AFCEA
CAPITOLO DI ROMA

2023
7° EDIZIONE

Un anno di attività

www.afcearoma.it

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

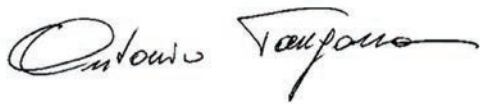
eccoci puntuali all'appuntamento con il numero annuale della nostra rivista giunta alla settima edizione.

A testimonianza del suo apprezzamento è significativamente incrementato il numero degli articoli dei nostri soci Corporate nella sezione dedicata che anche quest'anno presenta due articoli esclusivi scritti per la nostra rivista, uno dal Presidente e CEO di AFCEA International, il Lt. Gen. Susan Lawrence, USA (Ret.) ed l'altro dal General Manager di AFCEA Europe, il Maj. Gen. Ercih Staudacher, GEAF (Ret.)
Nel 2022, terminata l'emergenza COVID, abbiamo ripreso totalmente le attività in presenza che hanno registrato un notevole successo di partecipanti sia per gli argomenti trattati sia per la qualità dei relatori provenienti da diversi settori istituzionali, accademici e indutriali a cui va il più sentito apprezzamento e ringraziamento.

Mi piace ricordare che la nostra è un'associazione no-profit costituita da soci che operano su base esclusivamente volontaria e per i quali la miglior gratificazione è data dai riconoscimenti ottenuti da AFCEA International e da tutti coloro che ci seguono e apprezzano a livello istituzionale, accademico e indutriale e dal costante incremento dei soci sia individuali che corporate.
Posso quindi assicurare il continuo impegno del nostro Capitolo per il perseguimento del principale obiettivo di AFCEA International vale a dire la promozione del dialogo tra comunità militari, governative, accademiche e industriali per ampliare la cultura e le conoscenze professionali nei settori d'interesse.

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 ing. TANGORRA



Indice dei contenuti

AFCEA Capitolo di Roma

AFCEA International è un'associazione no profit 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 **138** capitoli in **33** Paesi.

Attraverso i suoi Capitoli, AFCEA International può contare attualmente su oltre **30.000** 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.
AFCEA International ogni anno assegna numerosi riconoscimenti ai capitoli e ai soci che si sono particolarmente distinti con il loro impegno in riconoscimento delle attività svolte e dei risultati ottenuti. Nel 2022 il nostro Capitolo è stato premiato con il *Model Chapter Award*. Il Dott. Vincenzo Vitiello con il *Meritorious Service Award*.

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; inoltre è stata recentemente nominata membro dell'Executive Committee di AFCEA International. 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 AFCEAn 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 oltre **400** soci individuali e **45** 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.

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 (https://www.afcea.org/signal-media#), 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 in "Optics and Quantum Information" presso l'Università di Roma La Sapienza.

L'Associazione ha stipulato convenzioni con altri Enti e liberi professionisti per fornire opportunità e facilitazioni ai Soci.

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 hanno la possibilità di mantenersi aggiornati e conoscere i contenuti dettagliati.
Tutti i soci hanno anche la possibilità di far 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 Donatella Dominici

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

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

Comitato Tecnico Scientifico
Dott.ssa Annamaria Nassisi (socio corporate Thales Alenia Space Italia)
Ing. Cinzia Crostarosa (socio corporate Larimart)
Ing. Giuseppe Tomasicchio (socio corporateTelespazio)
Ing. Eugenia Finocchiaro (socio corporate Crisel)
Ing. Claudio Santo Malavenda (socio singolo)

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)
Ing. 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:
Col. Gianluca Pedicini

Web Officer:
Dott.ssa Lucia Di Giambattista

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

Gli eventi 2022

DIGITAL TWIN: UN NUOVO ECOSISTEMA PER LA DIFESA

7 DICEMBRE 2022

Il "Digital Twin" – il gemello digitale, è annoverato tra le cinque tendenze emergenti che guideranno l'innovazione tecnologica per il prossimo decennio. Il Digital Twin è una metodologia industriale che si attua attraverso lo sviluppo e lo studio di modelli tramite la realtà virtuale. Il primo a coniare l'espressione Digital Twin fu Michael Grieves, ricercatore e professore presso l'Università del Michigan. Il Digital Twin è dunque una replica virtuale di risorse fisiche, potenziali ed effettive equivalenti a oggetti, processi, persone, luoghi, infrastrutture, sistemi e dispositivi, con vari ambiti di applicazione. A livello ideale un Digital Twin contiene tutte le informazioni dell'oggetto fisico attraverso una rappresentazione tridimensionale dei suoi aspetti a livello meccanico, a livello geometrico e a livello elettronico, ovvero software incorporato, micro-software, dati di prodotto, dati associati a sensori e attuatori, sempre più pervasivi. Grazie al mirroring virtuale in tempo reale gli ingegneri riescono a simulare il comportamento di sistemi complessi riuscendo a prevedere e prevenire guasti meccanici, riducendo così inefficienze e costi.

Vengono utilizzati per vari scopi, in particolare nella Difesa, in produzione e per la manutenzione predittiva. Per l'Industria 4.0, questo approccio è lo stato dell'arte. Con i Digital Twin è possibile testare e capire come si comporteranno i sistemi e i prodotti che si vogliono realizzare in un'ampia varietà di ambienti, usando lo spazio virtuale e la simulazione. I vantaggi sono molteplici, a partire dalla possibilità di accedere facilmente ai dati di molte fonti diverse, aggregarli e visualizzarli attraverso un unico cruscotto centralizzato, sincronizzato e condiviso, potendo aggiungere informazioni contestuali.

In questo contesto, con la consueta attenzione alle nuove tecnologie e alle loro ricadute, AFCEA Capitolo di Roma ha organizza to questo convegno, con l'obiettivo di fornire una presentazione divulgativa del digital twin illustrandone le caratteristiche fondamentali e le potenziali applicazioni. Pertanto, l'evento si è svolto coinvolgendo e mettendo a confronto il mondo accademico e istituzionale con le industrie del settore difesa e aerospazio, che hanno presentato lo stato dell'arte e le possibili evoluzioni in ambito tecnologico e operativo.

Prof. Alfonso PIERANTONIO – Università dell'Aquila – Digital Twin: Modellazione ed Applicazione

C.F. Gianluca MARCIGLI – Navarm – Impiego dei Digital Twin - Esperienze maturate presso NAVARM

Ing. Alessio CAMPANA – ELETTRONICA – Digital Twin methodology in EMSO

C.F. Andrea BERTAGNA – TCol. Marco BIAGINI – Segredifesa V Reparto – Digital Twin, tra immaginazione e realtà: modellare, simulare e proteggere un gemello digitale

Dott. Nicola GRANDIS – Digital Platforms – Intelligenza Artificiale ed IoT per il Digital Twin e per migliorare la sicurezza delle Operazioni

Dr. Marco CHESSARI – Dr. Emanuele BORASIO – Teleconsys – Tecnologie di registro distribuito a garanzia dell'affidabilità del Digital Twin e applicazione in scenari operativi

T.Col. Andrea MERCURIO – Comando Logistico A.M. – Digital Twin: possibili impieghi d'interesse in ambito "Efficienza Linea"

Dott.ssa Roberta COLOMBARI – Leonardo – Digital Twin: un'opportunità per Leonardo

Ing. Marco Evangelos BIANCOLINI – Università Roma Tor Vergata – Messa a punto di Digital Twin mediante simulazioni CAE in pieno dettaglio

SECURING THE FUTURE: EMERGING TECHNOLOGY TRENDS SHAPING THE FUTURE OF DEFENCE

17 NOVEMBRE 2022

Un ambiente di minacce asimmetriche e in continua evoluzione spinge le Agenzie di Difesa di tutto il mondo a ripensare il modo di raccogliere, elaborare, analizzare e distribuire dati geospaziali e intelligence. Per aiutare le comunità della Difesa a risolvere grandi sfide, Hexagon mantiene un dialogo costante a vari livelli con organizzazioni militari, integratori di sistemi e istituti di ricerca.

Questa interazione dinamica, conferma che i progressi della tecnologia giocano un ruolo significativo nel guidare i cambiamenti, anche drastici, nell'industria della Difesa. Con le nuove tecnologie e i nuovi strumenti, cresce la domanda di piattaforme performanti che incorporano nuove capacità per creare un vantaggio strategico e tattico. Come in altri settori, la trasformazione digitale nella Difesa richiede un cambiamento nel modo in cui piattaforme, processi e procedure sono concettualizzati e costruiti.

In questo contesto, AFCEA Capitolo di Roma in collaborazione con la società Hexagon ha organizzato un convegno per illustrare le tecnologie dell'azienda e dimostrare come queste tecnologie rappresentino una componente critica delle innovazioni emergenti nel settore della Difesa.

Durante il convegno sono stati approfonditi differenti temi quali Il cloud tattico, l' Interoperabilità globale, il Digital Twin sul campo di battaglia, l'analisi predittiva, l'autonomia, la gestione dei veicoli senza equipaggio e l'utilizzo dei sensori.

Domingos LOURENÇO – Regional Manager, EMEA, **Giovanni Fumia** – Account Manager, Hexagon – Introduzione

Vincent RIFICI – Director Defense EMEA and India, Hexagon – Securing the future with emerging technologies

Lucio CESARANO – Product Manager brAInt, e-GEOS – brAInt 4DVA: visual support tool for SAR data exploitation

Richard GOODMAN – Saurabh KUMAR – Business Development Presales Engineer, Hexagon – How Hexagon plays a defining role in emerging defence technologies

Derrold W. HOLCOMB – Advanced Sensor Software Manager, Hexagon – An all-seeing eye for defence: synthetic aperture radar

Richard GOODMAN – **Saurabh KUMAR** – Business Development Presales Engineer, Hexagon – Live demonstration of trending Hexagon technologies in defence

COMUNICAZIONI E INNOVAZIONE TECNOLOGICA VERSO NUOVI SCENARI OPERATIVI

8 NOVEMBRE 2022

Sono passati quattro anni dall'ultimo convegno "Le nuove tecnologie per l'evoluzione delle comunicazioni" svoltosi il 27 giugno 2018, presso la SCUTI (Scuola delle Trasmissioni e Informatica dell'Esercito Italiano). Anni che sono stati caratterizzati non solo da una forte innovazione tecnologica, ma anche da stravolgimenti negli scenari geopolitici soprattutto in Europa dopo l'invasione russa all'Ucraina.
Come la guerra in Ucraina ha dimostrato, le comunicazioni svolgono funzioni fondamentali nel contesto di un'operazione militare mantenendo allineate le unità operative e garantendone coerenza, tempestività e profondità, qualora si usino macchine pilotate da remoto. rappresentano la capacità fondamentale nel contesto di un'operazione militare. In questo senso lo scambio sicuro delle informazioni tattiche ha sempre svolto un ruolo fondamentale per il successo delle missioni. In particolare, il trasferimento delle informazioni tra le varie unità coinvolte in uno scenario operativo può, di fatto, modificare gli equilibri nelle fasi di pianificazione, esecuzione ed esito di un'operazione militare. Pertanto, in situazione di crisi, è fondamentale la disponibilità di infrastrutture dedicate (mission critical), svincolate dalle reti commerciali, in grado di assicurare le comunicazioni in un ambiente degradato. L'impiego inoltre di unità "unmanned", ad esempio i droni, magnifica la strategicità della comunicazione sicura integrandola con l'operatività diretta sul campo, aumentando la "profondità'" operativa.
Ne consegue quindi che l'uso di sistemi inviolabili sia nel senso della detezione/distorsione dell'informazione che nella protezione/robustezza dell'infrastruttura diventa elemento determinante nella definizione degli equilibri sul campo.
In questo scenario, durante il convegno si è fatto il punto sull'evoluzione delle nuove tecnologie di comunicazioni, con particolare focalizzazione sulle nuove forme d'onda, previste per le radio software (SDR) e nuovi data link, quali

quelli basati su: l'Integrated Waveform (IW) in banda UHF, i sistemi HF di nuova generazione, waveforms di tipo EPM (Electronic Protection Measures) e NCW (Network Centric Warfare) con Spread-Spectrum e/o Frequency-Hopping. Sono stati inoltre analizzati la Radio over Fiber (RoF) per i collegamenti radio a bordo delle unità navali e gli aspetti legati all'utilizzo del 5G e la sua interoperabilità con gli altri sistemi di comunicazione, come pure sulle comunicazioni satellitari.

Magg. Salvatore SALVAGGIO – Stato Maggiore Esercito VI Reparto – Principali programmi di ammodernamento dei sistemi di comunicazione dell'Esercito
Ing. Alberto LOREDO – Spirent – Radio channel emulation and its applications in the military space
C.F. Andrea RIGANTI – Stato Maggiore Esercito VI Reparto – La tecnologia Software Defined Radio nelle moderne comunicazioni tattiche militari
Ing. Renato IOVINE – IES Srl – Sistemi di comunicazione resilienti di nuova generazione ad elevata affidabilità.
C.F. Matteo FALZARANO – Teledife – European Secure Software Defined Radio (ESSOR) – stato del programma e prospettive future
Alessandro CARLETTI e Guglielmo LULLI – Thales Alenia Space Italia - Importanza delle comunicazioni sicure in situazioni di crisi ed evoluzione tecnologica a sostegno
C.C. Saverio FUMAROLA – Navarm – Telecomunicazioni ed innovazione tecnologica in ambiente Navale
Ing. Cinzia CROSTAROSA – Larimart – Visione prospettica degli equipaggiamenti Larimart, che consentono comunicazioni semplici ed affidabili nei domini applicativi

ARSENALE CYBER: LA NUOVA REALTÀ NEI CONFLITTI IBRIDI

13 SETTEMBRE 2022

I recenti conflitti ibridi (Iran VS USA e Russia vs Ucraina) ci hanno sicuramente reso evidente l'importanza di avere un arsenale di "armi" digitali per preparare, condurre un conflitto ibrido, per destabilizzare il nemico oppure rispondere secondo il proprio schema di cyber difesa e contrattacco. Niente che possa del tutto sostituire lo sforzo bellico per così dire cinetico, ma sicuramente con una forte incidenza sul morale del nemico sia militare che civile. È una situazione che non si manifesta solo a ridosso o in coincidenza di conflitti armati o solo verso infrastrutture militari, ma, ormai come ci insegna la realtà, è un fatto pressoché quotidiano che coinvolge quasi tutti gli ambiti della nostra società, finanziario, sanitario, infrastrutturale, industriale. Disinformazione, attacchi Ddos, Apt di vario genere, Ransomware, Malware attacchi indiscriminati ed asimmetrici verso le infrastrutture critiche del nemico sono tutti elementi per condizionare e destabilizzare un paese.È un attività che sperimentiamo da molto tempo, ma che il conflitto ucraino ha posto ulteriormente in risalto esponendo l 'occidente all'attacco di gruppi eventualmente sponsorizzati da stati avversari e che quindi deve per forza operare per difendere il perimetro digitale dei vari paesi. Tutte le tecnologie disruptive sono utilizzabili per creare danni all'avversario: Quantum, AI, Crittografia di nuova generazione, fake news, fake video, analisi delle vulnerabilità utilizzo di zero days non convenzionali, osint, closint, socmint, fimint, virtual humint etc.

Il Capitolo di Roma di AFCEA International, in tale contesto, ha deciso di organizzare un convegno tendente a stabilire quale è lo stato dell'arte in Italia per la Difesa Cyber Nazionale, quali sono i caposaldi della Difesa Digitale e individuare l'ecosistema industriale a servizio delle nostre forze armate, ma più in generale di tutti i comparti del nostro Paese. La velocità e la dannosità delle minacce impongono una rapidità e flessibilità che probabilmente richiedono anche una maggiore attenzione del "procurement" verso quelle Pmi e start up innovative che possono costituire una risposta decisiva contro i blocchi avversari. Pertanto il convegno si è rivolto non solo ai grandi attori nazionali del cyber ma anche a piccole realtà di grande spessore tecnologico.

L'evento ha ospitato nella prima parte una tavola rotonda, a cui è seguita una sessione di presentazioni specifiche e sono intervenuti rappresentanti del mondo istituzionale, della Difesa, del comparto industriale.

Tavola rotonda: Moderatore **Dott. Marco Braccioli** – CTS Capitolo di Roma

Ing. Domitilla Benigni – ELETTRONICA; **Ten.Gen. Angelo Gervasio** – Direttore TELEDIFE; **Dott. Matteo Lucchetti** – Direttore Operativo CYBER 4.0; **Dott. Alberto Manfredi** – Presidente CSA Italy; **Dott. Elio Digregorio** – Banca d'Italia; **Dott. Gennaro Faella** – SVP Divisione Cyber & Security Solution – LEONARDO; **Prof. Walter Quattrociocchi** – Head of the Data Science and Complexity Lab – Università La Sapienza Roma

Presentazioni

Dott. Fabrizio Cassoni – Fortinet – Kill Chain: Cyber Tools e Security Awareness

Dott. Mirko Leanza – Teleconsys – Sicurezza del dato e minaccia ibrida

Ten. Col. Francesco Passaniti – Comando Operazioni in Rete della Difesa – Il COR e il suo contributo alla sicurezza cibernetica nazionale

Col. GArn Antonio Di Pardo – Teledife – Ruolo e Contributo di TELEDIFE alla Cyber Resilience in ambito Difesa

Ing. Claudio Malavenda – Digital Platform – Capacità CEMA per la difesa dalla minaccia ibrida

Dott. Piero De Loiro – Forescout Technologies – La difesa attiva della tua Enterprise of Things (EOT)

Dott Valerio Fumi – Sistemi&Automazione – Reati e investigazioni nel dominio Cyber e Metaverso

Dott. Alessio Di Benedetto – VEEAM – Il backup come ultima linea di difesa

OSSERVAZIONE DELLA TERRA: SOLUZIONI PER LA CRESCITA TECNOLOGICA E LA RIPRESA ECONOMICA DEL PAESE

9 GIUGNO 2022

L'Osservazione della Terra sta vivendo un momento di particolare rilievo avvicinandosi sempre più alle esigenze degli utenti istituzionali e alla domanda di un settore commerciale in crescita. Gli attori protagonisti di questa sfida sono numerosi e tutti di rilievo come le Istituzioni Nazionali, sia in ambito civile (ministeri, agenzie, ecc.) che difesa (guarda costiera, marina, aeronautica, ecc.), le agenzie spaziali (europea e nazionale), il mondo accademico, con le università e i centri di ricerca, e l'intera filiera industriale dalle Large Company, alle PMI e start-up.
L'Italia da anni occupa una posizione di rilievo grazie alle sue capacità in questo settore con la costruzione di infrastrutture satellitari, del segmento di terra per la gestione degli assetti e del downstream, nonché di servizi in vari settori applicativi.
Per esaminare tale settore in un contesto europeo, il Capitolo di Roma di AFCEA International ha organizzato un convegno cui hanno partecipato rappresentanti della Difesa, delle Agenzie Spaziali, delle Accademie e dell'industria. Il convegno ha rappresentato un'occasione per mettere a confronto tutti gli attori su nuove tecnologie e soluzioni relative all'intera catena del valore, sui servizi tematici (fascia costiera e monitoraggio marino-costiero, qualità dell'aria, movimenti del terreno, monitoraggio copertura ed uso del suolo, idro-meteoclima, risorsa idrica, emergenza e sicurezza) per il PNRR e su altri servizi di carattere commerciale e militare.

Tavola rotonda: Moderatore **Dott. Giorgio Di Bernardo Nicolai**
Simonetta Cheli - Direttore ESA dell'Osservazione Terrestre e Capo dello Stabilimento ESRIN; **Ing. Roberto Formaro** – ASI; **Ten. Gen. Angelo Gervasio** – Direttore Teledife; **Ing. Massimo Comparini** – CEO di Thales Alenia Space Italia; **Ing. Luigi Pasquali** – CEO di Telespazio; **Dott. Giovanni Sylos Labini** – Presidente del Consorzio Osiride; **Gen. B.A. Danilo Morando** – Vice Capo del II° Reparto di SMD.
Presentazioni
Ing. Guido LEVRINI – ESA – La costellazione Iride
Ing. Diego CALABRESE – Thales Alenia Space Italia – Evoluzione dei sistemi spaziali SAR per una efficace risposta alla domanda
Dott.ssa Maria Lucia MAGLIOZZI – e-Geos – Sviluppo prototipi sulla base di dati prisma: qualità delle acque, mappe di combustibili, rilevazione di materiali e indicatori di vegetazione
C.V. Alberto GUERINI – Teledife – Remota videre
Ing. Giovanni FUGGETTA – Leonardo SpA – Prodotti e soluzioni Leonardo per l'osservazione della Terra
Ing. Francesco LONGO – ASI – I programmi dell'Agenzia Spaziale Italiana per l'osservazione della Terra
Ing. Massimiliano EVANGELISTA – Almaviva SpA – Ecosistemi informativi: garantire gli strumenti per orientare gli sforzi della P.A. per la salvaguardia ambientale
Dott. Claudio CARBONI – Esri Italia – Osservazione della Terra e piattaforma Esri per decisioni più veloci ed efficaci
Ing. Paolo SPERA – Consorzio OSIRIDE – Dal segmento spaziale ai servizi, soluzioni operative end-to-end per la costellazione Iride: il Consorzio Osiride
Dott.ssa Sara ZOLLINI – Università dell'Aquila – Integrazione tra immagini ottiche e SAR per l'estrazione della linea di riva
Ing. Valerio GAGLIARDI – Università degli Studi Roma Tre – Nuove frontiere di ricerca applicata: il ruolo dei dati satellitari e NDTS nel campo dell'ingegneria civile

LE TECNOLOGIE PER I SISTEMI RADAR DELLA DIFESA ITALIANA

28 APRILE 2022

Il radar, nella sua continua evoluzione tecnologica e nella diversità d'impiego, continua ad essere elemento fondamentale in campo e o militare per tutti gli ambienti operativi: aereo, navale, terrestre e spaziale. Ovviamente i sistemi devono evolvere tenendo conto da un lato del mutamento degli scenari e delle esigenze operative e dall'altro delle tecnologie disponibili, spingendo al contempo sulla ricerca per poter mantenere un'indispensabile supremazia tecnologica.

Il Capitolo di Roma di AFCEA International ha deciso di organizzare un nuovo evento sull'evoluzione dei sistemi radar nel contesto nazionale per fare il punto su alcuni importanti sviluppi nella progettazione dei nuovi sistemi radar e nel potenziamento di quelli esistenti; sviluppi legati all'evoluzione tecnologica e ai nuovi scenari operativi che richiedono un rapporto costo/efficacia sempre più favorevole, come pure una maggiore attenzione ai concetti di scalabilità e adattabilità a diverse piattaforme e ambienti.

A tale scopo l'evento ha avuto l'obiettivo di analizzare tutti gli aspetti di evoluzione tecnologica quali la digitalizzazione dei vari sottosistemi per incrementare le capacità di scoperta dei target, le funzioni TBM e, per estensione, BMD, la gestione ottimale dello spettro e.m., la capacità di resistenza ai disturbi e agli attacchi cyber, via network e via etere, le capacità SST/SSA per la sorveglianza dello spazio esterno. In quanto elemento di assoluto rilievo va considerata anche la capacità di neutralizzazione dei radar della controparte (jammer) e della possibile integrazione con altri sistemi radar. All'evento hanno partecipato rappresenti della Difesa e del mondo industriale italiani.

Magg. GArn. Andrea VENTIMIGLIA – Ufficio Generale Spazio – Space Situational Awareness (SSA): la Sorveglianza Spaziale della Difesa"

Ten. Col. Stefanino MONTECUOLLO – Stato Maggiore Aeronautica – Programmi di Ammodernamento/ Acquisizione Sensori Difesa Aerea

Ing. Domenico VIGILANTE – Leonardo – Tecnologie e architetture al servizio della Space Situation Awareness: il nuovo paradigma della Integrated Air, Missile and Space Defence

Col. Giovanni RESTA – Teledife – Il Procurement di Radar nella Difesa

C.F. Leonardo LEMBO – Navarm – I sistemi radar navali, storia e sviluppi futuri

Ing. Fabio STERLE – Leonardo – L'Evoluzione dei Radar Navali e Terrestri: dalle tecnologie alle architetture

Ing. Diego CALABRESE – Thales Alenia Space Italia – Tecnologie e radar satellitari: COSMO SkyMed seconda generazione e soluzioni future

Ing. Daniela PISTOIA – Elettronica – Collaborative Threat Engagement: a brick in the future of Electromagnetic Spectrum Operations

Ing. Raffaele FIENGO – National Instruments – Digital Transformation in Test and Evaluation of Phased Arrays Operating in New EMSO

Ing. Giuseppe SAVOIA – Keysight Technologies Soluzioni a segnali misti per il test di moduli T/R digitali (D-TRM)

L'IMPEGNO DI AFCEA CAPITOLO DI ROMA NELLE DISCIPLINE STEM: PRESENTAZIONE DELLE TESI DI MASTER DI SECONDO LIVELLO IN AMBITO "QUANTUM INFORMATION" E "SISTEMI DI COMUNICAZIONE, NAVIGAZIONE E SENSING SATELLITARE"

15 MARZO 2022

Il Capitolo di Roma di AFCEA International da molti anni ha deciso di finanziare borse di studio a favore di rappresentati delle Forze Armate nell'ambito di Master di II livello erogati da primarie Università, in linea con gli obiettivi di promozione delle discipline STEM, fondamentali nei settori d'interesse dell'Associazione e in coerenza con i principi fondanti espressi nel suo Statuto. L'impegno è iniziato nel 2012 con tre borse di studio per Esercito, Marina e Aeronautica, proseguendo annualmente senza interrzioni fino ad oggi, con il Master di II livello in "Ingegneria e Diritto Internazionale dello Spazio nei Sistemi di Comunicazione, Navigazione e Sensing Satellitare" erogato dalla Facoltà d'Ingegneria dell'Università degli Studi di Roma "Tor Vergata". Successivamente nell'Anno Accademico 2019/2020 tale impegno si è rafforzato con l'assegnazione di borse di studio per le tre Forze Armate nell'ambito del Master di II livello in "Optics e Quantum Information" organizzato dal Dipartimento di Scienze di Base e Applicate per l'Ingegneria della "Sapienza", Università degli Studi di Roma. Nonostante le difficoltà dovute al dilagare della pandemia COVID19, risultati sono stati sempre e comunque di altissimo livello come testimoniato dalle votazioni ottenute dai frequentatori dei Master. Al fine di dare evidenza e riconoscimento all'impegno degli Ufficiali frequentatori contestualmente all'assolvimento degli incarichi di servizio, il Capitolo ha deciso di organizzare un evento per la presentazione delle tesi svolte negli ultimi anni accademici, rappresentative dei due Master.

Prof. Concita SIBILIA/Prof. Fabio A. BOVINO – Università di Roma La Sapienza. Presentazione Master di Optics and Quantum Information

Cap. Salvatore DE MATTIA – NATO M&S Centre of Excellence, il Radar Quantistico

Ten. Vittorio CALLIGARIS – Reparto Sperimentale di Volo A.M – Swarm Based Mobile Quantum Network

Ten. Saverio DE VITO – Comando Logistico A.M. - RESIA Quantum Deep Learning: Il caso di studio delle Boltzmann Machines

Marcello Orlandesi – Reparto Sicurezza Cibernetica – E.I.Comunicazioni – Quantistiche Satellitari

Prof. Ernestina CIANCA – Università di Roma Tor Vergata – Presentazione Master in Ingegneria e Diritto Internazionale dello Spazio nei Sistemi di Comunicazione, Navigazione e Sensing Satellitare

Ten. Garn. Veronica VISSICCHIO – Comando Operazioni Spaziali- C.G.I.C. SICRAL Preliminary design of an inter-satellite link for COSMO and SICRAL constellations

T.V.(AN)Filippo MANNI – Stato Maggiore Marina – L'impiego dei sistemi satellitari per la sorveglianza marittima

C.C.(AN) Stefano D'AGOSTINO – Comando delle Operazioni Spaziali (COS) – Sistema di gestione per la sicurezza delle informazioni del Centro Nazionale PRS

Ten. Ing. Vincenzo LAMORTE – Segredifesa IV Reparto – Evaluation of performance and space operations of a geostationary satellite with electrical propulsion

Ten Col. (F)Alessandro GALLIANI – Comando Logistico A.M. – Centro Tecnico per la Meteorologia – CTM – Comparison of total column ozone values collected on board satellite...with data collected at ground...

I contributi dei soci

APPLYING LESSONS LEARNS FROM THE UKRAINE INVASION FOR A MORE SECURE FUTURE

AFCEA INTERNATIONAL LTGEN(R) SUSAN S. LAWRENCE

Russian's invasion in February 2022 of the sovereign and independent state Ukraine—and the annexation of Crimea before that 2014—calls into question not only the regional security of other European nations, but the status of security the world over. The conflict has shed light on the implications of frail critical infrastructure security around the globe, for one, but has also helped shape the advancement of cyber defensive and offensive efforts and even framed how governments, companies and academia train the cyber workforce. For certain, there are lessons to be learned from the kinetic operations as well as how advances in cyber analysis and security can be leveraged during wartime. We can also learn from the rapid and successful deployment of commercial off-the-shelf technologies, the importance of open source intelligence and the use of social media as information warfare, and the tremendous importance and value of actionable information on and off the battlefield.

Early on, U.S. officials and cyber experts braced for what they feared would be a barrage of debilitating Russian-backed cyber attacks, particularly against U.S. critical infrastructure. Perhaps the additional vigilance and the public and private sector rapidly coming together to build resiliency in the Ukrainian cyber domain thwarted the attacks, but they never really materialized as anticipated What did emerge, however, were new pro-Russian activist groups and cyber "hacktivism" against the West.

These new proxy, opportunist groups helped further Russian interests and reportedly share similar tactics, techniques and procedures—especially when carrying out denial of service, or DDoS attacks. Similarly, there is a notable uptick in e-crime associations, another attack landscape that organizations and companies should actively monitor for nefarious activity.

In February 2022, to Russian surprise, Ukraine stood its ground at the aggression and responded with its own dogged military might and a resilient citizenry. Europe and ally nations joined the push back, leveraging economic sanctions against Russia and supporting Ukrainian forces with funds, intelligence and military equipment. The response can serve as a lesson. On the battlefield, commercial technology was deployed at record speeds, putting solutions in the hands of warfighters when and where it was needed most. And while a physical war was fought on Ukraine soil, some warriors were able to join in cyber battles from long distances. Russia, its allies and proxy hacktivists resorted to cyber espionage and scanning tactics, particularly on critical infrastructure and supply chain and financial institution targets, and elevating

A building in downtown after Russian shelling in Kharkiv. Credit: Drop of Light/Shutterstock

efforts to access networks particularly using external-facing remote services. But it's not just the behind-the-scenes actors that go by names such as Killnet, Xaknet, REvil. The implications of global unrest are much broader. Shakespeare wrote "misery acquaints a man with strange bedfellows," and we're seeing this concept play out as Russia aligns itself not just with pro-Russian hacktivists and crime organizations, but with nation-states now working in concert to promulgate Russian interests. It's long been reported of strengthened economic and military alliances between Russia, China and Iran—a move that not only gives Russia new escalation options against Europe and the West, but could even foretell the composition of—and magnitude of— future conflicts.

I shudder at the thought. But organizations like AFCEA International and our Chapter volunteers, like you of the Rome Chapter, are addressing these topics—harnessing the power of our association's membership expertise to set the course for a more secure future. AFCEA activities are designed to open the lines of communication and to facilitate networking, education and problem-solving. The endurance of this conflict—which not only robbed Russia of an anticipated swift victory, could place limits on Russia's conventional escalatory options. As the kinetic conflict approaches the two-year anniversary this coming February and tests Russian resources, will Russia leverage other mechanisms that pose devastating consequences for global security? Will it launch truly debilitating cyber attacks? Or leverage more worrisome alternatives such as nuclear strikes? Already, Russia has weaponized both energy and food, cutting off nations from much resources—and at the height of the coldest of winter months. The possibilities are chilling, and we cannot afford to overlook any element, activity, relationship, alliance or partnership that advances Russian technology or feeds the government coffers and economy.

I wish you all the best. Go and do good work.

Best wishes,

Susan S. Lawrence

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

INTEROPERABILITY AMONGST MEMBER STATES OF NATO AND EU – INCREASINGLY IMPORTANT

AFCEA EUROPE MAJGEN ERICH STAUDACHER

National technological sovereignty – a mantra from the past?

Europe has now entered the times of war – again. After decades of peace, and after decades of debates on strategic independence, with economic and technological autonomy at its core, a turning point of times has arrived for European nations.

After a long time of pursuing national solo runs in producing high class weapon systems in each, at least in the bigger European countries, many factors changed and made European countries start thinking differently. Although cooperation in development, fielding and operating of expansive systems such as aircraft, submarines, and frigates started as early as in the 1970s, the idea of underlining national sovereignty and greatness by proving the national capability to produce weapon system disappeared only slowly. Around 2017, Europe countries owned 17 different types of main battle tanks, 27 different howitzers, 20 types of infantry fighting vehicles. But even at the "tactical level" of military radios, there are hundreds of different types.

This situation has been lamented about in parallel to the debate of autonomy also for decades. Many good reasons have been brought into the debate, mostly, however, in more a hypothetical way:

- If you train and fight together in an Alliance, why not make your equipment more interoperable and interchangeable?
- If you want to deploy and sustain operations, be them peacekeeping engagements or a peer-to-peer competition, why not reducing the logistic footprint by multi-usability of "consumables" like fuel, ammunition, frequencies, IT-modules?
- If you consider costs, you may remember Augustine's law that shows that defense budgets grow linearly but the unit cost of a new military aircraft grows exponentially. "In the year 2054, the entire US defense budget will purchase just one tactical aircraft. This aircraft will have to be shared by the Air Force and Navy 3½ days each per week except for leap year, when it will be made available to the Marines for the extra day." Why not sharing costs by joint production and ownership?

New reasons for interoperability and cooperation

Even if we can admit that already in the cold war era NATO, and recently the EU, undertook significant efforts to harmonize and standardize e.g. by STANAG agreements and joint legislation, it wasn't until lately that military, politicians, and industry realized it cannot continue like this, the mindset needs to change. Many reasons confluently triggered this turning point, let me just highlight a few:

Not only the current **war in Ukraine** opened eyes of Allies and partner nations of NATO and EU. A new NATO strategic concept emerged from the Madrid Summit in 2022, after some time of preparation in view of the ever increasing aggressiveness of Russia. EU's strategic compass, in the making also since 2020, addresses the security challenges for its community of member states in a 360 degree approach. The threat to NATO and EU is imminent, defence spending is up. While some projects in the rising national budgets in Europe are targeting in short term urgent deficiencies by buying available defence goods, others are increasingly funding joint projects. The EU activities in order to strengthen the Defence Industrial Base by identifying joint requirements (EU: PESCO) or supporting multinational programmes with seed money for development and prototyping (EU Commission: European Defence Fund) and helped to prepare the ground for more commonality.

After the pandemic, and reinforced by the Ukraine war, a global **supply chain crisis** troubled mostly the industrialized nations. Transport disruption, shortage in material, loss of small batch suppliers, security issues made it obvious that interchangeability can be key in times of need. Dependencies from other regions of the world, undiscovered at the beginning of the crisis may advocate for national independence, but cooperation amongst Western Allies should be considered from the outset. Not every country of a group of like-minded nations needs an own semi-conductor production.

Emerging and Disruptive Technologies (EDTs) are the talk of the town in Brussels and elsewhere. Opening up the defence world to new technologies from the private sector, with game-changing features, are essential for the Western nations to keep the upper hand in future

conflicts. Digitalization of the Armed Forces is a must for survival on the battlefield, ethical Artificial Intelligence will be indispensable for decision making processes, intelligence, cyber defence, logistics, military health systems and many more. When fielded and handed over to the operators for combat in future, many of the sough-after inventions have an inherent potential of interoperability and may be cast into joint practical solutions. Both, the NATO DIANA project and the European Defence Agency's HEDI hub will have to justify its joint budget's expenditures by provisions for as much commonality as possible. In addition, the dual use and the open source character of so many new technologies (pre-dominantly in the software field) are inherently carrying civil standards which are transnational by nature and support interoperability from the outset. But this applies for future solutions…

The new concept of **Multi-Domain Operations** (MDO) in NATO and its implications regarding command and control will bring a tremendous boost to interoperability. Inter-connecting data sources from allies, civil agencies, societies of many nations in order to gain unprecedented situational awareness and knowledge advantage, including the vast number of assets from the military Internet of things, will not be possible without technological solutions based on seamless interchangeability of data. Conceptually, MDO has arrived as a new and important requirement for all NATO nations, with regard to practical steps such as finalizing architectural solutions (the "data fabric") and the providing technological products in particular "at the edge" the next, coming phase of cooperation amongst nations still lays ahead.

Last, but not least, a new logic for a comprehensive understanding of all relevant elements in the C6ISR (Command, Control, Communications, Computers, Cyber Defense, Combat systems Information, Surveillance, Reconnaissance) universe called **Software Defined Defence** will enforce interoperability in a rather different way: Interoperability will no longer be a mental disposition or something which nations or individuals intentionally need to work on day by day, but something technology will provide automatically. Since technological progress is faster in software than in hardware, and software increasingly determines operational advantage in information superiority, hard- and software should be detached. If data-centricity and Artificial Intelligence/ Machine Learning in future is considered the core element of a combat's system capability and become the emphasis of a system's design, hardware of different origin and state of technology can be interlinked to a really agile, interoperable system.

Interoperability – What is happening right now?

It is NATO's natural interest to improve interoperability amongst its member states. It's definition of interoperability as "the ability to act together coherently, effectively and efficiently to achieve Allied objectives" describes the overarching task from the NATO Defence Planning Process (NDPP) to training and exercises to identifying new capabilities in jointness.

One may consider the whole NDPP a gigantic multi-year process to harmonize the national defence capability plans in order to avoid gaps – and to identify redundancy.

Amongst many others more practical and effective steps are the work of the longstanding Federated Mission Network (FMN), as a multi-national group activity, and the Coalition Warrior Interoperability Exercise CWIX, organized by Allied Command Transformation. FMN aims to "hard-wire" interoperability into the participating nations capabilities and make them ready for a "zero-day" connectivity and operability of a NATO mission. At the annual CWIX, NATO and partner nations are testing command and control capabilities and settings in preparation of upcoming NATO missions such as the NRF. While working closely with industry at CWIX, new and available solutions are tested under the guiding principles of interoperability for future NATO missions. Such solutions are essential for Multi-Domain operations and NATO's ongoing efforts for Digital Defence.

Any other military contingent exercise such as a VJTF certification, crisis-response test, or desk-top exercise, any symposium of one of the numerous NATO Centers of Excellence has an inherent effect towards more mutual understanding and interoperability. Any operational procedure or training requirement which is harmonized at the various international institutions (NATO E3A, European Transport Command, NCIA academy) is a step towards deeper interoperability.

AFCEA's contribution

So are the many activities of European AFCEA chapters and AFCEA Europe, as they support all the endeavors of NATO and EU to provide best-practice information across

nations, exchange of views between industry, academia and military, introduce new ways of thinking. Thanks to the Rome chapter, for example such important subjects as resilient communications, cryptography, artificial intelligence in military applications have been presented recently. Information from other chapters or AFCEA International have influenced the discussion. AFCEA Europe will feature a brand-new transatlantic conference in December 2023 which focusses on collaboration on the battlefield in C5ISR. It is in the genes of AFCEA to support interoperability.

As said, interoperability at all levels strategic, operational, tactical, technological, amongst EU and NATO nations is more needed than ever. AFCEA's support is more helpful than ever. I wish the AFCEA Rome chapter all success in fulfilling this mission.

WEB 3: L'INTERNET DEL FUTURO TRA EVOLUZIONE TECNOLOGICA E INNOVAZIONE SOCIALE

Carmine Cisca

ALMAVIVA

La cosiddetta terza generazione di Internet è più vicina di quanto pensiamo, l'avvento del Web3 apre le porte ad un nuovo modo di essere connessi che sta subendo un'evoluzione profonda e significativa. Questa evoluzione si basa su di un approccio **user-centric** e mette al primo posto le esigenze e i diritti degli utenti.

Siamo di fronte ad un nuovo paradigma che ponendo l'enfasi sulla **privacy** e l'**autonomia** delle persone permetterà loro di recuperare il pieno **controllo dei dati**. Questa trasformazione segna una svolta fondamentale rispetto alla cultura attuale di Internet, dove la condivisione e la **proprietà** dei dati spesso sfugge al controllo degli individui a favore di interessi più ampi.

Nel contesto del Web3, l'identità digitale assume un ruolo primario rispetto al modo in cui si interagisce online. Questa forma di **identità digitale** non solo offre maggiore sicurezza e verifica sugli accessi ai dati personali, ma consente di preservare la propria privacy decidendo chi può accedere alle informazioni sensibili. Inoltre, l'identità digitale nel Web3 facilita **l'interoperabilità** tra diverse piattaforme, grazie all'utilizzo di standard, consentendo una maggiore **fluidità** nell'accesso ai servizi e una migliore esperienza utente.

L'aspetto chiave del Web3 è sicuramente la sua natura **decentralizzata**, in cui i dati e le informazioni non sono più controllati da un'unica autorità centrale, ma vengono distribuiti su diversi nodi della rete. Questo nuovo approccio è reso possibile grazie alla tecnologia **Blockchain**, che introduce il concetto di verificabilità, e ai contratti intelligenti (***smart contract***) che consentono l'automazione, garantendo complessivamente una maggiore **sicurezza e resilienza**. Grazie a questa tecnologia si riduce la vulnerabilità a intrusioni e manipolazioni, ogni interazione sulla rete viene registrata in modo permanente e può essere facilmente sottoposta a audit garantendo una maggiore **trasparenza e responsabilità** nell'uso delle informazioni.

Un ulteriore elemento innovativo è, poi, la possibilità di interagire con l'**Intelligenza Artificiale**. In un contesto in cui l'AI Generativa si fa sempre più strada e diventa più accessibile a tutti, offrendo contenuti artificiali quasi indistinguibili da quelli naturali, questa sinergia tra tecnologie offre la possibilità di garantire la provenienza, la tracciabilità e la proprietà delle informazioni che accompagnano la nostra esperienza utente. Grazie a ciò, il grado di "explainability" della personalizzazione offerta agli utenti su internet potrà essere reso trasparente, sicuro e riconoscibile, offrendo operazioni più efficienti e mirate, in linea con i principi di etica, robustezza e regolamentari (AI Act).

Il Web3 è sinonimo di sicurezza e riservatezza anche per quanto riguarda la **comunicazione** tra membri di **ecosistemi**. Nello specifico, le reti decentralizzate basate su Blockchain consentono una comunicazione criptata, protetta e resiliente, che migliora notevolmente la coordinazione delle operazioni e la risposta alle situazioni critiche. Questo è particolarmente importante in contesti ad alta complessità, come le operazioni militari o di emergenza, dove la tempestività e la continuità delle comunicazioni possono fare la differenza tra il successo e il fallimento.

Le tecnologie Web3 apportano inoltre notevoli miglioramenti alla gestione delle **catene di approvvigionamento** e delle **operazioni logistiche**. Attraverso la tracciabilità delle informazioni, rese immutabili dalla *"notarizzazione"* su Blockchain, è possibile monitorare in modo più accurato il flusso delle risorse, riducendo i rischi di frodi e manomissioni.

Oltre all'evoluzione tecnologica, il Web3 promette, però, anche un profondo impatto sull'**innovazione sociale**. La decentralizzazione delle informazioni e il controllo degli utenti sulla propria identità digitale contribuiscono a garantire una maggiore privacy e sicurezza online in un ambiente digitale **"aperto"** e **"trasparente"**, reso in continua evoluzione dalle community opensource da cui trae la maggior parte delle risorse. Grazie a queste caratteristiche il nuovo ambiente digitale si trasforma in un web più affidabile e fidato, che promuove la condivisione di conoscenze e l'accesso a informazioni verificabili.

Affinché il Web3 plasmi un Internet **sostenibile, partecipativo** e realmente centrato sulle esigenze di tutti i cittadini, il prossimo passo è quello di affrontare l'utilizzo degli strumenti tecnologici in modo responsabile, verificabile e orientato a rendere il *"world wide web"* un luogo virtuale più sicuro e consapevole.

DALLA SICUREZZA FISICA ALLA CYBER-SECURITY: L'APPROCCIO DI ARUBA

Data Center e tecnologie: il ruolo della sicurezza

ARUBA

Fondata nel 1994, Aruba è il principale provider 100% italiano di servizi cloud e il leader in Italia per i servizi di data center, cloud, hosting, trust services, e-mail, PEC, registrazione di domini e firma digitale.
La società si rivolge a privati, professionisti, imprese e Pubblica Amministrazione e gestisce una vasta infrastruttura che comprende 2,6 milioni di domini registrati, 9,4 milioni di caselle e-mail, 8,8 milioni di caselle PEC e 130.000 server, per un totale di 16 milioni di utenti.

In quasi 30 anni di attività, Aruba ha maturato 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 campus – che al momento vede all'attivo già 3 data center dei 5 totali - si trova a Ponte San Pietro, in provincia di Bergamo, ed è caratterizzato da infrastrutture e impianti "green by design" progettati per ridurre al minimo l'impatto ambientale. Ad esso si aggiungono 2 Data Center ad Arezzo ed in intero campus in costruzione a Roma. A livello europeo, il network comprende data center partner in Francia, Germania, Inghilterra, Polonia ed un ulteriore data center proprietario in Repubblica Ceca.
I campus di Aruba sono dotati di soluzioni tecnologiche e di sicurezza all'avanguardia; vantano inoltre strutture e impianti conformi ai più alti livelli previsti dalle normative ANSI/TIA 942 e ISO 22237 che ne garantiscono la resilienza grazie ad una serie di scelte progettuali e realizzative che vanno dalla scelta del sito alla sicurezza fisica, dagli aspetti architettonici ai sistemi antincendio, impianti elettrici e alle infrastrutture di rete.

I requisiti di continuità operativa sono tenuti in considerazione nei processi aziendali già a partire dalla progettazione e il reparto Sicurezza si occupa di gestire scenari di resilienza cibernetica e abilitare una Business Continuity e Disaster Recovery "by design" integrata alla "security -by-design".
Business Continuity per Aruba è un fattore strategico che si esplica nel rendere l'organizzazione resiliente attraverso la capacità di fornire prodotti e servizi entro tempi garantiti e ad un livello predefinito anche a seguito di eventi che possono determinarne un'interruzione. Tali aspetti sono gestiti all'interno del reparto Sicurezza per favorire il costante allineamento tra le funzioni di Business Continuity e Cybersecurity reso necessario dalla crescente vulnerabilità degli asset digitali; solo con la correlazione di aspetti organizzativi, tecnologici e di sicurezza informatica e delle informazioni è infatti possibile fornire soluzioni e risposte adeguate all'evoluzione tecnologica, normativa ma anche a scenari che vedono attacchi informatici sempre più sofisticati.

La gestione delle infrastrutture e la protezione dei dati vengono assicurate seguendo i migliori standard di sicurezza applicabili al settore, comprovati da certificazioni specifiche. Il Gruppo Aruba ha adottato un Sistema di gestione per la Sicurezza delle Informazioni conforme alla ISO 27001, con estensione alle Linee Guida **ISO 27017** (Sicurezza delle Informazioni nei Servizi Cloud), **ISO 27018** (Protezione dei dati personali nei servizi Cloud) e **ISO 27035** (Gestione degli incidenti di sicurezza delle informazioni) per garantire la conformità dei servizi erogati agli standard di sicurezza e alla normativa di protezione dei dati personali considerando la gestione dei rischi ICT.
Sono infine un elemento imprescindibile le attività di awareness e formazione per il mantenimento efficace del sistema di gestione al fine di rendere tutti consapevoli dei rischi e attivare una importante linea di difesa.

Anche il personale è altamente qualificato a livello di competenze. Il reparto di Sicurezza è in grado di fornire protezione e sicurezza ai dati e alle infrastrutture dei clienti attraverso:

- servizi sicuri e resilienti su misura per le loro esigenze specifiche,
- il miglioramento continuo e l'allineamento alle esigenze di conformità,
- il raggiungimento di elevati standard di sicurezza fisica,
- il rilevamento tempestivo e la reazione a minacce e incidenti alla sicurezza.

La sicurezza degli asset dei clienti rappresenta per Aruba una priorità.

AVIOGEI: UN IMPEGNO PER UN FUTURO SOSTENIBILE

Come coniugare innovazione e sostenibilità

AVIOGEI AIRPORT EQUIPMENT

Aviogei, fondata nel 1970 è il principale produttore italiano di attrezzature dedicate all'assistenza aeroportuale. essendo attiva nella progettazione, produzione, certificazione e distribuzione di un'ampia gamma di prodotti per la movimentazione e il trasporto di passeggeri e merci, sia per uso civile che militare.

AVIOGEI con sede amministrativa ad Ariccia (RM), impiega circa 80 dipendenti e gestisce 2 stabilimenti, uno a Campoleone (LT), dedicato alle attività di progettazione e costruzione delle attrezzature, e uno all'interno dell'aeroporto air side di Fiumicino riservato esclusivamente alle manutenzioni e ristrutturazioni testimonianza, di fatto, dell'impegno dell'azienda nel sostenere l'ampliamento della propria offerta di servizi per essere player globale del settore. Nel corso della sua lunga e proficua esperienza maturata nell'ambito delle costruzioni GSE aeroportuali, AVIOGEI ha servito numerosi clienti in 110 paesi nel mondo, progettando e realizzando più di 132 diverse attrezzature suddivise tra scale passeggeri, nastri trasportatori, carrelli portabagagli, loader per merci, carrelli portacontainer e pallet, torri mobili di controllo, rampe per animali vivi, gru portatili, veicoli per la fornitura di acqua e per la pulizia, veicoli per servizi igienici e veicoli per la logistica militare.

La sfida di AVIOGEI è quella di conciliare lo sviluppo tecnologico dei veicoli semoventi con la sostenibilità, dunque, contribuire alla nascita di nuovi paradigmi sostenibili di produzione, trasporto e utilizzo finale dell'energia.
A tale scopo, la società sta seguendo diverse iniziative progettuali in collaborazione con Università ed enti di Ricerca per la realizzazione di innovativi sistemi di propulsione che richiedono un costante confronto con normative in materia di impatto ambientale.

In alternativa all'uso di una motorizzazione endotermica di ultima generazione ed in modo complementare, AVIOGEI ha sviluppato una sua gamma di attrezzature GSE a propulsione totalmente elettrica, inizialmente con l'utilizzo di batterie tradizionali al piombo, per poi passare alle più performanti batterie ai polimeri di litio.

L'impegno profuso nello sviluppo del sistema di propulsione elettrico, ha consentito ad AVIOGEI, di acquisire il Know-how tecnologico necessario per essere leader e all'avanguardia tra i costruttori di GSE, sviluppando una propria strategia di potenziamento e una linea di attrezzature elettriche che annovera, tra gli altri, l'elevatore semovente PRM denominato THUNDERLIFT

Nell'ambito della realizzazione di un sistema di propulsione ibrida, ci si propone, al contempo, di approfondire e implementare soluzioni innovative allo scopo di migliorare le caratteristiche tecniche e funzionali degli equipaggiamenti GSE.

A tal proposito recentemente AVIOGEI ha avviato lo studio di fattibilità per lo sviluppo di una attrezzatura a propulsione ibrida a celle di combustibile alimentata ad idrogeno con annesso sistema di gestione remotizzata al fine di facilitare le attività di manutenzione a distanza.

Il sistema sarà costituito da un gruppo di generazione (a cella di combustibile alimentata ad idrogeno e relativo serbatoio), convertitore, sistema di accumulo (pacco batterie), motore di trazione e relativi accessori. Lo scopo dell'attività che si intende realizzare è quello di verificare la fattibilità e le prestazioni di un sistema di propulsione ibrida, con caratteristiche funzionali di punta, per la movimentazione di veicoli per ambiti aeroportuali. In questa architettura, il sistema ibrido concepito può essere favorevolmente dimensionato per operare in condizioni di rendimento ottimali, mentre i sottosistemi di accumulo di energia elettrica forniscono l'energia assorbita dai picchi di carico. È importante sottolineare che allo stato attuale non sono presenti in ambito aeroportuale esempi simili di attrezzature ibride.

Le sfide davanti a una nuova tecnologia di questa portata sono ovviamente rilevanti, e sono state già intraprese collaborazioni con diversi centri ricerca specializzati volte al trasferimento tecnologico di competenze scientifiche.

NVG, NIGHT VISION GOGGLES, UN AIUTO AL VOLO NOTTURNO

Utilizzo dei visori in missioni HEMS

B.M.A.

Nella base HEMS di Pontives (Val Gardena), dove opera l'organizzazione di soccorso alpino Aiut Alpin Dolomites con un elicottero H135, lavoro io Davide Subrero, Flight Operator Manager di Star Work Sky, l'azienda che gestisce le operazioni del H135 I-AIUT.

Il 26 dicembre 2009, 4 ragazzi del soccorso alpino morirono travolti da una valanga durante un soccorso notturno effettuato a piedi nella zona di Val Lasties. Da quel momento prendemmo la decisione di poter volare anche di notte per portare, in qualche modo, le squadre di soccorso direttamente sul punto dell'incidente, in breve tempo e senza che essi stessi mettessero a rischio la loro vita lungo pendii pericolosi.
La normativa 965/2012 che prevede l'utilizzo degli NVG è stata recepita in Italia nell'anno 2014; dopo un addestramento nel 2015 presso una compagnia svizzera che già da decenni operava con gli NVG, abbiamo conseguito la certificazione nel gennaio 2017.

Abbiamo iniziato ad operare in single pilot con un HEMS crew member e le procedure adottate hanno dato subito risultati molto soddisfacenti. Attualmente operiamo con NVG di terza generazione che permettono al pilota e all'equipaggio di intervenire con serenità e consapevolezza dei rischi circostanti; si può dire che con l'introduzione di questa tecnologia la sicurezza del volo sia notevolmente aumentata perché offre un'ampia visione dell'ambiente in cui si interviene, degli ostacoli e delle minacce che ogni equipaggio deve affrontare per portare a termine una missione HEMS.

Numerosi sono gli interventi notturni effettuati dal 2017 ad oggi, e questa statistica è in costante aumento negli anni, anche perché questa tecnologia offre opportunità di soccorso che prima non si riuscivano a garantire. Alcuni numeri: 19 interventi nel 2017, 72 nel 2018, 78 nel 2019 fino ad arrivare a 129 interventi nel 2022, per un totale di 544 interventi primari negli ultimi 7 anni di attività.
Gli interventi sono frequenti, di conseguenza gli equipaggi che si avvicendano nella base di soccorso di Pontives devono essere sottoposti ad un continuo addestramento notturno, per poter mantenere la currency imposta dalla normativa, ma soprattutto per poter garantire un elevato livello di manualità e conoscenza delle procedure, soprattutto nelle missioni di massima criticità come quelle che necessitano del verricello (Helicopter Hoist Operation o HHO), nelle quali l'equipaggio si trova ad affrontare molteplici task: decollo e atterraggio notturni in aree non conosciute, operazioni di verricello, raggiungimento del target, recupero degli infortunati ecc, sono tutte operazioni che, nella condizione notturna, sono rese possibili dall'utilizzo dei visori e dei fari brandeggiabili dell'elicottero.

Delle operazioni notturne svolte in questi anni mi piacerebbe ricordarne alcune.
Era il 3 gennaio 2020 quando una chiamata del 118 richiese la ricerca di una persona dispersa nella zona del Rifugio Pisciadù. L'elicottero decollò dalla base di Pontives alle 18:45 per svolgere una missione che sarebbe durata circa 2 ore e 40'. In questo lasso di tempo portammo le squadre di soccorso a circa 2500m sulle cime del Gruppo del Sella, una ventina di professionisti con il compito di scendere a valle ed ispezionare i canaloni. Una volta trasportate le squadre, io e la guida alpina Adam Holzknecht iniziammo a perlustrare la montagna e tutti i canali che portavano a valle del rifugio Pisciadù. Grazie agli NVG e alle luci dell'elicottero, verso le 21:00, io ed il verricellista notammo un paio di sci ed una racchetta in un canale; riuscimmo ad indirizzarvi le squadre di soccorso, e in breve tempo fu ritrovato il corpo del giovane alpinista precipitato, purtroppo già senza vita.

Un altro intervento memorabile ebbe luogo in zona Piancavallo, per un alpinista con un ginocchio rotto a quota 2300m. Partiti da Pontives, raggiungemmo la località dell'intervento in circa 25 minuti e con l'aiuto degli NVG e delle coordinate dateci dalla centrale, individuammo subito il punto dell'intervento. Calato il soccorritore con il verricello, provvedemmo al recupero dell'infortunato e del suo compagno nonostante le condizioni proibitive (vento temperatura esterna di -20°); il ferito presentava la rottura di una gamba e una temperatura corporea di 31°. Trasportato subito all'ospedale di Belluno, l'alpinista se la cavò!
Belle o brutte che siano, queste storie oggi le possiamo

raccontare grazie alla possibilità di utilizzo degli NVG ed alla collaborazione con persone che con preparazione e dedizione svolgono il loro importante lavoro.
L'NVG TSO in ambito civile è una vera rivoluzione per il soccorso con l'elicottero in montagna e un ausilio per la sicurezza di tutti gli equipaggi HEMS.

Nota: l'articolo è stato scritto dal Com.te Davide Subrero, Pilota di Star Work Sky e Aiut Alpine Dolomites per B.M.A. Buizza Mazzei Agency, fornitrice dei visori notturni TSO della Ditta Elbit Systems of America

SASE, LA CYBER SICUREZZA DEV'ESSERE DOVE SONO GLI UTENTI: OVUNQUE

BARRACUDA

Come proteggere i team dedicati alla sicurezza dai cyber attacchi? Le domande che questi team si pongono ogni giorno – come difendere efficacemente persone, dati e oggetti nell'epoca del lavoro da remoto e in un mondo data-centrico – si confrontano con un'ulteriore dimensione se il bene da proteggere sono le organizzazioni e le persone che lavorano per garantire sicurezza ad altri.

Tra le altre cose, il rischio e l'impatto di un attacco riuscito possono risultare amplificati. Per fare un esempio, le sospensioni di operatività, il furto e l'esposizione di dati, il denial of service e l'interruzione delle comunicazioni sono dannosi per qualsiasi organizzazione. Ma immaginate l'impatto su squadre di soccorso geograficamente isolate, su unità di difesa o su addetti all'intelligence, e sulle reti operative e amministrative che li supportano.
I criminali possono colpire comunicazioni, email, applicazioni, servizi cloud, dipendenti fuori sede, dispositivi, reti, la supply chain e l'intero traffico di una rete che sopporta tutto il peso della connettività.

La cyber sicurezza deve sapersi adattare. Tenere chiuse porte e finestre non serve quando molti utenti, dispositivi, applicazioni e dati – metaforicamente parlando – stanno in giardino. E non funziona nemmeno mettere in sicurezza tutti gli elementi in modo isolato. Le misure di sicurezza in silos o una gamma di soluzioni puntuali di molteplici vendor aumentano i costi e la complessità, senza offrire un'immagine completa di ciò che accade.

È ora di prendere in considerazione il Secure Access Service Edge (SASE)
In un mercato pieno di acronimi, SASE potrebbe essere l'unico davvero necessario nel 2023.
SASE è un servizio o piattaforma in cloud che coniuga il networking e la sicurezza di rete. Per il primo aspetto, si affida al networking SD-WAN per ottimizzare il traffico e la disponibilità della rete; per il secondo, si basa su sofisticate tecnologie integrate per mettere in sicurezza utenti, siti e oggetti a prescindere dalla loro collocazione.
Una piattaforma unica, con un singolo pannello di controllo che offre agli utenti un accesso sicuro ai servizi richiesti o necessari, nel momento desiderato e ovunque essi si trovino.

SASE offre alle aziende un metodo per connettersi direttamente al cloud, in modo efficiente e sicuro, instradando il traffico in base alle intenzioni dell'utente e a specifici requisiti dell'applicazione richiesta, anziché rispedire ogni volta traffico attraverso il data center per le verifiche di sicurezza. Si ottiene tutto questo sfruttando funzionalità avanzate come il Firewall-as-a-Service e i Secure Web Gateways (FWaaS e SWG). Un'ulteriore ispezione di sicurezza può essere eseguita dai gateway SASE laddove necessario.

I benefici del SASE per le aziende
Implementare una piattaforma SASE aumenta l'integrazione, la visibilità e la sicurezza, e allo stesso tempo riduce la complessità e minimizza la superficie d'attacco. In secondo luogo, il SASE permette alle aziende di consolidare le proprie liste di fornitori di sicurezza, e il consolidamento dei vendor contribuisce all'ulteriore riduzione della complessità e dei costi aziendali.
In terza battuta, il SASE mette a disposizione potenti strumenti per l'accesso sicuro. Nel SASE ciascun utente ha una "identità", che si tratti di una persona, un'applicazione o un dispositivo. Inoltre, ha un "contesto", basato sulla posizione geografica, sull'orario, sulle caratteristiche di sicurezza del dispositivo (per esempio il fatto che il software sia aggiornato e che ci siano strumenti di sicurezza installati, o altro) e sulle applicazioni o servizi in uso o per i quali viene richiesto l'accesso.

Le policy SASE si basano sullo Zero Trust e considerano sia l'identità sia il contesto; inoltre, le policy possono cambiare al mutare del contesto. Per esempio, i requisiti di sicurezza potrebbero variare a seconda che si debba accedere a un'applicazione usando il computer di lavoro dall'ufficio oppure collegandosi con un telefono da una qualsiasi location.

Perché il SASE e perché adesso?
Implementare una soluzione SASE – quella di Barracuda si chiama SecureEdge – aiuta le aziende a mettere in sicurezza i propri utenti e operazioni in un mondo digitalizzato, dove tutto e tutti sono connessi e in movimento. Un mondo al quale le cyber minacce e i cyber attacchi hanno saputo rapidamente adattarsi.

Lo scenario operativo e l'ecosistema delle minacce cyber continueranno a evolvere. Mantenere semplice, scalabile e integrata la sicurezza aiuterà le aziende e i vendor di security a essere pronti per adattarsi a ciò che verrà.

IL RAPPORTO TRA SASE E IOT

BARRACUDA

Il SASE è la convergenza tra connettività e sicurezza e aiuta le aziende a implementare una strategia di sicurezza coerente, adottando un modello decentralizzato nel quale la cybersecurity è fornita direttamente nell'edge, ma tutte le componenti vengono gestite da un singolo pannello di controllo in cloud.
Nell'ambito dell'IoT le aziende gestiscono centinaia, migliaia di dispositivi. Non ci sono limiti di dimensioni, fattore di forma e prezzo del dispositivo, ma alcuni elementi tipici sono gli ambienti dislocati e le sfide di sicurezza. Ed è qui che il SASE può davvero fare la differenza.

Le sfide dell'IoT

Le vulnerabilità nei software dei dispositivi IoT non sono un fatto nuovo. In questi device, infatti, spesso la sicurezza scarseggia perché non viene considerata in fase di progettazione. I vendor di dispositivi solitamente non riescono a tenere il passo con l'installazione delle patch software che sarebbero necessarie per risolvere tempestivamente le vulnerabilità note. Ciascuna patch del software dev'essere accuratamente testata per evitare qualsiasi tipo di malfunzionamento, e l'installazione degli aggiornamenti software su un gran numero di dispositivi, spesso ubicati a distanza, può rappresentare una sfida. Tuttavia, i dispositivi IoT dovrebbero essere considerati sempre 'a rischio'.

Zero Trust per l'IoT

Di seguito, alcuni aspetti da considerare nella scelta di una soluzione IoT:

- Fare attenzione al numero di dispositivi che si vogliono adottare; i deployment in produzione hanno molti problemi di scalabilità ed è necessario tenerlo presente pensando alla crescita futura della rete e alla durata dei dispositivi.
- La connettività tramite LAN, Wi-Fi, 5G/4G/LTE o altre tecnologie richiede un dispositivo hardware. Idealmente, questo dispositivo avrà altre funzioni oltre alla semplice connettività.
- Dei dispositivi IoT non ci si può 'fidare'. Dovrebbero essere isolati da altri dispositivi e mai esposti su Internet. È consigliabile utilizzare un firewall IoT per fornire connettività e sicurezza e non assegnare mai un IP pubblico a un dispositivo IoT.
- È necessario poi mettere in sicurezza le comunicazioni su reti pubbliche e considerare i possibili difetti dei protocolli industriali. Una crittografia aggiuntiva ne impedisce la strumentalizzazione e nasconde le comunicazioni in chiaro. Per bloccare tutte le tipologie di contenuti malevoli serve una tecnologia VPN che protegga le comunicazioni e una sicurezza next-gen, come gli IPS e l'Advanced Threat Protection.
- La comunicazione di rete ammessa da e verso il dispositivo dev'essere ridotta allo stretto necessario. In passato era diffuso l'uso di set di regole firewall basate sugli IP e sulle porte, ma oggi le restrizioni si basano sulle applicazioni con instradamento intent-based.
- Se non c'è un esperto IT in ogni sede, distribuzione e sostituzione dell'hardware devono essere quanto più semplici possibile. Ciò richiede una tecnologia di deployment zero-touch. Chiunque sia presente sul posto deve poter collegare il dispositivo e completare l'installazione. Dell'installazione fisica può occuparsi un elettricista o assistente di vendita, ma le procedure di configurazione e licenza sono gestite da remoto. Questo sistema di deployment dovrebbe funzionare anche al di fuori del normale orario di lavoro.
- Una gestione centralizzata è cruciale per poter applicare i correttivi di sicurezza e gli aggiornamenti firmware e per manutenere le configurazioni dei dispositivi in tale infrastruttura. Sebbene i dispositivi IoT spesso possano sembrare tutti uguali, ognuno è unico e molte aziende necessitano di set di regole di sicurezza e configurazione granulari per poter avere massima fiducia nella propria sicurezza. Questo è possibile solo se esiste un portale gestionale centralizzato, semplice ma potente.
- Non esiste un approccio *fire-and-forget* nella sicurezza dell'IoT. A prescindere da quali siano i dispositivi distribuiti, bisogna sempre dare per scontato che sarà necessaria un'ulteriore adozione o ottimizzazione. È cruciale chiedersi come questi cambiamenti futuri possano essere implementati nel deployment e se si sarà in grado di fare delle modifiche su centinaia di dispositivi dislocati in più ambienti. Se si ritiene che questo non sarà necessario, allora forse si sta applicando una policy di sicurezza approssimativa.

Perché il SASE per l'IoT?

La convergenza di sicurezza e networking è esattamente ciò che serve per consentire ai dispositivi IoT di far parte delle infrastrutture aziendali senza rischi. Gli attuali ambienti ibridi richiedono una connettività sicura per le persone che lavorano da remoto e che accedono a workload in cloud pubblico, on-premise o tramite Software-as-Service. Il SASE è il modello più avanzato per una strategia di sicurezza coerente in tutti gli edge, a prescindere dall'ubicazione.

CRISEL INTRODUCE LO STATO DELL'ARTE NELLE APPLICAZIONI DEI SETTORI DEL BIM, AEROSPAZIO E DIFESA

Benvenuti nell'universo dell'innovazione tecnologica!

CRISEL

Siamo entusiasti di presentarvi tre incredibili articoli basati su soluzioni tecnologiche allo stato dell'arte. Sono esempi di applicativi che aiutano i nostri clienti a definire il modo in cui interagire con la tecnologia, migliorando l'attività quotidiana di chi esegue rilievi per il BIM e i test in aerospazio e difesa.

Rilievo speditivo: elemento essenziale nel flusso di lavoro BIM (Building Information Modeling)

Negli ultimi anni, l'industria dell'architettura, dell'ingegneria e delle costruzioni (AEC) hanno fatto grandi passi nell'adozione del Building Information Modeling (BIM), una metodologia che permette di creare e gestire informazioni digitali dettagliate per un'infrastruttura o un edificio durante l'intero ciclo di vita del progetto. Una componente fondamentale del flusso di lavoro BIM è rappresentata dal rilievo speditivo, un processo che consente di acquisire dati geometrici accurati e completi del sito di costruzione in modo rapido ed efficiente.

Il rilievo speditivo sfrutta tecnologie avanzate come i sistemi di rilievo mobile laser (Lidar) della Stonex l'X120GO, la fotogrammetria e i dispositivi di scansione 3D terrestre come lo Stonex X100 per catturare le caratteristiche fisiche dell'ambiente circostante in modo preciso e dettagliato con tecnologia SLAM (Simultaneous Localization And Mapping) e vSLAM (Visual Simultaneous Localization And Mapping. Questi strumenti consentono ai rilevatori di creare una rappresentazione digitale tridimensionale del sito di costruzione, inclusi gli edifici esistenti, il terreno, le infrastrutture e tutti gli altri elementi rilevanti.

Uno dei principali vantaggi del rilievo speditivo è la sua capacità di ridurre significativamente i tempi di acquisizione dei dati rispetto ai metodi tradizionali, infatti mentre in passato era necessario effettuare rilievi manuali laboriosi e dispendiosi in termini di tempo, oggi è possibile ottenere una quantità considerevole di informazioni in tempi molto ridotti. Ciò consente agli operatori di rilevare e completare il lavoro più velocemente, accelerando così l'intero processo di progettazione e costruzione.

Oltre alla rapidità, il rilievo di questa tipologia offre anche un livello di dettaglio e precisione molto elevato. Le moderne tecnologie consentono di catturare anche i dettagli più minuti del sito di costruzione, inclusi elementi architettonici complessi, sfumature di colore e altre caratteristiche visive. Questo livello di dettaglio consente agli architetti, agli ingegneri e ai progettisti di lavorare con informazioni accurate e complete, migliorando la qualità complessiva del progetto e riducendo al minimo gli errori e le imprecisioni.

Un altro beneficio, nel contesto del flusso di lavoro BIM, è la sua integrazione senza soluzione di continuità con gli altri processi di progettazione e costruzione. I dati acquisiti possono essere facilmente importati in software BIM dedicati, consentendo agli operatori di creare modelli digitali completi e dettagliati del progetto. Questi modelli (digital twin) possono poi essere utilizzati per analisi, simulazioni e coordinamento tra i vari professionisti coinvolti nell'attività e nella comunicazione efficace con il cliente.

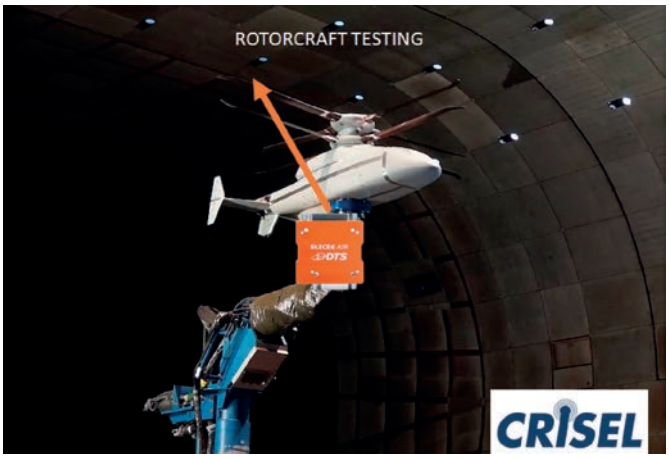
Un esempio concreto di come il rilievo speditivo si integri nel flusso di lavoro BIM è rappresentato dalla modellazione dell'esistente. Utilizzando i dati acquisiti durante la fase di rilievo, è possibile creare una rappresentazione digitale accurata degli edifici esistenti e del contesto circostante. Questo modello digitale fornisce una base solida per lo sviluppo del progetto e consente di evitare costosi errori di progettazione legati alle incongruenze tra il progetto e la realtà fisica.

In conclusione, il rilievo speditivo svolge un ruolo fondamentale nel flusso di lavoro BIM. Grazie alle tecnologie avanzate di acquisizione dei dati, è possibile ottenere informazioni precise e dettagliate del sito di costruzione in tempi ridotti, migliorando l'efficienza e la qualità complessiva del processo di progettazione e costruzione. L'integrazione senza soluzione di continuità con gli altri processi BIM consente di massimizzare i vantaggi di questa metodologia e di realizzare progetti di successo.

Tracciamento e Monitoraggio degli eventi transitori di asset di valore con il TSR Data Logger di DTS Diversify Technology Solutions

La gestione degli asset di valore è diventata una sfida critica per le imprese di ogni settore. Monitorare e tracciare gli eventi transitori che coinvolgono questi asset può garantire la sicurezza, la responsabilità e la massimizzazione del loro valore. In questo contesto, il TSR Data Logger di DTS -Diversify Technology Solutions è una soluzione avanzata per il tracciamento ed il monitoraggio

affidabile degli eventi transitori. DTS-Diversify Technology Solutions, un leader riconosciuto nel campo delle soluzioni di Test & Measurement, propone il TSR Data Logger che fornisce: **Registrazione dei dati**, è in grado di registrare una vasta gamma di parametri come la temperatura, l'umidità, le vibrazioni, la posizione GPS e molti altri, a seconda delle esigenze specifiche della funzione. Questi dati vengono registrati in modo continuo o in base a eventi predefiniti, consentendo un monitoraggio completo delle condizioni in cui l'asset si trova durante tutto il suo ciclo di vita. **Tracciamento GPS**: è dotato di un modulo GPS integrato che consente di localizzare in tempo reale l'asset di valore. Ciò consente di tracciare la posizione dell'asset durante il trasporto o in caso di smarrimento, migliorando notevolmente le possibilità di recupero. **Allarmi e notifiche:** è in grado di generare allarmi e notifiche in tempo reale in caso di anomalie o superamento di soglie predeterminate. **Interfaccia user-friendly e analisi dati:** offre un'interfaccia intuitiva che consente agli utenti di accedere e analizzare facilmente i dati registrati. In conclusione il TSR Data Logger di DTS- Diversify Technology Solutions, offre una soluzione affidabile e avanzata per il tracciamento e il monitoraggio degli eventi transitori degli asset di valore elevato grazie alla registrazione dei dati, al tracciamento GPS, agli allarmi e alle analisi dei dati, in questo modo le aziende possono garantire la sicurezza, la responsabilità e la massimizzazione del valore dei loro asset.



DTS - Diversify Technology Solutions Slice6 Air: Dati su vibrazioni, sollecitazioni e tensioni – senza la necessità di slip ring

Nell'ambito del Flight & Rotor Testing, la raccolta accurata e affidabile dei dati sulle vibrazioni, sollecitazioni e tensioni è di fondamentale importanza per garantire la sicurezza e l'affidabilità delle attrezzature e dei veicoli aerei. In passato, l'acquisizione di tali dati richiedeva l'uso di complessi sistemi di trasmissione basati su slip ring, che potevano essere costosi, ingombranti e soggetti a usura nel tempo. DTS Diversify Technology Solutions produce lo Slice6 Air che rappresenta un'innovazione significativa nel campo del Flight & Rotor Testing. La tecnologia all'avanguardia utilizzata in Slice6 Air consente di acquisire dati precisi sulle vibrazioni, sollecitazioni e tensioni. Grazie alle sue dimensioni e peso ridotti lo Slice6 Air consente la rimozione degli slip ring e semplifica notevolmente l'installazione e l'utilizzo dei sistemi di acquisizione dati nel contesto del Flight & Rotor Testing eliminando anche la necessità di manutenzione periodica degli slip ring, risparmiando tempo e costi operativi. La tecnologia di acquisizione dati di Slice6 Air è stata progettata per garantire una precisione e una affidabilità senza compromessi. Con sensori altamente sensibili questo dispositivo è in grado di raccogliere dati accurati sulle vibrazioni, sollecitazioni e tensioni durante i test di volo e dei rotori. Ciò consente agli ingegneri e agli operatori di prendere decisioni avendo informazioni accurate e migliorare la progettazione, l'affidabilità e la sicurezza delle attrezzature e dei veicoli aerei. Inoltre, la sua resistenza alle condizioni ambientali estreme e alle vibrazioni garantisce un funzionamento affidabile anche in situazioni critiche. Grazie alla tecnologia innovativa di DTS - Diversify Technology Solutions, gli Slip Ring non sono più necessari per la raccolta di dati sulle vibrazioni, sollecitazioni e tensioni nel campo del Flight & Rotor Testing. Lo Slice6 Air offre una soluzione affidabile, precisa e conveniente per acquisire dati critici durante i test di volo e rotorici. La riduzione dell'ingombro e dei costi di manutenzione, garantiscono la sicurezza e l'affidabilità dei propri veicoli aerei senza compromettere la qualità dei dati raccolti.

IL MODEL-BASED SYSTEMS ENGINEERING (MBSE) PER LO SVILUPPO DI SISTEMI COMPLESSI: L'APPROCCIO DI DASSAULT SYSTÈMES

DASSAULT SYSTÈMES ITALIA

La trasformazione digitale del mondo militare prevede l'utilizzo di un grado elevato di tecnologia lungo l'intero ciclo di vita dei sistemi e mezzi utilizzati dalle Forze Armate. Le funzionalità sofisticate dei sistemi di nuova generazione, però, non sempre vengono sfruttate appieno. A volte, infatti, i team di ingegneri si occupano delle attività di analisi, design, sviluppo, testing e validazione in modo indipendente e senza coordinazione. Si generano così grandi quantità di dati difformi che rendono poi complessa la condivisione tra i vari reparti produttivi della conoscenza, delle metodologie e di eventuali criticità riscontrate lungo il processo.

La soluzione a questo problema è data dal **Model Based System Engineering (MBSE)**, un approccio collaborativo orientato alla gestione requisiti, alla progettazione, all'analisi, alla verifica e alla validazione nei processi di progettazione e sviluppo di sistemi complessi. Contrariamente agli approcci tradizionali dell'ingegneria di sistema, principalmente incentrati sulla redazione di documenti tecnici in grado di descrivere caratteristiche e funzionamento, l'MBSE si focalizza sulla creazione e l'utilizzo di modelli di dominio quale mezzo principale di progettazione e di scambio di informazioni.

Grazie all'utilizzo dell'approccio MBSE, gli ingegneri 'parlano' la stessa lingua attraverso l'uso di modelli, favorendo così l'integrazione dello sviluppo dei componenti meccanici, elettrici, elettronici e informatici in un'unica piattaforma. È possibile modellare un sistema interdisciplinare e simularne gli aspetti funzionali, logici e fisici in modo completo, arrivando a comprendere sia la visione d'insieme sia la visione di dettaglio lungo l'intero ciclo di vita. Si tratta del cosiddetto **gemello virtuale (Virtual Twin)**, non solo una replica digitale del sistema, ma un modello virtuale che permette di simulare molteplici soluzioni e scenari alternativi e consente di seguire la sua evoluzione nel tempo. Il Virtual Twin rimane connesso al sistema fisico e può integrare i dati sul comportamento reale. Questo feedback virtuoso tra simulazione virtuale e verifica nel mondo reale costituisce un asset imprescindibile per raggiungere l'eccellenza nelle prestazioni. Il digital twin viene comunemente definito come una rappresentazione digitale, un modello software che rispecchia un oggetto, processo o sistema del mondo reale. Con il concetto di «Virtual Twin Experiences» ci spingiamo oltre, andando a visualizzare, modellare e simulare anche l'ambiente in cui l'oggetto, il processo o il sistema sarà inserito e le esperienze di chi ci interagirà e lo utilizzerà nella realtà. Tutto ciò permette di accelerare in modo significativo l'innovazione e migliorare la collaborazione dell'intero value network.

Grazie al Virtual Twin e al MBSE è quindi possibile realizzare sistemi sempre più complessi in modo semplice, ottimizzando ed apportando le migliorie al gemello digitale ben prima di arrivare al prodotto finale, evitando così costosi sprechi; i modelli virtuali ottenuti, inoltre, sono riutilizzabili e adattabili, e consentono di risparmiare tempo e denaro nello sviluppo di progetti futuri.

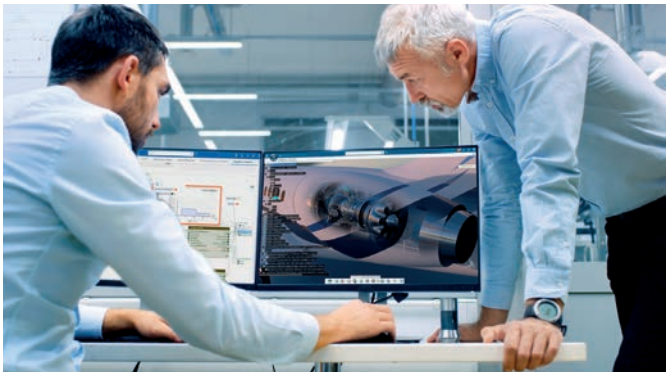
La piattaforma 3DEXPERIENCE di Dassault Systèmes

Gli universi virtuali basati sulla piattaforma 3DEXPERIENCE di Dassault Systèmes contribuiscono ad accelerare l'innovazione sostenibile e ad abilitare una produzione più flessibile, generando valore sia per le aziende che per le Forze Armate. I vantaggi dell'utilizzo degli applicativi scalabili e personalizzabili della 3DEPERIENCE si esplicano non solo a livello di produzione, ma anche per la progettazione e la gestione degli asset della Difesa lungo il ciclo di vita migliorando l'esperienza degli utenti finali e offrendo nuovi strumenti di feedback volti a ridurre le richieste di assistenza.

La soluzione Catia, basata sulla piattaforma 3DEXPERIENCE, offre la capacità non solo di modellare qualsiasi prodotto o sistema attraverso il suo ambiente di progettazione CAD, ma di farlo nel contesto del suo comportamento atteso, grazie alle sue applicazioni MBSE. In questo modo architetti di sistemi, ingegneri, progettisti, professionisti e collaboratori condividono gli strumenti per sviluppare e definire sistemi di successo.
L'ambiente collaborativo, sicuro e affidabile di CATIA è disponibile on premise e on cloud, e permette agli attori coinvolti nel progetto di utilizzare i dati quando necessario, rendendoli subito disponibili per la massima agilità dei flussi di lavoro, e in tutta sicurezza grazie all'assegnazione di ruoli specifici.

L'approccio sistemico per portare la modellazione ad un livello superiore

Un importante risultato da parte di Dassault Systèmes è stato quello di portare la modellazione oltre il tradizionale focus sull'hardware, un passaggio dai prodotti alle "esperienze" in grado di abbattere i silos tra hardware e software. Un approccio che ha concesso di attrarre diverse tipologie di utilizzatori che hanno sfruttato la soluzione di Dassault Systèmes per migliorare la *user experience.*



Sono molteplici i campi di applicazione che possono trarre beneficio dal MBSE e dall'ingegneria dei sistemi. La soluzione CATIA basata sulla piattaforma 3DEXPERIENCE è oggi usata con successo nei settori aerospaziale e difesa, automobilistico, navale, energetico, high tech e medicale. Grazie all'approccio MBSE è possibile risolvere anticipatamente la maggior parte delle problematiche, nonché prendere le giuste decisioni nelle fasi iniziali del processo di sviluppo riducendo rischi e costi, ed abilitando processi di progettazione al passo con prodotti sempre più innovativi e complessi che mettono al centro l'esperienza dell'utente finale.

Le Forze Armate sviluppano sistemi sempre più complessi che richiedono integrazioni e test significativi, MBSE diventa sempre più prezioso come strumento di ingegneria dei sistemi anche in ambito aerospaziale. Grazie alla sua capacità di ridurre gli sprechi e promuovere l'efficienza e la collaborazione durante tutto il processo di sviluppo del sistema, MBSE è un'innovazione che darà un chiaro vantaggio.

Il *Digital Engineering* e l'approccio MBSE sono quindi abilitatori tecnologici cruciali dell'innovazione strategica e sostenibile. Dipartimenti della Difesa internazionale già fanno affidamento su una solida ingegneria dei sistemi per sviluppare gli armamenti, i satelliti e i sistemi di comunicazione necessari per mantenere la superiorità sugli avversari. I recenti progressi tecnologici hanno reso il MBSE una soluzione praticabile, soprattutto in ottica *"System of Systems"*. Un campo di battaglia digitale, in cui gli utenti possono creare ambienti sperimentali customizzati per esplorare una particolare tecnologia, pianificare una missione, validare o concettualizzare le operazioni mediante *war-gaming* o forme di addestramento avanzate, non può più prescindere dall'applicazione delle metodologie di MBSE e del Virtual Twin.

"SPLINTERNET": LA LIBERTA' PERDUTA DEL WORLD WIDE WEB

Marco Braccioli - Executive VP Defence & Cybersecurity

DIGITALPLATFORMS

Internet è sempre stato una Pangea geologica americana e guidata dallo sviluppo tecnologico e dall'impronta culturale americana. In tempi recenti si sta assistendo a una progressiva deriva dei continenti con Paesi come la Russia, che attraverso proxy nazionali possono divenire isole Internet quando vogliono, dove si parla russo, dove si scrive in cirillico non traslitterato e si paga solo con la carta di credito Mir, che è l'unica accettata nel loro circuito e-commerce. In altre parole Internet passa per dei nodi controllati dallo stato e lo Stato può intervenire a suo piacimento, in altre parole crea un Proxy Nazionale di controllo di tutto il traffico Internet. Molti Paesi cominciano o hanno cominciato ad essere tentati da questo modello, che sancirebbe se non la fine della globalizzazione digitale del web, almeno una sua forte balcanizzazione con una naturale perdita di quella matrice un po' anarchica ma anche democratica che per anni è stata la Netiquette del Web. Nascono così nuove cortine digitali di ferro, che limitano la libertà degli user internet di diversi paesi e tendono a controllare comportamenti anomali, comportamenti critici o antagonisti. Del resto, già qualche anno fa l'allora Ceo di Google Schmidt immaginava Internet divisa in futuro in blocco cinese e americano. Proprio su queste basi nasce lo "Splinternet" che trasforma il mito della terra della Libertà digitale senza frontiere in un sistema di reti sorvegliate, spesso chiuse ai rapporti esterni per paura di contaminazione culturale o di minaccia ibrida. Va anche detto che spesso la minaccia è lo spauracchio per obbligare gli utenti di certi paesi ad usi parzializzati della rete. Anche i giganti del web si stanno piegando alla frammentazione: i GAFA (Google, Amazon, Facebook e Apple) stanno imponendosi autolimitazioni dei loro servizi alle barriere, ai firewall, alle circonvenzioni imposte da certi governi pur di rimanere in certi mercati. Questo rigido controllo digitale cinese per assurdo, si è dimostrato un plus valore durante la lotta alla pandemia Covid, adottando una biopolitica digitale basata sui big data disponibili attraverso i providers cinesi cosa che da noi sarebbe impensabile senza consenso del utente e senza il controllo delle autorità per la Privacy. Sapevano tutto di ogni cittadino. Se dovessimo analizzare lo "splinternet" tra Europa, USA e Cina e Cina like, avremmo tre differenti risposte di utilizzo della rete: Europa proteggere gli users, Usa responsabilizzare gli users e Cina controllare gli users, prevedendo rispettivamente regole pesanti (GDPR) in Europa, regole leggere negli USA e rigide direttive statali da parte delle autorità Cinesi nel terzo caso. Del resto l'organo di controllo del web è ICANN (Internet Corporation for Assigned Names and Numbers), che risiede in Usa sottostando alle leggi americane, ecco perché ' chi ha valutato seriamente in Cina il tema della sovranità digitale ha voluto un proprio, quadro giuridico, hardware e protocollo di instradamento, il "The Golden Shield" in Cina che noi occidentali chiamiamo "The Great Firewall". In fondo queste sono le paure legate ai fornitori di tecnologia 5/6G Cinesi questa forte dipendenza dal loro Stato Centrale che il Patto Atlantico sta cercando di fronteggiare. Altri paesi però ne hanno seguito l'esempio, nel 2019, la Duma russa ha approvato una legge che sancisce l'indipendenza di Runet (il cyberspace russo). Le autorità hanno già testato nello stesso anno la "secessione "tecnologica dal world wide web. Elencare tanti paesi che ricorrono a pratiche censorie per la loro rete stupisce ma è anche indice dell'insicurezza del mondo che viviamo, la rete ha perso la sua fanciullezza, la sua anarchia, il suo potere di arrivare alla gente e viene avvertito dai Governi Autoritari come uno splendido modo per controllare i propri cittadini. Oltre Russia e Cina, l'Etiopia, Corea del Nord, Bielorussia, Siria, Arabia Saudita, Vietnam, Sudan, Camerun, Guinea, Ciad, Venezuela, Uzbekistan, Somalia, Eritrea e soprattutto Cuba, Turchia e Iran che stanno sviluppando un proprio ecosistema digitale per la rete, in altre parole questi Governi vogliono controllare le proprie Reti Nazionali per impedire ai cittadini di accedere a notizie che sveglino le coscienze e mettano in cattiva luce i propri Governanti.

TOC (BE) OR NOT TOC (BE)? THAT IS THE QUESTION!

ENAV

"Ci sono più cose in cielo e in terra, Orazio, di quante ne sogni la tua filosofia"... parafrasando il principe Amleto anche ENAV e Techno Sky (di certo più modestamente di Shakespeare, ci mancherebbe), sanno bene che ci sono tante cose in cielo e altrettante che, in terra, permettono alle prime di attraversare quello spazio celeste in sicurezza, puntualità e serenità. E sono, sì, il traffico aereo e tutto il sistema tecnologico (e umano) che quel traffico dirige, sorveglia e aiuta ad essere il modo più veloce e moderno di viaggiare; un vasto e corposo dispiego di mezzi e azioni che necessita, per la propria complessità intrinseca, di essere gestito in modo altrettanto moderno e razionale. Torri di controllo, RADAR, aiuti per la radionavigazione, comunicazioni e sistemi di supporto come il condizionamento o l'energia possono essere pensati, quindi, come un complesso orologio che deve sempre e comunque segnare l'ora...giusta!

Non può mancare allora... l'orologiaio: ENAV e Techno Sky lo hanno ideato e sviluppato come un sistema di controllo che, allo stesso tempo, è accentrato in una sede singola (Roma ACC, il più grande centro di controllo RADAR europeo) e distribuito operativamente su tutto il territorio nazionale: il **TOC**, che si presenta fisicamente come una (molto) grande sala di regia tecnica. Ma "chi" è, "cosa" è davvero questo TOC? L'acronimo un po' ci aiuta: è un *Centro Tecnico Operativo* (Technical Operation Centre) con il quale ogni attore della rappresentazione che ogni giorno è messa in atto per garantire il traffico aereo si misura e agisce. Come funziona? Cosa lo anima "dentro", qual è il suo vero motore? La risposta sta, secondo noi, nel citarne alcuni elementi fondanti:

- Il TOC è stato interamente progettato e realizzato da Techno Sky: è dunque il frutto di esperienza maturata da anni (decenni!) nel settore manutentivo su impianti e sistemi *mission critical*
- Il TOC è orientato, come prima ricordato, ai domini fondamentali dell'elemento tecnico che asserve il Controllo del Traffico Aereo (**Sorveglianza**/RADAR; **Comunicazioni** di ogni tipo, terra/bordo/terra, fonia, dati; **Navigazione** – Radiofari e RadioAssistenze; **Software (ATM)** di gestione del traffico aereo in volo e di partenza/arrivo e molto altro, **METEO** per le necessarie informazoni sullo stato del tempo atmosferico eccetera), con l'obiettivo di gestirne i meccanismi sempre più profondamente ed intimamente. Il TOC tende, quindi, all'incremento della *Safety* nelle Operazioni; a centralizzare la *governance* e standardizzare i processi, rendendoli univoci e chiaramente applicabili in ogni contesto; a ridurre i tempi di intervento di ogni problematica con la possibilità di agire sempre più efficacemente a distanza
- Il TOC rappresenta, proprio per questo, l'evoluzione sempre più spinta dei sistemi e dei processi *core* della manutenzione
- Il TOC è il "filo" che unisce, accorcia e sempre più unirà ed accorcerà le distanze tra le strutture territoriali

Il TOC, perciò, è stato pensato per dare una svolta profonda al lavoro di tutti coloro che sono immersi nel controllo del traffico aereo, per essere non soltanto un mero *strumento* operativo ma una rivoluzione nel modo di concepire (ed agire) *Tekhne* che, se per i greci antichi era la personificazione dell'Arte, dell'abilità e della perizia professionale, per noi è la sempre più profonda padronanza delle regole del nostro "mestiere"; non ultima, infatti, la considerazione che il TOC non è animato da un'Intelligenza Artificiale ma è fatto di *persone* che, convivendo in una stessa sala e rappresentando sistemi e strutture diversi, concorrono a rendere tutto unito da questo spirito.

Il TOC, insomma, è e sarà sempre più il sale della nostra vita lavorativa; è il domani che è già qui e che opera nel nostro presente, è un'anticipazione in presa diretta di quello che accadrà prossimamente, quando l'automazione *intelligente* dei processi del nostro lavoro sarò sempre più spinta e - governata dalla volontà di agire per il meglio – più capace di garantire sicurezza, affidabilità ed efficienza. Shakespeare e il suo Principe di Danimarca ci vengono per fortuna ancora una volta in aiuto: per noi, *Essere o non Essere* (il futuro) non è un dilemma, il TOC ci sta già dicendo che la risposta giusta è la prima!

THE CHANGING CONTOUR OF AIR THREATS: THE ROLE OF EMSO IN FUTURE AIR DEFENSE SCENARIOS

By Daniela Pistoia – Corporate Chief Scientist @ ELT Group
Emanuele Ermini – Scientist Office, Scenario Expert @ ELT Group

ELETTRONICA

Introduction

Since the raison d'etre for the existence of air defense on land, sea or in the air is to counter an adversary's air threats an assessment of these, both in terms of quality and quantity, must be the starting point for all deliberations on air defense.

The terms "air threat" implies the cumulative potential danger which our adversary holds as his ability to cause damage (to physical infrastructure and/or information and data) to our vulnerabilities. The adversary can achieve this through the use of aircraft and airborne ordnance and munitions in furtherance of, or in support of their military effort. This danger can be assessed in two dimensions: The first is the qualitative dimension. This includes the lethality, severity, and technological condition of the adversary's air threat vehicles. The second is the quantitative dimension regarding the numerical strength of this air threat. As a riposte, the defender aims to assemble land, sea and air resources to counter this threat. Thus, the air threat on one side and air defense on the other are tied to each other in a continuous cause-effect relationship.

The multi-dimensional growth of air threats over time has mainly taken place along two major axes. The first is the multiplicity of air threats. The erstwhile duo of fixed- and rotary-wing aircraft as the main threat vehicles, are today joined by a multi-dimensional strike punch. This comprises Uninhabited Aerial Vehicles (UAVs), tactical ballistic missiles, cruise missiles, precision guided munitions, Anti-Radiation Missiles (AAMs) and emerging soft-kill offensive weapons. The latter includes offensive cyberwarfare capabilities using wireless links as their delivery systems.

The other axis is the threat's spatial growth in the three dimensions of range, altitude and temporal applicability. Today, air threats can perform deep strike with precision and accuracy from long ranges by standing off hundreds of kilometers away beyond the defenders' sensory domain. Multiple threat vehicles can strike at any time of the day or night and remain nearly invisible to defenders' radars. UAVs, with their multiple intelligence-gathering and kinetic capabilities can hit targets with both hard and soft kill munitions.

Current Concepts of Employment

Generally speaking, Ground-Based Air Defense (GBAD) is a multi-layered concept. Doctrinally, GBAD faces incoming threats using a plethora of hard- and soft-kill countermeasures with different interception altitudes and ranges. An approaching air threat must pass these multiple shields of intercepting fighters armed with Air-to-Air Missiles (AAMs), Surface-to-Air Missiles (SAMs) and finally Anti-Aircraft Artillery (AAA). These greatly frustrate the ability of the air threat to home in on its intended target. This section analyses two aspects relevant to current concepts of air defense employment and their evolution over time. We will answer the following two questions:

1. Why hard-kill capabilities like AAMs, SAMs and AAA alone are not adequate?
2. Why is an integrated family of air defense resources necessary?

Why Hard-Kill Capabilities Alone are not Adequate?

Air defense exists for the sole reason of protecting one's own selected vulnerabilities from an adversary's air threat. Qualitative and quantitative developments in the air threat's severity over time is tied to the development of GBAD weapon systems in a cause-effect relationship. To this end, a process of metamorphosis in GBAD concepts, doctrines, procedures and assets is observable over time:

- In the early 1960s the air threat was mainly prosecuted by fixed- and rotary-wing aircraft. . Both first- and second-generation aircraft types were primarily for use in clear weather. They were equipped with forward-firing guns, unguided bombs and rockets.
- Vulnerable Areas/Points (VA/VP) requiring GBAD protection were limited and essentially required protection from the above aircraft largely executing the terminal phase or 'end game' of their attack in the visual domain.
- The resulting trend was to deploy multiple ring of AAA around potential targets providing point defence, or to increase the density of guns surrounding a VA/VP.
- As time went by two dimensions of the air threat became increasingly visible. The first was the multiplicity of air threat vehicles. The second was the exponential rise in their range and altitude. Aircraft and helicopters were joined by UAVs and their armed Uninhabited Combat Aerial Vehicle (UCAV) counterparts, cruise missiles, ARMs and more. Technological developments facilitated the introduction of all-weather capabilities for aircraft, longer ranges, and the ability to perform deep strikes with precision- and stand-off capabilities.
- These trends continued exponentially over the subsequent

years. Eventually, AAA systems which just a few kilometers range and a few thousand feet of engagement altitude became largely inadequate for engaging all-weather air threats equipping with precision-guided weapons.

Why is an Integrated Family of Air Defense Resources Necessary?

- The sheer numbers of VAs/VPs witnessed an exponential rise as more assets came under the "attackable reach" of constantly evolving air threat vehicles. It soon became impossible to protect each one of them using point defense concepts. Furthermore, point defence proved ineffective in the face of all-weather, multiple-platform, multiple-layer, multiple-ordnance air threats delivered with increasing precision from stand-off ranges.
- Defenders realized that, instead of the point defense of single VAs/VPs, it was necessary to create an area air defense capability at the theatre or strategic level. This took the form of Integrated Air Defense Systems (IADSs). An IADS could be deployed to protect a specific territory or area, such as a nation's airspace. An IADS could also be deployed into the field to protect theatre-level deployments of ground forces, for example. Integrated Air Defense Systems could detect threats at long ranges and engage these targets using GBAD weapons in successive range and altitude brackets from long-to-medium, and short-to-terminal ranges.
- The birth of the IADS during the Second World War triggered the concept of layered and tiered air defenses. This provided theatre-wide or strategic defense by using Long Range (LR), Medium Range (MR) and short range/very short-range sensors and weapons. These created overlapping areas of range and altitude kill zones with seamless switching from one weapon system to the other as the target traversed the defended airspace.
- As technology advanced, the basic concept of layered and tiered defense was further enhanced through the adoption of state-of-the-art sensors and weapons. These were networked into associated Battle Management Command and Control (BMC2) systems. Although this networked concept had been pioneered by the Royal Air Force and Luftwaffe (German Air Force) during the Second World War, the advent of solid-state electronics and digital communications from the 1960s greatly improved the IADS' efficacy.
- As we fly deeper into the 21st century, new threats are emerging at breakneck speed. UAVs and UCAVs of all sizes continue to perform dull, dirty and dangerous missions. However, they can now work closely with inhabited aircraft exploiting Manned-Unmanned Teaming (MUT) concepts. Today's and tomorrow's threats are hallmarked by all-weather, all-aspect stealth, nano-technology driven structurally lighter and stronger airframes with minimal radar, thermal and acoustic signatures, common data links providing seamless connectivity across dissimilar platforms, high survivability in hostile electromagnetic environments and ever- increasing stand-off ranges.

To sum up, the following concepts of employment emerge for IADs to counter contemporary and future threats:

- An integrated family of GBAD systems is required, consisting of AAA and SAMs stretching from very short range to short range and medium-to-long range.
- A combination of active and passive multispectral radio-frequency and optical sensors, hard- and soft-kill weapons including AAA, missiles and electronic attack systems, and fully-integrated BMC2 systems capable of seamlessly integrating similar and dissimilar systems are required to equip an IADS.

EMSO as a Force Multiplier

Electromagnetic Spectrum Operations (EMSO) can make a valuable contribution to GBAD.

Recent and ongoing conflicts have underscored how UAVs and UCAVs can lessen the capabilities of radar-based air defense systems. Uninhabited aircraft possess great maneuverability, have low Radar Cross Sections (RCSs) and can launch unexpected attacks, including cyberattacks. They hide easily in the Earth's contours which, together with their low RCSs make them difficult to detect by radar. Furthermore, the evolving abilities of UAVs and UCAVs to fly in coordinated swarms can saturate the tracking functions of conventional radars. Furthermore, in wartime ground-based radars must be operated judiciously lest their signals invite attack by suppression/destruction of enemy air defense weapons like ARMs.

Contemporary warfare environment calls for immediate reactions as information concerning an enemy's position or their intentions to launch a surprise attack may only become available at short notice. Consequently:

- Air surveillance should not rely exclusively on radars, but should use other sensors to obtain situational awareness without the emission of radio signals which can be used by an adversary to cue weapons or fires onto those radars.
- Defensive strategies should be developed which can neutralize rather than destroy which may help reduce the danger of escalation.

Air defense's ultimate goal is the kinetic engagement and destruction of the target. Nevertheless, an analogous goal

must be to deny the adversary the accomplishment of their mission. This is especially relevant regarding intelligence, surveillance and reconnaissance missions which help enhance the adversary's situational awareness.

For this reason, **Electronic Support Measure (ESM) and Signals Intelligence (SIGINT) capabilities** can play important roles in strategic, operational and tactical surveillance across large and small critical areas. Both ESMs and SIGINT can assist:

- Non-cooperative target recognition,
- Specific emitter identification/emitter fingerprinting,
- Covert early warning

All these capabilities are characteristic of ESMs and SIGINT systems which can be IADS surveillance gap fillers and force multipliers.

Accordingly, Electromagnetic Countermeasures (ECMs) can be applied to any target but are especially appropriate for the engagement of tactical UAVs and UCAVs These ECMs can attack the radio link connecting the UAV/UCAV to its pilot or the satellite link which the aircraft may depend upon for navigation information. Uninhabited aircraft can be detected and located via their radio communications links and emissions from their radars.

The ECM can be used to prevent the UAV/UCAV's successful reception or transmission of data. This may be achieved through simple narrowband jamming by which a specific frequency being used by the aircraft is jammed. Alternatively, more sophisticated approaches are available. For example, a communications ECM may exploit information contained within the radio data link used by the aircraft to share still or video imagery with the pilot on the ground. This is similar to a cyberattack. However, temporal constraints must be considered, especially regarding swarm attacks during which isolating and attacking individual UAV/UCAV targets may prove too difficult.

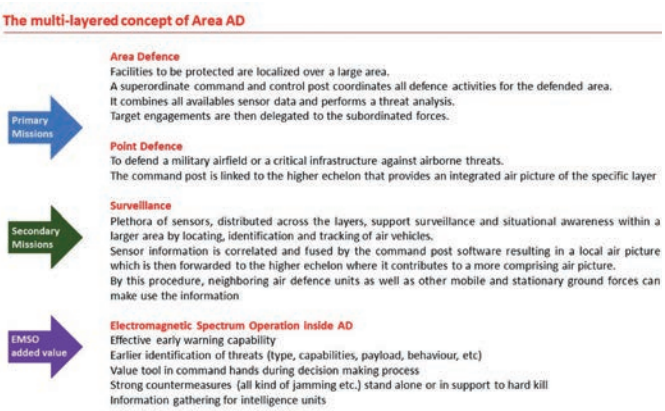
An ECM can also attack the aircraft's Global Navigation Satellite System (GNSS) signal that it receives from space. GNSS signals tend to be very weak as such they can sometimes be easily jammed. However, the aircraft may be equipped with GNSS protection techniques. These may amplify the satellite signal to avoid the jamming or simply ignore the area from where the jamming is originating to receive the GNSS signal from another direction. An ECM may also spoof the GNSS signal, although this approach can be difficult. Thus, EMSO provides several options that could be exploited:

- Denial - Negate or degrade the use of the electromagnetic spectrum to provide guidance in the form of GNSS signals or data transfer via radio link to the pilot at the Ground Control Station (GCS).
- Deception - Negate or degrade the use of the spectrum by electromagnetic sensors on board the vehicle.
- Make the UAV/UCAV imagery or audio data unavailable to the GCS and other users.
- Hacking – Exploit the UAV/UCAV's radio signals.
- Spoofing - Confuse the aircraft with false GNSS information or command the UAV/UCAV to fly in the wrong direction.

Modern forces are required to operate within an increasingly complex Electromagnetic Environment (EME). The EME has been recognized as an "operational environment" by NATO (publication reference: MC 64/11 "NATO recognizes the Electromagnetic Environment (EME) as an operating environment").

This has resulted in the realization of a new operational discipline known as Electromagnetic Spectrum Operations (EMSO). EMSO consist not only of "traditional" Electronic Warfare (EW), but includes several other disciplines which depend on the EME like information operations, SIGINT, spectrum use management, navigation warfare and cyberwarfare. As EW has evolved, from isolated operations in the EME at the tactical level towards joint EMSO at strategic and operational levels, electronic warfare remains EMSO's preeminent combat discipline.

Commanders are tasked to attain the level of superiority needed to enable the effective use of the EME while simultaneously exploiting, preventing or reducing adversary EME usage. NATO doctrine recognizes that alliance operations are complicated by an increasingly congested and contested EME. All forces depend on the EME. This creates vulnerabilities and opportunities for electronic warfare. Today's communication, sensing and guidance devices which depend on electromagnetic energy, are increasingly used both unilaterally and in a networked fashion by civilian and military organizations.



EMSO-C2 as a Must-Have Capability

It is clear that EMSO demands a level of coordination and synchronization which is impossible without specialized capabilities to support EME situational awareness, coordination and prioritization of actions. Therefore, EMSO Command and Control (EMSO C2) is a growing need.

EMSO C2 encompasses developmental and implementation activities associated with EMSO supporting functional services like mission simulation and support and training.

To achieve a complete EMSO capability able to support GBAD need to develop a technology roadmap to facilitate the integration between traditional Air defense Unit with the new concept of APIS (Area of Protection Integrated System) following these steps:

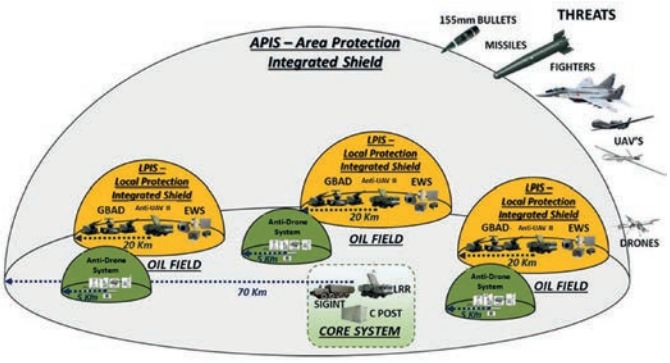
- Carefully identifying a self-contained operational layer of Electromagnetic Spectrum Operations inside an IADS encompassing EW, SIGINT, spectrum management and Cyber Electromagnetic Activities (CEMA) across all GBAD levels, providing a flexible modular solution adaptable to different types of operational organization, installation constraints and cost requirements.
- Positioning this EMSO capability as high as possible at system level. By federating different kinds of equipment using ELT products using standardized and flexible relevant architectures and software designs to take advantage of rapid sensor and effector technological evolutions
- realize that EMSO C2 at the operational level constitutes an operational breakthrough, which is "by design" enhances the knowledge of the EME and informs commanders' decisions. The ultimate goal of this process being to achieve Electromagnetic Spectrum Superiority.
- Realizing a technical/technological breakthrough in hardware and software which differentiates ELT from its competitors. Specific radar and communications emitter identification and fingerprinting, infrared countermeasures and ground-based communications jamming are potentially interesting avenues for hardware development to counter emerging threats. For software, artificial intelligence-based identification modules and decision-taking operator support will help make EMSO systems quasi-autonomous. These software approaches are being developed by ELT. Even if Cyber EW is still immature in many cases, it could open a new horizon of applications and business, as a result of the expertise gained by the company via some specific case studies and funded research programs.

Value Proposition

The following table describes the parameters of a selected use case in terms of geographical constraints, expected threats, potential deployed capabilities, and emerging requirements.

Geographical constraints	The sensitive sites/critical infrastructures to be protected are sparse over a large desert area, in the north-eastern region.
The threats	Vertical (typology) and horizontal (technology) evolution of the threat. The expected threats, both traditional (missiles, fighters, rockets) and emerging (UAVs, drones), and their mode of employment (rapidly evolving) require an integrated response including Radar, SIGINT, EW and Hard-Kill.
Capabilities	• SAM systems • Counter-drone (class I) systems • Counter-UAV (class II) systems • Tactical EW system (Radar EW, COMM EW) • SIGINT asset
The need	A combination of sensors (active/passive surveillance and fire control systems), shooters (guns, missiles, jammers) and a fully packaged battle management systems, capable of seamlessly integrate similar and dissimilar systems, is required to form an integrated global shield over the area of interest
The unseen threat	The cyber threat, both passive (information gathering) and active (to degrade/negate the functionalities of the integrated system), has to be taken into account and proper measures/procedures/actions must be put in place

The picture below sketches the envisaged physical deployment of the assets/capabilities in the area. The resulting architecture has been nicknamed the "Area Protection Integrated Shield" (APIS).



APIS acts as a central node in a territory's air defense and is easily integrated at the operational level with an IADS' other components.

Area of Protection Integrated System needs to be composed by new actors specialized in facing new threats as Drones and UAVs, coordinating by a Tactical Electronic Warfare System capable of Command and Control:

- Anti-Drone class I, Low Altitude, Slow Speed and Low RCS threats
- Anti-UAV class II, controlled by Radio-Link or GPS waypoints
- Tactical Electronic Warfare System, equipped with passive and active sensors.

COUNTER DRONE Class I (Micro/Mini/Small)

With this federated air defense architecture in mind (APIS), a full structure should be able to rely on a complete set of systems-of-systems intended to satisfy all EMSO demands facing LSL Threat (Low Altitude, Slow Speed, Low RCS).

An Air defense system need to be capable of protecting against Class 1 mini, micro and small UAVs, the typical counter-drone capability required for the protection critical infrastructure and sensitive areas points.

The system complements the IADS in the Ultra-Short-Range Air Defense (USHORAD) mission. A multi-sensor, multi-domain approach is the key to an effective detection, classification, identification, and neutralization posture for Class 1 UAV threats. The system should have:

- 3D radar suitable to detect Class 1 UAV and track them.
- Direction-finder for radio frequency up/down-link detection and tracking (drone and radio control).
- Electrooptical and Infrared (EO/IR) cameras for auto-tracking and visual confirmation of the threat, with advanced image recognition processing for threat classification.
- Radio-link demodulation and decoding for UAV protocol type recognition.
- Real-time data fusion across all sensors.
- Smart jamming waveforms for the UAV's radio link.
- GNSS navigation disruption techniques such as jamming and spoofing executed with directional antennas
- Wi-Fi electronic attack to facilitate hijacking the UAV.
- Command and Control post providing cartographic views, C2 and video streams.

Further, the system should be able to operate 24/7 in any harsh environment, capable of detecting and reacting, and should be remotely controlled and/or supervised by a dedicated operator.

External systems Interfaces allow the networking operations of other counter-drones systems, the functional integration with a hard kill reaction chain and with the IADS though the EMSO C2.

COUNTER UAV Class II

Anti-UAV System integrated in APIS should be capable of providing protection against Class 2 and Class 2 tactical UAVs, complementing an IADS' Very-Short Range Air Defense (VSHORAD) capabilities.

A multi-sensor, multi-domain approach is the key to effective detection, classification, identification and neutralization for Class 2 and Class 3 threats.

The system needs to include:

- A high-class 3D radar to guarantee extended detection and tracking of Class 2 drones.
- EO/IR camera queued by the radar and/or the Radio Direction Finder (RDF) to confirm the drone's identity and assist tracking.
- RDF passive sensor to intercept video and telemetry downlink signals to determine the drone's bearing.
- Automatic Dependent Surveillance-Broadcast (ADS-B) receiver which – This sensor receives the ADS-B signal, monitors local air traffic and displays the local air picture on a map.
- Command and control to manage all the system's components, implement sensor data fusion and perform weapon assignment.
- Artificial intelligence-based image recognition and emitter identification for target classification
- Anomalous behavior detection-classification and loaded/unloaded target recognition.

Able to operate 24/7 in any harsh environment, Anti-UAV need to work in automatic detection and reaction capabilities and can be remotely controlled. External systems interfaces enable the networking of other counter-drone systems, integration with the most advanced soft kill countermeasures via TEWS (see below) and with a hard kill chain as well as with the IADS though the EMSO C2.

TACTICAL ELECTRONIC WARFARE SYSTEM

The TEWS (Tactical EW System) is a very powerful integrated system-of-systems supporting GBAD. It is integrated with several networked, mobile, rapidly deployable tactical platforms.

The TEWS mission is to:

- Provide situation awareness and SIGINT on opponent assets and emitters through the compilation of an Electronic Order of Battle (EOB).
- Detect an opponent's emitters located "deep" in neutral/enemy territory thus providing vital early warning information in effectively counter any likely aggression.
- Maintain a local or regional air picture in case supporting radars are switched off to avoid ARM attack.
- Deny the use of the electromagnetic spectrum to the threat's sensors and/or communications, acting both in reactive mode for area protection and providing electronic attack for in a preventive mode.

TEWS need to be capable of:

- Surveillance of the electromagnetic spectrum in the area of

operations with angular coverage, 360 degrees' coverage or coverage across selectable angular sectors.
- Detection of radar and radio communication Signals.
- Emitter geo-location.
- Automatic analysis of detected emitters.
- Deep technical analysis employing analysis tools and operator-controlled computer aids.
- Emitter identification and fingerprinting.
- Long-term data recording for post-mission analysis.
- Full remote control capability.
- High operational sensitivity to intercept low effective radiated power radars at long distance.
- Very high accuracy direction of arrival measurement.
- Networking capabilities to perform emitter location in cooperation with other similar systems.
- Multiple radar and emitter high-power jamming through active electronically scanned array technology.
- Communication jammer against hostile tactical communications.
- Possibility to manage defensive cyber electromagnetic activities.

Conclusions

The electromagnetic spectrum is a (physical) resource in which, from which and through which all military, military-supported and asymmetric missions are performed.

Actions in the spectrum can have digital, kinetic and human effects and consequences.

After air, land, sea and space, the spectrum has become a key domain and enabler for cyberwarfare too. The capability to master the spectrum and achieve spectrum superiority will lead to superiority in all other domains of warfare, including cyberspace.

Given the increasing complexity of the operational environment, it is clear that EMSO demands a level of coordination and synchronization which is impossible without specialized capabilities that support situational awareness, coordination and priority of actions across the EME. Therefore, EMSO command and control is growing as an emerging need, including development and implementation activities associated with the supporting functions like mission simulation and support, and training).

EW and SIGINT assets in their fundamental roles providing passive intelligence and active protection, have evolved over several years becoming important elements of C4ISTAR systems, and system of systems.

DAI DRONI ALLA REALTÀ AUMENTATA, COME LE TECNOLOGIE GEOSPAZIALI CAMBIANO LE OPERAZIONI MILITARI

La piattaforma Esri a supporto della Difesa

ESRI ITALIA

Le organizzazioni che lavorano nella Difesa devono intraprendere azioni rapide e decisive sulla base di dati provenienti da numerosi sistemi, sensori e fonti. Utilizzando soluzioni basate sui sistemi informativi geografici (GIS), tutti gli operatori e i decisori riescono a prendere decisioni più consapevoli.

Con l'ausilio delle tecnologie geografiche possono essere aggregati e integrati dati di diverse tipologie, possono essere analizzati e visualizzati tutti gli aspetti dell'ambiente operativo, possono essere armonizzate le operazioni del personale, per favorire la collaborazione tra i vari settori.

La piattaforma ArcGIS di Esri, l'azienda leader nelle soluzioni geospaziali, è disponibile sul cloud e può essere configurata per ambienti senza connessione, con connessione intermittente o con connessioni particolari, a supporto di tutte le missioni e funzioni militari.
Le organizzazioni coinvolte nella Difesa possono integrare ArcGIS in qualsiasi sistema per le missioni, perché è una piattaforma interoperabile che fornisce un framework IT moderno, grazie ai suoi standard, all'architettura aperta e all'estensibilità.

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.
A tal fine, è possibile impostare vari flussi di lavoro per creare una ricostruzione dell'ambiente in 3D da utilizzare in GIS e VR. Per l'acquisizione delle immagini del territorio si può ricorrere, con molti vantaggi, alla rilevazione da parte dei droni.

L'uso del drone permette di acquisire dati e poi gli strumenti Esri consentono di ricostruire, rapidamente, anche in meno di 30 minuti, una ambientazione in 3D. Con una esperienza immersiva tridimensionale gli operatori possono poi esplorare e camminare virtualmente nella zona delle operazioni militari.

ArcGIS Drone2Map è un'app intuitiva che consente agli utenti di generare facilmente mappe dalle immagini dei droni, grazie alla sua elaborazione offline e alle funzionalità di mappatura rapida sul campo. Per le organizzazioni che utilizzano immagini di droni ad alta risoluzione, per prendere decisioni rapidamente, specialmente sul campo, questa app consente agli utenti di elaborare e analizzare immagini di droni senza essere connessi a Internet. Le accurate rappresentazioni 2D e 3D, del mondo reale, generate da Drone2Map possono poi essere facilmente condivise.

Oltre a Drone2Map, Esri propone anche **Site Scan for ArcGIS**, l'app per droni basata su cloud di Esri, che consente agli utenti dislocati geograficamente di raccogliere, elaborare e archiviare set di dati di grandi dimensioni.
Vari strumenti consentono di creare un ambiente in 3D a partire dalle immagini dei droni, come Esri CityEngine e ArcGIS Pro. Con strumenti per le realtà virtuali, ad esempio Unreal Engine, che ha una stretta collaborazione con Esri, si possono esplorare gli ambienti attraverso i visori. Gli scenari ricostruiti sono estremamente realistici, con un elevato livello di dettaglio. È possibile simulare diverse ore del giorno e della notte e diversi mesi dell'anno, per sperimentare diverse condizioni dell'ambiente. Oppure si può scegliere di dedicare un focus specifico agli edifici strategici che connotano la zona in esame.

Per costruire scenari in 3D estremamente realistici, Esri ha lanciato un nuovo strumento, che si chiama ArcGIS Reality, di cui Drone2Map e Site Scan for ArcGIS fanno parte.
ArcGIS Reality include una suite di prodotti che consente agli utenti di creare rendering digitali accurati di oggetti e scene a diverse scale, da un singolo sito fino a intere città e persino Paesi.
Con ArcGIS Reality, gli utenti possono trasformare tutti i tipi di immagini aeree rilevate da droni, aerei e satelliti in mappe e modelli 3D altamente accurati. La tecnologia consente di interagire con un mondo digitale che mostra luoghi e situazioni estremamente realistici.

ArcGIS Reality Studio è una nuova app mirata per la mappatura della realtà e aiuta gli utenti a utilizzare le immagini aeree e ad applicarle alla cartografia del territorio oggetto di analisi. La sua interfaccia interattiva è progettata per flussi di lavoro di produzione su larga scala e consente

agli utenti di fornire in modo efficiente rappresentazioni della realtà di livello topografico.
Reality Studio permette di costruire rappresentazioni in 3D di qualsiasi area in modo da poter creare le basi per un gemello digitale in 3D. 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.

ArcGIS Reality for ArcGIS Pro è una nuova estensione di ArcGIS Pro che consente agli utenti di inserire immagini da droni, satelliti o aerei nel software GIS desktop, per generare output 3D altamente accurati per la mappatura della realtà. Si possono realizzare, per esempio, modelli digitali del terreno, 3D mesh e Ortofoto rettificate con grandissima precisione.

L'elaborazione e gli output sono perfettamente integrati con ArcGIS, quindi sono rapidamente pronti per l'uso, l'analisi e la visualizzazione. Gli strumenti GIS consentono, poi, di creare digital twin per analizzare modelli di situational awareness, scenari particolarmente utili in un contesto militare.

Dalla raccolta di dati dei droni all'elaborazione di scenari realistici in 3D alla esplorazione virtuale degli ambienti ricostruiti, le tecnologie geospaziali sono, dunque, un valido sostegno per costruire flussi operativi a sostegno della buona riuscita delle operazioni militari.

NUOVE TECNOLOGIE NEI RADAR METEOROLOGICI

The future of weather radar design is here. And it's solid

EURELETTRONICA ICAS

Le organizzazioni che lavorano nella Difesa devono Vaisala è entrata nel mercato dei radar meteorologici nel 2006 con l'acquisizione della società Sigmet Inc, azienda statunitense con oltre tre decenni di esperienza nella fornitura di sistemi di elaborazione dati di radar meteorologici. Dal 2006 Vaisala è rapidamente diventata il principale fornitore di radar meteorologici Doppler a doppia polarizzazione sia in banda C sia in banda X. Il progetto del radar Vaisala è sempre stato ispirato all'innovazione tecnologica, per migliorare l'affidabilità, la sostenibilità e ridurre i costi del ciclo di vita. L'antenna del radar Vaisala è un'antenna espressamente ottimizzata per misure affidabili e di qualità in doppia polarizzazione. Ogni antenna prodotta da Vaisala viene misurata e i test report forniti al cliente in fase di collaudo tecnico. Il disegno innovativo del piedistallo consente che l'antenna e il sistema ricetrasmittente possono essere fissati vicino al centro di gravità, senza necessità di impiego di pesanti contrappesi. Il piedistallo combina una struttura leggera con un basso momento d'inerzia e un meccanismo di trasmissione a cinghia, scelta questa molto affidabile, diversamente dai sistemi con meccanismo a ingranaggio, in quanto non vi è gioco nel sistema di distribuzione e la tensione della cinghia è mantenuta costante. Questa soluzione è ispirata a principi di bassa manutenzione e non c'è necessità di sostituire olii o lubrificare il piedistallo. Una delle importanti innovazioni dei radar meteorologici Vaisala in banda C ed in banda X, è il consolidato utilizzo dei trasmettitori allo stato solido (SSPA -Solid State Phase Array) in alternativa ai trasmettitori con tubi magnetron, nel pieno rispetto dell'equivalenza di tutte le funzionalità e di tutti i parametri di funzionamento. Oltre ai benefici nel campo delle misure e delle prestazioni di sistema, la scelta del trasmettitore a stato solido nell'architettura di sistema di un radar meteorologico in banda C comporta diversi vantaggi:

- Il trasmettitore a stato solido non ha componenti consumabili che devono essere sostituiti durante l'esercizio operativo, laddove invece il trasmettitore a tubo magnetron è un consumabile che deve essere sostituito ad intervalli programmati, tipicamente ogni 4 anni. In tal modo si eliminato i tempi di fermo per l'intero sistema laddove invece l'impiego di trasmettitori a tubo magnetron rappresenta un "single point of failure"
- Il trasmettitore a stato solido non contiene elementi radioattivi, laddove il trasmettitore a tubo magnetron, per sua natura, è una sorgente radioattiva e come tale deve essere gestita quando viene dismesso e smaltito.
- Il trasmettitore a stato solido, rispetto al trasmettitore a tubo magnetron consente di ridurre, in un rapporto da 10 a 1, la potenza delle onde elettromagnetiche trasmesse, necessarie per eseguire le misure in atmosfera; ciò salvaguarda la salute pubblica della popolazione, in quanto ne riduce l'esposizione ai suddetti campi elettromagnetici e, di conseguenza, agevola l'installazione di radar meteorologici su eventuali nuovi siti.
- I trasmettitori a stato solido sono ampiamente disponibili sul mercato, trattandosi di una nuova tecnologia ed ha diverse fonti di approvvigionamento, laddove per il trasmettitore a tubo magnetron (in uso da diversi decenni) esiste ormai un solo costruttore al mondo negli Stati Uniti d'America al quale tutti i costruttori di radar meteorologici devono rivolgersi per l'acquisto di trasmettitori a tubo magnetron.

Per sfruttare al meglio le potenzialità dei radar meteorologici e degli altri strumenti di remote sensing come i LIDAR, Vaisala ha sviluppato la specifica suite software IRIS Focus, di facile utilizzo, web based, che consente agli utenti di accedere e analizzare i dati di telerilevamento in modo rapido e guidato. Al fine di promuovere le innovazioni per un futuro sostenibile, Vaisala ha costruito ed inaugurato nel 2021 in Finlandia, accanto alla propria sede centrale, un nuovo centro di ricerca e sviluppo e innovazione all'avanguardia che impiega professionisti qualificati nei vari campi d'interesse, dalla fisica, all'intelligenza artificiale al machine learning.

FORESCOUT TECHNOLOGIES: CONTROLLO E SICUREZZA AGENTLESS E REAL-TIME PER L'AMBIENTE ENTERPRISE OF THINGS (EOT)

FORESCOUT TECHNOLOGIES

Forescout Technologies, azienda leader specializzata nel settore della visibilità e del controllo real-time di dispositivi eterogenei, offre una piattaforma in grado di individuare la totalità di dispositivi (IT, OT, IoT e IoTM inclusi) connessi a reti campus, data center, cloud e ambienti OT, garantendone la protezione mediante efficienti tecniche di controllo e contenimento.

La soluzione Forescout consente sia alle aziende sia alle amministrazioni pubbliche di avere una visione completa dei loro ambienti operativi, riducendo il rischio informatico. La piattaforma intercetta e classifica, senza agent, in tempo reale, qualsiasi dispositivo con connessione IP, valutandone il livello di sicurezza e bloccando l'insorgenza di rischi correlati al mancato rispetto delle policy aziendali e delle normative di settore.

I dispositivi IoT e OT che accedono a una rete non adeguatamente segmentata rappresentano un grave rischio a causa della loro intrinseca insicurezza: sono un facile punto di ingresso a partire dal quale spostarsi verso target vitali per l'operatività aziendale.

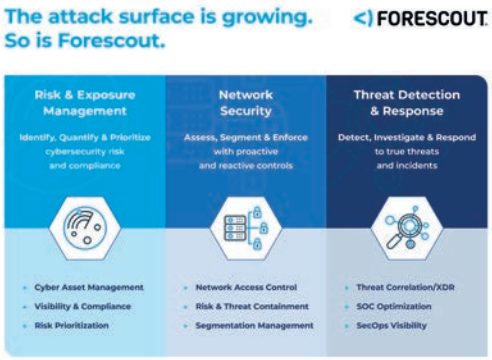
Se per tutti gli ambienti e i dispositivi si adottasse una strategia Zero Trust, definendo criteri di accesso diversi per un computer del front desk e il laptop del CEO, il rischio di attacco sarebbe drasticamente ridimensionato.

Per implementare una strategia di sicurezza efficace e ottenere visibilità e controllo totali, è necessario disporre della totalità dati relativi ai dispositivi connessi. Nel data center, nell'ambiente OT o nel cloud è preferibile consentire ai dispositivi accesso limitato anziché esteso all'intera rete.

In accordo al modello "Zero Trust" ogni accesso alla rete deve essere verificato e autorizzato. Al fine di garantire la perfetta efficienza delle politiche di segmentazione e, in particolare per mettere in sicurezza i dispositivi IoT e OT non altrimenti difendibili, Forescout ha lanciato "eyeSegment", una soluzione che controlla i flussi di traffico intra ed extra rete raggruppando utenti e dispositivi per tipo e contesto aziendale in zone dinamiche e, allo stesso tempo, limita l'accesso alla rete unicamente alle risorse ritenute strettamente necessarie a fini dell'operatività (principio di minimo privilegio).

Impegno in innovazione: Forescout XDR

I team dei Security Operation Center (SOC) analizzano elevate



quantità di informazioni, costituite da avvisi incompleti, imprecisi, decontestualizzati, spesso rappresentanti falsi positivi. Le ultime stime indicano che un SOC tipico riceve più di 11.000 avvisi al giorno, la maggior parte dei quali irrilevanti per la sicurezza e/o falsi positivi.

Forescout XDR, soluzione di detection e reaction estesa, converte la telemetria e i log in minacce reali tali da richiedere l'attenzione del SOC. In particolare, Forescout XDR automatizza il processo di detection, di indagine, di ricerca e di risposta alle minacce rilevate su tutti gli asset connessi (IT, OT/ICS, IoT e IoMT), dal campus al cloud, dal data center all'edge, raggruppando tecnologie e funzioni SOC in un'unica piattaforma cloud-native, visualizzabile e azionabile, a sua volta, da un'unica console. La soluzione XDR, in altri termini, riduce il rischio e la portata di un attacco o di una violazione dei dati eliminando il "rumore di fondo" proveniente dagli avvisi.

Sintetizzando, Forescout XDR assolve ai seguenti compiti:

- riduce le spese del SOC relative a licenze e gestione di più soluzioni all'interno del Security Operation Center (SOC), tra cui data lake, analisi della sicurezza, orchestrazione, automazione e risposta della sicurezza (SOAR), analisi del comportamento di utenti ed entità (UEBA) e piattaforme di threat intel;
- accelera i processi di indagine delle minacce, acquisendo informazioni complete e dati contestuali; tutto da una console unificata che si integra con altre soluzioni Forescout e con SIEM, sistemi di gestione dei casi e soluzioni di risposta di terze parti;
- offre una maggiore visibilità sull'intero ciclo di vita delle minacce attraverso dashboard preconfigurati e personalizzabili, con indicatori di performance chiave (KPI) personalizzati per analisti/IR, ingegneri, responsabili SOC, responsabili della conformità/rischio e dirigenti;
- fornisce archiviazione dei log, rilevamento automatico delle minacce e threat intelligence per supportare la conformità alle normative;
- aumenta il valore delle soluzioni Forescout e, in generale, delle soluzioni di sicurezza, endpoint e cloud, indipendentemente dal fornitore.

CYBER STRATEGY EVOLUTION

Honeypot e servizi di intelligence sempre più indispensabili nella cyber security

FORTINET

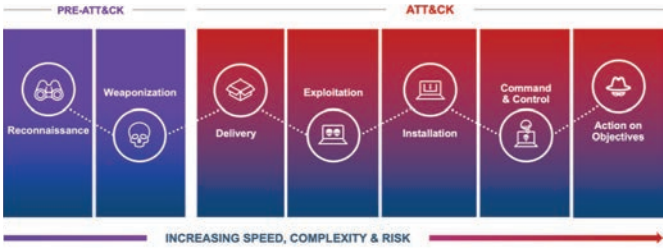
Nel corso degli ultimi anni abbiamo osservato un drammatico aumento degli attacchi informatici e un crescente numero di aziende che ne sono diventate vittime. Spesso ci si accorge della minaccia quando è ormai troppo tardi, trasformando ciò che inizialmente poteva essere un semplice evento registrato in un SIEM (Security Information and Event Management) in un reale incidente, che è penetrato profondamente nelle organizzazioni e si è diffuso ampiamente all'interno dei sistemi. Ecco che si interviene con Incident Responce e War Room, contattando specialisti di settore e non badando a spese per evitare che l'inevitabile si concretizzi.

Tuttavia, cercare di prevenire, concentrando gli investimenti nell'acquisizione di soluzioni di sicurezza in grado di effettuare attività di rilevazione e mitigazione delle minacce, potrebbe non bastare. Non solo gli attacchi stanno diventando altamente sofisticati, ma anche gli Hacker provano costantemente a utilizzare strategie sempre più mirate. In questo scenario, diventa cruciale andare ad adottare delle politiche che ci permettano di affinare continuamene i nostri sistemi di difesa e renderli ancor più efficaci, andando ad intervenire quanto prima e impedire "le infezioni".

A tal punto potrebbe essere opportuno andare ad analizzare il ciclo di vita delle minacce informatiche, in gergo chiamato "Cyber Kill Chain". Di fatto, la Cyber Kill Chain è un modello utile a identificare la sequenza di eventi necessaria all'esecuzione di un attacco verso una determinata organizzazione ed è composta da sette fasi distinte, divise in due macrogruppi: nel primo sono racchiuse tutte le attività che vengono effettuate precedentemente a un attacco, nel secondo troviamo le azioni che vengono concretamente messe in pratica per portare a termine con successo l'attacco.

Un aspetto interessante di queste due macrofasi è la tempistica che viene impiegata per portarle a termine, in quanto le fasi di ricognizione e di preparazione possono proseguire per diversi giorni, mesi, o addirittura anni, a seconda della complessità delle informazioni da reperire o introdurre, mentre le fasi successive, in particolare quella di delivery, potrebbero durare anche qualche minuto.

Un attacco che è già arrivato nelle fasi finali della "kill chain" potrebbe essersi infiltrato in modo diffuso e



Cyber Kill Chain

aver compromesso gli asset aziendali in maniera più profonda, comportando un maggiore dispendio di tempo e di risorse finanziarie per il ripristino dei sistemi e la mitigazione della situazione.

Si evince, quindi, quanto è diventato cruciale andare ad individuare le minacce informatiche anticipatamente, in particolare nella fase iniziale di preparazione, in quanto, pure piccole intercettazioni potrebbero svelare dei vettori di attacco importanti.

In particolare, si distinguono due fasi di pre-attacco: quella ricognitiva, in cui l'hacker inizia a scegliere e, conseguentemente, studiare il suo target, e quella successiva di Weaponization, in cui decide e forgia "l'arma" da sferrare. Così come l'attaccante studia accuratamente la sua vittima, in maniera analoga è opportuno che la vittima stessa analizzi accuratamente le strategie e le mosse del suo avversario. Questo studio potrebbe essere rilevante per addestrare adeguatamente i propri sistemi di difesa.

In tale ambito si stanno affermando sempre con maggior efficacia le soluzioni di "Active Deception", che riprendono il concetto legacy di "honeypot", lo estendono alle "honeynet" e ne migliorano l'efficacia, sia in termini di gestione che di integrazione, automazione e Incident Response.

L'obiettivo è quello di creare ed inserire una serie di asset in rete, emulando i sistemi esistenti ed eludendo l'eventuale attaccante che, di fatto, crede di accedere a risorse reali e cerca di violarle e comprometterle. Si parla di decoy (server esca), lures (servizi esca) e breadcrumbs (indizi esca) per creare un ambiente quanto più possibile verosimile. Ovviamente, tutte le attività vengono tracciate, per essere poi consultate ed analizzate dai "blue team", correlate con le altre informazioni e adoperate per migliorare le strategie di difesa.

Dunque lo scopo è duplice: distogliere l'attenzione degli attaccanti dall'infrastruttura reale e monitorare le loro azioni per comprenderne meglio le tattiche utilizzate. Soluzioni di questo tipo trovano ancor più efficacia in ambienti industriali dove sono presenti infrastrutture ICS (Industrial Control System) con sistemi OT. Tali sistemi ICS, per svolgere al meglio il loro compito, hanno la necessità di

comunicare sia tra loro sia con gli altri sistemi informatici presenti all'interno dell'azienda. Ovviamente risulta di vitale importanza proteggere non solo queste comunicazioni, ma anche i dispositivi stessi; la loro compromissione potrebbe danneggiare importanti asset aziendali, così come la business continuity. La complessità di questi scenari è data anche dal fatto che queste aziende spesso operano in settori critici e sono dotate, molto spesso, di sistemi legacy, difficilmente sostituibili, i cui aggiornamenti risultano complessi a causa dell'elevato livello di segmentazione dell'infrastruttura.

Di conseguenza, è evidente che la gestione della cybersecurity in tali contesti, tanto diversi dal tradizionale mondo enterprise, richieda approcci e tecniche specifiche e altamente mirate rispetto a quelle comunemente utilizzate.

Fortinet è attiva su questo fronte con una soluzione di Deception che riesce ad essere efficace sia in ambito IT che in ambito OT/Industrial, al punto da poter personalizzare i servizi esca rendendoli quanto più simili a quelli reali, con la possibilità di integrazione con soluzioni NGFW, NAC, EDR proprietarie o di terze parti, in ottica mesh architecture (Fortinet Security Fabric).

Un ulteriore strumento, fondamentale per l'efficacia nella prevenzione degli attacchi informatici, è costituito dai servizi di Intelligence, in particolare quelli di Digital Risk Protection, che permettono il monitoraggio attivo della sicurezza degli asset aziendali da un punto di vista "esterno" (public-facing). Si può pensare, ad esempio, alla presenza di personale specializzato, "sotto copertura", sia negli ambienti dei social media che negli ambienti del dark web, per rilevare eventuali pericoli come il furto di credenziali, la distribuzione di applicazioni rogue, phishing in tutte le sue varianti o, nel peggiore dei casi, l'utilizzo di Ransomware as-a-Service (RaaS).

Il servizio FortiRecon di Fortinet serve proprio a questo: fornire informazioni volte a conoscere le debolezze e le vulnerabilità dei propri asset prima che vengano sfruttate da avversari malintenzionati, per fini economici o di compromissione della reputazione del brand.

Oggi impiegare strumenti e risorse per rilevare e analizzare le fasi iniziali di un attacco è un investimento importante, con dei benefici enormi, che permette di prendere decisioni e adeguate contromisure correttive. La strategia vincente sfrutta al meglio il fattore "tempo", che diventa così un alleato di chi difende e non un vantaggio per chi attacca, per non arrivare durante il conto dei danni nell'anlisi "post mortem" a porsi la fatidica domanda: "Si sarebbe potuto fare qualcosa per evitarlo?"

Intelligence FortiRecon

DIFESA AEREA: UN NUOVO MODELLO DI GUERRA

L'attuale guerra Russo-Ucraina e le conseguenze sugli attuali modelli di conflitto

GM SPAZIO S.R.L.

L'aggressione della Russia all'Ucraina sta creando un nuovo modello di guerra in cui paradigmi storicamente consolidati, come la guerra terrestre condotta con veicoli corazzati, artiglieria e fanteria supportati dall'aviazione tradizionale, sono stati integrati con massicci attacchi missilistici dal cielo, dalla terra e dal mare, operati con vettori diversi come missili convenzionali e ipersonici, droni kamikaze e munizioni vaganti, proiettili di artiglieria guidati, attacchi informatici, azioni di propaganda e contropropaganda, ecc.

Per interagire efficacemente con gli scenari operativi più attuali, dove la cooperazione integrata tra le varie forze di difesa e contrattacco diventa indispensabile, è necessario adottare nuove strategie e tattiche di combattimento. Queste forze devono sincronizzarsi in modo efficace per reagire in modo tempestivo, massimizzando le risorse disponibili.

L'artiglieria antiaerea, un tempo non molto lontano era considerata la cenerentola delle Forze Armate, ha assunto un ruolo nuovo di primo piano, è improvvisamente emersa come protagonista principale del teatro operaivi dopo anni in cui era stata praticamente quesi dimenticata.

È dimostrato, in particolare, che la capacità di interdizione a medio e corto raggio, costantemente messa alla prova per sventare al meglio il numero massiccio di attacchi volti a distruggere le infrastrutture necessarie alla vita quotidiana delle popolazioni interessate dal conflitto, è diventata la principale capacità di difesa e di resilienza della nazione attaccata.

Ad oggi, l'unico esempio assimilabile a questo specifico sottoinsieme del conflitto russo-ucraino, con le dovute differenziazioni e interpretazioni, è quello del conflitto asimmetrico israelo-palestinese, dove lo Stato di Israele si difende dagli attacchi della controparte attraverso il noto sistema IronDome. Tuttavia, il contesto specifico di ciò che accade in quella regione è sufficientemente diverso da quello che accade nell'Europa dell'Est, alcuni elementi di somiglianza possono tornare utili nella nostra analisi, in particolare il numero massiccio di munizioni utilizzate contemporaneamente e il breve raggio di interdizione in cui operare il relativo contrasto.

Con queste premesse, appare chiaro che, al di là di una valutazione più ampia dei fattori coinvolti nell'analisi di un conflitto pervasivo come quello russo-ucraino, concentrarsi sulla questione specifica del contrasto agli attacchi aerei a medio e corto raggio ci pone di fronte alla necessità di valutare quali siano le misure più efficaci da attuare per essere efficaci e di successo.

Gli alleati occidentali stanno fornendo all'Ucraina sistemi di difesa aerea per proteggersi da missili, attacchi aerei convenzionali e attacchi di droni. Questi sistemi sono in grado di rilevare, ingaggiare e distruggere vari tipi di aerei, elicotteri, missili da crociera e velivoli senza pilota.

Tutto questo potrebbe non bastare perché resta il fatto che, di fronte a questo nuovo tipo di minaccia, le contromisure attuate attraverso le batterie antiaeree convenzionali sono poco utili; sono certamente efficaci e precise ma, allo stesso tempo, limitate dalla scarsità di mezzi e dai relativi costi di dispiegamento. Il teatro operativo ci mostra che sta diventando necessario tornare all'uso di sistemi di difesa aerea convenzionali "manned" e "unmanned" possibilmente semoventi (come le torrette di difesa a bassa quota degli assetti navali, in grado di operare una contromisura locale e sufficientemente efficace a corto raggio attraverso la classica nuvola di proiettili di medio-piccolo calibro, circa 20 mm), una soluzione efficace a corto raggio (SHORAD e V-SHORAD) in attesa che le armi a energia diretta passino dal "mercato della ricerca" al vero e proprio "mercato del consumo".

In questo contesto multiforme e dinamico, gli strumenti di modellazione e simulazione (M&S), robusti programmi informatici utilizzati per simulare una serie di scenari relativi alla difesa aerea, assimilabili ad un vero e proprio gemello digitale della realtà (Digital Twin), consentono agli esperti militari di valutare le prestazioni delle loro attuali strategie difensive in situazioni paragonabili a quelle reali, senza la necessità di spendere tempo e denaro per prove reali limitando i rischi e le spese ad esse connessi.

Le capacità dei sistemi M&S possono essere utilizzate anche per misurare e confrontare le prestazioni di diversi sistemi difensivi e per analizzare l'impatto delle condizioni ambientali sulle prestazioni dei sistemi di difesa aerea.

In generale, la validazione attraverso la modellazione e la simulazione svolge un ruolo essenziale nella difesa contro le minacce aeree, contribuendo a garantire che le forze militari stiano impiegando le contromisure più efficaci per proteggersi dagli avversari aerei

SPACE WEATHER: STUDIARLO PER MITIGARE I RISCHI

Le tempeste geomagnetiche possono causare ingenti danni all'Umanità intera

GM SPAZIO S.R.L.

Fin dall'inizio della storia dell'umanità, l'uomo ha dovuto affrontare i capricci del tempo: i cacciatori e gli agricoltori hanno lottato con piogge abbondanti, nevicate e inondazioni, i marinai con venti forti e tempeste marine, i piloti con nuvole e vento di taglio.

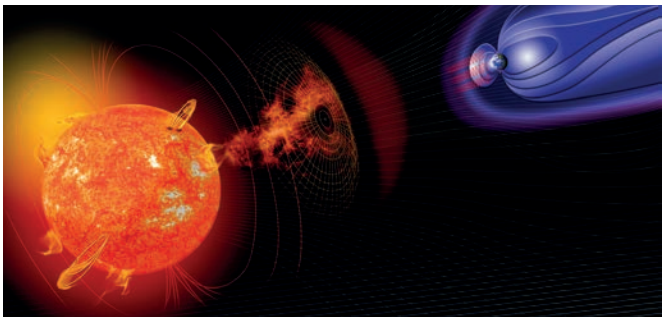
Così ora, dall'inizio dell'avventura spaziale, abbiamo dovuto affrontare un ambiente più pericoloso, quello extra-atmosferico, dove le radiazioni sono letali per la maggior parte degli esseri viventi, a parte i virus e i batteri estremi in grado di sopravvivere ai viaggi nello spazio profondo.

Lo Space Weather si riferisce alle condizioni nello spazio che possono avere un impatto sui sistemi tecnologici come satelliti, GPS e infrastrutture terrestri (reti elettriche e di telecomunicazioni), nonché sulla salute e sulla sicurezza umana, dagli astronauti fino a tutti gli abitanti del pianeta. Queste condizioni sono determinate principalmente dal Sole e dalle sua attività, inclusi i brillamenti solari, le espulsioni di massa coronale (CME) ed il vento solare ad alta velocità.

I brillamenti solari sono esplosioni improvvise e intense di radiazioni che possono rilasciare un'energia pari a quella di milioni di bombe atomiche. Sono causati dal rilascio di energia nella corona solare e possono produrre giganteschi campi elettromagnetici capaci di interferire in maniera significativa con i sistemi elettrici ed elettronici intorno alla Terra e sulla Terra stessa. Ad esempio, possono disturbare le comunicazioni satellitari e causare blackout nelle reti elettriche. Possono anche rappresentare un rischio per la salute degli astronauti che si trovano al di fuori del campo magnetico terrestre.

Le CME sono massicce eruzioni di gas e campi magnetici provenienti dal Sole, che possono viaggiare nello spazio e interagire con il campo magnetico terrestre. Quando entrano in collisione con il campo magnetico, possono causare disturbi nell'atmosfera terrestre che possono influire sulle comunicazioni radio e sulle reti elettriche. Possono anche produrre splendidi spettacoli di luce più comunemente noti come aurore boreali.

Il vento solare ad alta velocità è un flusso di particelle cariche che fluisce dal Sole e può viaggiare a velocità fino a 500 km/s e quando interagisce con il campo magnetico terrestre, può causare tempeste geomagnetiche che possono produrre aurore e interrompere le reti elettriche, le comunicazioni satellitari e i sistemi GPS.



Lo studio dello Space Weather è importante perché può aiutarci a capire e a mitigare i rischi associati ai fenomeno derivati dall'attività solare. Le previsioni meteorologiche spaziali possono essere considerate alla stregua di quelle terrestri, ma sono molto più impegnative a causa delle complesse interazioni tra il Sole ed il campo magnetico terrestre e vengono utilizzate dalle agenzie spaziali, dalle compagnie elettriche e da altri attori istituzionali ed industraili per mitigare gli effetti derivati dall'attività solare.

Oltre alle sue applicazioni pratiche, lo Space Weather è anche un'importante area di ricerca scientifica. Lo studio del Sole e della sua attività può aiutarci a comprendere le origini e l'evoluzione del nostro sistema solare, nonché la fisica dei plasmi e dei campi magnetici. Può anche aiutarci a capire l'abitabilità dei pianeti intorno ad altre stelle, poiché l'attività solare può influenzare gli ambienti atmosferici e magnetici di quei pianeti.

In conclusione, lo Space Weather si riferisce alle condizioni nello spazio che possono avere un impatto sui sistemi tecnologici e sulla salute e sicurezza degli esseri umani. Lo studio e la previsione di questi fenomeni sono temi importanti da approfindire per mitigare i possibili danni e per far progredire la nostra comprensione dei fenomeni relativi all'attivita del Sole e della fisica dei plasmi e dei campi magnetici.

IL COVERT SENSING E.M. PER IL CONTROLLO DELL'EMSO

Il Dott. Italo Trisolini Longobardi, già Ufficiale Superiore della MMI e responsabile per la nuove Tecnologie della INTECS SOLUTIONS SpA, ha proposto e fatto realizzare con successo da un agguerrito team di tecnici INTECS, una interessante ricerca riguardante il Covert Sensing

INTECS SOLUTIONS

Oggi e sempre di più domani le operazioni belliche sono e saranno attuate nei 5 Domini: terra , mare, aria, spazio e cyber. Lo Spettro e.m. è lo sfondo comune per tutti i 5 Domini: chi padroneggia lo Spettro e.m. Opertivo (EMSO) ha sicuramente vantaggi operativi importanti rispetto la controparte in ogni Dominio.

Per padroneggiare l'EMSO è necessario avere la capacità di lettura dello Spettro e.m., su di una larghezza di banda la più ampia possibile, in real time, con sensori numerosi, facilmente dislocabili ovunque, cooperanti e distribuiti per copertura di area geografica più ampia ed ambientalmente diversificata possibile sia dal punto di vista orografico che urbanistico: fondamentalmente realizzare un Sistema costituito da sensori con un rapporto costo efficacia compatibile con i ridotti budget nazionali.

INTECS possiede un solido, profondo e comprovato a livello Internazionale, KH nella tecnica Software Defined Radio da più di 20 anni e da più di 10 nella A.I..

INTECS ha quindi proposto al Segretariato Generale della Difesa nel 2012/13 un Programma di ricerca tecnologica che è stato cofinanziato, per ricercare e realizzare un dimostratore di Sistema di Cooperative Sensing, denominato "C-SENSE" che, basato su tecnologia Software Defined Radio (SDR), garantisce una completa conoscenza dello spettro elettromagnetico (RF Situational Awarness).

Nell'ambito del programma C-SENSE sono state individuate e studiate quelle che si ritengono ad oggi le migliori tecniche di Cooperative Spectrum Sensing (CSS) per ottenere una visione completa e accurata dello scenario di un'area geografica, sopperendo ai noti problemi di shadowing ed ostruzione fisica, con la distribuzione su più sensori radio dell'elaborazione dei dati.

I sistemi di monitoraggio cooperativo nel 2012/2013 erano una tematica di frontiera della ricerca scientifica, per i quali esistevano all'inizio del progetto, solo modelli matematici o implementazioni all'interno di ambienti di simulazione.

La realizzazione di un prototipo ha rappresentato quindi un avanzamento significativo delle conoscenze nel dominio del Cooperative Spectrum Sensing (CSS).

All'inizio del progetto la maturità tecnologica del CSS, allo stato dell'arte, era riconducibile al massimo al TRL 2. Il Sistema C-SENSE, che è stato realizzato al termine del programma nel 2020, ha ottenuto un avanzamento tale da portare la tecnologia ad un livello di maturità pari a TRL 6, andando a dimostrare la realizzabilità pratica del CSS tramite un dimostratore in scala ridotta, composto da sei sensori radio.

METODOLOGIA

Le tecniche per lo spectrum sensing cooperativo sono differenti a seconda delle necessità; nel nostro caso gli algoritmi ricercati sono stati adattati alla modalità distribuita ed è stato implementato un modello di cooperazione opportuno. Così facendo, i nodi possono autonomamente organizzarsi in coalizioni disgiunte indipendenti, massimizzando la probabilità di detezione in funzione dei costi di cooperazione. In base a questo approccio ogni nodo decide autonomamente di formare o rompere una coalizione con l'obiettivo di massimizzare la probabilità di detezione. Al fine di verificare la presenza del segnale si utilizza il test di Neyman-Pearson.

UTILIZZI E RICADUTE DELLA TECNOLOGIA

I potenziali utilizzi degli studi condotti sono riconducibili sia in ambito civile che militare. Nel primo scenario gli impieghi sono essere molteplici.

Nel contesto militare, tanto per citarne una, la valenza operativa di aumentare la capacità comunicativa evitando in tempo reale azioni di disturbo, volontario o meno, aumenta il grado di affidabilità degli ordini verso l'intera linea di comando in teatri ostili.

Da evidenziare che la Intecs Solutions, al termine di questo studio, ha realizzato un prodotto per la rilevazione, identificazione, localizzazione in frequenza e stima della direzione di RPAS. Il prodotto, oggi commercializzato, denominato DEDALO, offre numerosi vantaggi sia in termini di economicità, di leggerezza e portabilità sia nelle sue caratteristiche di analizzatore di spettro totalmente passivo.

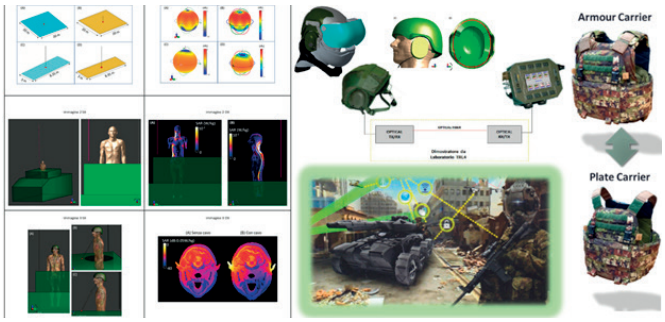
Il futuro di questo filone tecnico è ottimizzare la cooperazione tra i sensori oltre all'intercettazione delle interferenze con il massiccio impiego dell'A.I.

LARIMART TRA INNOVAZIONE E PRODUZIONE

Obiettivo: sicurezza ed operatività della persona nei domini complessi

LARIMART

La realtà industriale e manifatturiera della Larimart considera essenziale promuovere nuove idee, attraverso le quali sviluppare progetti e realizzare futuri prodotti innovativi. La produzione, squisitamente di matrice italiana, realizza Soluzioni Elettroniche e di Protezione Personale di Utente per le specifiche esigenze tecnico-operative di "End-User" nei contesti di impiego Difesa e Sicurezza. I progetti di ricerca si articolano seguendo l'offerta dei prodotti Larimart e spaziando tra le due realtà operative, che sono alimentate dalle due unità di progettazione elettronica e protezioni personali. I prodotti Larimart sono caratterizzati da semplicità ed affidabilità nei servizi base, ma allo stesso tempo aperti ad evoluzioni e servizi più complessi. Di seguito sono descritti brevemente alcuni percorsi e risultati dei progetti nazionali di ricerca militare svolti nella realtà lavorativa della Larimart:



Uno dei progetti di ricerca è il PNRM **PBI-G12-EVO**, che propone un'evoluzione dei **giubbetti antiproiettile della famiglia PBI-G12**. Il progetto è articolato su diversi temi, dai quali sono stati sviluppati dei prototipi di TRL 6, ognuno dei quali apporta innovazioni su vari aspetti logistici e operativi, come il miglioramento complessivo del confort; l'incremento della modularità del sistema; l'evoluzione delle protezioni balistiche in termini di riduzione di peso ed estensione della protezione verso nuovi tipi di minacce; la disponibilità di informazioni a supporto della gestione logistica. Grazie alla realizzazione dei prototipi TRL 6, il progetto ha potuto quantificare sperimentalmente l'efficacia delle innovazioni proposte. L'obiettivo del progetto è di incrementare il livello di modularità, consentendo di passare da una configurazione Plate Carrier di livello IV stand alone ad una configurazione Armour Carrier, aggiungendo elementi di protezione flessibile di livello IIIA.

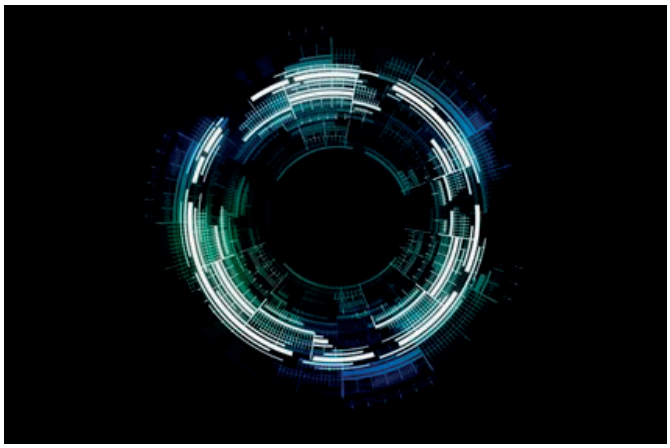
In ambito veicolare un altro programma di ricerca è **HELTEAM**, che si pone l'obiettivo di sviluppare un **Sistema Casco High-Tech**, con protezione estesa con una capacità di realtà virtuale aumentata, in grado di supportare il soldato in teatro operativo a bordo di mezzi tattici terrestri, sia di giorno che di notte. Tale sistema innovativo del casco consentirà un livello di protezione dell'udito idoneo ad operare in ambienti altamente rumorosi, garantendo la salute dell'operatore, comunicazioni cristalline e la necessaria percezione spaziale dell'audio all'interno dei veicoli corazzati.

Sempre nell'ambito operativo dei mezzi tattici terrestri l'obiettivo generale del progetto di ricerca denominato "**HEPROSYS – HERP Electromagnetic Protection System**" è quello di investigare, analizzare e sviluppare possibili dispositivi di mitigazione dell'esposizione ai campi elettromagnetici di un operatore a bordo di piattaforme veicolari militari. Grazie alla collaborazione sinergica tra **LARIMART S.p.A.**, **SAPIENZA UNIVERSITA' DI ROMA** e **CE.POLI.SPE.** (CEntro POLIfunzionale di SPErimentazione), l'inizio della ricerca si è focalizzata sulla comprensione e sulla caratterizzazione dello scenario elettromagnetico presente su un veicolo "tipo" in dotazione alla Forza Armata. In particolare, lo studio si è concentrato sul veicolo VBM 8x8 "Freccia". Sono state analizzate le possibili configurazioni più rilevanti dal punto di vista dell'esposizione ai campi elettromagnetici del personale a bordo del mezzo, inoltre sono state analizzate le metodologie per le misure HERP (Hazards of Electromagnetic Radiation to Personnel). L'indagine ha permesso di individuare, tramite studio dosimetrico e modelli simulanti campi ed interazioni elettromagnetiche, valori del SAR (Specific Absorption Rate) e del Campo Elettrico, comunque sempre inferiori ai limiti imposti dalle normative cogenti di riferimento. Parallelamente, sono state proposte e realizzate possibili soluzioni hardware (schermature indossabili e sistemi di collegamento in fibra ottica) atte a ridurre l'esposizione elettromagnetica ed i rischi connessi per gli operatori di bordo. In sintesi, la prima parte del progetto ha portato alla definizione di dettaglio dei problemi connessi all'esposizione ai campi elettromagnetici da parte del personale a bordo delle piattaforme veicolari militari. Le attività hanno inoltre riguardato lo sviluppo di soluzioni capaci di contribuire alla mitigazione dell'esposizione. I risultati emersi dalle simulazioni numeriche, eseguiti in banda HF, mostrano che l'elmetto in dotazione non introduce perturbazioni sensibili delle distribuzioni di Campo Elettrico e di SAR nell'operatore, che lo indossa. In particolare, i valori simulati di Campo Elettrico e SAR risultano sempre ampiamente al di sotto dei limiti previsti dalle normative. La collaborazione tra l'Industria (LARIMART S.p.A.), il comparto accademico (Sapienza) e la Forza Armata (CE.POLI.SPE.) ha portato alla pubblicazione di un paper scientifico dal titolo "**Numerical Evaluation of Human Body Near Field Exposure to a Vehicular Antenna for Military Applications**".

GESTIONE DEL RISCHIO AEREO ASSOCIATO AI DRONI NEI DIVERSI SCENARI

Un approccio tecnologico modulare

MATICMIND



Nel mondo moderno, l'uso dei droni ha conosciuto una crescita esponenziale, trovando applicazioni in settori che vanno dalla fotografia aerea alla consegna di oggetti, fino al monitoraggio del territorio per la tutela e sicurezza di persone e cose.

La tecnologia ha abilitato l'utilizzo del drone inteso come vero e proprio potenziale strumento utile al compimento di missioni in scenari tattici e bellici.

L'opportunità tecnologica sviluppa una minaccia di offesa derivata dal volo di oggetti di svariate dimensioni a seconda della missione per cui l'oggetto volante è programmato.

La normativa vigente in Italia contrasta gli abusi e sapientemente limita l'azione del drone a volo automatico e autonomo, vincolandone l'operato ad un pilota in possesso di regolare patente, permesso di volo con drone nel campo visivo. **Il gruppo Maticmind** ha iniziato il percorso di studio sul volo dei droni correlato alla eventualità di sorvolo non autorizzato di aree sensibili e strutture che poteva costituire una minaccia a vario titolo. I primi esperimenti sono stati condotti per verificale il sorvolo di penitenziari per il trasporto e contrabbando di sostanze stupefacenti o interscambio informazioni, strutture civili sensibili come sedi governative e situazioni nei quali il drone può fungere da strumento per trafugare informazioni attraverso rilevazioni ambientali audio-video, strutture sensibili ove il volo di un drone poteva corrispondere a minaccia di interferenza con operazioni di volo di velivoli passeggeri e merci.

L'esperienza suddetta è stata fondamentale per definire e raffinare un approccio di rilevazione basato sulla tecnologia ad **Intelligenza Artificiale** e **Deep Learning** applicato alle **scansioni real-time** dello streaming video di sistemi ad-hoc. Questo approccio è stato innestato su una base di analisi del segnale frutto di una esperienza ventennale nell'applicazione degli **algoritmi** basati sulle **reti neurali**.

I test condotti sono stati svolti con varietà di condizioni meteo, con parametri di FoW 44° H effettuando l'individuazione dell'oggetto e resolution tracking maggiore o uguale a 4 pixel con telecamere termografiche pressoché nel 100% dei casi.

Gli studi condotti in questo settore si sono concentrati nella direzione dell'analisi real-time dello streaming video grazie agli asset del gruppo Maticmind considerando che in alcuni scenari gli approcci basati su tecnologie Radar potevano essere inapplicabili per interferenza con strutture e strumentazioni pre-esistenti dove il segnale Radar poteva essere inficiato o inficiare a sua volta l'ambiente circostante. Per questo motivo nessun altro sistema ausiliario è risultato indispensabile per il completamento del compito.

Sempre considerando la fase di individuazione del drone, muovendoci nello scenario di applicazione di natura militare, l'ingegnerizzazione delle **soluzioni antidrone** diventa un esercizio di integrazione modulare per inserire sistemi ausiliari indispensabili per la specifica applicazione.

In questo caso quindi, tornano utili sistemi già in utilizzo in ambito militare come Radar, LiDar,e RF Scanners.

L'applicazione militare per sua natura stessa deve contemplare vari sistemi a supporto per garantire una copertura omogenea sulla dimensione spaziale. Per perseguire la precisione ottimale e l'affidabilità, si deve perseguire la perfetta integrazione dei vari moduli e tecnologie di rilevazione. L'intelligenza artificiale ed il deep learning vengono nuovamente a supporto, oltre al modulo di analisi realtime dello streaming video, nella fase di **correlazione dei dati** rilevati dal sistema principale ed ausiliari interpolando le informazioni ed effettuando tracking e calibrazione per la messa in atto di azioni di contrasto ideali.

In seguito alla rilevazione tempestiva e precisa dei droni di qualsiasi dimensioni e tecnologia di volo, le reazioni dipenderanno anch'esse dallo scenario di applicazione. Nello scenario di **protezione** di **infrastrutture critiche** e **strutture civili** si possono mettere in atto contromisure come l'atterraggio forzato mediante interazione con le native di pilotaggio del software di controllo del drone.

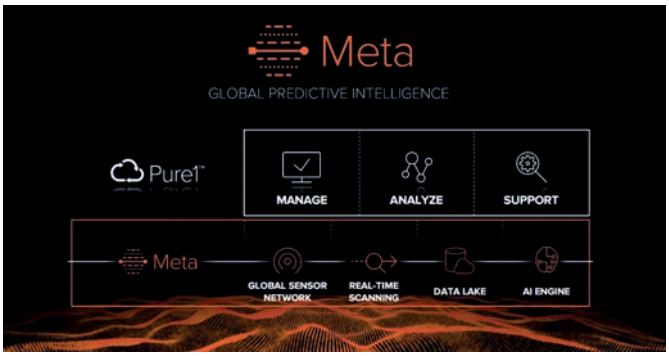
Nell'ambito militare le reazioni vanno tipicamente dall'utilizzo di droni intercettori, abbattimento mediante sistemi di difesa, jamming del segnale radio e disturbo del segnale GPS.

Maticmind mette a disposizione le proprie competenze specialistiche per la progettazione, realizzazione, integrazione e gestione di soluzioni tecnologiche innovative per le FF.AA in tutte le aree dell'Information & Communication Tecnology.

PURE STORAGE: LA GESTIONE AUTOMATICA DEL DATA CENTER AD ALTE PRESTAZIONI

Enterprise Storage con il pilota automatico

PURE STORAGE



Pure1 Meta è la piattaforma di analisi full-stack guidata dall'intelligenza artificiale alla base del sistema di gestione dello storage a guida autonoma di Pure

Gran parte del mondo contemporaneo è basato su applicazioni critiche, che sono entrate in modo pervasivo nella vita di tutti i giorni: dalle più tradizionali applicazioni mobili per accesso al proprio conto bancario, ai nuovi workload nel mondo degli analytics che hanno alla base algoritmi di intelligenza artificiale o machine learning che prevedono elaborazioni real time. Il comune denominatore che lega questo tipo di servizi applicativi è che debbano essere attivi 24 ore al giorno, 7 giorni su 7, 365 giorni all'anno con tempi di risposta pressoché istantanei.

Un altro filo comune è che la garanzia di continuità di servizio sia affidata ad apparecchiature informatiche residenti nei data center (cloud privati o pubblici). La gestione dell'infrastruttura informatica di Datacenter è quindi totalmente responsabile della continuità del servizio applicativo critico. La gestione ottimale dell'infrastruttura informatica richiede un numero considerevole di ore/uomo, spese nel gestire e proteggere i dati da potenziali attacchi.

Il settore Difesa non fa eccezione, anzi il paradigma sopracitato assume ovviamente aspetti ancor più critici in quanto la stessa Sicurezza Nazionale si fonda sul sistema C4IS che necessita di un'infrastruttura informatica sicura, resiliente e altamente performante sia sul teatro delle operazioni sia nel data center.

Pure Storage è un'azienda nata in California (USA) oltre 12 anni fa, specializzata in infrastrutture informatiche, in particolare in sistemi storage completamente basati su memorie flash, in grado non solo di dare le massime performance applicative, ma anche di garantire un livello di servizio 24×7, 365 giorni all'anno. L'idea fondante di Pure Storage è che anche un tecnico generalista, non specializzato su infrastrutture storage, sia in grado di gestire facilmente gli spazi dedicati ai dati applicativi critici e sensibili.

Viene semplice fare un parallelo con un oggetto quotidiano come lo smartphone, in cui tutto funziona grazie al perfetto connubio tra software di gestione e hardware; i nostri dati vengono protetti costantemente e qualora il telefono sia perduto, siamo in grado di ripristinare applicazioni e dati in tempi molto rapidi su un altro telefono.

Allo stesso modo le infrastrutture Pure Storage sono in grado di offrire protezione automatica contro attacchi ransomware, grazie a sistemi di intelligenza artificiale, capendo immediatamente quando un attacco è in corso, e ripristinando velocemente i dati che eventualmente siano già stati criptati in modo malevolo.

Queste caratteristiche, differenzianti rispetto alle altre architetture Storage presenti sul mercato, hanno fatto in modo che importanti analisti come Gartner abbiano riconosciuto un primato assoluto a Pure Storage per quanto riguarda lo storage primario Enterprise in tutto il mondo (https://www.purestorage.com/resources/gartner-magic-quadrant-primary-storage.html).

Le caratteristiche differenzianti dei sistemi Pure Storage risiedono in gran parte nella capacità di aggiornare, sia dal punto di vista hardware che software, i propri sistemi senza dover mai spegnere le applicazioni critiche e senza mai dover effettuare complesse migrazioni dati, di solito necessarie durante gli aggiornamenti tecnologici.

Un altro punto cardine della gestione ordinaria delle Infrastrutture di Data Center risiede nell'interazione con il supporto dei vendor, a fronte della necessità di intervento. Se l'amministratore di sistema rileva un problema tipicamente apre una chiamata al supporto di riferimento, richiedendo un intervento specialistico. I sistemi Pure Storage hanno alla base un sistema di monitoraggio basato su intelligenza artificiale, in grado di ingaggiare automaticamente il supporto, prima che si verifichi un problema potenzialmente bloccante. Tali caratteristiche sono state molto apprezzate dall'esercito britannico per la realizzazione del private cloud di forza armata https://www.purestorage.com/uk/customers/british-army.html e dalla NASA per le propria Digital Transformation nell'ambito analitycs basata su AI e ML https://www.purestorage.com/customers/nasa.html.

Il contributo che i sistemi Pure Storage sono in grado di dare ai sistemi informatici militari è fondamentale: da un lato offrono il massimo delle performance applicative consentendo ai sistemi C4IS una risposta pressochè real-time e dall'altro offrono una sorta di pilota automatico in grado di togliere dalle spalle degli amministratori le complessità di gestione infrastrutturale.

DIGITAL CARDS

Alla scoperta della società che propone in Italia le soluzioni di Entrust, player a livello globale per l'emissione di carte nel mondo Government e Finance

N.I.D.O. S.R.L.

N.I.D.O. Srl, società nata a Roma e attiva da oltre vent'anni in vari rami dell'IT, occupandosi di commercializzazione, manutenzione, integrazione e sviluppo di soluzioni hardware e software, punta sempre più alla digitalizzazione delle Cards, e lo fa grazie anche a una partnership d'eccezione. Quella che intrattiene da più di venti anni con Entrust, Certification Authority nota in passato come Datacard, che è oggi un player di livello globale per la personalizzazione di carte fisiche e digitali.
Per saperne di più, ne abbiamo parlato con Giorgio Mestici, Direttore Commerciale della Divisione Card ID Management di N.I.D.O. Srl. La società, con sede a Roma, dispone attualmente di 15 professionisti e ha un fatturato nell'ordine dei 5 milioni di euro. *"circa il 50% del fatturato N.I.D.O. Srl proviene dalla mia Divisione in cui ho la fortuna di collaborare con persone di assoluto valore, esordisce Mestici, spiegando che "in questo ambito operiamo come veri e propri opinion leaders di riferimento del mercato Italiano, oltre a sviluppare software specifico e a offrire servizi di integrazione e formazione. Tutti i ns servizi, tradizionali ed evoluti, vengono erogati direttamente da personale dipendente della Società".*

Emettere Cards

"La nota caratteristica della Ns Società è quella di essere riuscita, nei 20 anni di storia, a sviluppare e consolidare la ns posizione dominante sul mercato partecipando da protagonisti a tutti i progetti Governativi (Carta di Identità Elettronica, Carta Nazionale dei Servizi (CNS), Tessera Sanitaria, Passaporto Elettronico, Patente di Guida...) e affermando la ns presenza in tutti i Service Bureau che, per conto degli Istituti Bancari, personalizzano Carte di Credito e Carte di Debito".

La nuova sfida

Le Carte Digitali e l'emissione istantanea sono la nuova normalità. *"Le persone oggi cercano la comodità al di là di ogni altra cosa" chiarisce Mestici "sono abituati alle esperienze digitali e mobili nella vita di tutti i giorni e desiderano servizi digitali convenienti, semplici e senza interruzioni"*. In questo nuovo mondo, la carta digitale sta rapidamente diventando un complemento essenziale della carta plastica.
"I clienti si aspettano esperienze digital-first. Per soddisfare le loro esigenze, le Pubbliche Amministrazioni e le Banche ora devono offrire ai propri clienti un'esperienza istantanea e mobile first. Questa è la nuova normalità e ora uno standard di mercato" aggiunge Mestici.
Le carte digitali accelerano questo cambiamento nel comportamento dei clienti e consentono l'emissione di carte istantanee sul proprio dispositivo mobile. Ciò lascia la carta fisica come opzione: le carte digitali possono quindi esistere come offerta assestante o come complemento di una carta fisica esistente.
"Le Grandi Organizzazione Pubbliche e Private possono quindi offrire ai propri clienti un'ampia gamma di nuovi servizi basati sulle carte digitali. Inoltre, l'emissione di carte completamente digitali riduce i costi e l'impatto ambientale di un'Azienda poiché la plastica non è più necessaria" aggiunge Mestici.

Il nostro Mercato

L'offerta di Entrust in Partnership con N.I.D.O. Srl riguarda tutti gli aspetti fondamentali di emissione, utilizzo e gestione di carte digitali.
I clienti N.I.D.O. rappresentano il più alto valore del ns mercato di riferimento; possiamo infatti annoverare tra loro: IPZS, SOGEI, Ministero del Lavoro, NEXI Payments, Sinergia, ARUBA, ST Microelectronics, Amedea solo per fare qualche nome. *"Ma l'aspetto più importante è la passione e l'entusiasmo delle donne e degli uomini del nostro Team che da anni rappresentano il vero valore aggiunto della ns Organizzazione"* conclude Mestici.

CYBER SOLUTIONS

Alla scoperta della società che propone in Italia soluzioni di Cyber Security verticali e basate sulla certezza dell'identità fisica e digitale e sulla forza della crittografia per garantire la sicurezza e l'integrità dei dati

Stefano Penna, Direttore Divisione Cyber Security

N.I.D.O. S.R.L.

N.I.D.O. srl, società all'avanguardia nello sviluppo di soluzioni hardware e software, nella loro integrazione, commercializzazione e manutenzione, punta ad offrire alla sua clientela un portafoglio di prodotti sexy e sempre più innovativi. Per saperne di più abbiamo parlato con Stefano Penna, Direttore Commerciale della Divisione Cyber Security di N.I.D.O. Srl, società con oltre 20 anni di esperienza nei vari rami dell'IT, 15 professionisti attualmente sul campo e un fatturato nell'ordine dei 5 milioni di euro.

"Circa il 50% del fatturato N.I.D.O. Srl proviene dalla mia Divisione in cui ho la fortuna di collaborare con persone di assoluto valore" così si esprime Penna "Tutte le nostre proposte di sicurezza sono volte a coprire dei verticali di mercato, dove la competenza e la professionalità fanno la differenza tra un'identità sicura e una incerta e nella tutela dell'assoluta segretezza dei preziosi dati aziendali dei nostri clienti. Tutti i nostri servizi, tradizionali ed evoluti, coerentemente con la nostra mission vengono erogati da personale dipendente della Società.

Data Protection

"Per noi, prosegue Penna, la Data Protection è la salvaguardia dell'integrità della comunicazione garantita da una crittografia supportata da algoritmi forti e predisposta contro gli attacchi Post quantum. Le nostre proposte prevedono un potente orchestratore di tutte le chiavi di crittografia privata e la messa in sicurezza, tramite HSM evoluti, di tutti i secret aziendali compresi i codici sorgente dei preziosi applicativi dei nostri clienti.

Identità fisiche e digitali certe

N.I.D.O. srl rappresenta al 100% Entrust, una storica Certification Authority tra le più rilevanti a livello mondiale. Pertanto, conferma Penna, "siamo in grado di erogare qualsiasi certificato SSL/TLS/IoT e sistema di gestione. Grazie inoltre ad una potente piattaforma di Autenticazione Multifattore e SSO, possiamo garantire con i più alti standard di sicurezza e certificazioni correlate, la certezza delle identità che accedono alle risorse aziendali dei nostri clienti.

Applicativi sicuri

ASOC un processo olistico di sicurezza delle applicazioni al fine di ridurre al minimo i rischi aziendali legati all'utilizzo delle applicazioni. Nessuna applicazione si può ritenere sicura fino a quando non viene testata e certificata.

Digital On Boarding

Con questo termine, spiega Penna, si indicano soluzioni in grado di leggere un documento fisico d'identità digitale (passaporto/CIE/etc) tramite un'applicazione installabile su di uno smartphone, verificare che il documento digitale corrisponda alla persona che ha in mano lo smartphone ed anche che lo smartphone è della persona che lo sta utilizzando e lo stato in vita dell'utilizzatore. Con questo 'triage' si definisce un indice di compatibilità tra il documento e la persona ed essendo i dati del microchip in sola lettura all'interno del documento, si avrà un'identità certa della persona. Con queste tecnologie, continua Penna, si possono sviluppare decine e decine di soluzioni per la PA, l'Esercito e le aziende private. Unendo quindi il documento digitale, lo smartphone e la persona fisica, si ottiene un'identità digitale verificata e riconosciuta in tutta Europa, atta anche alla firma qualificata di documenti tramite apposito certificato. In pratica quello che possiamo fare con SPID/CIE in Italia come cittadini italiani, conclude Penna, lo rendiamo possibile per tutti i cittadini europei e non solo".

Le soluzioni di N.I.D.O. srl si prefiggono lo scopo di garantire le basi della Cyber Security a tutto tondo:

- Identità certificate sia fisiche che digitali
- Crittografia forte sia in termini di robustezza del certificato sia in termini di gestione e cicli di rinnovo
- Firma digitale qualificata

Queste stesse soluzioni hanno vinto negli anni la fiducia di clienti prestigiosi sul piano nazionale ed internazionale tra i quali gruppi bancari, Pubbliche Amministrazioni e molteplici società di servizi che continuano ad apprezzare anno dopo anno questa preziosa collaborazione.

L'INTELLIGENZA ARTIFICIALE AL SERVIZIO DELLA FOTOINTERPRETAZIONE MILITARE

Nuovi orizzonti nell'analisi delle immagini

PLANETEK ITALIA S.R.L.

L'evoluzione dell'intelligenza artificiale (IA) ha rivoluzionato l'analisi delle immagini nel contesto militare, offrendo un supporto senza precedenti nella fotointerpretazione. Grazie ai recenti sviluppi nell'apprendimento profondo (o *Deep Learning*), la fotointerpretazione assistita dall'IA consente di estrarre informazioni rilevanti e prendere decisioni tempestive basate su dati di immagini provenienti dai sensori di remote sensing. Inoltre, l'IA accompagnata dal calcolo processato su schede grafiche (*GPU*), può elaborare una quantità enorme di dati ad una velocità molto superiore rispetto ai classici computer che usano solo *CPU*. In questo articolo, esploreremo come l'IA, attraverso il riconoscimento automatico di oggetti, il target detection ed il conteggio degli oggetti, stia trasformando il campo della fotointerpretazione militare.

Il riconoscimento automatico di oggetti: L'IA basata su reti neurali convoluzionali (CNN) ha dimostrato una straordinaria capacità di riconoscere automaticamente oggetti all'interno di una immagine. Ad esempio, utilizzando l'addestramento su un ampio dataset di immagini etichettate (*training set*), una CNN può riconoscere e classificare veicoli, aerei, navi e persino armamenti militari. Questa capacità di riconoscimento automatico consente agli analisti di individuare rapidamente elementi di interesse nelle immagini, identificando oggetti critici per le operazioni militari e fornendo un supporto prezioso nell'analisi delle situazioni sul campo.

In Figura 1 è mostrato un dataset disponibile on-line (RarePlanes), che raccoglie più di 14000 aerei acquisiti su immagini satellitari ad altissima risoluzione (*VHR*), che permette di addestrare una rete neurale a riconoscere aerei sia civili che militari. Inoltre, data la capacità delle CNN di apprendere dai dati caratteristiche comuni, come ad esempio, le forme, le ombre e gli spigoli (dette *features*), è possibile utilizzare immagini nelle sole bande dello RGB fino ad arrivare in alcuni casi alla possibilità dell'uso di sensori prettamente pancromatici. Infine, la grande dinamicità dell'IA permette anche di poter integrare tra di loro dati provenienti da sensori differenti per poter estrarre dalle immagini di riferimento le features più importanti. In questo modo, i dati SAR e i dati ottici possono essere usati in modo combinato per aumentare le accuratezze nell'individuazione di alcuni oggetti, per esempio, navi.

Il conteggio degli oggetti: L'IA può anche essere utilizzata per contare oggetti di interesse nelle immagini, fornendo una stima accurata del numero e della distribuzione. Ad esempio, nella sorveglianza di confini o di aree sensibili, l'IA può essere addestrata per contare veicoli o individui che attraversano determinati punti di accesso. Questo può essere di grande valore per monitorare l'attività nemica, il flusso di migranti o per garantire la sicurezza nelle operazioni militari. Il conteggio di oggetti può essere molto utile anche per ricercare cambiamenti sospetti in determinate aree che presentano per un certo periodo un numero stabile di oggetti e che, improvvisamente, ne contano molti di più o molti di meno.

L'IA trova numerose applicazioni nell'ambito militare, offrendo vantaggi significativi alle forze armate. Ad esempio, nel campo della sorveglianza aerea, l'IA può aiutare a identificare e tracciare aerei nemici o non autorizzati nel proprio spazio aereo. Nell'ambito del riconoscimento facciale, l'IA può contribuire all'identificazione di persone sospette o di interesse per la sicurezza nazionale. Inoltre, l'IA può sostenere l'analisi di immagini satellitari, identificando cambiamenti nella copertura del terreno, l'insorgenza di nuove infrastrutture o la presenza di installazioni militari nemiche. L'uso dell'IA nella fotointerpretazione militare solleva importanti questioni etiche e sfide operative. È fondamentale garantire che le decisioni prese dall'IA siano controllate e validate da esperti umani, evitando possibili errori o conseguenze negative. Infatti, l'accuratezza dell'IA è interamente collegata al dato di training che gli viene fornito in addestramento. Se viene inserito un errore sistematico nel dataset di addestramento, l'IA lo imparerà e lo propagherà durante la ricerca degli oggetti. Inoltre, la privacy e la sicurezza dei dati devono essere attentamente gestite per evitare abusi o violazioni. È quindi importante sottolineare ancora una volta come l'IA può supportare e migliorare le capacità umane, ma non può sostituirle completamente. L'integrazione dell'intelligenza artificiale nella fotointerpretazione militare ha aperto nuovi orizzonti nella capacità di analisi delle immagini. Il riconoscimento automatico di oggetti, la target detection e il conteggio degli oggetti sono solo alcune delle potenziali applicazioni dell'IA nel campo. Tuttavia, è fondamentale utilizzare l'IA in modo etico e responsabile, bilanciando la sua automazione con l'esperienza e il giudizio umano. Soltanto attraverso una collaborazione efficace tra intelligenza artificiale ed esperti umani si potranno ottenere risultati avanzati e innovativi nell'ambito della fotointerpretazione militare.

Planetek Italia, in collaborazione con Hexagon Geospatial, si pone come pioniere nell'implementazione di soluzioni di intelligenza artificiale per la fotointerpretazione, utilizzando i potenti strumenti di analisi ed elaborazione di immagini di ERDAS IMAGINE, M.AppX ed ERDAS APOLLO. Questi software rendono l'IA facilmente implementabile e scalabile, consentendo agli utenti di sfruttare appieno le potenzialità dell'IA per l'analisi delle immagini nel contesto militare.

L'impegno di Planetek Italia nell'implementazione di soluzioni avanzate di intelligenza artificiale nel campo della fotointerpretazione militare si basa sulla consapevolezza dell'importanza di un approccio integrato, in cui l'IA e gli esperti umani lavorano a stretto contatto per raggiungere risultati ottimali. Con il supporto delle tecnologie Hexagon Geospatial e dell'esperienza trentennale nel campo del telerilevamento, Planetek Italia è in grado di fornire strumenti affidabili e all'avanguardia per migliorare le capacità di analisi e contribuire alla sicurezza e alla difesa nazionale."

Figura 1: Dataset disponibile on-line per addestrare una rete neurale a riconoscere aerei civili e militari. @Credits: RarePlanes

LE NOSTRE SOLUZIONI RFDS A BORDO NAVE

POLOMARCONI.IT S.P.A.

POLOMARCONI.IT Spa è un'azienda privata italiana nata da oltre 25 anni, dall'acquisizione di aziende storiche specializzate nel settore delle **Radiofrequenze**.
POLOMARCONI.IT sviluppa e distribuisce prodotti standard e personalizzati con la massima qualità offrendo soluzioni di radiocomunicazione per diversi mercati, in ambito Civile e della Difesa. Oggi più che mai **POLOMARCONI.IT** supporta il Cliente nella progettazione dei sistemi di comunicazione a bordo nave gestendo le interferenze di co-locazione nelle bande **VHF** ed **UHF**. Grazie alla sua **esperienza nel campo RF**, POLOMARCONI.IT fornisce soluzioni dedicate in base alle esigenze del cliente.
Le soluzioni di **POLOMARCONI.IT**, già installate nelle piattaforme navali, sono applicabili anche per gli spazi ridotti di **sommergibili e sottomarini**.

ANTENNE NAVALI:
- Antenna dipolo a larga banda 100 - 2000 MHz
- Sistema d' antenna wraparound VHF/UHF
- Antenne SATCOM in polarizzazione V/H
- Antenne a pannello RHCP

FILTRI E COMBINATORI NAVALI:
- Filtri automatici e manuali VHF/UHF
- Filtri automatici broadband 100 - 512 MHz
- Combinatori a doppio ponte VHF/UHF
- Matrici d'antenna e selettori DC - 1 GHz

LE SFIDE A BORDO
- Scarso isolamento (disaccoppiamento) tra i canali
- Interferenze di co-siting causate dalla presenza di diverse antenne installate vicine tra loro
- Bassa tenuta in potenza per ciascun segnale radio trasmesso
- Elevati costi di manutenzione e tempo dedicato alle sostituzioni
- Numero elevato di cavi RF presenti nelle condotte

LA NOSTRA SOLUZIONE: RADIO FREQUENCY DISTRIBUTION SYSTEM
L'**RFDS** di Polomarconi, viene progettato e personalizzato secondo la tabella SIMOP, mantenendo la flessibilità e la scalabilità dell'architettura grazie al design modulare. Inoltre grazie al protocollo SNMP integrato, è possibile monitorare lo stato e controllare l'intero RFDS direttamente dal Command Control Managment System.

I BENEFICI
- Riduzione delle interferenze di co-locazione grazie alla combinazione di più canali in un'unica antenna.
- Eccezionale isolamento tra ciascun canale grazie alla soluzione che comprende combinatori in configurazione a doppio ponte
- Elevata gestione della potenza fino a 100 Watt per ciascun canale.
- Minor numero di antenne installate a bordo
- Riduzione dei costi e rapida sostituzione grazie al design modulare
- Facilità di espansione del sistema
- Protocolli di comunicazione radio personalizzati
- Percorsi RF ridondanti sia per ricetrasmettitori che per le antenne
- Possibilità di isolare una singola antenna o un gruppo di antenne da trasmettitori
- Capacità di ricezione migliorata con l'impiego di LNA ad alto guadagno

IL FREQUENCY HOPPING
L'**RFDS** POLOMARCONI supporta la modalità **Frequency Hopping** secondo gli standard STANAG utilizzando:
- Matrici d'antenna e selettori
- Filtri Agili
- Filtri automatici con by pass

I VANTAGGI DELLE NOSTRE SOLUZIONI
- Semplificazione logistica
- Riduzione dei tempi di inattività del sistema
- Riduzione dei tempi di fornitura
- Riduzione del costo complessivo del sistema RF a bordo
- Riduzione del numero delle parti di ricambio necessarie
- Sistema trasparente rispetto alle forme d'onda applicate e compatibile con tutte le Radio
- Assistenza, attività di manutenzione, riparazione e supporto
- Formazione specializzata per l'uso del sistema a bordo e la sua manutenzione

Le soluzioni di POLOMARCONI includono uno studio complessivo del sistema finalizzato a ridurre il numero di antenne installate e ad evitare potenziali interferenze e la progettazione su misura orientata ad ottenere il miglior rapporto prestazioni di segnale, le dimensioni ridotte e il minor costo totale del sistema.

FENOMENOLOGIE E METODOLOGIE NEGLI SCENARI DI ANALISI IN EPOCA DI GUERRA COGNITIVA

SISTEMI & AUTOMAZIONE

La sostanziale ed invasiva incertezza su cui da sempre s'impernia l'esistenza dell'Uomo, sembra aver raggiunto il suo massimo storico, Anno Domini 2023.

Viviamo in un'era identificata da un contrasto permanente, una Cognitive Warfare caratterizzata da una miriade di realtà diverse, spesso in conflitto tra loro. L'incertezza diventa per l'appunto la condizione prevalente; i cambiamenti rapidi e incessanti, l'accelerazione tecnologica, e l'abbondanza di informazioni creano confusione e ansia.

Nel 1996 il primo clic sulla barra di ricerca di Google – che proponeva una grafica eccessivamente fanciullesca per esser preso sufficientemente sul serio – stava concretamente innescando una nuova dimensione dell'essere: sembrava una scoperta badiale poter raggiungere hic et nunc qualunque patrimonio informativo, ed era facile benedire Sergey Brin e Larry Page per aver portato nelle vite di tutti uno strumento efficace in grado di eseguire il suddetto task – senza badar troppo alle necessarie riflessioni etiche che sarebbero state allora anacronistiche e prive di senso.

Un eccellente esempio di innovazione tecnologica dirompente, senza dubbio.

Gli allora analisti Intelligence – complice la ludica grafica, la scarsa conoscenza del mezzo e, non ultima, l'incapacità oggettiva di prevedere il futuro – neanche potevano immaginare che di lì ad un ventennio più tardi sarebbe stato il precursore di un nuovo paradigma di analisi. Quel tipo di analisi che è chiamata a muoversi e fornire risposte e soluzioni efficaci nella dimensione dei Big Data.

Oggi la sovrabbondanza di dati ha concretamente pervaso qualunque sfera dell'esistenza umana, complice la continua innovazione tecnologica che avanza senza sosta, gli endemici mutamenti ingenerati sulla mente umana dal periodo pandemico, il climate change, la necessità di imparare, disimparare e reimparare continuamente.

Le cose stanno anche cambiando sugli scenari di analisi e Intelligence. Sia essa su territorio di guerra o in altri campi dello scibile. Un approccio fenomenologico e metodologico al Dato diviene sempre più necessario per comprendere e navigare gli scenari di analisi nella nostra epoca.

Purtroppo, la metodologia odierna rifiuta spesso l'idea di un'unica "verità" oggettiva, preferendo piuttosto una pluralità di verità. Ciò ha inevitabilmente influenzato anche la pratica dell'analisi in modi diversi. In primo luogo, c'è una maggiore attenzione alla diversità di prospettive e voci, piuttosto che ad una singola narrativa dominante. Inoltre, dobbiamo fare i conti anche con il fenomeno della Cognitive Warfare, la nuova dimensione dei conflitti si basa sulla manipolazione delle percezioni e delle credenze. Nell'era della post-verità e della manipolazione delle informazioni, la Cognitive Warfare è diventata una componente critica della strategia militare e politica.

È qui che entra in gioco la fenomenologia che, nel suo significato più generale, costituisce lo studio dell'esperienza e della coscienza. Applicata agli scenari di analisi, un approccio fenomenologico può aiutare a comprendere le percezioni, le esperienze e la coscienza di questi professionisti operanti sul campo d'indagine. Ogni analista ha un'esperienza individuale unica - basata sulla propria formazione culturale e professionale – capace di influenzare la percezione e l'interpretazione delle informazioni. La fenomenologia può inoltre identificare e affrontare i bias cognitivi e altre distorsioni che influenzano l'analisi dell'intelligence. Ad esempio, può aiutare a comprendere come la sovrabbondanza di dati, i "deficit" cognitivi possono influenzare la percezione e l'interpretazione delle informazioni e dunque le decisioni da intraprendere. Tuttavia, è importante notare che la fenomenologia è uno strumento descrittivo e non prescrittivo. Non può dire agli analisti come dovrebbero percepire o interpretare il Dato, ma può aiutare a comprendere come queste percezioni e interpretazioni si sviluppano e si influenzano a vicenda.

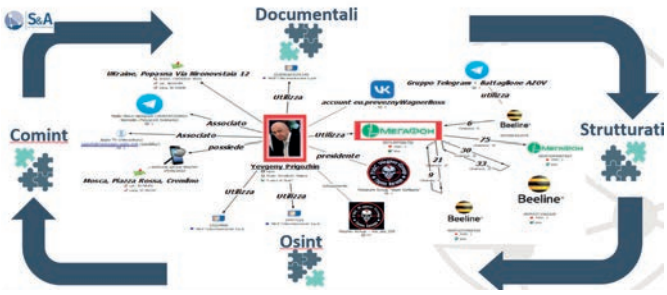
La facilità di acquisizione del dato a volte ha scavalcato la pianificazione e la scelta ponderata delle fonti e delle caratteristiche del dato stesso.

L'esempio del traffico di cella scaturito dall'utilizzo dei telefoni cellulari, spesso richiesto per qualsiasi attività investigativa, negli ultimi anni ha portato alla luce con forza questo problema. Avere tanti dati non sempre è un vantaggio, se non si è in grado di gestirli fin dalla fase di richiesta, e spesso si trasforma nell'averne troppi generando stress, rallentamenti e crisi nel processo di analisi.

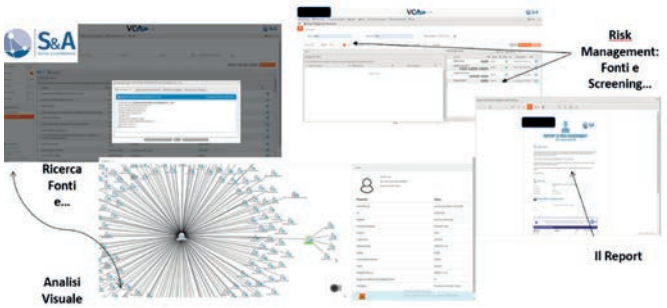
La tecnologia fornisce continuamente soluzioni attraverso l'evoluzione dei sistemi software, ma ciò non toglie che alcuni problemi di analisi abbiano una grande componente metodologica che può aiutare a tracciare percorsi consistenti di gestione del dato.

La consapevolezza di ciò che serve come dati, acquisita attraverso corrette ricerche di sfondo dell'area di studio o di investigazione, come ci insegna la teoria dell'intelligence, è sempre più imprescindibile anche se la tecnologia dell'Intelligenza Artificiale promette

di elaborare e correlare facilmente moli enormi di dati, anche inutili, fornendo risposte prive di rischi. È cronaca attuale che non sia proprio così.
L'uomo, anzi l'analista umano, resta ancora imprescindibile in tutto il processo di analisi, dall'inizio alla fine per esercitare il ruolo fondamentale di controllore, revisore e rigeneratore dell'intero flusso. La tecnologia deve fare quello che da sempre fa, fornire velocità, memoria a lungo termine, consistenza, reportistica veloce e fornire rivedibilità e ripetibilità dell'intero processo di acquisizione, analisi e produzione di informazione e conoscenza. La tecnologia della analisi visuale è da sempre lo strumento di riferimento per l'analisi e la correlazione del multiverso informativo a beneficio dell'analista. Esempi della sua efficacia sono disseminati negli uffici e nelle aule del modo investigativo e dell'analisi di intelligence e in molti casi sono una prassi operativa ormai indispensabile.
Tuttavia, si è fatto e si sta facendo molto di più in questi anni. È stata intrapresa la strada della correlazione automatica di più fonti (vedi figura), della reportistica che raccoglie informazioni da queste offrendo strumenti di consultazione chiari ed esaustivi, la creazione di algoritmi che forniscano analisi chiare e veloci del comportamento sociale e geografico di persone da profilare velocemente.



Ma soprattutto la flessibilità e la rivedibilità di questi strumenti è la vera chiave di volta per supportare gli analisti. Non solo poter salvare il risultato delle analisi e renderlo fruibile nella disseminazione è importante, ma anche fornire la possibilità di recuperare velocemente il percorso di analisi attraverso il salvataggio dei parametri delle ricerche e delle elaborazioni costruite dall'analista e permettergli di recuperarle, rieseguirle, modificarle in qualsiasi momento anche a distanza di tempo.
Preservare il percorso di analisi con tutte le scelte fatte e ricostruirlo nei minimi dettagli è la sfida per fornire all'analista uno strumento che lo metta al riparo da errori di valutazione forzati dai tempi stretti riservati al processo decisionale. Quindi tutte le metodiche e gli strumenti teorici e pratici descritti finora, portano alla necessità di elaborare un approccio olistico all'analisi, che intenda coadiuvare l'analista nella riduzione dell'incertezza decisionale e che possa concretamente rappresentare un valido alleato in fase di disseminazione, grazie alla chiarezza espositiva nella rappresentazione dei dati raccolti.



Uno strumento che possa fungere al contempo da "raccordo" per le varie tipologie di fenomeni di cui la vita reale consta, tradurre i Dati grezzi in informazioni significative, supporti la memoria dell'analista in fase di recupero di queste nozioni ed informazioni hic et nunc. Il grafo visuale, presente in tutti i prodotti della Sistemi & Automazione S.p.A, coadiuva quelle tipologie di calcolo sistemico che sfuggono alla precisione e spesso alla percezione della mente umana e al contempo sono in grado di ricevere e mettere a sistema l'eterogeneità endemica dei Dati necessari a fornire risposte che si approssimino quanto più possibile alla risposta corretta agli eventi reali.

ESISTE UN SISTEMA DI PROTEZIONE FIREWALL A BORDO DEI VELIVOLI MILITARI?

STORMSHIELD

Di pari passo con gli sviluppi degli aerei civili, i velivoli militari stanno sempre più abbracciando le tecnologie digitali e si affidano a una pletora di connessioni con i sistemi a terra.
Se da un lato questa iperconnettività fornisce una soluzione a requisiti operativi vitali, dall'altro può essere fonte di nuove vulnerabilità informatiche.
Ma quali sono queste minacce? E quali le difese disponibili? In questo articolo sulla cybersecurity diamo una panoramica sugli scenari da tenere in considerazione.
Agosto 2018. Il segretario dell'aeronautica statunitense, Will Roper, dichiara senza mezzi termini alla stampa nazionale: "*Uno dei nostri aerei potrebbe essere abbattuto con pochi colpi di tastiera*". Questa scioccante ammissione arriva sulla scia di un esperimento condotto dal Pentagono, in cui gruppi di hacker denominati "White Hat" sono stati incaricati di violare i sistemi di bordo dell'F-15 dell'US Air Force.
E il loro obiettivo è stato raggiunto: la (teorica) possibilità di abbattere un aereo da guerra a mezz'aria. "*Questo hack è frutto di decenni di negligenza da parte dell'aeronautica militare statunitense nei confronti della sicurezza informatica*", ammette Will Roper.

Iperconnettività: sinonimo di efficienza... ma anche di vulnerabilità

Naturalmente, i dettagli tecnici di questo hacking non sono stati resi noti e rimangono altamente riservati. Tuttavia, il motivo per cui questi "White Hat" sono riusciti a violare un aereo da combattimento così importante è che - come molti altri aerei - l'F-15 è ormai altamente digitale e connesso. "*Il software dei moderni aerei da combattimento si basa su milioni di linee di codice. Se questo codice venisse stampato su carta, si creerebbe una pila alta più di 10 metri*", spiega in un'intervista Matthias Bertram, vice responsabile del sottoprogetto di ingegneria del progetto "New Fighter Aircraft" in Svizzera.
La questione della protezione informatica degli aerei da combattimento è una preoccupazione reale per la Svizzera, che intende acquistare i nuovi F-35 americani nel prossimo futuro. Questi aerei da guerra sono presentati come ultramoderni, ma sono altresì stati criticati per la loro ampia superficie esposta agli attacchi digitali. Sono, dunque, un esempio da manuale delle minacce informatiche a cui può essere esposto oggi un velivolo di tale importanza strategica.
In un rapporto dell'Istituto francese per le relazioni internazionali (IFRI) sugli sforzi dell'esercito francese per affrontare i rischi informatici, tre dei principali sottosistemi dell'F-35 sono stati identificati come critici:

1. il software per il riconoscimento dei bersagli,
2. il software per la manutenzione predittiva dell'aereo
3. i simulatori di volo.

Il primo sottosistema, il Joint Reprogramming Enterprise, elabora un elevato numero di firme note degli aerei da combattimento esistenti e consente di rilevare e identificare automaticamente le minacce prossime al velivolo (carri armati, droni, ecc.). Ciò fornisce ai piloti informazioni cruciali, aiutandoli a prendere decisioni tattiche in tempo reale.
La falla consiste nel fatto che "*una manomissione dei suoi aggiornamenti, permetterebbe agli hacker di iniettare dati falsi all'interno del sistema rendendo certi bersagli non rilevabili o ingannando il sistema di tiro*".
Il secondo sottosistema considerato critico è l'Autonomic Logistics Information System, un altro programma di bordo. Il suo scopo è migliorare le capacità di manutenzione predittiva del velivolo effettuando una autovalutazione dello stato di usura di alcuni dei suoi componenti.
Trasmettendo questo flusso di informazioni alla sede centrale di Lockheed Martin (dove risiede il costruttore del velivolo), è possibile approvvigionarsi delle parti di ricambio prima ancora del verificarsi di potenziali guasti, ottimizzando così la disponibilità operativa del velivolo - un vantaggio significativo durante una situazione di conflitto.
Tuttavia, se questo flusso di dati venisse intercettato, gli esperti temono che "*i potenziali nemici acquisirebbero informazioni sulla struttura dell'aereo e sul contenuto delle sue missioni*".
Infine, la terza criticità attenzionata.
Prima di lasciare il suolo, i piloti dell'F-35 vengono addestrati utilizzando i simulatori di volo. Tali simulatori sono estremamente avanzati e programmati per offrire un'esperienza di pilotaggio ultra-realistica. Anch'essi, però, sono altamente connessi (soprattutto per scopi manutentivi) e, se violati, potrebbero consentire ai nemici cyber di "*dedurre informazioni chiave sul funzionamento dei caccia*".
Tutte queste diverse vulnerabilità evidenziano i rischi informatici che accompagnano lo scambio di dati tra aerei e infrastrutture di terra. Per questo motivo, "*in ambito militare, cerchiamo di ridurre al minimo tali connessioni, che forniscono anche vettori di minaccia per il velivolo*", spiega Alain Mingam, architetto della sicurezza di Airbus.
Ma le circostanze operative attuali richiedono che le comunicazioni con i sistemi di terra siano comunque disponibili, senza rinunciare a misure di sicurezza adeguate.
"N*egli ultimi 15 anni, l'industria dell'aviazione militare si è resa conto di questa debolezza. Per diversi decenni, la sicurezza*

operativa è stata fortemente integrata nel processo di sviluppo dei velivoli", afferma Christopher Cachelou, ingegnere pre-vendita specialista nel settore difesa presso **STORMSHIELD** (Azienda francese leader in Europa per la progettazione di soluzioni Cyber Security in ambito IT e OT).

"*Si basa su un'analisi del rischio funzionale per garantire il corretto funzionamento del dispositivo, sia in termini hardware sia in termini software. La cybersecurity a livello di prodotto è molto più recente e meno integrata nel processo di sviluppo. Si basa anch'essa su un'analisi del rischio, ma in questo caso del rischio informatico, come ad esempio nel caso del metodo EBIOS*".

Mingam conferma questo stato di fatto, sia nell'aviazione militare sia in quella civile.

"*Con l'ACARS (per la gestione delle operazioni di volo, il controllo del traffico aereo e la manutenzione), il FOMAX (per la manutenzione predittiva) e i sistemi di intrattenimento in volo (IFE), il numero di strumenti digitali che comunicano con la terra è molto maggiore nell'aviazione civile e sono in circolazione da molto più tempo*".

Contrariamente a quanto si potrebbe pensare, l'industria civile spesso apre la strada a quella militare in termini di sicurezza informatica. Ad esempio, è risaputo che l'A400M (aereo da trasporto militare) progettato da Airbus e proposto all'Organizzazione europea per la cooperazione in materia di armamenti (OCCAR) abbia tratto grande beneficio dagli studi sulla protezione informatica condotti per l'A380.

Rischiamo di assistere a una guerra cibernetica nei cieli?

La natura segreta e poco documentata della guerra cibernetica fa sì che il numero di studi sulla minaccia cibernetica in ambito militare sia inevitabilmente limitato. Ad ogni modo, è interessante porre l'attenzione sul numero di attacchi informatici sferrati contro aerei e infrastrutture civili.

Secondo l'Agenzia europea per la sicurezza aerea (EASA), questa cifra ha superato i 1.000 attacchi al mese in media dal 2016. E, sebbene le informazioni relative all'F-15 siano state ottenute grazie al pentesting, sono già state riportate notizie di azioni di hacking (più o meno riuscite) contro aerei militari di diversi Paesi.

Nel 2009, i computer della base aerea 107 di Villacoublay sono stati infettati dal virus Conficker, il quale si pensa si sia diffuso attraverso postazioni Windows non aggiornate. Secondo una lettera confidenziale inviata al sito web Intelligence Online, in quell'occasione diversi velivoli Rafales sono rimasti bloccati a terra per due giorni.

Alcuni documenti classificati rivelati da Edward Snowden hanno anche mostrato che i servizi di intelligence statunitensi e britannici sono stati in grado di intercettare e decriptare i feed video dei droni aerei israeliani e dei caccia F-16, fornendo loro importanti informazioni tattiche ai margini delle tensioni geopolitiche in Iran.

Allo stesso tempo, il rapporto dell'IFRI riporta la testimonianza dell'ex capo della difesa cyber francese, il contrammiraglio Arnaud Coustillière, che spiega che un drone francese Harfang è stato vittima di un tentativo di dirottamento in Afghanistan. L'attacco alla fine fallì, ma si dice che abbia comunque portato all'interruzione della missione del velivolo.

Infine, anche i dati sensibili conservati all'interno dell'infrastruttura di terra sono un obiettivo privilegiato.

Nel 2017, infatti, quasi 30 GB di dati commerciali (non classificati) relativi a programmi di difesa australiani sono stati esfiltrati durante un attacco informatico ai danni di un fornitore governativo.

Un altro episodio simile si è verificato nel 2020, quando Leonardo (uno dei principali gruppi industriali aerospaziali europei e di origine italiana) ha notato un flusso anomalo di dati in uscita dai suoi sistemi e ha prontamente allertato le autorità italiane. L'indagine ha stabilito che uno dei computer violati conteneva informazioni classificate sul progetto sperimentale "nEUROn". Sotto il controllo francese dal 2012, l'obiettivo di "nEUROn" è progettare un nuovo aereo da difesa militare europeo.

Più recentemente, un gruppo di criminali informatici ha pubblicato sul dark web i dettagli tecnici del Globaleye svedese-canadese (un aereo militare di sorveglianza e intelligence). Le informazioni sembrano essere state raccolte dai sistemi informatici di Bombardier, il costruttore canadese coinvolto nella produzione dell'aereo.

Anche se rara, la minaccia di dirottamento digitale delle apparecchiature militari è presa molto sul serio da tutte le nazioni che utilizzano tali dispositivi. In Francia, l'esercito ha già istituito un contingente di 1.100 cyber-combattenti, che sarà rafforzato da 5.000 unità aggiuntive nel 2025, suddivise tra le forze armate, la Direzione generale degli armamenti (DGA) e i servizi segreti francesi (DGSE).

Si tratta, forse, di un'iniziativa in previsione di una guerra cibernetica? No, secondo il generale di brigata dell'aeronautica Didier Tisseyre, vicedirettore del centro di comando Comcyber, come riportato da IFRI: "*Abbiamo già condotto attacchi informatici nei teatri operativi in cui è impegnato l'esercito francese, come nelle regioni del Levante e del Sahel. Ciò può comportare l'intercettazione di informazioni prima di un'operazione, l'inganno dei radar antiaerei o l'immobilizzazione delle difese nemiche*".

Azione preventiva: quali sono allora le opzioni disponibili?

La protezione informatica degli aerei da combattimento è quindi una questione molto delicata. In teoria, proteggere un aereo da combattimento dalle minacce informatiche è

simile alla protezione di qualsiasi terminale connesso a una rete civile, come sottolinea Bertram.

Per una maggiore protezione in ambito militare, viene eseguita una suddivisione delle funzionalità a livello di aeromobile congiuntamente a un'analisi dell'impatto sulla sicurezza e in modo particolare attraverso un documento chiamato "Functional Hazard Assessments" (FHAs). "*Questo ci permette di mappare con precisione le varie funzionalità dell'apparecchiatura e le eventuali conseguenze in caso di malfunzionamento*", spiega Mingam. "*Possiamo quindi esaminare i vettori di attacco digitale che potrebbero potenzialmente comprometterle, identificarne il rischio associato e dedurre i componenti di sicurezza che devono essere installati sul percorso del possibile attaccante per far sì che il rischio sia accettabile*".

Ma quali sono i requisiti in questo settore?

In Francia, gli operatori civili e privati di importanza vitale devono rispettare i requisiti di cybersecurity stabiliti dall'articolo 22 della legge francese sulla pianificazione militare. Tali requisiti riguardano sia i processi organizzativi sia le soluzioni tecnologiche da implementare per proteggere le infrastrutture fisiche e digitali. A livello europeo, la direttiva NIS include alcuni operatori del settore del trasporto aereo nell'elenco degli operatori di servizi essenziali.

Da un punto di vista organizzativo, la sicurezza generale di un aereo da combattimento si basa sulla combinazione di tre sistemi complementari:

1 - sicurezza delle infrastrutture di terra: è di competenza del responsabile del sito e consiste nella messa in sicurezza di basi, aeroporti, centri di comando e altre strutture militari (e civili) essenziali per il funzionamento quotidiano dei mezzi militari;

2 - sicurezza dei sistemi informativi e delle infrastrutture di rete (ISS): è di competenza dell'OSSI ed è tradizionalmente coperta da una carta di sicurezza informatica che regola i processi operativi, i diritti dei dipendenti e del personale militare e civile di accedere e visualizzare le risorse digitali, ecc;

3 - sicurezza del prodotto: è la responsabilità del Product Security Officer (PSO), che coinvolge tutte le soluzioni hardware e software direttamente installate sul prodotto in questione (in questo caso, l'aereo da combattimento) per portarlo agli standard di sicurezza richiesti.

In termini di prodotti, Bertram cita, a titolo di esempio, l'uso di firewall che forniscano "firme, crittografia, accesso basato sui ruoli, scanner antivirus e analisi in tempo reale dei sistemi in esecuzione". Queste soluzioni devono anche essere progettate per resistere a condizioni fisiche estreme (temperatura, pressione, urti, ecc.) per consentire il monitoraggio delle apparecchiature nei vari ambienti.

Quali sono le sfide di domani?

Gli aerei militari devono essere creati come "cybersecure by design". Ma se questo è il quadro futuro, sorge un'altra domanda: come assicurare una protezione sufficiente per tutto il ciclo di vita dell'apparecchiatura?

Un aereo da combattimento medio ha una durata di vita di 30 anni. Con la straordinaria velocità con cui si evolve il mondo digitale, le minacce informatiche di domani saranno drasticamente diverse da quelle di oggi. In risposta a questo problema, i produttori stanno aggiungendo un servizio di manutenzione di sicurezza (o MCS) ai loro servizi di manutenzione operativa (MCO). "L'MCO assicura che l'aeromobile sia mantenuto in condizioni operative per tutto il suo ciclo di vita", spiega Cachelou. "Allo stesso tempo, l'MCS assicura che l'aeromobile sia mantenuto in condizioni di sicurezza per tutto il suo ciclo di vita. Garantisce che il velivolo sia costantemente aggiornato ai livelli di sicurezza appropriati a fronte di rischi e minacce informatiche in costante evoluzione". Si ritiene, ad esempio, che sia stata l'aggiunta di nuove funzionalità digitali, unitamente alla mancanza di aggiornamenti di sicurezza informatica, a rendere vulnerabile l'F-15 statunitense.

Alain Mingam ci porta ancora un passo avanti nel futuro. Mentre attualmente si pensa alla sicurezza informatica come a una serie di barriere volte a prevenire o rallentare qualsiasi tentativo di attacco informatico, i produttori e gli editori stanno preparando le risposte future. "*Stiamo implementando sistemi di protezione; ma nessuna protezione è impenetrabile, quindi dobbiamo inventarci qualcosa di diverso*". E se queste protezioni fossero in grado di reagire ed evolversi per rispondere meglio a un'offensiva, o se potessero addirittura consentire al difensore di contrattaccare?

"*La nostra divisione di difesa informatica è dedicata a questo tema e stiamo elaborando architetture composte da dispositivi di monitoraggio e capacità di reazione. Ci stiamo muovendo verso processi di difesa elettronica in tempo reale*". In una guerra di questo tipo, proprio come in una guerra "reale", la sicurezza informatica non sarebbe più solo una sfida a sopportare i colpi, ma anche a saper contrattaccare.

IL TRIBUNALE UNIFICATO DEI BREVETTI

Lorenzo Sordini

STUDIO TORTA

Dal 1° giugno 2023 sono entrati in vigore il brevetto unitario (già oggetto di un articolo pubblicato nell'edizione 2022 di questa rivista) ed il Tribunale Unificato dei Brevetti (Unified Patent Court - UPC). All'UPC sono delegate le vertenze brevettuali basate sia sul brevetto unitario sia, in prospettiva, su tutti i brevetti europei.

In particolare, le vertenze aventi ad oggetto il brevetto unitario, fatta eccezione per le azioni di rivendica (titolarità del brevetto), sono di competenza esclusiva dell'UPC che ha anche competenza esclusiva sui brevetti europei "tradizionali", anche se per questi ultimi è previsto un periodo transitorio di sette anni (eventualmente rinnovabile) nel corso del quale il titolare può sottrarre il proprio brevetto alla competenza esclusiva dell'UPC depositando una richiesta di rinuncia (cosiddetto opt-out). Il titolare ha anche la possibilità di ritirare l'opt-out, ma non di richiedere nuovamente l'opt-out una volta ritirato.

Più nello specifico, l'UPC ha giurisdizione sui seguenti titoli: i brevetti europei con effetto unitario, i certificati di protezione supplementare rilasciati per prodotti protetti da brevetto, i brevetti europei "tradizionali" che non sono ancora scaduti alla data di entrata in vigore dell'accordo sull'UPC (Unified Patent Court Agreement - UPCA), nonché quelli rilasciati dopo tale data, e le domande di brevetto europeo che sono pendenti alla data di entrata in vigore dell'UPCA o depositate dopo tale data.

L'UPC comprende una Corte di prima istanza, una Corte d'Appello e un registro avente la funzione di cancelleria. L'UPC ha l'obiettivo di autofinanziarsi per cui le parti in causa devono pagare delle tasse (court fees) relativamente elevate, almeno rispetto agli standard del sistema giudiziario italiano. Un altro obiettivo dell'UPC consiste nel concludere la prima istanza di giudizio nell'arco di un anno.

L'UPCA prevede che la Corte di prima istanza comprenda una divisione centrale con sede a Parigi, due sezioni distaccate a Londra e Monaco di Baviera e delle divisioni locali/regionali. La sede della Corte d'Appello è in Lussemburgo. La distribuzione delle cause nelle varie sezioni avviene secondo la classificazione brevettuale internazionale.

Sebbene l'UPCA non sia stato aggiornato a seguito della Brexit, è evidente che Londra non possa ospitare una delle sezioni della divisione centrale. Al momento si è deciso di distribuire provvisoriamente le competenze di Londra fra Parigi e Monaco, anche se in futuro Milano potrebbe diventare sede di una sezione della divisione centrale responsabile delle cause relative ad uno o più settori tecnologici inizialmente assegnati alla sede di Londra.

I paesi aderenti all'UPCA possono avere una divisione locale o aggregarsi per definire una sezione regionale di prima istanza. Qualsiasi Tribunale di prima istanza ha un collegio giudicante di composizione multinazionale, che nei tribunali locali può variare in funzione del numero di cause. Qualsiasi Collegio giudicante della Corte d'Appello ha una composizione multinazionale di cinque giudici, tre dei quali togati e di nazionalità diversa e due dei quali tecnici con qualifica ed esperienza nel campo tecnologico su cui verte la causa.

L'UPC ha competenza esclusiva sulle seguenti fattispecie: azioni di contraffazione, accertamento negativo di contraffazione, azioni per misure provvisorie e protettive, azioni di revoca di brevetti e dichiarazione di invalidità di certificati complementari di protezione, azioni per danni o compensazioni derivate da protezioni provvisorie conferite da una domanda di brevetto europeo pubblicata, azioni relative all'uso dell'invenzione prima del rilascio del brevetto o al diritto di pre-uso, azioni per compensazioni di licenze e azioni relative a decisioni dello European Patent Office nell'esecuzione dei compiti relativi alla gestione del brevetto unitario.

Indipendentemente dalla sede che decide il caso, la decisione ha effetto sull'intero territorio in cui il brevetto è efficace: per il brevetto europeo con effetto unitario in tutti paesi che hanno ratificato l'UPCA (17 paesi a oggi) e per il brevetto europeo tradizionale in tutti in paesi che hanno ratificato l'UPCA, in cui è stato convalidato ed è in vigore.

Attualmente l'orientamento dei titolari di brevetti europei e di domande di brevetto europeo sembra essere caratterizzato dalla prudenza per cui i brevetti più importanti sono oggetto di opt-out mentre i brevetti meno importanti vengono convalidati in pochi Paesi. Più in generale, il brevetto unitario sembra essere poco richiesto, mentre l'opzione preferita sembra essere l'opt-out.

T-DROMES: LA PIATTAFORMA TELESPAZIO PER I SERVIZI CON I DRONI

TELESPAZIO S.P.A.

Ormai da qualche anno i droni si stanno rivelando strumenti chiave nella trasformazione dell'industria: permettono di ottimizzare la ripetitività delle operazioni ed al tempo stesso di migliorare l'impatto ambientale. Inoltre, offrono la possibilità di acquisire dati ed immagini, seppur su aree ristrette, con risoluzioni rivoluzionarie rispetto ai metodi tradizionali, come l'osservazione via satellite o l'aviazione tradizionale. Infine, non avendo un pilota fisico sul mezzo, possono arrivare in ambienti pericolosi per il monitoraggio, o al limite anche per l'intervento, come anche permettere di intervenire in situazioni di emergenza dovute ad esondazioni, frane ed incendi.

L'expertise di Telespazio anche in questo dominio si è formata negli anni grazie alla realizzazione di numerosi progetti che hanno avvicinato lo spazio al mondo dei droni, relativi ad esempio all'integrazione ATM/UTM, alla mobilità aerea urbana ed ai servizi applicativi in molteplici ambiti (e.g.: law enforcement, monitoraggio delle infrastrutture, agricoltura e logistica sanitaria).
La piattaforma T-DROMES è la matura espressione delle competenze digitali di Telespazio applicate al mondo dei servizi ed è stata sviluppata per cogliere le esigenze del nuovo mercato dei droni e per affrontarne le sfide, legate alla possibilità di effettuare su larga scala voli BVLOS e BRLOS autonomi / automatici, in piena sicurezza. Con T-DROMES, Telespazio ha implementato il modello "Drone as a Service" (DaaS) che, con un approccio integrato, consente di gestire servizi con i droni a 360 gradi: dalla pianificazione e gestione della missione e delle operazioni, svolte da Telespazio e/o da altri Operatori, al processing e presentazione dei dati acquisiti per la consegna al cliente delle informazioni utili.

Una tale soluzione integrata offre al cliente finale la possibilità di non doversi occupare della scelta del drone e/o del sensore migliori per un determinato servizio, né degli aspetti di sicurezza, safety e delle autorizzazioni necessarie. Consente inoltre al cliente di non dover affrontare i costi di acquisto e manutenzione di droni e sensori, del training del personale e del set-up e del continuo aggiornamento del sistema di gestione della qualità.
In particolare, la piattaforma fornisce il monitoraggio dello stato del drone nella fase pre-operativa, durante l'esecuzione della missione ed suo al termine. La funzionalità di pianificazione copre tutti gli aspetti della progettazione della missione, compresa l'interfaccia con i sistemi dell'autorità di regolamentazione ed il supporto alla valutazione del rischio. Inoltre, T-DROMES fornisce:

- funzionalità dedicate alla fase esecutiva della missione, per la gestione remota automatica delle operazioni attraverso funzioni di tracciamento, comando e controllo;
- monitoraggio e analisi della missione, sia durante l'esecuzione della missione che ai fini post-analisi, inclusa la telemetria del payload;
- elaborazione e gestione dei dati, comprese le applicazioni AI per l'estrazione e la generazione di informazioni utilizzabili (da video e qualsiasi tipo di sensore di immagini).

Elemento distintivo della soluzione risiede nell'integrazione in T-DROMES delle competenze chiave del gruppo Telespazio, maturate in oltre 60 anni di business:

- la geo-informazione, per la gestione e processing dei dati acquisiti nei diversi verticali, inclusa l'elaborazione attraverso algoritmi di AI customizzati per i vari casi applicativi;
- la navigazione satellitare, per avere in ogni momento la posizione del drone con estrema precisione, utilizzando i dati multi-costellazione ed EGNOS, e valutandone inoltre l'integrità al fine di aumentare la sicurezza;
- la comunicazione satellitare, poiché attraverso una COM-BOX proprietaria Telespazio è in grado di accedere ad una rete di comunicazione ibrida (satellitare ed LTE) aggiuntiva rispetto a quella nativa radio del drone, su un canale dedicato e sicuro;
- le operazioni, i centri operativi di Fucino, Matera, Lario e Scanzano, permettono di avere personale altamente qualificato operativo 24/24h e 7/7g;
- il foot print geografico. L'azienda è presente in oltre 15 paesi nel mondo, assicurando in tal modo a grandi clienti la possibilità di avere un servizio presente in ogni paese.

Ma comunicazioni satellitari affidabili, posizionamento GNSS accurato ed immagini satellitari geo-referenziate ad alta precisione sono solo alcune delle tecnologie spaziali fornite da Telespazio per abilitare le operazioni BVLOS/BRLOS. Con i suoi servizi a valore aggiunto Telespazio vuole andare oltre la sola esecuzione di voli BVLOS/BRLOS, fornendo T-DROMES per la gestione ed il controllo remoto di flotte senza pilota che operano in ambito urbano erogando una varietà di servizi applicativi, favorendo così appieno il potenziale e la crescita del mercato dei droni.
L'unione delle tecnologie spaziali e aeronautiche sta infatti rendendo molto più vicino il futuro che abbiamo immaginato e Telespazio vuole mettere a disposizione i propri servizi e le proprie capacità per realizzarlo.

UN SISTEMA DI COMUNICAZIONE E NAVIGAZIONE PER L'ESPLORAZIONE LUNARE

TELESPAZIO S.P.A.

I recenti sviluppi tecnologici ed in ambito spaziale hanno portato ad un rinnovamento dell'interesse nei confronti della Luna e della possibilità di sfruttarne risorse per migliorare l'esplorazione spaziale. La nuova Space Economy, infatti, trova fondamenta solide nel progetto di colonizzare il suolo lunare nell'ottica di sfruttarne le risorse, di creare habitat per gli esseri umani, di realizzare nuovi sistemi di sorveglianza e protezione planetaria e di sviluppare tecnologie innovative. In questa prospettiva l'iniziativa dell'Agenzia Spaziale Europea (ESA), Moonlight (logo in Figura 1), mira a sviluppare una Lunar Economy attraverso la realizzazione di un sistema di comunicazione e navigazione per il supporto di orbiters, landers, rovers, missioni commerciali, missioni istituzionali e di tutti gli attori che saranno coinvolti nell'esplorazione lunare e spaziale nei prossimi anni. Lo scopo di Moonlight è di minimizzare i costi per le future missioni spaziali attraverso la realizzazione di un LCNS (Lunar Communication and Navigation Services) che potrà essere customizzato in base alle necessità degli users, alle performance richieste e che, inoltre, diminuirà la complessità delle missioni, rendendo disponibili segnali di navigazione che distribuiranno un servizio di posizionamento ad alta precisione ed affidabilità.

Figura 1: Consorzio per la fase A/B1 di Moonlight (Prime: Telespazio; Partners: Altec, Argotec, Hispasat, Inmarsat, MDA, Nanoracks, OHB, PoliMi, SDA Bocconi, Thales Alenia Space Italia)

Telespazio, a partire da Maggio del 2021, è stata prime contractor di uno dei due consorzi selezionati da ESA (Figura 1) per portare avanti lo studio di missione di fase A/B1 al fine di comprendere le esigenze e gli aspetti tecnici necessari per garantire servizi di comunicazione e navigazione sulla Luna e, soprattutto, di studiare come sviluppare il progetto in maniera finanziariamente sostenibile per promuovere lo sviluppo di una futura economia lunare (Figura 2).

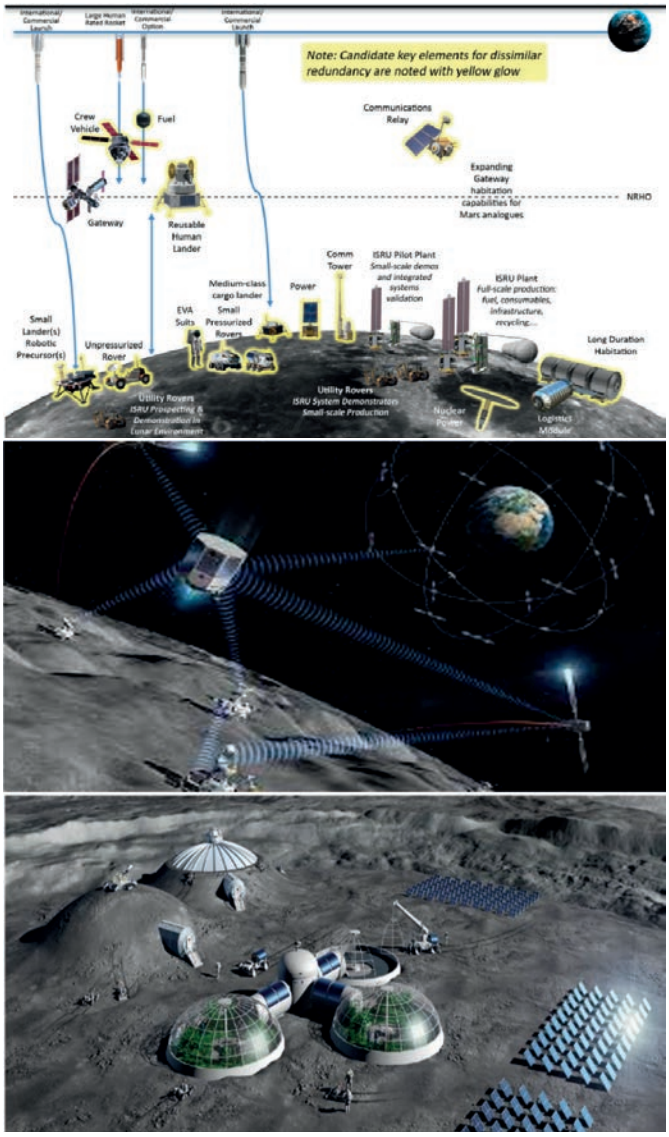


Figura 2: Concept per l'esplorazione lunare (Credits: Global Exploration Roadmap and ESA)

Il consorzio ha prodotto un'analisi di missione per il design ed il dimensionamento di una costellazione satellitare attorno alla Luna (Figura 3). L'infrastruttura sarà composta da stazioni lunari e terrestri e da una rete di satelliti (i cui i primi lanci sono previsti per il 2027) con il Centro Spaziale del Fucino di Telespazio nel ruolo essenziale di coordinamento del Controllo di Missione e di collegamento di tutti gli attori coinvolti. La rete di satelliti consentirà di fornire servizi di comunicazioni e navigazione per le future missioni, soprattutto per quelle dirette nelle regioni lunari non visibili dalla Terra. La regione lunare che dovrà essere maggiormente coperta dal servizio sarà il Polo Sud. Nell'ottica di sviluppare una Lunar Economy, infatti, sarà fondamentale lo sfruttamento delle risorse che l'ambiente lunare sarà in grado di offrire (vedi Figura 2). Il polo Sud, a tal proposito, è stato scelto per l'abbondanza di materiali quali: l'Elio3, le terre rare, riserve di ghiaccio, ecc.

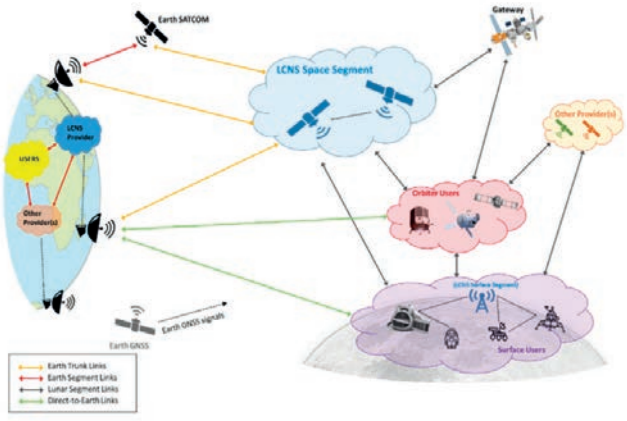


Figura 3: Sistema di costellazione satellitare attorno alla luna (credits: ESA)

Lo studio di progetto intrapreso per Moonlight ha permesso di definire i requisiti e le specifiche che si dovranno seguire per lo sviluppo dei sottosistemi nelle fasi successive (B2/C/E). Lo sviluppo delle tecnologie che faranno parte di questi sottosistemi vedrà coinvolti vari attori, tra cui il gruppo Leonardo, Telespazio ed il mercato industriale nazionale. Le analisi di sistema e di missione, fondamentali in una fase di studio A/B1, sono state condotte sfruttando l'ambiente Figura 4), messo a disposizione da Telespazio. La C2DF di Telespazio è stata fondamentale per condurre l'analisi di missione seguendo l'approccio Model Based System Engineering (MBSE), fortemente richiesto da ESA, al fine di identificare e tracciare i requisiti, le architetture, le analisi di missione e di sistema.

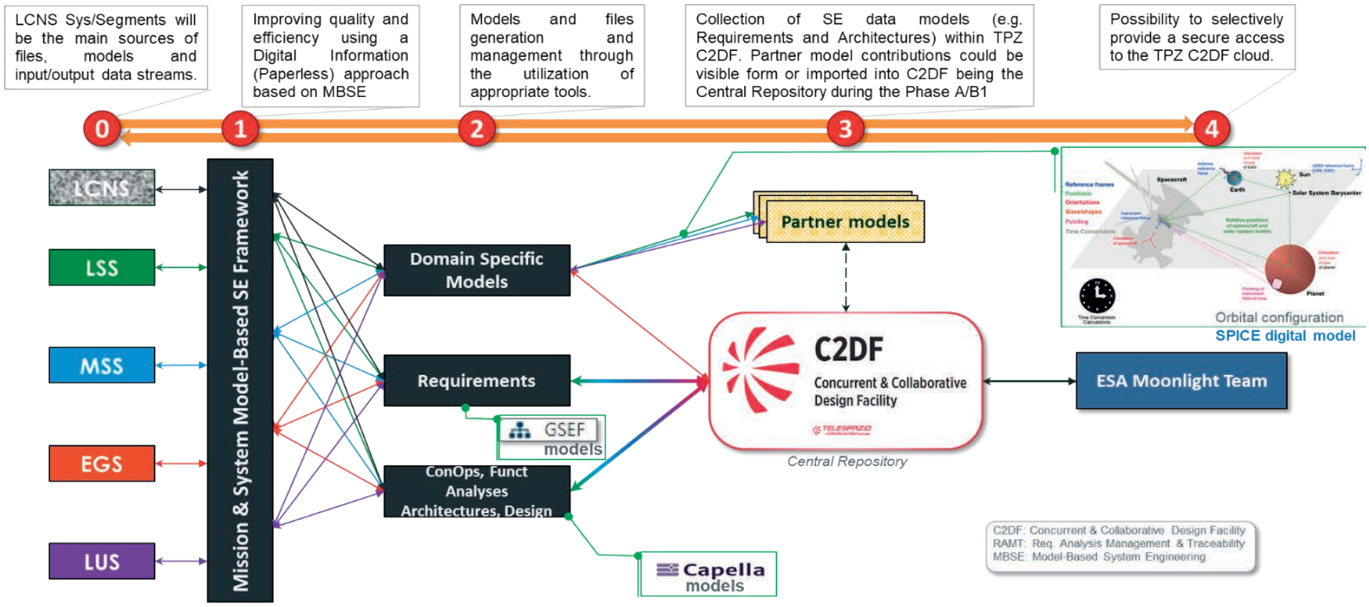


Figura 4: Mission & System Digital Modelling nello studio di Progetto LCNS) sfruttando la C2DF di Telespazio

RIFERIMENTI

1. ESA. (2021, May 20). Moonlight: bringing connectivity to the Moon. Tratto da https://www.esa.int/ESA_Multimedia/Videos/2021/05/Moonlight_bringing_connectivity_to_the_Moon
2. NASA. (2021, Oct 7). LunaNet: Empowering Artemis with Communications and Navigation Interoperability. Tratto da:https://www.nasa.gov/feature/goddard/2021/lunanet-empowering-artemis-with-communications-and-navigation-interoperability
3. G.Tomasicchio, C. Albanese, L. Spazzacampagna, M. Lavagna, G. Zanotti, A. Pasquale, J.Prinetto, M. Ceresoli, Satellite Constellation Mission Analysis and Design Aspects For Future Lunar Exploration Services, 26th Ka Broadband Communication Conference, 27-30 Sept. 2021
4. G. Tomasicchio, M. Brancati, A. Ceccarelli, A. De Matteis, L. Spazzacampagna, An Integrated Concurrent & Collaborative Design and Verification approach for the Telespazio Research & Innovation Laboratories, POLARIS Innovation Journal, n. 45/2021

RAFFORZARE LA CYBERSICUREZZA CON LA CYBER RECOVERY NELL'ERA DELL'ARCHITETTURA ZERO TRUST

Teleconsys e Rubrik: una partnership vincente

TELECONSYS

Nell'era digitale, in cui le minacce cibernetiche sono sempre più sofisticate, è essenziale adottare soluzioni innovative per proteggere le infrastrutture critiche delle forze armate. Questo articolo si concentrerà sulle potenzialità offerte da Teleconsys e dal partner tecnologico Rubrik, leader nel campo della Cyber Recovery e analizzerà come processi, competenze e capacità possano contribuire a rafforzare la cybersicurezza nel contesto della architettura Zero Trust, in accordo con il framework NIST e la direttiva NIS2.

Teleconsys e Rubrik sono aziende specializzate nella protezione dei dati e nella Cyber Recovery. La soluzione progettuale, unica nel suo genere, combina tecnologie avanzate di backup e ripristino con funzionalità specifiche per il recupero da attacchi cibernetici. Le due aziende sono in grado di offrire un approccio olistico per la protezione dei dati, garantendo la resilienza delle infrastrutture militari contro le minacce informatiche.

Com'è noto, nell'ambito della cybersicurezza militare l'architettura Zero Trust è diventata un punto di riferimento imprescindibile. Questo approccio si basa sulla premessa che nulla debba essere considerato attendibile all'interno delle reti e dei sistemi informatici, nemmeno le risorse interne. Teleconsys e Rubrik sono totalmente conformi a questo modello e in grado di realizzare un ambiente di protezione sicuro in cui l'accesso e l'autorizzazione sono rigorosamente controllati per mitigare i rischi di infiltrazione e movimenti laterali dei cybercriminali.

Framework NIST per la cybersicurezza. Il National Institute of Standards and Technology (NIST) ha sviluppato un framework di cybersicurezza ampiamente adottato dalle forze armate per proteggere le infrastrutture critiche. Rubrik si integra con il framework NIST, fornendo funzionalità di monitoraggio e risposta agli incidenti, nonché soluzioni di backup e ripristino atte a garantire la continuità operativa in caso di attacco cibernetico, coprendo per intero le categorie della funzione Recovery.

La direttiva NIS2 e la protezione delle infrastrutture critiche. La direttiva Network and Information Security (NIS) dell'UE è stata recentemente aggiornata con la direttiva NIS2 che impone agli stati membri di adottare misure specifiche per la protezione delle infrastrutture critiche. Teleconsys e Rubrik offrono un approccio consulenziale e progettuale conforme alle direttiva NIS2, consentendo alle forze militari di adeguarsi alle normative e di garantire un'adeguata protezione delle infrastrutture critiche attraverso la Cyber Recovery.

SIRE

Il pericolo ed il costo di un attacco cyber è misurato nel tempo medio di ripristino a valle di un attacco: un tempo non accettabile per servizi mission-critical potrebbe essere drammatico. È necessario avere una strategia che vede il recupero come il mezzo per evitare o mitigare tali impatti: essa può basarsi su un Secure Isolated Recovery Environment (SIRE). Il SIRE deve presentare punti di forza negli ambiti della restoration, dell'integrazione con SecOps. A tale proposito rappresentano un supporto imprescindibile le funzionalità di automazione e di gestione di test e di ambienti di recupero multipli e/o isolati.

L'architettura Zero Trust della soluzione Rubrik offre queste capacità e risponde a tutti gli standard di sicurezza imposti dal Governo americano. Viene garantito l'utilizzo degli standard di sicurezza più elevati in campo militare per l'encryption come:

- DODIN APL, Common Criteria EAL2+, FIPS 140-2 Level 2;
- Dischi di tipo SEDs certificati per l'encryption a livello di drive;
- Utilizzo del Bring Your Own Key per la gestione della chiave privata utilizzando HSM certificati come Thales ed Entrust.

Tutte le soluzioni possono essere implementate on-prem in ottica cloud privato tramite RSC-P (Rubrik Secure Cloud Private). Concludendo, la cybersicurezza è diventata una priorità strategica per le forze militari e l'utilizzo della soluzione di Cyber Recovery di Rubrik, con le sue capacità di Data Resilience, Observability e Remediation, risulta essere un componente fondamentale di una architettura di sicurezza disegnata per garantire la protezione delle infrastrutture critiche.

Realizzando l'architettura Zero Trust con questa soluzione, si ottiene un approccio completo e avanzato per affrontare le sfide della cybersicurezza militare nell'era digitale. Le forze militari possono sfruttare le potenzialità di Rubrik per mitigare i rischi cibernetici e utilizzare la competenza di Teleconsys per garantire la continuità operativa, preservando così l'integrità dei loro dati e delle loro missioni.

DISTRIBUZIONE QUANTISTICA DI CHIAVI CRITTOGRAFICHE PER LE TELECOMUNICAZIONI SICURE

Sviluppi in vista di una dimostrazione satellitare

M. Ottavi, P. Conforto, A. Geraldi, L. Bruno, G. Riccardi, S. Di Bartolo, M. Petrone

THALES ALENIA SPACE

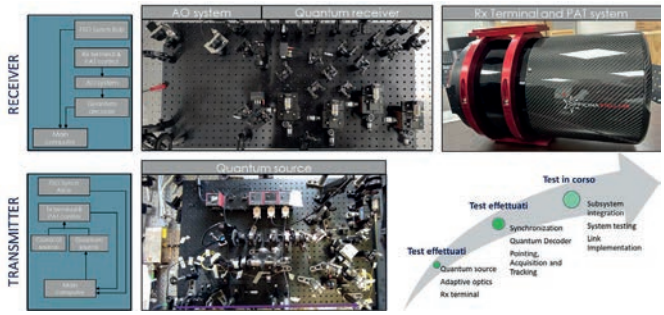


Figura 1 - Laboratorio di ottica quantistica di Thales Alenia Space

Le moderne telecomunicazioni rappresentano la spina dorsale alla base di molte infrastrutture critiche, particolarmente sensibili ai temi della cyber security che si può sintetizzare nella necessità di rispettare i requisiti di CIA (Confidentiality, Integrity e Availability) relativi a riservatezza, integrità e disponibilità delle informazioni scambiate.

La sicurezza basata sugli attuali schemi crittografici si fonda sulla complessità computazionale ed è esposta all'avvento dei computer quantistici che presto possiederanno un numero di qubit sufficiente a violare gli attuali protocolli a chiave pubblica. Tra le applicazioni delle tecnologie quantistiche, la distribuzione quantistica delle chiavi (Quantum Key Distribution, QKD) rappresenta senza dubbio la tecnica più matura. Impiegando la trasmissione di singoli fotoni, la QKD consente di stabilire chiavi comuni la cui riservatezza, integrità e disponibilità siano garantite dai principi della meccanica quantistica permettendo una transizione verso sistemi di telecomunicazione di nuova generazione la cui sicurezza non sarà messa in pericolo dai futuri computer quantistici.

Gli stessi principi della meccanica quantistica che impediscono qualsiasi tentativo di misurare e clonare un bit quantistico senza alterarne lo stato impongono dei limiti di distanza invalicabili: le elevate perdite associate alle comunicazioni in fibra e l'impossibilità di amplificare un segnale quantistico limitano le distanze raggiungibili con la QKD a poche centinaia di chilometri, a meno che non si impieghi un numero elevato di nodi terrestri che funzionino da "ripetitore" ma che incrementerebbero i "point of failure" del sistema, più vulnerabile a possibili attacchi.

Un'infrastruttura satellitare, d'altro canto, consente di superare le limitazioni delle infrastrutture terrestri, abilitando la QKD su distanze globali e permettendo di collegare utenti situati a migliaia di chilometri di distanza, con forti implicazioni per casi d'uso sia civili che militari. Infatti la QKD risulta essere particolarmente rilevante a supporto di applicazioni militari in quanto consentirebbe di collegare in modo sicuro asset strategici remoti, come basi militari e ambasciate situate in Paesi potenzialmente ostili, portaerei e basi NATO.

Sul fronte governativo, sono in corso diverse iniziative come il progetto ESA "SAGA", orientato alla realizzazione di una costellazione QKD, e la costellazione IRIS2, con la quale la Commissione Europea ha l'obiettivo di sviluppare un sistema di connettività spaziale europeo che fornirà servizi di comunicazione sicuri all'Unione Europea (UE) e ai suoi Stati membri, ed all'interno del quale la QKD svolgerà un ruolo chiave.

Thales Alenia Space Italia è in prima linea su tali iniziative e, sfruttando la consolidata esperienza nell'ambito delle telecomunicazioni satellitari, sta sviluppando un centro di competenza specifico per la progettazione e lo sviluppo di infrastrutture satellitari per le comunicazioni quantistiche.

A partire da tali competenze, l'azienda si sta ritagliando un ruolo chiave nello sviluppo della sistemistica e della tecnologia necessaria per le comunicazioni quantistiche spaziali e di guida della filiera italiana, al servizio delle esigenze istituzionali e commerciali, intraprendendo una serie di attività cruciali sia per la definizione di una missione dimostrativa italiana sia per l'espansione verso una costellazione QKD europea pienamente operativa. Elemento centrale di questa strategia è lo sviluppo realizzato negli ultimi anni del laboratorio di ottica quantistica. L'infrastruttura (alcuni elementi sono mostrati in Figura 1), collocata presso la sede di Thales Alenia Space in Roma, è in grado di interfacciarsi con l'infrastruttura terrestre in fibra e di connettersi con la dorsale Quantum italiana. Nel laboratorio al momento sono in corso esperimenti di comunicazione quantistica sia in fibra che in spazio libero utili per approfondire gli effetti di propagazione indotti dal canale atmosferico sui segnali quantistici e caratterizzare e validare i modelli propagativi.

A complementazione della parte dimostrativa, è in fase di finalizzazione lo sviluppo di uno strumento software di modellizzazione dell'intero sistema end-to-end, in grado di modellare scenari che coinvolgono satelliti che vanno da VLEO a GEO, permettendo di supportare la progettazione di una vasta gamma di applicazioni.

Tali iniziative rappresentano le fondamenta per la realizzazione e la validazione di missioni QKD in orbita e permetteranno all'industria italiana ed alle piccole e medie imprese di posizionarsi strategicamente in Europa e nel mondo nelle future missioni di telecomunicazioni sicure.

AN ITALIAN DEMO MISSION FOR IN-ORBIT SERVICING

M.A.Perino, S.Ferraris, M.Gajeri, M.Montagna, F.Musso, D.De Rosa, A.Pilati, S.Mazzeo, S.Landenna, R.M.Grillo, E.Cavallini, R.Formaro

THALES ALENIA SPACE

Introduction

A consortium of companies led by Thales Alenia Space has signed a contract with the Italian Space Agency to develop the enabling technologies for an In-Orbit Servicing demonstration mission. The consortium of companies is formed by Thales Alenia Space (lead contractor), Leonardo, Telespazio, Avio and D-Orbit.

An autonomous robotic vehicle will be developed to make space more sustainable by providing advanced in orbit operational capabilities such as satellite life extension and upgrades, de-orbiting/debris removal and relocation. The mission will be developed in the framework of the National Recovery and Resilience Plan (PNRR). Set to launch by end 2026, the demonstration mission will operate in low Earth orbit (LEO) both the servicer satellite and the target satellite developed within the contract together with the relevant mission control centre.

In Orbit Servicing

The development of In Orbit Servicing (IOS) capabilities will pave the way to a more sustainable exploitation of the space environment and the new emerging commercial space market. The IOS demo mission will validate all the technological building blocks and the systems required to fulfil these challenging objectives. Starting from a near future point of view, a IOS servicer would need to provide several services to different unprepared customer satellites, and to prepared satellites in a second stage.

The goal of the national Demo Mission is to enhance the national competitiveness and to pave the way for an Italian solution for In Orbit Services and the future serviced LEO/GEO satellites. This project leverages on the existing national skills and experiences and involves the key players with the needed competences, maximizing the complementarity and the synergy between LSI companies with solid experience in complex space projects and new emerging space companies with a more agile approach to shape the future space ecosystems, fostering Italian competitiveness into this global shifting paradigm that space economy is facing.

Demo Mission Objectives

The objective of the proposed IOS Demo Mission is to validate the enabling technologies needed to fulfil challenging operations for both prepared and unprepared satellites including approaching, inspection, rendezvous and docking, life extension, refuelling, repairing, assembly, relocation and de-orbiting.

The following capabilities represent the main functions to be foreseen, that will be demonstrated during the IOS demo mission:

- Orbit transfer: to reach a similar orbit w.r.t. the customer satellite
- Target tracking & Inspection: to track and identify the customer satellite
- Rendezvous: to safely rendezvous and approach the customer target
- Capture: to execute a berthing with robotic arm up to the achievement of the final rigid stack-configuration (rigid link between servicer and target)
- In orbit services:
  - to control the attitude and the orbit of the customer satellite (AOCS Takeover)
  - to relocate the customer satellite in a different operative orbit
  - to perform a validation of refuelling technology with a simulant
  - to perform disposal operations for a customer satellite at End-of-Life
  - to perform an unmating and separation manoeuvre to disengage the customer

In a mid-term future, it is reasonable to take into account the use of standard interfaces or dedicated servicing items that would simplify the in-orbit operations, minimizing the IOS time and costs. The installation of prepared items on-board the customer satellites would also lead to an increase of the proximity operations safety, enabling new type of services to be provided.

Therefore, additional functions would be required w.r.t. the *near future* point of view:

- to refuel the customer satellite tanks
- to refurbish a customer satellite (Orbit Replaceable Units replacement)
- to assemble new components/parts on the customer satellite

The IOS Demo mission will be performed in Low Earth Orbit, validating all the required technologies to enable the IOS capabilities previously described, by developing both the servicer and the target satellite and the relevant mission control center. The mission will be launched as baseline from Kourou with a VEGA launcher.

Acknowledgement

The In orbit Servicing Demo Mission will be developed within the ASI Contract No. n. 2023-15-I.0 / CIG 9498798016 / CUP F83D22001720005 financed by the Next Generation EU via the Italian National Recovery and Resilience Plan (PNRR).

USO DELLE COSTELLAZIONI SATELLITARI PER LE TELECOMUNICAZIONI RESILIENTI E STRATEGICHE

Concetto di comunicazione in un sistema di sistemi

M. Gargiulo, N. Lamorgese, S. Wahib, P. Conforto, M. Petrone, A. Pisano

THALES ALENIA SPACE

Negli ultimi decenni si è assistito ad un'enorme crescita dell'uso dei sistemi di telecomunicazione globale, guidata dalle esigenze commerciali, istituzionali e militari. La richiesta di connettività ad alta velocità, bassa latenza e disponibile a livello globale è aumentata notevolmente e si prevede che crescerà ulteriormente nel corso dei prossimi anni. Le soluzioni proposte da Thales Alenia Space Italia prevedono una costellazione ibrida multi-dimensionale e multi-*layer* di satelliti per telecomunicazioni in orbita bassa (LEO, *Low Earth Orbit*), caratterizzata da differenti tipologie di satelliti con distinte capacità e caratteristiche orbitali (combinazione di varie altitudini, numero e inclinazioni dei piani orbitali). L'obiettivo principale di questo Sistema di Sistemi (SdS) è quello di supportare diversi tipi di missione, includendo nuove promettenti tecnologie abilitanti (come illustrato nella Figura 1). Il sistema presentato consentirà una connettività di rete a stella e a maglia, attraverso collegamenti dinamici ed efficienti tra tutti i differenti nodi della rete. Al fine di fornire accesso sicuro e resiliente e connettività agli utenti finali della rete, la costellazione deve quindi instradare e inoltrare il traffico dati tra i suoi satelliti. Inoltre, l'uso di una combinazione di bande di frequenza permetterà di servire scenari eterogenei, che vanno da aree remote a scenari urbani di sistema, compreso l'ambiente rurale grazie alla capacità di penetrazione del segnale nelle zone a fitta vegetazione e a bassi angoli di elevazione. Allo stesso tempo, una delle direzioni evolutive dei settori delle telecomunicazioni è rappresentata dall'Internet of Things (IoT). Questo nuovo paradigma si basa sull'interconnessione di dispositivi pseudo-intelligenti, sensori e attuatori in un'unica rete globale. La rivoluzione dell'IoT sta svolgendo un ruolo importante in diversi settori verticali, tra cui il controllo delle infrastrutture critiche e/o strategiche di interesse nazionale, *unmanned units* (robot, piccoli mezzi mobili e droni collocati in zone tattiche), applicazioni *Machine-to-Machine* (M2M), ecc. Un requisito fondamentale e cruciale di qualsiasi infrastruttura IoT è garantire una connettività onnipresente ai terminali a basso costo e a basso consumo distribuiti in tutto il mondo.

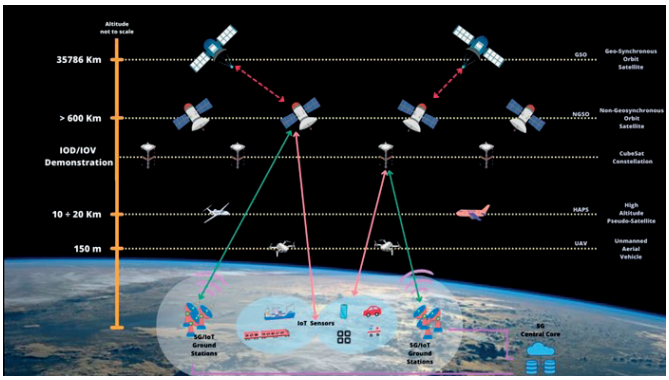


Figura 1 - Laboratorio di ottica quantistica di Thales Alenia Space

E' ampiamente riconosciuto che questi requisiti non possono essere soddisfatti dalla sola rete terrestre. Infatti, le reti terrestri possono non essere in grado di assicurare l'accesso a un servizio di connettività affidabile e di raggiungere le aree remote a causa di una copertura irregolare o insufficiente. Di conseguenza, per consentire agli utenti finali di accedere ai servizi di telecomunicazioni richiesti ovunque e in qualsiasi momento, è necessaria l'integrazione di una infrastruttura di comunicazione satellitare. Thales Alenia Space Italia è coinvolta attualmente nella definizione di missioni militari, istituzionali e commerciali per la realizzazione di costellazioni LEO per le telecomunicazioni in grado di soddisfare i prossimi bisogni degli utenti. Bassa latenza nello scambio dati (adatta ai tipi di servizi da fornire), alta disponibilità, elevato *throughput*, accessibilità continua alla rete per diversi tipi di terminali (personali, mobili, fissi, trasportabili, ecc.), copertura su aree non servite (non raggiunte dalla rete terrestre o da altri assetti spaziali esistenti) sono solo alcuni esempi di requisiti da considerare. Esempi di applicazioni a valenza militare abilitate dalle soluzioni proposte includono il monitoraggio dello stato di infrastrutture (oleodotti/elettrodotti/ponti/ferrovie) tramite sensori in accesso diretto a satellite, il monitoraggio di container o casse di materiale sensibile per analisi di pesi, manomissioni, localizzazione, *tracking*, stato del carico in ambito depositi, ottimizzazione della logistica, il controllo di frontiere o di zone remote, comunicazioni in area tattiche con infrastrutture dispiegabili, comunicazioni ad elevata robustezza rispetto ad attacchi cyber, servizio in scenario post-crisi nel quale la rete terrestre può subire gravi danneggiamenti. In questo contesto, la componente LEO ha una serie di punti di forza: assicura vantaggi in termini di link budget, fornisce servizi a bassa latenza grazie al ridotto ritardo di propagazione del segnale elettromagnetico, riduce i costi e consente un possibile riutilizzo di tecnologie e protocolli terrestri.

COME BEDROCK STREAMING È MIGRATO DA VMWARE A VATES UNA DELLA TANTE STORIE DI SUCCESSO DEI CLIENTI VATES

Marc Pezin, Charles-H. Schulz

VATES S.A.S.

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 Cybersecurity 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),

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

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.

DIAL ATMOSPHERIC PROFILER – VAISALA DA10

Previsione meteorologiche e modellazione climatica più accurate grazie a profili di vapore acqueo in tempo reale

VAISALA INC.

Misurare il vapore acqueo nell'atmosfera è sempre stato un processo manuale, dispendioso sia in termini di tempo e sia a livello economico, eseguito, finora, quasi esclusivamente dalla comunità scientifica.

Il rivoluzionario lidar ad assorbimento differenziale progettato, prodotto e recentemente introdotto sul mercato da Vaisala, differential absorption lidar DIAL DA10, è il primo profilatore atmosferico con funzionamento automatico, per il monitoraggio del vapore acqueo all'interno dello strato limite. E' in grado di operare in modo continuo e autonomo 24 ore su 24, 7 giorni su 7, fornendo a meteorologi e previsori un controllo costante dell'umidità atmosferica per migliorare le osservazioni ed essere più precisi nell'emettere avvisi di condizioni meteorologiche avverse.

Mentre le osservazioni nello strato superiore della troposfera forniscono un quadro generale dei modelli di umidità, il profilatore DIAL DA10 misura continuamente il vapore acqueo all'interno dello strato limite, in qualsiasi luogo, in qualsiasi condizione, permettendo per la prima volta l'accesso a dati locali di dettaglio per la modellazione NWP (Numerical Weather Prediction) e svolgendo anche la funzione di super ceilometer con profili ultra puri.
In combinazione con la modellazione meteo-climatica, i servizi meteorologici possono così avere accesso a osservazioni locali altamente accurate e affidabili, che permettono l'emissione anticipata di allerte per condizioni meteorologiche avverse, quali temporali, nubifragi o inondazioni improvvise, per le comunità locali.

Il sistema DIAL DA10 è certificato CE e rispetta le direttive LVD, EMC e RoHS; è di Classe 1M secondo IEC / EN 60825-12014.

Il sistema DIAL DA10 esegue misure di vapore acqueo fino a 4 km e fornisce profili di backscatter fino a 18 km ed include anche finzioni di celiometro. Il sistema è configurabile, monitorato e programmato tramite un collegamento Ethernet.
Il sistema è in grado di acquisire i seguenti profili:

- "Water vapor mixing ratio" in g/Kg
- "Attenuated backscatter"
- "Uncertainty for water vapor mixing ratio"

Il sistema è in grado di rilevare i seguenti parametri:

- Altezza base nubi fino a 5 strati;
- Spessore e indice di penetrazione delle nuvole;
- Rilevamento precipitazione/nebbia;
- Stato del cielo (sky condition);
- Pressione, Temperatura e Umidità di superficie.

Il sistema DIAL DA10 funziona automaticamente, ha un'estesa autodiagnostica e analisi del guasto incorporata ed è adatto a siti non presidiati: non necessita calibrazione né regolare manutenzione e perciò la necessità di visitare il sito è ridotta al minimo.

STIAMO ASPETTANDO UNA PANDEMIA DIGITALE O CI STIAMO PREPARANDO?

Edwin Weijdema, Field CTO EMEA & Global Cybersecurity Technologist

VEEAM ITALIA

Da diversi mesi si parla di ChatGPT e di IA generativa. Non è certo una cosa negativa. In questo modo si crea una trasparenza che ci permetterà di capire cosa ci sta arrivando. Come nel caso della cybersicurezza e dei ransomware, non dobbiamo essere ciechi di fronte ai rischi e a tutto ciò che deve accadere intorno a questa nuova tecnologia. Fortunatamente, la paura non è necessaria, ci siamo già passati più di una volta. E siamo sopravvissuti ogni volta.

Da ChatGPT a un cane robot che si muove nel salotto di casa, l'intelligenza artificiale sta iniziando a lasciare il segno nella società. Da un lato, questo presenta enormi opportunità. Pensiamo, ad esempio, al settore medico, dove nanobot o minuscoli robot stanno per salvare vite umane. Ma dall'altro lato, dobbiamo anche avere il coraggio di chiederci chi sarà responsabile se le cose andranno male con l'IA? La parte che ha programmato il sistema? Il fornitore dello strumento? L'utente finale? O una combinazione di tutti e tre?

Dobbiamo avere il coraggio di pensare all'impatto che la tecnologia sta avendo sulla nostra società. Purtroppo gli esseri umani non sono mai stati bravi a cambiare e preferiscono mettere la testa sotto la sabbia. Finché qualcosa non ha un impatto effettivo sulla nostra vita personale. Basti pensare al modo in cui utilizziamo il backup. All'inizio si era consapevoli dell'importanza del backup, ma nessuno voleva pagare per averlo. Finché il ransomware non è diventato improvvisamente onnipresente e le organizzazioni hanno capito che un buon backup dovrebbe essere al primo posto nella catena della sicurezza. Anche la tecnologia AI potrebbe gradualmente salire nella catena.

Come dobbiamo affrontare gli sviluppi tecnologici che hanno il potenziale per rimodellare completamente il nostro modo di lavorare? In realtà, conosciamo già la risposta, perché abbiamo già sperimentato tutto questo. Si può addirittura parlare di un ciclo che si verifica quando si lancia una nuova invenzione o tecnologia nel mondo. Quasi tutto viene sviluppato con l'intenzione di fare del bene, eppure vediamo che arriva sempre un momento in cui qualcuno inizia ad abusare di una soluzione. La polvere da sparo è stata inventata con le migliori intenzioni, finché non si è scoperto che con essa si potevano far esplodere le cose. Le applicazioni informatiche avanzate consentono alle aziende di generare più affari, finché gli hacker non vedono l'opportunità di diffondere ransomware attraverso questi canali. I sistemi di intelligenza artificiale fanno cose rivoluzionarie, finché le cose non vanno male perché si sono insinuati dei pregiudizi nella soluzione.

Quando introduciamo una nuova tecnologia, seguiamo sempre lo stesso processo in tre fasi. Innanzitutto, cerchiamo di prepararci al meglio. Nella fase successiva, reagiamo ai problemi che si presentano. Infine, risolviamo ciò che è andato storto. Ad esempio, non si può fermare completamente un hacker con uno strumento di sicurezza, ma si possono limitare i danni rallentando l'attacco e spingendolo in un'altra direzione.

Prima chiudiamo il cerchio, prima possiamo sfruttare l'impatto positivo che la tecnologia ha sulle nostre vite.

È quindi essenziale una preparazione adeguata. E per questo è necessaria la trasparenza. Se sappiamo cosa sta succedendo nel mercato e quali cambiamenti sono in arrivo, possiamo anticiparli meglio e sviluppare una politica o una legislazione. La trasparenza è la migliore difesa per costruire qualcosa in modo sostenibile. Di solito i pezzi del puzzle si trovano in parti diverse e dobbiamo riunire il maggior numero possibile di prospettive.

Inoltre, sia negli affari che in politica, è importante mettere persone con il giusto background tecnico nei luoghi in cui si prendono le decisioni. O che i leader e i responsabili politici siano circondati da esperti con le giuste competenze. Non a caso, i giganti della tecnologia sono le aziende di maggior successo al mondo. Sono dirette da persone con una visione del futuro e una prospettiva che ispira gli altri.

Proprio come gli esperti di salute si trovavano improvvisamente negli studi dei telegiornali durante l'era Covid, riempiendo i giornali e influenzando le decisioni coronografiche, gli esperti di tecnologia digitale devono ora assumere il loro ruolo per preparare la nostra società e le aziende. Solo una preparazione adeguata può evitare che la nostra società cada presto in una pandemia digitale. Dopo tutto, siamo di fronte alla più grande innovazione dai tempi della Rivoluzione industriale.

In ogni rivoluzione che l'umanità ha vissuto, all'inizio non sapevamo cosa fare. Ma ogni volta ne siamo usciti. Ora abbiamo il vantaggio di essere più preparati perché conosciamo già una parte del processo. E il resto? Scopriamolo insieme.

Soci
Corporate

ALMAVIVA, Gruppo leader italiano nell'Information & Communication Technology, sinonimo di innovazione digitale, 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 ad un network globale con 46.000 persone, 7.000 in Italia e 39.000 all'estero, e 1.096 milioni di euro di fatturato nel 2022
www.almaviva.it/it_IT

Aruba, fondata nel 1994, è il principale provider italiano di servizi cloud e il leader in Italia per i servizi di data center, cloud, hosting, trust services, e-mail, PEC, registrazione di domini e firma digitale. La società, con un capitale interamente italiano, si rivolge a privati, professionisti, imprese e PA. Aruba gestisce una vasta infrastruttura che comprende 2,6 milioni di domini registrati, 9,4 milioni di caselle e-mail, 9 milioni di caselle PEC e 130.000 server gestiti, offrendo servizi a un totale di 16 milioni di utenti. In quasi 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.
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. La 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 cybersecurity, 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

Crypt-Security è una PMI Innovativa che opera nell'ampio quadro di riferimento dell'Ecosistema delle Comunicazioni ed in particolare nel mercato della Sicurezza Informatica, settore che sta rivestendo sempre più una importanza strategica.
Grazie alla stretta collaborazione tra le attività di ricerca e l'interesse al mercato, Crypt-Security ha maturato competenze realizzative di altissimo livello nella progettazione e realizzazione di:

- Algoritmi di encryption-decryption;
- Sistemi di sicurezza;
- Soluzioni crittografiche;
- Consulenza sui temi della sicurezza, della probabilistica e della statistica applicata;
- Formazione sui temi della sicurezza.

www. crypt-security.com

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.
3DEXPERIENCE, il logo Compass logo e il logo 3DS, CATIA, BIOVIA, GEOVIA, SOLIDWORKS, 3DVIA, ENOVIA, EXALEAD, NETVIBES, MEDIDATA, CENTRIC PLM, 3DEXCITE, SIMULIA, DELMIA e IFWE sono marchi commerciali o registrati di Dassault Systèmes.
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 SpA (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 nove aziende ed impiega 450 risorse, tra ingegneri, programmatori, consulenti informatici, tecnici di laboratorio, ricercatori, operanti da tredici 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).
E' inoltre vendor certificato presso il Consiglio d'Europa e presso la Nato.
www.dplatforms.it

Eles Semiconductor 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. Da oltre 70 anni è un leader mondiale nei sistemi di Difesa elettronica. Grazie alla gestione innovativa dello spettro elettromagnetico, realizzata attraverso tecnologie proprietarie ed integrate, oggi il brand è un Gruppo internazionale con un approccio multidominio che copre anche Cyber, Spazio e Biodifesa. ELT Group è presente nei principali programmi della Difesa europea con tecnologie all'avanguardia per il supporto all'intelligence e per la difesa di equipaggi e di piattaforme.
Ha il proprio headquarter in Italia ed è presente in 11 Paesi dislocati nei 4 continenti attraverso uffici commerciali e società strategiche in Germania e nel Golfo.
ELT Group ha tra i propri pilastri l'innovazione permanente, investendo ogni anno circa 13 Ml di euro in R&S.
Ha costruito la propria centralità sul benessere delle proprie persone, infatti negli ultimi 6 anni ha conseguito la certificazione 'Great Place to Work', entrando anche tra le Best Workplaces, la classifica delle migliori aziende in cui lavorare in Italia e anche in Europa. È inoltre nella classifica dei 'Most Attractive Employers'.
Fanno parte di ELT Group anche CY4GATE, specializzata in Cyber security e Cyber Intelligence e E4Life, prima società italiana di Biodifesa.
www.elt-roma.com

ENAV S.p.A. unico Provider ATC al mondo quotato in Borsa, gestisce il controllo del traffico aereo civile in Italia, garantendo sicurezza e puntualità. La Società controlla 2,05 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 controllata 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 degli Unmanned Aerial Vehicles (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. ENAV Group: leader in providing ATM services and solutions, worldwide.
www.enav.it

Esri Italia, 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 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 3,1 milioni di clienti su rete fissa e 3,3 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+" (Strong). Dal gennaio 2022 Fastweb è società Benefit.
www.fastweb.it

Fata Informatica S.r.l. opera dal 1994 nel campo delle tecnologie dell'informatica e delle telecomunicazioni.
Dal 2005 sviluppiamo SentiNet³® primo ed unico sistema italiano di Unified Proactive Monitoring per il monitoring di infrastrutture IT.
Con la divisione di Cybersecurity (CyberSecurityUP.it) garantiamo consulenza e servizi per strategie di difesa e gestione del rischio cyber a 360°.
Vulnerabilty assessment e Penetration Test; monitoraggio e threat hunting, sono solo alcuni dei servizi erogati dal nostro SOC.
Cyber Security Awareness nasce per aumentare la consapevolezza dei dipendenti sui pericoli indotti da comportamenti poco opportuni nell'utilizzo dei devices informatici.
In ambito formativo Fata Academy, offre corsi specialistici inerenti le attività di sviluppo, il processo di vulnerability assessement e l'ethical hacking.
www.fatainformatica.com

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 nonchè la analisi posturale e lo stato dell'apparato individuato.
www.forescout.com

Fortinet rrende 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 680.000 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, dai sistemi di telecomunicazione e radiocomunicazione agli impianti e opere civili. La I&C opera in conformità alle norme: ISO 9001, OHSAS 18001 e AQAP 2110.
www.intconsulting.it

IBM. Con più di 110 anni di storia, IBM è leader nell'Innovazione in oltre 170 paesi. Cloud ibrido, intelligenza artificiale, sistemi hardware mainframe e storage, cybersecurity e quantum computing: queste le aree in cui IBM è riconosciuta come leader a livello globale e come brand dal forte impegno etico. La ricerca scientifica guarda continuamente al "What's Next in Computing" per creare e integrare le tecnologie con le quali risolvere le grandi sfide del mondo, generando nuove opportunità di miglioramento in ogni ambito. Ciò ha assicurato ad IBM numerosi primati nella classifica dei brevetti depositati negli Stati Uniti. IBM opera in Italia dal 1927 contribuendo allo sviluppo dell'innovazione e della sostenibilità in ogni settore economico.
www.ibm.com/it-it/about

IES 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 SOLUTIONS S.p.A. società tutta italiana, progetta e sviluppa SW/HW e prodotti per i mercati Aerospazio, Difesa, Trasporti, TLC e Smart Systems. INTECS è un System Integrator con ventennale esperienza in sistemi elettronici Safety e Mission-critical già in servizio da anni presso la rete ferroviaria di RFI. In cinquant'anni INTECS, affiancando i protagonisti industriali ed istituzionali nella progettazione, realizzazione e verifica di sistemi complessi come Tactical Data Link, C&C, Estrattori e Tracciatori Radar, Sistemi d'Arma missilistici, ha dimostrato le sue sviluppato alte competenze nel SW Engineering, Systems Engineering, Validation & Verification, Cyber Security, RAMS Analysis, SDR ed A. I.
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., fondata nel 1960, è una società controllata da Leonardo S.p.A., da sempre leader nella realizzazione di soluzioni elettroniche di utente e di protezione personale in ambito Difesa, Sicurezza ed Emergenza. Ogni sistema o prodotto Larimart nasce da un costante affiancamento degli utilizzatori finali e dei clienti, durante ogni fase del ciclo di vita progettuale. Dalla prima identificazione delle esigenze fino allo sviluppo, qualifica, fornitura e manutenzione, ogni dettaglio progettuale è ispirato a criteri di affidabilità e mantiene un'apertura all'evoluzione tecnologica per estendere la vita degli apparati. Larimart, capofila del Consorzio PBI, detiene la più alta capacità italiana, tecnologica ed industriale, nell'importante e strategico settore delle protezioni balistiche personali (elmetti e giubbetti). Il Consorzio PBI è responsabile dello sviluppo, della progettazione e della produzione del più innovativo ed affidabile Giubbetto Antiproiettile di livello IV in servizio nelle FF.AA. italiane.
Larimart collabora con Agenzie Industrie Difesa per la realizzazione dei Giubbetti Anti Proiettile delle Forze Armate Italiane e ha recentemente acquisito la quota di maggioranza di DPI srl, azienda leader nelle protezioni per le vie respiratorie, consolidando la sua posizione come leader nazionale nel campo delle protezioni individuali."
www.larimart.it

Leonardo tra le principali aziende leader dell'Aerospazio, Difesa e Sicurezza, realizza capacità tecnologiche multidominio in ambito Elicotteri, Velivoli, Aerostrutture, Elettronica, Cyber & Security e Spazio. Con oltre 51.000 dipendenti nel mondo, l'azienda ha una significativa presenza industriale in Italia, Regno Unito, Polonia, Stati Uniti e Israele, e opera in 150 paesi anche attraverso aziende controllate, joint venture e partecipazioni. Protagonista dei principali programmi strategici internazionali è partner tecnologico e industriale di Governi, Amministrazioni della Difesa, Istituzioni e imprese. 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

N.I.D.O. Group è leader di mercato da oltre 20 anni per i processi di stampa delle identità fisiche: Passaporto, CIE e Codice Fiscale.
L'inevitabile sviluppo dell'identità fisica è l'identità digitale. Nell'ottica della protezione delle identità digitale e dei dati si sono strette importanti partnership per offrire soluzioni come:

- Soluzioni ASOC per la sicurezza delle applicazioni con test statici, dinamici.
- Soluzioni di Data Protection/Migration e Disaster/Ransomware per i vostri Data Base e le Vs apps durante tutto il percorso verso il Cloud e/o il MultiCloud
- Soluzioni di Digital On Boarding / e-Timestamp / e-Signature / e-Delivery
- Soluzioni per combattere il phishing e lo spoofing
- Soluzioni di Identity Access Management e Multifactor Authentication
- Sistemi di distribuzione e management dei certificati SSL e certificati per IoT

www.nidogroup.it

National Instruments. Da oltre 40 anni NI accelera la produttività, l'innovazione e la scoperta attraverso una piattaforma aperta e basata sul software. Questo approccio consente disviluppare e aumentare le prestazioni dei test e dei sistemi di misura automatizzati. I clienti di quasi tutti i settori, dall'Healthcare all'Automotive, dall'Aerospazio e Difesa all'Elettronica di Consumo e al mondo scientifico, utilizzano la piattaforma hardware e software integrata di NI per migliorare il mondo in cui viviamo, per superare le complessità delle sfide tecnologiche e le proprie aspettative. Con oltre 40 filiali presenti in tutto il mondo ed una base clienti di oltre 35000 aziende, National Instruments è l'azienda leader nel settore del test, della misura e del controllo automatici.
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 fornisce un'esperienza cloud che consente alle organizzazioni di ottenere il massimo dai dati riducendo complessità e costi di gestione dell'infrastruttura. L'impegno di Pure nel fornire uno storage as-a-service offre ai clienti l'agilità per rispondere alle mutevoli necessità dei dati. Pure può incidere sulla riduzione delle emissioni dei data center in tutto il mondo grazie all'impegno verso la sostenibilità ambientale, inclusa la progettazione di prodotti che consentono ai clienti di ridurre le emissioni di carbonio e l'impatto energetico. Con un indice di soddisfazione del cliente NPS che la vedono nel top 1% delle aziende B2B, Pure registra un numero sempre maggiore di clienti, che sono tra i più soddisfatti al mondo
https://www.purestorage.com/it/

Rubrik la Zero Trust Data Security™ Company, offre alle organizzazioni resilienza, osservabilità e recupero dei dati. Rubrik mantiene i vostri dati al sicuro e facili da recuperare in caso di attacchi informatici e guasti operativi. Ora potete recuperare i dati di cui avete bisogno, in qualsiasi modo e in qualsiasi momento, per mantenere la vostra attività operativa.
www.rubrik.com

Serco Italia S.p.A. é la filiale italiana di Serco group Plc con sede nel Regno Unito ed é parte del dipartimento "Serco UK and Europe". Serco Italia ha oltre 40 anni di esperienza nel settore dello spazio e dell'Information Technology ed oltre 200 impiegati altamente qualificati nel settore spaziale. Considerando l' integrazione con le altre filiali in Europa, Serco ha una esperienza unica nel fornire supporto operativo ad organizzazioni quali:

- Organizzazioni internazionali (UE, Parlamento Europeo, BCE)
- Agenzie governative (ESA, ASI)
- Difesa (Esercito belga, Aeronautica Militare Italiana)
- Industria aerospaziale (Telesapazio)
- Istituzioni scientifiche (CNR, CERC)

Serco Italia offre soluzioni per l'intera gamma in ambito spaziale in Italia ed in Europa:

- Osservazione della Terra
- Utilizzo dei dati Copernicus
- Servizio Meteorologici
- Scienze spaziali
- Tecnologia

www.serco.com

SIPAL S.p.A. Società leader nel settore dell'ingegneria, SIPAL SPA nasce nel 1978 ed entra nel gruppo FININC nel 1988. Con un know-how storico nel Supporto Logistico Integrato si rivolge al mercato civile e militare, con uno staff di oltre 500 professionisti altamente specializzati.
Con 15 sedi in Italia e una lunga esperienza, SIPAL lavora con flessibilità e competitività, personalizzando in ogni dettaglio i servizi offerti.
Dal 2018 SIPAL produce device TEMPEST, 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/

Studio Torta, leader nella consulenza della Proprietà Intellettuale, fornisce i più alti livelli di assistenza per la valorizzazione della creatività nel campo di brevetti, marchi e design, dalla fase delle ricerche preliminari al deposito delle domande di registrazione a livello nazionale e internazionale, dalla gestione nelle procedure amministrative all'assistenza nel contenzioso giudiziario. Fondato a Torino nel 1879, ha oggi uffici anche a Milano, Roma, Bologna, Treviso, Rimini.
Lo Studio è strutturato come Società per Azioni con 63 professionisti, alcuni di madrelingua cinese, giapponese, tedesca e francese, specializzati per i mercati internazionali e oltre 130 membri dello staff. Le competenze dei professionisti e il consolidato network di corrispondenti in tutto il mondo garantiscono un'assistenza puntuale nei più diversi settori industriali.
www.studiotorta.com

Teleconsys SpA, PMI innovativa, opera nell'ambito della consulenza, della integrazione di sistemi, dello sviluppo applicativo, della cybersecurity e della erogazione di servizi nel settore Information & Communication Technology, attraverso l'ideazione e la realizzazione di infrastrutture, applicazioni e piattaforme digitali innovative e l'erogazione di servizi specialistici ad alto valore aggiunto per la propria clientela di riferimento.
Teleconsys offre ai clienti competenze strategiche, consulenziali, tecnologiche, operative, condividendo le eccellenze presenti nel suo ecosistema dell'innovazione aperta per sviluppare, in maniera integrata, tutte le dimensioni necessarie per il successo di iniziative di innovazione digitale: cultura, persone, modelli di business, processi, tecnologie, ed operations.
www.teleconsys.it

Telespazio 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 dei satelliti; dai servizi di osservazione della Terra, comunicazioni integrate, navigazione e localizzazione satellitare, fino ai programmi scientifici. Telespazio gioca un ruolo da protagonista nei mercati di riferimento facendo leva sulle competenze tecnologiche acquisite in 60 anni di attività, le proprie infrastrutture, la partecipazione a programmi spaziali come Galileo, EGNOS, Copernicus e COSMO-SkyMed. Telespazio è una joint venture tra Leonardo (67%) e Thales (33%); nel 2022 ha generato un fatturato di 650 milioni di euro e può contare su oltre 3000 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

TS-WAY. è un info-provider specializzato in cyber threat intelligence e sicurezza offensiva, con un'offerta di servizi e tecnologie e un approccio alla sicurezza completi, a garanzia della continuità del business dei clienti.
Fondata nel 2010 a Orvieto (TR), TS-Way sviluppa tecnologie e servizi di sicurezza intelligence driven per realtà istituzionali e aziende di medie e grandi dimensioni. La sua piattaforma di servizi trasforma i dati delle minacce globali in fonti esclusive di tipo strategico, tattico, operativo e tecnico, consentendo alle organizzazioni di risparmiare tempo e risorse, anticipare le minacce, comprenderne la portata, potendo contare su un partner affidabile in caso di incidente informatico.
www.ts-way.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 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® è leader nelle soluzioni di backup, ripristino e gestione dei dati che offrono una Modern Data Protection. L'azienda fornisce un'unica piattaforma per ambienti Cloud, virtuali, fisici, SaaS e Kubernetes. I clienti Veeam hanno la certezza che le loro app e i loro dati siano protetti da ransomware, disastri e malintenzionati, e sempre disponibili grazie alla piattaforma più semplice, flessibile, affidabile e potente del settore. Veeam protegge oltre 400.000 clienti in tutto il mondo, tra cui l'81% della Fortune 500 e il 70% della Global 2.000. Veeam ha sede in Columbus, Ohio e ha uffici in oltre 30 Paesi. L'ecosistema globale di Veeam comprende oltre 35.000 partner tecnologici, rivenditori, fornitori di servizi e partner dell'alleanza e ha uffici in più di 30 paesi. Per saperne di più, visita il sito o segui Veeam su LinkedIn @veeam-software e Twitter @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: