: supporto alle operazioni umanitarie; difesa dei confini; missioni militari internazionali.
www.planetek.it

Polomarconi.it S.p.A. società italiana con competenze specifiche nel settore delle comunicazioni a radiofrequenza con sedi a: Verona, Bergamo e Trento propone progetti di ricerca e sviluppo di sistemi a RF per i propri clienti nei settori ATC, LAND & NAVAL, TRANSPORT, PMR, DAS & 5G, M2M e MICROWAVE.
I principali clienti di Polomarconi.it sono system integrators, produttori di radio e organizzazioni governative. I sistemi offerti da Polomarconi.it per installazioni terrestri, aeree e navali includono combinatori multicanale automatici, filtri, accoppiatosi amplificati per la ricezione, duplexer, multiplexer, antenne e sistemi di antenne. Per i progetti più innovativi, Polomarconi.it collabora con istituti di ricerca e eccellenze universitarie in Italia e all'estero.
www.polomarconi.it

Pure Storage (NYSE: PSTG) propone la piattaforma di archiviazione dati più avanzata del settore per memorizzare, gestire e proteggere i dati su qualsiasi scala. Con Pure Storage, le aziende possono contare su semplicità e flessibilità assolute, risparmiando tempo, denaro ed energia. Dall'AI all'archiviazione, Pure Storage offre un'esperienza cloud con un'unica piattaforma Storage as-a-Service unificata per ambienti on premise, cloud e hosted. La nostra piattaforma è costruita sulla nostra architettura Evergreen che evolve di pari passo con le aziende, sempre rinnovata e migliore, con zero tempi di inattività pianificati, garantiti. I nostri clienti aumentano attivamente la propria capacità e potenza di elaborazione, riducendo al contempo in modo significativo le emissioni di carbonio e l'impatto energetico. Pure è orgogliosa di essere una realtà customer-first come prova l'indice Net Promoter Score più alto di tutto il settore. Per ulteriori informazioni:
https://www.purestorage.com/it/

Rubrik (NYSE: RBRK) è in missione per proteggere i dati del mondo. Con la Zero Trust Data Security™, aiutiamo le organizzazioni a raggiungere la resilienza aziendale contro i cyberattacchi, gli insider malintenzionati e le interruzioni operative. Rubrik Security Cloud, basato sul machine learning, protegge i dati nelle applicazioni aziendali, cloud e SaaS. Aiutiamo le organizzazioni a mantenere l'integrità dei dati, a garantire una disponibilità dei dati che resista a condizioni avverse, a monitorare costantemente i rischi e le minacce ai dati e a ripristinare le aziende con i loro dati quando l'infrastruttura viene attaccata. Per maggiori informazioni visitate il sito www.rubrik.come seguite @rubrikInc su X (conosciuto precedentemente come Twitter) e Rubrik su LinkedIn.
www.rubrik.com

SIPAL S.p.A. nasce a Torino nel 1978 ed entra nel gruppo FININC nel 1988. Presente da oltre 46 anni sulla scena nazionale ed estera, oggi SIPAL è un partner globale nei settori dell'ingegneria e della costruzione di attrezzature meccaniche. Con 15 sedi in Italia, oltre 500 addetti altamente specializzati, SIPAL lavora con flessibilità e competitività, personalizzando in ogni dettaglio i servizi offerti. Sipal progetta e realizza infrastrutture CIS e SAP-F per il trattamento dei dati classificati, dal 2018 produce dispositivi TEMPEST (Level A, B, C), è NATO BOA Partner ed è in possesso di un Laboratorio CE.VA. accreditato; possiede altresì le abilitazioni necessarie per operare ai più elevati livelli di segretezza, supportando il cliente, nell'ambito della cyber security, con una consulenza ad ampio spettro nella scelta dei sistemi più adatti alle singole esigenze. SIPAL è presente anche su scala internazionale, con snodi cruciali in India, Brasile, Romania, USA.
www.sipal.it

S&A è la società leader in Italia nella progettazione e realizzazione di prodotti e soluzioni per l'analisi delle informazioni per tutte le forze di Polizia Italiane e l'intelligence. Attiva sul mercato dell'Information Technology da oltre 25 anni, è da oltre 20 anni distributrice esclusiva di i2 Ltd nel nostro Paese, utilizzando per prima metodologie e tecnologie per l'analisi visuale.
S&A ha saputo coniugare il meglio della tecnologia con quanto raccolto sul campo dal supporto diretto offerto agli utenti e dallo studio delle migliori esperienze maturate in altre nazioni, nel medesimo settore.
S&A, basandosi sulla contiguità metodologica e tecnologica, ha realizzato vari prodotti e soluzioni destinate anche al mercato corporate (nazionale e estero), trasferendo in questi contesti l'esperienza maturata in ambito Law Enforcement.
www.sealink.it

Stormshield è un'azienda 100% di proprietà del Gruppo AIRBUS.
Attiva nel settore della Sicurezza Informatica da oltre 15 anni, Stormshield offre ad Aziende e Organizzazioni di tutto il mondo un'alternativa europea affidabile per la protezione delle Infrastrutture Critiche, dei Dati Sensibili e degli Ambienti Operativi.
In un contesto geopolitico sempre più complesso che coinvolge Stati e grandi attori digitali, Stormshield è impegnata in un ambizioso progetto strategico: diventare la prima scelta europea in materia di Sicurezza Informatica. Unica azienda totalmente europea che progetta, sviluppa e produce prodotti hardware e software di Network Security, Data Security e Endpoint Security su territorio europeo.
www.stormshield.com/it/

Teleconsys SpA è una Digital Innovation Company la cui missione è supportare le organizzazioni pubbliche e private nel loro viaggio di scoperta, adozione, trasformazione ed evoluzione digitale, facendo leva sulla sicurezza, sull'innovazione aperta e sulla sostenibilità.
Grazie ad oltre venti anni di esperienza in settori ad alta intensità tecnologica e in costante trasformazione, realizziamo soluzioni innovative componendo sapientemente l'offerta delle quattro Business Unit - Cybersecurity & Governance, Modern Application Development, Next Generation Infrastructure, IT Services - con le tecnologie emergenti alla base del web 4.0. quali AI, xR, DLT.
In quanto PMI innovativa e certificata ISO 56002, investiamo mediamente ogni anno più del 4% dei ricavi in Ricerca, Sviluppo e Innovazione e abbiamo costruito importante network dell'innovazione aperta che ci vede collaborare con prestigiose Università, Competence Center, Cluster, Digital Innovation Hub e Venture Capital.
www.teleconsys.it

Telespazio, una joint venture tra Leonardo (67%) e Thales (33%), è tra i principali operatori mondiali nel campo dei servizi spaziali: dalla progettazione e sviluppo di sistemi spaziali, alla gestione dei servizi di lancio e controllo in orbita di satelliti; dai servizi di osservazione della Terra, comunicazioni integrate, navigazione satellitare, fino ai programmi scientifici. L'azienda gioca un ruolo da protagonista nei mercati di riferimento facendo leva sulle competenze tecnologiche acquisite in oltre 60 anni di attività, le proprie infrastrutture, la partecipazione ai principali programmi spaziali europei. Telespazio, che insieme a Thales Alenia Space forma la "Space Alliance", nel 2023 ha generato un fatturato di 700 milioni di euro e può contare su 3300 dipendenti in quindici Paesi.
www.telespazio.com

Thales Alenia Space. Forte di un'esperienza ultra-quarantennale e di un insieme unico di competenze, expertise e culture, Thales Alenia Space offre soluzioni economicamente vantaggiose nel campo delle Telecomunicazioni, Navigazione, Osservazione della Terra, gestione ambientale, Esplorazione, Scienza e Infrastrutture orbitali. Sia l'industria privata che governativa conta su Thales Alenia Space per progettare sistemi satellitari che forniscano connessione e posizionamento ovunque e in qualsiasi luogo, monitoraggio del nostro pianeta, potenziamento della gestione delle sue risorse ed esplorazione del nostro Sistema solare e oltre. Thales Alenia Space considera lo spazio come un nuovo orizzonte, che consente di migliorare e rendere più sostenibile la vita sulla Terra. Una joint venture Thales (67%) e Leonardo (33%), Thales Alenia Space insieme a Telespazio forma, inoltre, la partnership strategica "Space Alliance", in grado di offrire un insieme completo di servizi. Nel 2022 la società ha realizzato un fatturato consolidato di 2,2 miliardi di euro e ha circa 8.500 dipendenti in 10 paesi con 17 siti in Europa e uno stabilimento negli USA.
www.thalesaleniaspace.com

Vaisala è azienda leader mondiale nel campo delle misure ambientali e industriali, fondata nel 1936 dal Prof. Vilho Vaisala a Helsinki (Finlandia). Ha più di 2000 dipendenti. I sistemi VAISALA sono installati ed operativi in 100 paesi del mondo: stazioni meteorologiche automatiche, sistemi di radiosondaggio automatici, sistemi AWOS per aeroporti, nefoipsometri, visibilimetri, sistemi di rilevamento fulmini. VAISALA si è distinta in particolar modo nella radar meteorologia, portando sul mercato un Radar meteorologico innovativo, il cui disegno progettuale è basato su elevata qualità e disponibilità dei dati e basso costo del ciclo di vita, con l'impiego di un trasmettitore allo stato solido. Vaisala produce radar meteorologici in banda X e in banda C.
VAISALA è leader nel campo della fornitura di Lidar per monitoraggio dei campi di vento in diverse applicazioni e recentemente ha anche introdotto sul mercato sistemi Lidar per i profili di vapore acqueo. L'innovazione e la tecnologia sono da sempre i capisaldi del successo VAISALA con un investimento annuo di circa il 12% delle vendite nette in Ricerca e Sviluppo.
VAISALA supporta la comunità scientifica per migliorare le conoscenze sui cambiamenti climatici e aiutare le nazioni a comprendere meglio le proprie vulnerabilità e diventare resilienti attraverso misure e previsioni meteorologiche allo stato dell'arte.
www.vaisala.com

Vates is an Open Source software editor specialized in virtualization solutions. We develop in particular two software: XCP-ng (Xen Cloud Platform - new generation), a complete virtualization hypervisor that embeds its API and is based on Xen hypervisor. Xen Orchestra, on the other side, is a management interface that allows you to completely manage a virtual infrastructure based on XCP-ng or Citrix Hypervisor, from the creation and migration of VMs to the delegation of resources, including continuous replication and backup of VMs. Innovation is at the heart of our preoccupations and we invest considerably in R&D in order to improve the performance of our platforms, their security and thus be able to respond to emerging needs, particularly in terms of hybrid infrastructure and edge computing.
www.vates.fr

Veeam® leader mondiale nella protezione dei dati e nel recupero da ransomware, aiuta ogni organizzazione a non limitarsi a riprendersi da un'interruzione o da una perdita di dati, ma a continuare a far funzionare le loro attività. Con Veeam, le organizzazioni ottengono una resilienza radicale attraverso la sicurezza dei dati, il recupero dei dati e la libertà dei dati per il loro cloud ibrido. Veeam Data Platform offre un'unica soluzione per ambienti cloud, virtuali, fisici, SaaS e Kubernetes che offre ai responsabili IT e della sicurezza la tranquillità di sapere che le applicazioni e i dati sono protetti e sempre disponibili. Con sede centrale Seattle, Veeam protegge oltre 450.000 clienti in tutto il mondo. La resilienza radicale inizia con Veeam.
www.veam.com

AFCEA Capitolo di Roma
Via Arno 38, int. 9 Roma
tel +39 0694376483
fax +39 06 8845112
www.afcearoma.it

Il team editoriale ringrazia tutte le istituzioni civili e militari per il prezioso contributo fornito all'associazione.

Seguiteci anche su: