2021
5ª EDIZIONE

AFCEA
CAPITOLO DI ROMA

1 anno di attività

REPORT 2020

www.afcearoma.it

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

nonostante la pandemia abbia condizionato pesantemente le nostre vite e le nostre attività, non poteva mancare la nuova edizione, la quinta, della nostra rivista sia per la qualità dei contenuti che per il gradimento la vicinanza manifestata da coloro che ci seguono fin dalla prima edizione.
I vari condizionamenti imposti dalla situazione pandemica non hanno consentito di svolgere alcuna attività in presenza, tuttavia siamo riusciti per il 2020 a realizzare un evento nel mese di novembre, via webinar, che ha confermato l'interesse e la stima da parte sia dei Soci che dei nostri fedeli estimatori che hanno partecipato in modo consistente. Un solo evento, però, non sarebbe stato sufficiente a giustificare la realizzazione di quella parte della rivista che normalmente fornisce una panoramica degli eventi svolti nel corso dell'anno e che rappresenta il cuore della rivista stessa.

Per tale ragione, al fine di garantire continuità nella pubblicazione della rivista, massimizzando la rilevanza e visibilità dei nostri Soci anche in un momento così complesso, per quest'anno abbiamo deciso di realizzare una nuova sezione ad hoc della rivista, costituita da una raccolta di articoli su argomenti di interesse per AFCEA, redatti principalmente da ciascuno dei nostri soci Corporate sulla base delle proprie competenze. Le altre sezioni della rivista sono rimaste inalterate nell'impostazione, proprio per assicurare continuità e riconoscibilità alla rivista. Tali aggiustamenti hanno comportato un maggior lavoro da parte del Comitato di Redazione cui va il mio sincero ringraziamento per aver operato ben al di fuori dei propri impegni lavorativi.

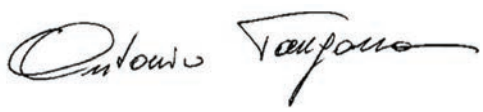
Sebbene nel 2020 sia stato realizzato un solo evento, il Capitolo è rimasto vivo e operativo incrementando in modo significativo, grazie al supporto di alcuni soci, la pubblicazione sul sito e la segnalazione via mail di articoli, report, documenti tecnici e notifiche di webinar organizzati dalle aziende Socie e da AFCEA International sui temi di rilevanza e attualità nei campi d'interesse dell'Associazione.

Ciò ha consentito di perseguire, anche in una situazione di oggettiva difficoltà, il principale obiettivo di AFCEA, vale a dire la promozione del 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.

In conclusione mi piace ricordare che il Capitolo di Roma è costituito da soci che operano su base esclusivamente volontaria con impegno e passione ed esprimere un sentito ringraziamento a coloro che, operando quotidianamente anche al di là dei propri impegni personali e lavorativi, assicurano l'operatività di uno dei maggiori Capitoli dell'Associazione, consentendogli di ottenere numerosi e importanti riconoscimenti da parte di AFCEA International.
Voglio cogliere dunque l'occasione per ringraziare ancora una volta tutti coloro, Soci e non, che ci seguono con attenzione, stima, partecipazione, suggerimenti spronandoci a fare sempre meglio.

Nell'invitarvi a seguirci sempre sul nostro sito, 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.
Nel 2021 ricorre il 75° anniversario della sua costituzione, avvenuta negli Stati Uniti nel 1946, dopo la seconda guerra mondiale, per raggruppare i veterani dei "battaglioni SIGNAL". Già dalla sua fondazione, AFCEA International cominciò a includere la componente industriale. A partire dal 1979 ha avuto inizio il processo di internazionalizzazione che ha portato alla creazione di Capitoli, oltre che negli Stati Uniti, in Canada, Sud America, Europa, Asia, Australia, per un totale di 139 capitoli in 30 Paesi.
Attraverso i suoi Capitoli, AFCEA International può contare attualmente su circa 30.000 soci individuali e circa 1.500 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.

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. Il 2020 è stato particolarmente ricco di soddisfazioni; infatti, il nostro Capitolo è stato premiato con il Model Chapter Award, l'Individual Member Growth, l'Individual Member Recruiting, l'Individual Member Retention e lo Special Recognition; quest'ultimo, assegnato per la prima volta al Capitolo di Roma, viene conferito ad un capitolo che è andato molto al di sopra degli obiettivi prefissati. È stato inoltre premiato il dott. Marco Braccioli con award individuale, 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, 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, la Dott.ssa Fiorella Lamberti è la rappresentante del Capitolo in Women in AFCEA Subcommittee , il Dott. Stefano Tangorra è il rappresentante in Young AFCEAn in Europe.

L'organizzazione

Come tristemente noto, nel 2020 la pandemia dovuta al COVID19 ha fortemente condizionato la vita e le attività di tutti i settori a tutti i livelli. Il Capitolo di Roma non ha fatto eccezione e, se ad oggi può contare su circa 450 soci individuali e 44 corporate ed essere tra i più grandi in Europa, lo si deve all'entusiasmo dei soci e ad una organizzazione consolidata ed efficace. Tutti i soci iscritti al Capitolo formano 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, ha il compito di assicurare che le attività dell'Associazione propongano contenuti tecnico-scientifici adeguati ed innovativi, attraverso la selezione di argomenti e tematiche che possano stimolare una divulgazione puntuale ed uno scambio culturale tra tutti partecipanti alla vita dell'Associazione. Inoltre, il Capitolo di Roma ha costituito il Comitato di Redazione, che ha la responsabilità di tutte le attività Editoriali e di Comunicazione tra cui quelle svolte tramite il sito web.

Il Capitolo di Roma ha inoltre creato al proprio interno due sezioni dedicate, Women in AFCEA e AFCEA Youth e, in linea con le corrispondenti commissioni già istituite da AFCEA International:

- **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).
- **AFCEA Youth** ha lo scopo di coinvolgere giovani studenti nella vita dell'associazione, per avvicinarli sempre di più al mondo del business nei settori della difesa e della sicurezza.

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, dello Spazio nell'ambito della Difesa, della Sicurezza e dell'Industria che opera in tali settori.

A tal fine, il Capitolo definisce ogni anno il proprio programma di attività, raccogliendo il contributo dei soci per organizzare riunioni, seminari, conferenze, visite o altre iniziative per mantenere i suoi membri aggiornati sulle problematiche nei settori d'interesse. L'accesso ai seminari e conferenze è libero per tutti gli interessati. La comunicazione degli eventi avviene tramite il sito dell'Associazione e Linkedin. Il calendario degli eventi è pubblicato anche sul sito di AFCEA International. A questa vengono poi inviati i report di ogni evento per la pubblicazione su SIGNAL, rivista ufficiale dell'Associazione, offrendo così anche l'opportunità, a coloro che hanno preso parte, in qualità di relatori agli eventi, di presentarsi sfruttando una vetrina di carattere 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 ed attualità attraverso la partecipazione delle principali istituzioni coinvolte, del mondo accademico e delle 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 disseminazione 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 diversi anni tre 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. Da due anni vengono inoltre finanziati tre Master di II° livello in "Optics and Quantum Information" presso l'Università di Roma La Sapienza

Come detto, la pandemia ha di fatto bloccato tutta l'attività in presenza e, causa la situazione di estrema incertezza, è stato possibile organizzare un solo evento a distanza, dal titolo "Contrasto e prevenzione delle minacce ibride in ambito infrastrutture critiche digitali: strategie e risposte a confronto" di cui nel seguito si riporta una sintesi. In compenso, con il supporto dei soci, il Capitolo ha incrementato molto la pubblicazione di articoli, documenti e l'organizzazione di webinar da parte delle aziende associate e da AFCEA International nei campi d'interesse dell'Associazione. 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, oltre ad una panoramica dei 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 fare conoscere le proprie attività professionali attraverso la pubblicazione di articoli e di notizie di rilevante interesse.
Sono inoltre disponibili informazioni sugli accordi e convenzioni stipulati con altre Associazioni e Organizzazioni.

L’evento

CONTRASTO E PREVENZIONE DELLE MINACCE IBRIDE IN AMBITO INFRASTRUTTURE CRITICHE DIGITALI: STRATEGIE E RISPOSTE A CONFRONTO

18 novembre 2020

Definita dalla NATO come l'impiego di strumenti militari e non-militari e di mezzi segreti e non, quali la disinformazione, gli attacchi condotti nel cyberspazio, la pressione economica e l'uso di gruppi armati irregolari, la minaccia ibrida ha lo scopo di destabilizzare, intimorire e confondere le popolazioni-bersaglio, al fine di ottenere un vantaggio politico. Tra gli obiettivi tipici della minaccia ibrida rientrano le infrastrutture critiche, sistemi o risorse la cui distruzione, interruzione o anche parziale o momentanea indisponibilità, può avere l'effetto di indebolire in maniera significativa il normale funzionamento di uno Stato, fino a comprometterne l'efficienza.

Per approfondire ed analizzare tale tematica, lo scorso 18 novembre AFCEA Capitolo di Roma ha organizzato l'evento dal titolo "Contrasto e prevenzione delle minacce ibride in ambito infrastrutture critiche digitali: strategie e risposte a confronto", con l'obiettivo di contestualizzare e definire il concetto di "minaccia ibrida" all'interno del nostro Paese, nel momento in cui esso è impegnato, come tutta l'Unione Europea, nella definizione di una strategia di transizione verso il digitale; grazie agli interventi di importanti rappresentanti del mondo istituzionale ed industriale, si sono messe a confronto possibili strategie e soluzioni per prevenire, mitigare e contrastare tale fenomeno, soprattutto all'interno di ambiti sensibili come quello della Difesa e della Pubblica Amministrazione.

T.Col.(C.C.) Alessandro CIMA - Comando Operazioni in Rete SMD - Il Perimetro di Sicurezza Nazionale Cibernetica quale misura di prevenzione e risposta alla minaccia ibrida. Il ruolo della Difesa

Gen.B.A. Luca CAPASSO - Ufficio Generale Spazio SMD-Difesa e Spazio: una nuova governance per la protezione e difesa delle infrastrutture strategiche spaziali

Dott. Aldo DI MATTIA - FORTINET - Dalla minaccia informatica alla minaccia ibrida

Dott. Rocco Nazario RICCIARDI - LEONARDO - La gestione della crisi informatica al tempo delle minacce ibride

C.V. Francesco A. MARCHETTI - V Reparto SEGREDIFESA - Critical Infrastructure: National Military Research Plan's strategic relevance for the European context

Dott.ssa Luisa Franchina - Presidente AIIC - Le azioni dell'Italia per il contenimento della minaccia ibrida sulle IC

I contributi dei soci

INTELLIGENCE: STRUMENTI E STRATEGIE PER IL NUOVO DOMINIO VIRTUALE

ALMAVIVA

In ambito Intelligence l'applicazione della strategia, della tattica e dell'operatività si modula su un nuovo dominio, che prescinde da quello aereo, terrestre e marittimo: il dominio virtuale. Pura tattica disegnata attraverso l'arte dell'informazione. Con il termine PsyOp (Psychological operation) si intende la pianificazione di attività in grado di accompagnare verso un modus cogitandi ancor prima di un modus operandi per conseguire obiettivi di natura politico-militare.

Il concetto di "guerra asimmetrica" - altrimenti detta "guerra ibrida" o "guerra irregolare" - rappresenta una costante sempre più comune e di prassi applicativa. Di fatto, si tratta di mera applicazione di strategie e tattiche modulate sugli attuali scenari, possibile frutto di cavilli giuridici (law warfare) o del coinvolgimento di attori non statuali. Parlare di warfare in tal senso, significa quindi prepararsi anche a multi-domain operations (Mdo) che contemplino nuove soluzioni a nuove, ma anche vecchie, minacce.

In una realtà geo-politicamente sempre più complessa, segnata dall'emergenza pandemica e dall'aumento di rischi Cyber, Almaviva, the Italian Innovation Company, è a fianco di Forze Armate e Polizia con soluzioni e servizi innovativi e integrati.

L'allargamento dei confini europei e flussi migratori sempre più marcati hanno radicalmente trasformato finalità, tecniche e obiettivi dei controlli effettuati quotidianamente da Forze dell'Ordine e corpi militari. E così l'Intelligence trova il suo volto e le sue declinazioni nelle discipline OSINT (Open Source Intelligence) e SocMint (Social Media Intelligence).

L'era della nuova informazione, che passa per l'estrazione, il filtraggio, la valorizzazione e la comparazione del dato (Open Source Data, Open Source of Information, Open Source Intelligence, Open Source of Intelligence Validated) diventa situational awereness, consapevolezza della situazione. In questo ambito gli strumenti sviluppati da Almaviva si prefissano come obiettivo l'individuazione del giusto target, della giusta informazione, nel tempo e nella giusta forma.

Strumenti evoluti di ricerca, analisi e visualizzazione permettono di applicare la Social Media Analysis (SMA) e la Social Network Analysis (SNA), filtrando per fonte e contenuto e mostrando lo scenario, gli attori coinvolti e le correlazioni, con diverse modalità di vista.

L'applicazione della Social Media Listening (SML) e del Social Media Monitoring (SMM) trovano piena realizzazione tramite un supporto di Intelligence Query che monitora, individua e suggerisce correlazioni altrimenti non note.

La strategia parte dall'operatività. Un Team di specialisti in analisi e studi di scenario, ad esempio, ha prodotto un report sulla cosiddetta "Rotta fantasma" - il flusso migratorio tra Algeria e Sardegna -comparando i dati open della Prefettura di Cagliari sugli sbarchi in Sulcis nel periodo tra 2014 e 2017, con quelli delle testate giornalistiche nazionali e locali.

Figura 1_L'immagine è meramente illustrativa. Si considera come porto di partenza Annaba (maggiormente utilizzato).

Con forte evidenza ne è risultato un sentiment locale negativo, nonostante la diminuzione degli sbarchi, e una correlazione tra reati minori e immigrazione. Parallelamente gli studi condotti hanno portato all'individuazione di una pagina aperta presente sul canale social Facebook, relativa a una community che, con tag apparentemente innocui come viaggi, svago, acquisti, creava un nodo di collegamento tra attori inseriti nell'immigrazione clandestina e le vittime del traffico.

Ciò a dimostrare quanto il piano di azione si sia spostato su territorio virtuale e quanto tecnologie, competenze e strumenti digitali di frontiera possano essere i nuovi e più adatti strumenti per una strategia di intelligence sugli attuali scenari di minaccia.

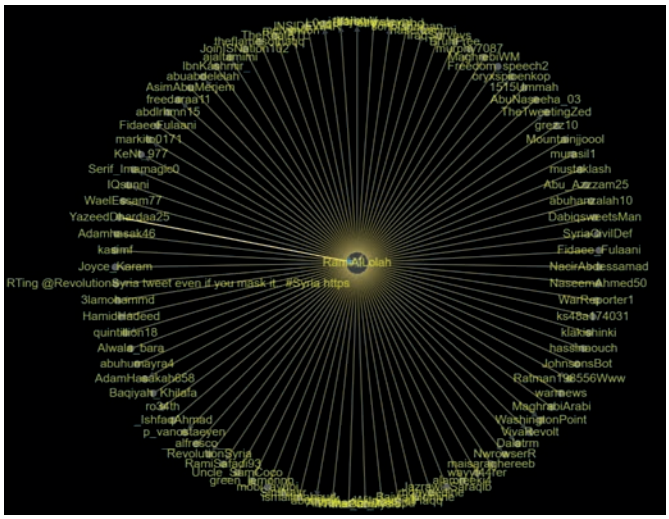


Figura 2_L'immagine è meramente illustrativa. Si considerano studi affini effettuati, utilizzando come Social Twitter.

ALEA IACTA EST. NEL 2021, INTELLIGENZA ARTIFICIALE NON È PIÙ UN OGGETTO DIVERSO DALLA CYBER SECURITY

Implicazioni legate alla Sicurezza delle informazioni

ASC27

La Sicurezza delle Informazioni, sia guardata dai bastioni difensivi, che dal punto di vista dell'attaccante, si basa su alcuni paradigmi fondamentali ricorrenti che sono accesso, comprensione e tracciabilità. L'attaccante ed il difensore, storicamente sono stati impegnati o per conquistare o per proteggere questi elementi costitutivi della catena di Sicurezza delle informazioni.

Un nuovo attore ha richiamato l'attenzione della platea e lo ha fatto da Game-Changer, la chiamiamo volgarmente Intelligenza Artificiale. Se fino a qualche anno fa, le fasi di conquista e mantenimento della Sicurezza erano pensate per resistere o per abilitare degli esseri umani, attualmente devono fare i conti con una nuova capacità delle macchine. Non parliamo, ancora, di sistemi sensienti o dalle capacità soprannaturali, ma di tecniche algoritmiche corroborate dalla meccanica dei Big-Data Analytics, che consentono ad una macchina di eseguire operazioni "intelligenti", facendo leva su una grande dose di Matematica e sull'abilità di nuove generazioni di sviluppatori software in grado di capitalizzarle.

In questo nuovo teatro delle operazioni, la Cyber deve confrontarsi con questo nuovo e potente avversario in grado di svolgere compiti fino a poco tempo fa non prevedibili, né per tipologia, né per velocità di esecuzione su scala. Un'AI può generare migliaia di volti sintetici al secondo per forzare un accesso biometrico, può leggere ed interpretare milioni di documenti al secondo per identificare notizie utili all'apertura di una cassaforte, può interpretare migliaia di segnali deboli col discernimento tipico delle persone per eseguire previsioni attendibili e può persino decidere di scrivere propri contenuti, sintetizzarli in una voce realistica e farli interpretare ad un avatar sintetico con le sembianze che l'AI possa ritenere più opportune rispetto al suo target.

Nel terzo decennio del secondo millennio, attacchi e minacce gestite da Intelligenze Artificiali non sono più un'ipotesi, ma un fatto; per questo motivo, mentre la veterinaria e la CyberSecurity restano materie distinte, l'AI entra prepotentemente a confluire direttamente, nel cuore, della Cyber.

In ASC27 ci occupiamo di due materie, Intelligenza Artificiale e CyberSecurity e lo facciamo bene, dalle fondamenta, con un approccio da scienziati di 30 anni (questa l'età media dei 20 componenti) che applicano nuove tecniche e gli ultimi risultati della Ricerca, a temi che conoscono nell'estremo dettaglio. Siamo una startup innovativa che non affitta AI dal Cloud, noi l'AI la facciamo. Gli asset dell'Azienda sono proprio i Bricks che compongono la nostra Cognitive Pipeline, componenti che sviluppiamo generalmente in ambito Industriale e che poi riportiamo nel mondo della CyberSec. Un processo continuo ed avvincente che ci ha portato a sviluppare soluzioni estremamente innovative e performanti, ma che ci ha anche mostrato in modo tangibile quanto e come la Sicurezza nello spazio Cyber sia collegata doppio filo con la Scienza dell'Intelligenza Artificiale Applicata.

Nel nostro mondo e nel nostro tempo, l'AI ha invaso la Cyber Security ed in molti ambiti ne ha anche preso possesso. Le strutture difensive si stanno adeguando, in un processo che dovrà essere necessariamente rapido ed efficace perché gli antagonisti lo stanno già facendo.
Nasce l'era in cui le informazioni devono essere sicure anche rispetto ad un attacco AI-Based. Nei moderni campi di battaglia si schierano anche le AI. Siamo da poco entrati nel decennio dell'Intelligenza Artificiale.

UNA PIATTAFORMA PER IL CONTROLLO E LA GESTIONE DEI PROCESSI A 360 GRADI

ASCITAL

La Società Consortile Ascital comprende 14 PMI operanti nei settori dell'ICT, della sicurezza globale, della Secure Digital Transformation, dell'Innovation & Cyber Security, degli impianti tecnologici, dei sistemi evoluti di automazione industriale. Attraverso le sue Società consorziate è in grado di fornire soluzioni competitive complete, ad ampio spettro da applicare in svariati ambiti del lavoro specie nel mondo della Difesa.

In particolare la Società consorziata Topnetwork, che offre servizi e soluzioni ad altissima innovazioni, ha sviluppato in proprio la Piattaforma AI4 per il controllo e la gestione dei processi a 360° ed è stata progettata per integrarsi con molteplici tecnologie, come i più diffusi protocolli IoT, di comunicare con dispositivi di domotica ed automotive per monitorare qualsiasi tipo di oggetto.

In questo modo, veicoli, persone e infrastrutture - sia fermi che in movimento - sono gestiti in maniera armonica, indipendentemente dalle proprie caratteristiche distintive.

La piattaforma consente una gestione uniforme e semplificata dei dispositivi IoT che intende monitorare, ed è in grado di analizzare i dati prodotti e costruirci sopra soluzioni verticali basate sull'Intelligenza Artificiale o qualsivoglia altra ulteriore tecnologia.

ALCUNE APPLICAZIONI DELLA PIATTAFORMA AI4

Gestione di un magazzino intelligente (AI4 Stock). Attraverso la verticalizzazione della piattaforma AI4 Stock consente la movimentazione, il posizionamento e il tracciamento dei beni stoccati, mediante l'utilizzo di sensori, telecamere e blockchain. Mediante l'analisi comportamentale è possibile monitorare anche le attività svolte dal personale sui beni presenti nei depositi e nei magazzini, così le azioni non autorizzate vengono prontamente segnalate tramite l'invio di notifiche o avvisi sui dispositivi preposti.

Gestione di aree industriali complesse o sensibili e ad alto rischio (AI4 Pipe). Con questa declinazione della piattaforma il sistema integra robot intelligenti (Rov aerei, terrestri, subacquei ma anche impianti di video sorveglianza) con il fine di monitorare condutture ed impianti individuando guasti, perdite idriche, sversamenti di sostanze oleose.

Dai dati raccolti dalle osservazioni periodiche è possibile creare un "gemello virtuale" dell'impianto che consente di effettuare un'efficace manutenzione predittiva, utile a evitare danni e perdite di fatturato improvvise.

Gestione dei flussi dei passeggeri sui mezzi (AI4 Move). Tramite l'installazione di pensiline intelligenti è in grado di analizzare i flussi ed i comportamenti dei passeggeri sui mezzi, per garantire una gestione dinamica delle corse.

Gestione delle colture (AI4 Farm). E' la soluzione dedicata alla gestione delle colture. Si tratta di un sistema di controllo autonomo basato su componenti hardware e software governati dall'intelligenza artificiale, con l'obiettivo di analizzare e prevedere la produzione di settore.

Individuazione e monitoraggio di scarichi illegali (AI4 Spot). La soluzione prevede l'utilizzo di robot aerei e subacquei in grado di collaborare ed identificare scarichi illegali all'interno di bacini idrici. Grazie ad un sofisticato sistema di reti neurali addestrate, i software incrocia i dati provenienti dalla termocamera e dalla camera multispettrale per creare mappe di rischio.

Riconoscimento semantico con AI (AI4 Web). Applicando l'AI ad un web crawler si è ottenuto uno strumento capace di discriminare a livello semantico i contenuti di un sito web. L'applicazione tipica è la ricerca di siti illegali in una data categoria con protezione della propria operatività.

Inoltre la piattaforma è in grado di gestire e analizzare tutte quelle azioni che attraverso telecamere, droni o mezzi aerei prevedono il pattugliamento di territori per la ricerca di persone scomparse o per la sorveglianza intelligente di aree ad alto interesse.

Attraverso l'utilizzo dell'AI si è in grado di individuare e segnalare tutte quelle anomalie rispetto ad un determinato contesto ed inviare degli allert ad una determinata control room. Grazie all'analisi video si può riconoscere intrusioni e di individuare precisamente se si tratti di persone, animali o veicoli e tanto altro.

COME ACCELERARE LO SVILUPPO DI SISTEMI RADIO PER LA DIFESA

La piattaforma di simulazione dei canali wireless

CRISEL

La creazione di un programma di test RF che sia veramente efficacie per sistemi radio tattici e altri sistemi radio mission critical richiede tecniche specializzate.
La modellizzazione del canale RF standard utilizzata nei tipici test radio, cellulari e Wi-Fi può non essere all'altezza. I dispositivi mission critical infatti incontrano doppler più elevati, gamme di frequenza inferiori, più percorsi da dispositivo a dispositivo e altre sfide che rendono inadatti i modelli di canale standard e gli approcci di test convenzionali.
I test di laboratorio svolti con piattaforme di emulazione di canali RF si sono dimostrati una metodologia che copre sistematicamente condizioni difficili da controllare sul campo e di fatto un approccio superiore ai test sul campo, poiche' garantisce vantaggi nella validazione di performance precise oltre a dare la possibilità di utilizzare piattaforme di test completamente automatizzate in condizioni ripetibili e quindi piu' stabili rispetto al test.
La Strategia di test è fondamentale: un test consuma molte risorse e tempo e va ottimizzata rispetto alla situazione specifica mentre cerca di imitare le condizioni del campo, cioè cambiare tutti i parametri dinamicamente, non è una strategia di test sistematica e non isola gli errori di sistema.

Il test su modelli di propagazione molto complessi non garantisce risultati migliori, è necessario gestire i principi di progettazione dello scenario di test.

La strategia di test radio inizia dalla definizione dei parametri critici:

- cosa influenza le prestazioni del ricetrasmettitore
- il PHY layer: Doppler, SNR, delay, correlazione

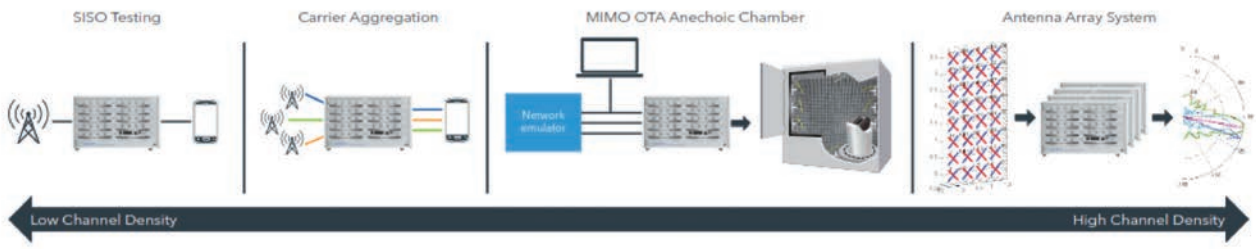
Da cui la necessita' della modellazione multi-tap di grandi delay e Doppler in un dato intervallo SNR (+ correlazione).
Andando un po' piu nel dettaglio, il fading rispetto a banda e rispetto al tempo e' selettivo, quindi in un sistema a banda stretta con frequency hopping, il canale è costante all'interno di un hop ma diverso tra più hop per cui e' necessaria la modellazione multi-tap a banda larga.
A differenza delle comunicazioni cellulari standard, le radio mesh sperimentano una doppia mobilità, il doppler non è mai un valore fisso basato su impostazioni predefinite, può variare con valori piccoli e grandi durante un periodo di simulazione, per cui le modalità Doppler fisse standard non sono sufficienti; si ha bisogno di variare il Doppler.

La stessa rete può avere ritardi sia grandi che piccoli a seconda della distanza dei collegamenti di comunicazione ed anche i nodi possono essere contemporaneamente mobili e statici.
Lo sweep del rapporto segnale-rumore (SNR) può essere ottenuto sia con lo sweep tradizionale in cui il rumore è aumentato o con la modellazione dinamica del canale; avere il controllo in tempo reale (RTC) nei casi dinamici è essenziale per testare l'adattabilità delle radio.
Nelle radio MIMO (Multiple Input Multiple Output), la correlazione definisce il modo migliore in cui i segnali possono essere risolti nella stessa banda di frequenza con la funzione di dispersione del segnale e separazione dell'antenna

Correlazione = 1 si traduce in cattive prestazioni MIMO
Correlazione = 0 si traduce in buone prestazioni MIMO

Riassumendo quanto sopra per eseguire un test nelle corrette condizioni, abbiamo bisogno di fading a banda larga, di variare Doppler, delay e SNR e di correlazione variabile nelle radio MIMO.

Crisel promuove un sistema con una configurazione HW e SW che include: un front-end RF modulare ed un potente core di elaborazione del segnale, mentre l'emulatore di canale ha un livello di scalabilità e flessibilità, che consente di affrontare in modo efficiente un'ampia gamma di applicazioni: da una bassa densità di canali come SISO o 2x2 MIMO ad alta densità di canale richiesta per scenari 5G, MIMO beamforming, MIMO OTA, carrier aggregation e massive MIMO.



COME L'INNOVAZIONE STA RIVOLUZIONANDO IL FUTURO DELL'AVIAZIONE

di David Ziegler Vice President, Aerospace & Defense

DASSAULT SYSTEMES

L'aviazione non sarebbe diventata quello che è oggi senza l'ambizione e la visione dei pionieri che per primi hanno immaginato che l'uomo potesse spiccare il volo. Senza il desiderio di sfidare i limiti del possibile, i viaggi aerei non sarebbero diventati una routine quotidiana, i velivoli militari non sarebbero mezzi allo stato dell'arte, e non avremmo esplorato nuove frontiere del sistema solare.

Questa spinta continua ancora oggi. La mente degli innovatori corre sempre alla prossima sfida. E gli innovatori non sono solo gli aviatori e le tradizionali compagnie aeree, ma anche realtà che non fanno parte da sempre del settore, ad esempio aziende di tecnologie e informatica, determinate a proporre soluzioni che le faranno diventare i prossimi pionieri dell'aviazione.

Oggi esiste la possibilità che, nel corso della nostra vita, potremo non solo diventare turisti spaziali, ma anche utilizzare un aerotaxi drone elettrico per raggiungere il terminal aerospaziale da cui comincia il nostro viaggio. Questa prospettiva riunisce in sé tre grandi obiettivi del mondo dell'aviazione: i viaggi spaziali, la mobilità aerea urbana e l'aviazione sostenibile. Altre innovazioni che stanno emergendo nel nuovo panorama spaziale sono migliori comunicazioni per aumentare la connettività a disposizione di tutti e l'obiettivo supremo dell'esplorazione spaziale: la possibilità di portare il genere umano su un altro pianeta. Solo dieci anni fa tutto questo sembrava impossibile, quindi è entusiasmante pensare a quali nuove opportunità potrebbero nascere nei prossimi dieci anni grazie ai pionieri che stanno reinventando il cielo.

L'aspetto più interessante di questo balzo in avanti delle tecnologie spaziali è che un settore finora controllato da agenzie governative si è aperto all'iniziativa di grandi industrie e imprenditori pionieri. Fra le realtà più rivoluzionare ci sono Space X, Blue Origin e Ball Aerospace nell'ambito spaziale, Bell, Zuri e Joby Aviation nel mercato aeronautico. Un'altra area nella quale si stanno distinguendo molte startup è lo sviluppo di tecnologie per la mobilità aerea urbana.

L'utilizzo crescente di velivoli senza equipaggio ha aumentato rapidamente l'affidabilità e la disponibilità delle relative tecnologie, e le menti più brillanti hanno capito che queste tecnologie avrebbero potuto essere applicate in nuovi ambiti come i trasporti.

I velivoli a decollo e atterraggio verticale (eVTOL) vengono attualmente sviluppati sia da grandi costruttori (OEM) sia da piccole startup. Queste aziende sono in gara per essere le prime a sviluppare un sistema certificabile e la relativa infrastruttura, puntando a un mercato il cui valore viene stimato in 7,9 miliardi di dollari entro il 2030.

Il software di modellazione sarà un fattore abilitante per realizzare il pieno potenziale di questi progetti in modo veloce ed efficiente. Una piattaforma in cloud come la piattaforma 3DEXPERIENCE può aiutare le startup ad accelerare questa evoluzione, consentendo loro di analizzare, simulare, certificare e sperimentare i velivoli eVTOL in un ambiente virtuale.

Uno dei vantaggi principali degli eVTOL è la motorizzazione elettrica, che ne fa un'alternativa più sostenibile agli aeromobili con motori a combustione.

Il settore dell'aviazione è ben consapevole del suo ruolo nella riduzione dell'impronta di carbonio e - insieme ai carburanti per aviazione sostenibile e, in prospettiva, all'idrogeno - la propulsione elettrica è uno dei modi principali per raggiungere tale obiettivo, così come tutte le modifiche che possono essere apportate al processo produttivo.

La piattaforma 3DEXPERIENCE porta ulteriori benefici in tal senso, mettendo a disposizione un ambiente virtuale nel quale modellare e progettare le fabbriche, con la possibilità di individuare i margini di efficientamento e apportare modifiche laddove necessario già nella fase di pianificazione, invece di farlo dopo che le fabbriche sono già state costruite.

I velivoli a idrogeno saranno un altro elemento che contribuirà a raggiungere l'obiettivo delle zero emissioni, grazie agli investimenti già in atto. Airbus, per citare un esempio, ha svelato i propri progetti per sviluppare tre modelli di propulsione a idrogeno (a turbina, a elica e a fusoliera integrata, o Blended Wing Body), per azzerare le emissioni entro il 2035.

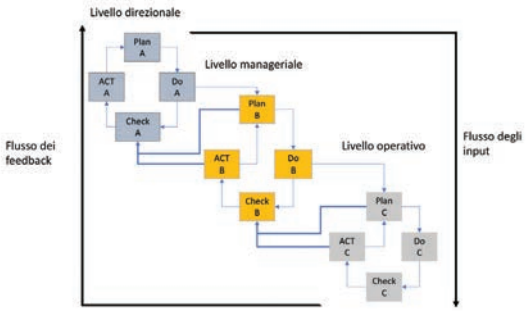
Il settore continua a spingersi oltre i limiti del possibile e, con le giuste soluzioni messe a disposizione dai fornitori di tecnologie, vecchie e nuove realtà del comparto continueranno a cambiare il modo in cui viaggiamo.

GESTIRE IL CAMBIAMENTO NELLE ORGANIZZAZIONI ATTRAVERSO LA VALORIZZAZIONE DEI DATI

DEIMOS

Il capitale immateriale (intangibles) delle imprese (processi interni conoscenza, competenza del personale) sta diventando sempre più rilevante nella definizione della strategia di mercato ed in particolare stanno assumendo sempre maggiore importanza i dati in possesso dell'azienda (sia relativo ai processi interni che i dati esterni) e la capacità di comprenderli.

Un approccio data driven consente di valorizzare le informazioni (data base) e la conoscenza (data analisys e visual data) permettendo ad ogni livello dell'organizzazione (direzionale – manageriale – operativo) di valutare e migliorare le proprie performances.



Il flusso dei dati è una catena che trasporta dentro l'azienda il ciclo di miglioramento

DEIMOS ha affiancato alcune esperienze di innovazione e di miglioramento organizzativo attraverso TABLEAU e STRATEGY COMPASS.

Per Aziende di Trasporto Pubblico Locale, Deimos ha studiato una soluzione che ha organizzato i dati atomici forniti dai differenti gestionali presenti nel sistema (esercizio programmato, servizio effettivo, contapasseggeri, sistema di vendita fisica e vendita virtuale, call center, reclami, sito internet e APP) in maniera usufruibile realizzando una Data Warehouse utile per alimentare un insieme di dashboard organizzati secondo uno schema di Balanced Scorecard. Nel settore della distribuzione ricambi auto, Deimos ha affiancato una importante realtà nel dotarla di una piattaforma di analisi e reporting che consenta sia al responsabile acquisti, al responsabile vendite e al Management di esplorare i dati in modo semplice, analizzarli velocemente e rappresentarli in report visuali di facile lettura, per comprendere meglio i risultati e condividerli in Azienda ed all'esterno. Particolare attenzione è stata posta per monitorare i livelli di scorta, e suggerire quando e quanto ordinare per evitare il fenomeno della rottura di scorta di magazzino. In questo caso Tableau è stato integrato con il gestionale aziendale ed in sistema WMS di gestione operativa del magazzino, che permette una gestione dinamica delle allocazioni di stoccaggio che minimizza i percorsi di carico e scarico: i prelievi sono agevolati dalla possibilità di verificare la situazione di magazzino in tempo reale, consentendo un controllo diretto degli ordini in evasione. Attraverso il collegamento "real time" con il sistema Gestionale Aziendale, supervisore contabile alle attività di magazzino: viene trasferito al wms il dettaglio della merce in accettazione e le liste dei materiali da prelevare per ottenere, in risposta dal WMS, il dettaglio dei movimenti di magazzino effettuati, al fine di mantenere l'allineamento contabile e numerico delle giacenze.

Il vantaggio competitivo fornito dalla conoscenza del proprio capitale organizzativo (processi interni - performances) soprattutto se inserito in un management strategico supportato da una Balanced Scorecard, può "fare la differenza" nel successo dell'impresa.

Nel campo del Machine Learning, Deimos è stata in grado di offrire risultati di valore nell'anomaly detection in campo medico. L'Obiettivo è quello di migliorare le attività amministrative attualmente svolte dai medici delle aziende sanitarie, eliminando errori da cui poi derivano mancati o eccessivi rimborsi economici riconosciuti alle varie strutture. Deimos, utilizzando il sistema di Robotic Data Correction di Rulex nato per la pulizia automatica dei dati negli ERP, ha sviluppato una soluzione in grado di riconoscere automaticamente le anomalie a partire dai dati storici e di correggerli automaticamente o di segnalarli all'utente per verifica.

Sempre in campo medico Deimos ha utilizzato Rulex per l'analisi dei dati dei pazienti affetti da patologie croniche a fini di Knowledge discovery, identificando dei pattern ricorrenti che possono inficiare l'efficacia terapeutica, fornendo così utili indicazioni alla comunità medico scientifica (e all'industria farmaceutica) su alcuni aspetti prioritari che, se indirizzati, potrebbero produrre un impatto positivo sugli outcome di cura.

[1] *Mappe strategiche. Come convertire i beni immateriali in risultati tangibili - Robert S. Kaplan - David P. Norton – ISEDI, Torino 2015*

Capitalismo senza capitale. L'ascesa dell'economia intangibile – Haskel J. – Franco Angeli, Milano 2018

[2] *https://www.deimosengineering.it/*

LA SOLUZIONE ELES PER LA QUALIFICA, L'AFFIDABILITA' E LO SCREENING ACCELERATO DEI MODULI ELETTRONICI

La metodologia mutuata dai semiconduttori

ELES SEMICONDUCTOR

Eles Semiconductor è leader mondiale nel settore della qualifica e dell'affidabilità dei semiconduttori. Grazie alle sue soluzioni di test sia hardware che software, affinate da oltre trenta anni di esperienza, i clienti riescono ad ottenere vantaggi dimostrati e significativi nella gestione del processo di sviluppo di un nuovo dispositivo semiconduttore.

Da questa esperienza è poi derivata l'attività rivolta ai produttori di moduli elettronici impiegati sia nel modo automotive che militare, dove le esigenze di affidabilità sono spinte ai massimi livelli.

La metodologia che guida l'approccio Eles è la AEC (Q100) applicabile a diversi settori:

- Aerospace
- Automotive
- Unmanned Operating Machines
- Medical

Negli ambiti di cui sopra la metodologia prende in considerazione diversi aspetti del prodotto e la sua interazione con il mondo che lo circonda:

- Preservare l'ambiente
- Incrementare la funzionalità
- Evolvere le performance

Se solo si considera l'incredibile incremento di presenza di dispositivi elettronici in tutto ciò che ci circonda, sia a livello personale che sociale, è evidente che il problema della sostenibilità debba essere messo al centro di qualsiasi analisi affidabilistica e diventi quindi primario.

Sviluppare prodotti con elevate prestazioni, ma con bassi consumi, e con elevata resistenza a fattori ambientali esasperati, garantendo un basso livello di difettosità, tendente allo zero, è la mission che compete ai nostri clienti, Eles ha l'importante compito di fornire soluzioni e metodologie per stressare, accelerare, misurare e dare evidenza che la centralina progettata sia in grado di assolvere la missione assegnata.

La soluzione R.E.T.E. (Reliability Embedded Test Electronic) proposta da Eles si fonda su librerie di test proprietarie sviluppate nel tempo grazie al continuo lavoro a fianco delle aziende di semiconduttori.

Grazie a R.E.T.E. ed ai sofisticati algoritmi embeddati nelle funzioni di test, qualsiasi potenziale causa di failure del modulo può essere ricondotta alla sua origine, analizzata e risolta sia a livello di design o immediatamente dopo in fase di qualifica.

Utilizzando parti circuitali a basso impatto, possono essere aggiunte ed integrate facilmente nei moduli in analisi funzioni di DfRT (Design for Reliability Test) e di TfR (Test for Reliability) che consentono poi successivamente di poter testare funzionalmente tutti i nodi interni significativi del modulo durante le fasi di ciclatura termica, determinando quindi la condizione ottimale di stress + test in grado di evidenziare qualsiasi potenziale debolezza.

Eles disegna, ingegnerizza e produce tutte le sue soluzioni in Italia, impiegando le migliori risorse Italiane, impegnandosi continuamente nel sociale e nel basso impatto ambientale.

Di recente Eles si è quotata in borsa a Milano per ottenere ulteriori risorse da investire sia su linee innovative di ricerca che per strutturare operazioni di M&A in grado di rafforzare la propria leadership a livello internazionale.

SMART MASK SYSTEM – ACTIVE HUMAN PROTECTION AND DATA SHARING IN HIGHLY CONTAMINATED ENVIRONMENT

ELETTRONICA

The modern command and control function poses challenges and questions to which adequate answers have to be given. Response time and technology play a decisive role in preventing threats as well as protecting decision making. The availability of individual protection and information management systems is an indispensable condition for guaranteeing command and control capabilities i.e. during NBC support operations or in contaminated areas.
In this context Smart Mask System, here presented by ELT Group, foresees the distribution of man-wearable multi-sensor masks and connectivity standard devices, sharing data related to "air quality" in a given area while protecting the human from pollutants and pathogenic elements.
The System, who is patent pending, consists of two parts:

- Active part: composed of sensors and actuators with low energy consumption and a part of algorithmic intelligence and calculation placed in a portable electronic device (smartphone, tables etc.) equipped with sufficient processing resource and graphics interface. In detail the sensors are integrated in a removable section of the system and by means of a microprocessor an RF (Radio Frequency) transceiver (i.e. bluetooth) they exchange data and commands towards the computing device that processes such raw data to provide complex high-level functions to the user.
- Passive part: it mainly consists of a semi-facial mask with integrated filter which performs the function of protection against external pathogens agents.

The sensors and actuators functions are detection and transmission of data regarding the "air quality" with respect to VOCs (Volatile Organic Compounds); one of the actuators integrated in the active part allows to increase the protection capacity of the filter placed inside the System through the use of UV-C leds of proven germicidal and disinfection capacity. The signals generated by the various sensors are collected and digitized by a microprocessor and subsequently transmitted via RF signals (bluetooth) to the implemented computing section (dedicated app) on a portable device (smartphone, tablet etc.) which analyze and presents the results to the user that can share such data with the command and control post. The passive part consists of a plastic semi-facial mask with integrated filter which is constantly sanitized by the UVGI (Ultraviolet Germicidal Irradiation) actuators with relative lengthening of its duration. The System is equipped with an integrated and rechargeable power supply (i.e. Lipo battery) able to power sensors and actuators for a given time (about 4 hours). The long-lasting use mode is ensured by connecting the System via USB to an external power device such a power bank or the same computing device, sharing the battery. The system is scalable and continuously upgradeable by adding additional sensors/actuators which with is possible to implement new functions.

TORRI DI CONTROLLO VIRTUALI PER VALIDAZIONE DI NUOVI CONCETTI OPERATIVI

Piattaforme di simulazione al servizio di ANSP

Giuseppe Di Bitonto, Luna Babusci, Antonio Nuzzo

ENAV

ENAV assicura l'assistenza alla navigazione agli aeromobili durante tutte le fasi del volo nello spazio aereo nazionale. L'erogazione di tale servizio implica un'importante fase di formazione e addestramento in ambito ATM del personale coinvolto, anche attraverso piattaforme di simulazione, permettendo lo sviluppo di competenze tecniche e di decision making per la gestione del traffico aereo.

La possibilità di modellare scenari aeroportuali esistenti o futuri e sperimentare diverse condizioni di esercizio, fanno dell'impiego della simulazione un fattore essenziale, non solo per quanto concerne il training del personale, ma anche per la validazione di nuovi concetti operativi. Il gruppo ENAV, mettendo a fattor comune le esigenze operative attuali e future (e.g. Remote Tower Centre) con quelle industriali e di mercato, punta al consolidamento di prodotti di simulazione che siano fruibili da tutte le parti coinvolte, con l'obiettivo di incrementare l'efficienza operativa, assicurando gli adeguati standard di safety.

Il programma SESAR (Single European Sky ATM Research) si prefigge di studiare e validare concetti tecnici e operativi a supporto di un sistema evoluto di gestione del traffico aereo per lo spazio aereo europeo.

In questo ambito, ENAV è in prima linea su molteplici progetti del programma SESAR relativi a tematiche aeroportuali, di rotta e avvicinamento, comprendendo aspetti di pianificazione, gestione delle informazioni e interoperabilità. L'utilizzo di piattaforme di simulazione è un aspetto fondamentale per permettere la validazione in modalità real-time e in ambienti pre-operativi.

Una delle sfide che il gruppo ENAV sta affrontando riguarda l'efficientamento nella fornitura del servizio di controllo aeroportuale. Attualmente, su ogni aeroporto in cui il servizio è fornito da ENAV insiste una torre di controllo fisica, con controllori del traffico aereo responsabili del controllo degli aeromobili sia durante la movimentazione a terra, all'interno dell'area di manovra, sia sulla pista per decolli e atterraggi e sia nei circuiti di traffico. La strategia incrementale prevista nel piano industriale di ENAV prevede un primo step, in cui le torri di controllo definite "convenzionali" verranno sostituite singolarmente da torri digitali, e un secondo step, in cui le nuove torri digitali verranno raggruppate in due centri di

controllo.

L'obiettivo a cui ENAV mira nel progetto PJ05 Digital Technologies for Tower e nello specifico nella Solution 35, intitolata "'Multiple Remote Tower and Remote Tower Centre", corrisponde all'eventuale terzo step, cioè validare il concetto di controllo di aeroporti multipli da parte di un unico controllore.

Sarà creato un centro di controllo aeroportuale ad hoc per l'esercizio SESAR presso la sede dell'Academy ENAV di Forlì. Il centro sarà costituito da due isole di controllo, chiamate Remote Tower Module (RTM), equipaggiate con tutti gli strumenti necessari all'erogazione del servizio ATS (e.g. presentazione visiva, strip elettroniche, canali voce, schermo radar, info meteo) e una postazione per il Supervisore operativo, responsabile dell'assegnazione dinamica di tre aeroporti sui due RTM, sulla base di parametri che concorrono alla previsione dei livelli di workload percepiti dai controllori del traffico aereo nel breve-medio periodo (e.g. volume e tipologia di traffico, condizioni meteo, ecc.).

Sempre nell'ambito SESAR, nel progetto PJ02 "Digital evolution of integrated surface management", ENAV insieme a NavCanada, ANSP canadese, ha in programma di sperimentare con una piattaforma di simulazione congiunta tra i due ANSP, un altro concetto operativo afferente alla gestione del traffico sull'area di manovra. Attraverso un sistema virtuale di luci (Virtual Stop Bar) ci si pone l'obiettivo di efficientare la movimentazione in maniera dinamica, anche in presenza di condizioni di visibilità ridotte (LVP). La validazione sperimentale assume maggiore importanza e credibilità per una futura applicabilità del nuovo concetto operativo, grazie all'utilizzo di piattaforme di simulazione aderenti alle reali implementazioni operative e grazie al coinvolgimento del personale ATC, pseudo-pilot e del team di ingegneria.

L'approccio metodologico, che utilizza la simulazione come strumento di validazione, e la flessibilità d'impiego degli asset di simulazione possono costituire un valore aggiunto anche in caso di scenari e casi d'uso in ambito militare. L'esperienza ENAV può facilitare l'applicazione di tale metodologia per scopi di operazioni militari, anche in termini di hosting, essendo dotata di un sito concepito per tali scopi, il National Test Facility presso la sede di Ciampino.

MITIGARE I RISCHI DELLE CENERI VULCANICHE PER L'AVIAZIONE E LE INFRASTRUTTURE

Impiego della tecnologia del Lidar Vaisala CL61

EURELETTRONICA ICAS

Le eruzioni vulcaniche sono un fenomeno globale. Però, non esiste una rete di strumenti atti al rilevamento delle eruzioni o al monitoraggio dei pennacchi di cenere. Inoltre, spesso, è difficile osservare le eruzioni utilizzando le immagini satellitari, poiché gli strati di nuvole possono limitarne la vista. La cenere vulcanica viene sia portata verso l'alto all'interno del pennacchio della nube sia trasportata dal vento per distanze molto lunghe; man mano che la cenere cade, può potenzialmente interessare aree di centinaia, o addirittura migliaia, di chilometri quadrati. La ricaduta di cenere sul terreno può causare danni significativi ad edifici, trasporti, acque superficiali, alimentazione elettrica, apparecchiature per le comunicazioni, agricoltura e così via, con conseguenti impatti sull'economia delle comunità colpite. Le polveri sottili della cenere, inoltre, possono causare effetti sulla salute di esseri umani e animali.

La cenere vulcanica trasportata dall'aria rappresenta un grande pericolo per l'aviazione. Le nubi di cenere possono diminuire la visibilità, danneggiare i sistemi di controllo dell'aeromobile e causare il guasto dei motori. I controllori del traffico aereo e i piloti devono essere informati tempestivamente circa eventuali eruzioni vulcaniche per evitare le nuvole di cenere vulcanica formatesi.

Negli ultimi anni sono stati raggiunti numerosi progressi nella fornitura di informazioni relative alla presenza di cenere vulcanica nell'atmosfera. Nel campo del trasporto aereo è stato implementato un sistema di monitoraggio delle ceneri vulcaniche lungo le vie aeree internazionali, dotato di centri regionali di consulenza che garantiscono un monitoraggio continuo e quasi globale. Questi centri emettono avvisi sulle ceneri vulcaniche fornendo informazioni sulla presenza di ceneri in atmosfera e sui loro spostamenti previsti. L'interruzione del traffico aereo europeo causato dalle eruzioni vulcaniche Eyjafjallajökull e Grimsvötn in Islanda nel 2010 e nel 2011 ha indicato la necessità di tracciare continuamente il profilo verticale degli aerosol utilizzando la tecnologia Lidar. Il telerilevamento con un celiometro Lidar è un modo efficace, accurato e conveniente per misurare i profili atmosferici verticali e per migliorare la comprensione delle condizioni meteorologiche attuali e future.

La tecnologia dei celiometri Lidar è stata migliorata negli ultimi anni e ora questi sistemi offrono l'opportunità di monitorare continuamente il profilo verticale degli aerosol, ivi comprese le ceneri vulcaniche e l'altezza dello strato di mescolamento.

Con il celiometro di nuova generazione CL61, Vaisala ha introdotto per la prima volta in un sistema commerciale, una caratteristica innovativa: la misurazione della depolarizzazione. La radiazione emessa dal laser di un sistema Lidar risulta essere polarizzata linearmente. Il fascio laser inviato dall'apparato subisce un processo di depolarizzazione in seguito allo scattering (diffusione) da particelle non sferiche. Le nuove capacità di misura della depolarizzazione, che sono state finora utilizzate solo nei Lidar per applicazioni di ricerca, consentono di differenziare fra precipitazioni liquide e solide, di rilevare polvere, sabbia e gli strati delle ceneri vulcaniche.

Il CL61 sfrutta le impareggiabili tecnologie di intelligenza meteorologica di Vaisala per fornire in maniera continua dati del profilo, 24 ore su 24, anche nelle condizioni meteorologiche più difficili, per una migliore comprensione delle condizioni atmosferiche. I dati forniti dallo strumento possono essere utilizzati per correggere i modelli della qualità dell'aria, fornire la verifica dei dati e consentire il nowcasting e la sicurezza dei viaggi aerei e le attività correlate. Il celiometro Vaisala CL61 è dotato di ottiche a lente singola che migliorano significativamente il rapporto segnale-rumore per fornire profili di retrodiffusione ad alta risoluzione.

Con funzionalità finora disponibili solo nei Lidar per applicazioni di ricerca, il CL61 ha un prezzo molto conveniente, è semplice da installare ed utilizzare, non necessitando di manutenzione nè di calibrazione. CL61 è l'unico prodotto nella sua categoria disponibile sul mercato per applicazione di monitoraggio non presidiato, in modo continuo ed in tutte le condizioni meteorologiche. Sin dagli anni 1980 Vaisala è stata pioniere nella tecnologia dei Celiometri Lidar e vi sono migliaia di unità installate in più di 110 paesi.

UTILIZZO DI PIATTAFORME UNMANNED IN OPERAZIONI 4D IN AMBIENTE A SUPPORTO DEGLI UMANI IN APPLICAZIONI DUAL USE

Verso una maggiore interazione tra umani e robot per una vita migliore

Pietro Lapiana - Presidente

EUROLINK SYSTEMS

Eurolink Systems è stata pioniera nel 2009 nel proporre al mercato Italiano piattaforme mini e micro UAV senza pilota per impieghi nelle situazioni 4D (Dull, Dirty, Dangerous, Dear) dimostrando una (delle molteplici a seguire) applicazione per le riprese video in alta definizione.

Per la prima volta nella storia ed in anteprima mondiale nel 2011, un quadricottero ad eliche intubate di Eurolink Systems volò al 197° Anniversario di fondazione dell'Arma dei Carabinieri. Sempre nella stessa cerimonia ancora una volta, primi al mondo, fu fatto volare il Tricolore sopra 15.000 partecipanti all'evento. Da quella storica presentazione, Eurolink Systems ha continuato non solo a distribuire ma anche a sviluppare piattaforme Unmanned, aeree di classe mini sino ai 20Kg e terrestri dai 3Kg ai 60 Kg. Il loro utilizzo in teatro operativo con FFAA Italiane ed estere, ne ha mostrato l'efficacia e il prezioso aiuto agli esseri umani in operazioni cIED o per videosorveglianza, per analisi su strutture o per ricostruzione 3D di scenari.

Tali utilizzi hanno sempre comportato di fatto il "prolungamento" dei sensi dell'operatore il quale, a distanza di sicurezza, sino a 42Km linea di vista per i mezzi aerei e ai 2 km per i mezzi terrestri, poteva rendersi conto di potenziali minacce o di effettuare rilievi in sicurezza in aree pericolose. Una interessante sperimentazione fatta in passato da Eurolink Systems assieme ad un Centro di Eccellenza di difesa Internazionale ed il maggiore Gruppo di difesa nazionale, ha consentito di iniziare a testare realmente un nuovo approccio in aree pericolose ovvero l'utilizzo di sciami di droni terrestri ed aerei. Essa prendeva in considerazione lo studio dei sistemi auto-organizzati, nei quali un'azione complessa deriva da un'intelligenza collettiva, come accade in natura nel caso di colonie di insetti o stormi di uccelli, oppure banchi di pesci, o mandrie di mammiferi. Le piattaforme Unmanned sono diventate famose come "droni" principalmente per il loro utilizzo bellico, nelle versioni armate ma in realtà, possiamo avere nuovamente moltissime applicazioni in ambienti diversi dal militare. Negli ultimi anni si sente parlare ad esempio di "Agricoltura 4.0" o "Precision Farming" che altro non è che una strategia di gestione dell'attività agricola con la quale i dati vengono raccolti, elaborati, analizzati e combinati con altre informazioni per orientare le decisioni in funzione della variabilità spaziale e temporale al fine di migliorare l'efficienza nell'uso delle risorse, la produttività, la qualità, la redditività e la sostenibilità della produzione agricola.

Analogamente alle applicazioni nei teatri operativi militari o urbani, i sistemi Unmanned si prestano particolarmente anche per tali attività, come anche nel "search and rescue", in caso di "disaster recovery" naturali o artificialmente creati.

Prima di stabilire quale tipologia di attività demandare a sistemi costituiti da piattaforme "intelligenti" ovvero droni terrestri ed aerei (UGV e UAV), è necessario caratterizzare lo scenario operativo. Quest'ultimo dipende principalmente dalla morfologia del territorio di operazione e dal profilo di missione e quindi, ad es., nello specifico per l'Agricoltura 4.0, dalle tipologie di allevamento e potatura praticati nelle colture principali da analizzare È facilmente intuibile come questi fattori influenzino le modalità con cui i sistemi collaborativi di UAV e UGV potranno svolgere le loro attività.

In considerazione delle peculiarità del terreno destinato ad esempio alle coltivazioni agricole, l'implementazione di soluzioni di agricoltura di precisione relative al monitoraggio e alla gestione agronomica e automatizzata dei fondi potrebbe richiedere l'impiego di piattaforme "smart", senza pilota, che dovranno avere le seguenti caratteristiche:

- UGV di peso ed ingombro relativamente contenuto, versatili, provvisti di locomozione cingolata e gommata in modo tale da superare agevolmente le pendenze del terreno e di adattarsi ad esempio a filari stretti e disomogenei;
- UAV di classe Mini in versione multi-rotore o ad ala fissa a seconda del profilo di missione assegnato. I primi per consentire un'alta persistenza su un determinato oggetto, i secondi per garantire il sorvolo di aree geografiche estese in tempi ridotti;
- adozione di una propulsione elettrica per minimizzare l'impatto ambientale;
- necessità di non più di 1-2 persone per il dispiegamento ed il controllo della navigazione sullo scenario operativo assegnato;
- le singole piattaforme in grado di operare in modalità collaborativa dovranno poter essere riconfigurabili (modifica del payload) a seconda del profilo di missione assegnato.

L'INTELLIGENZA ARTIFICIALE NELLE LEGALTECH. TELEFORUM FOR® È TRA LE SOLUZIONI PIÙ INTERESSANTI DI ENTERPRISE LEGAL MANAGEMENT

EUSTEMA

La trasformazione digitale delle avvocature nelle grandi organizzazioni pubbliche e private e l'evoluzione delle legal tech (legal technology) sono tra i temi al centro delle attività del Gruppo Eustema che, con uffici operativi a Roma, Milano e Napoli contribuisce, sin dal 1989, alla crescita e alla trasformazione digitale del Paese. «Siamo specializzati nella realizzazione di complessi sistemi informativi, che rispondono a esigenze quali alte performance, elevata numerosità di utenti, sicurezza delle informazioni-spiega Paola de Rosa Direttore Operations di Eustema tra i nostri punti di forza rientrano le competenze per la gestione dell'intero ciclo di vita del Dato; in questo settore siamo partiti da una ventina di anni, facendo nostro il tema dell'innovazione. Stiamo proseguendo, partendo dalle architetture Big Data e arrivando al machine learning, all'intelligenza artificiale, con il supporto di validi data scientist. Tra le soluzioni più strategiche rese disponibili dal Gruppo Eustema per il settore dell'enterprise legal management c'è Teleforum For. Il Market Guide for Enterprise Legal Management Solutions di Gartner ha inserito il nostro prodotto Teleforum For tra i principali vendors nel settore LegalTech. Siamo partiti dall'obiettivo di digitalizzare i processi di gestione delle pratiche legali e oggi con Teleforum For supportiamo la definizione di un vero Legal Data Hub che concretizzi il valore delle attività legali e faciliti il miglioramento dei processi di business dell'organizzazione. La necessità di digitalizzare le informazioni conservate in modalità cartacea, si è ben presto estesa all'automazione dell'intera area legale, con l'introduzione di soluzioni di Business Process Management, Document Management e Analytics per il supporto alle decisioni operative e strategiche dell'Area Legale e la gestione del Rischio Finanziario Legale. Le funzionalità di Collaboration native nel prodotto si sono dimostrate fondamentali per il repentino passaggio allo Smart Working vissuto ora anche dalle aree legali». Oggi la digital transformation e i recenti sviluppi dell'intelligenza artificiale stanno guidando l'enterprise legal management nell'era 4.0. Secondo Gartner il settore dell'automazione delle attività legali sarà tra quelli che beneficeranno maggiormente delle nuove tecnologie dal momento che nell'area LegalTech gli investimenti cresceranno tra il 20 e il 50%. Obiettivo di

Teleforum For è supportare tutte le attività legali all'interno delle organizzazioni, con forte focalizzazione sul contesto legislativo italiano. «Il machine learning, in Teleforum For, supporta la gestione del singolo contenzioso, suggerendo elementi che possono aiutare l'impresa a trovare la migliore modalità di gestione dello stesso – spiega Sergio Palma Chief Technology Officer - il machine learning non può e non vuole sostituirsi all'azione legale, ma ha l'obiettivo di permettere che la conoscenza acquisita in azienda possa diventare un valore per quanti devono utilizzarla nell'impresa. Un secondo livello di operatività del machine learning riguarda l'organizzazione dell'area legale per capire come gestire al meglio la struttura, per comprendere se stanno emergendo nuove tipologie di contenzioso che possono mettere a rischio l'organizzazione stessa. Queste informazioni utilizzeranno algoritmi di analisi predittiva dei dati. Attraverso modelli predittivi sarà possibile, inoltre, evidenziare punti di miglioramento dei processi di business che permettano di limitare il contenzioso o di evitarlo». L'integrazione con i processi telematici, in Italia, ha acquisito sempre più importanza da quando è stato avviato il processo di digitalizzazione della giustizia, partito una decina di anni fa con il Processo Civile Telematico. «Teleforum integra il processo civile telematico, consentendo di depositare e consultare atti, velocemente, in modo guidato e riducendo le possibilità di errore – conclude Palma - gestiamo anche la parte di e-billing, ovvero la gestione della spesa legale e sono disponibili integrazioni native con strumenti produttività e office automation». Da circa tre anni Eustema ha avviato anche il servizio in cloud Teleforum SaaS, che consente di erogare la soluzione alle realtà che vogliono utilizzarla senza doversi dotare di un'infrastruttura Il servizio Cloud è qualificato AgID.

LA PIATTAFORMA JOINT MULTIPLE SCENARIOS SYSTEM

Un sistema modulare per la gestione di scenari

FABARIS

È ormai da qualche anno che l'area di Modeling & Simulation (M&S) della Fabaris sta concentrando le sue attività nel campo della realizzazione di territori urbani.

Tale esperienza nasce nel 2015 quando ACT NATO ci richiese di realizzare Archaria, una megalopoli del 2035, per supportare l'analisi dei suoi possibili interventi in tale ambito in relazione al fenomeno dell'urbanizzazione sempre più crescente.

L'approccio richiesto dalla NATO non poteva che essere omnicomprensivo, ritenendo in effetti che la complessità del territorio urbano, effetto cumulativo di una serie di livelli interconnessi di società e infrastrutture, non potesse essere affrontato solo da un punto di vista militare.

Il modello di Archaria continua ancora oggi ad essere richiesto e, dopo aver raggiunto la necessaria maturità, è stato di supporto a varie esercitazioni. Fu proprio durante queste esperienze e dalla tipologia di richieste che ci pervenivano dai partecipanti, che capimmo di dover sviluppare una nuova modalità di approccio per la realizzazione di tali scenari.

L'idea partì dal fatto che, concettualmente, una qualsiasi serie di esperimenti di laboratorio condotti indipendentemente su un sistema, si basano principalmente sull'idea che le condizioni iniziali del sistema esaminato, devono essere sempre le stesse o almeno che eventuali differenti configurazioni inziali siano conosciute e gestite.

Per tale motivo, la visione principale fu quella di realizzare una "piattaforma di scenari" per avere la disponibilità di molteplici "Archaria" sulle quali i vari i gruppi di lavoro, in maniera indipendente, potessero sviluppare le loro COA (Course of Action) a mitigazione degli eventi proposti.

In fase di After Action Review i risultati ottenuti dai vari gruppi di lavoro avrebbero potuto quindi essere confrontati e le loro eventuali difformità essere oggetto di discussione e approfondimento a supporto della scelta della "migliore" decisione operativa da intraprendere.

Nacque quindi l'idea dell'implementazione di una piattaforma di rappresentazione del territorio urbano che, a partire della realizzazione di una città, potesse creare in maniera molto veloce un numero qualsiasi di istanze di metropoli identiche e usufruibili in maniera indipendente da più gruppi di lavoro.

Tale piattaforma è già stata realizzata dalla Fabaris con il nome JMSS – Joint Multiple Scenarios System. Tale piattaforma è stata sviluppata in ottica Dual Use ed è

operante e in continua evoluzione presso il NATO Modeling & Simulation Centre of Excellence (NATO M&S COE) alla Cecchignola (Roma) con il nome di WISDOM.

I contesti applicativi ai quali si rivolge la piattaforma sono di sicuro interesse: il training per la capacità di fornire al discente scenari di crisi simulati sui quali prendere decisioni e il wargaming per la possibilità di analizzare i possibili risultati di pianificazioni operative.

Una attenzione significativa viene attualmente conferita allo sviluppo di connettori per il collegamento della piattaforma con più sistemi esterni con particolare riferimento a quelli di M&S utilizzati nella NATO (JTLS, JCATS…). In questo modo, a partire dalla realizzazione di uno scenario comprendente le informazioni geo-referenziate di interesse (popolazione, edificato, POI, network di utility, etc.), sarà possibile utilizzare la piattaforma nelle seguenti modalità:

- Single System - supportando attività di training e wargaming mediante l'utilizzo di una singola o di multiple istanze di uno degli scenari presenti nella piattaforma;
- Multiple Systems - supportando attività di training e di wargaming mediante la rappresentazione dinamica sullo scenario di dati provenienti da sistemi di M&S collegati alla piattaforma;
- Scenario Gateway - supportando attività di training e di wargaming mediante la possibilità del sistema di connettersi ad ulteriori sistemi di rappresentazione evoluta (es. tavoli olografici, tattici etc.) per la visualizzazione dinamica dello scenario (in modalità single o multiple systems).

Oltre alle modalità già citate, è importante sottolineare che la piattaforma è HLA compliant permettendo l'interfacciamento a federazioni costituite da sistemi di simulazione di questa stessa natura e consente la creazione, utile per disporre della corretta consapevolezza della situazione proposta, di story-telling per la diffusione e condivisione di informazioni afferenti allo scenario di interesse.

L'EVOLUZIONE 5G

Una tecnologia orientata ai servizi che nasce con l'obiettivo di costruire il nuovo futuro

FASTWEB

La nuova tecnologia 5G nasce per rispondere ai limiti delle precedenti generazioni di reti mobili, che non riescono a soddisfare le nuove esigenze dei servizi in termini di capacità, numero di dispositivi connessi, latenza ed affidabilità.

Il 5G è in grado di coprire esigenze di servizi caratterizzati da requisiti prestazionali eterogenei, in modo da rendere le reti di quinta generazione mobile una piattaforma abilitante la crescita digitale, in grado di supportare molteplici mercati verticali, nella realizzazione e nella conduzione di un'ampia varietà di applicazioni innovative.

Si fonda sulle seguenti caratteristiche che ne contraddistinguono anche gli scenari di utilizzo che direttamente ne beneficiano:

- Enhanced Mobile Broadband (eMBB), che permette velocità di trasmissione a banda elevata con throughput dell'ordine dei Gbps;
- Ultra Reliable Low latency Communication (URLLC), che permette comunicazioni a bassissima latenza e la creazione di una rete ad elevata affidabilità;
- Massive Machine Type Communication (mMTC), che permette la connessione di un elevatissimo numero di dispositivi mobili per singola antenna.

La famiglia di servizi di tipo eMBB ha come caratteristica principale quella di fornire accessi ultra-broadband sul mobile. In questo contesto il requisito fondamentale da soddisfare è l'elevata velocità di picco per utente. Questo requisito prevede, oltre all'utilizzo di un'ampia porzione di spettro frequenziale, anche l'introduzione in rete di tecnologie di accesso radio evolute come, ad esempio, tecniche di massive MIMO (Multiple-Input-Multiple-Output) ad elevato numero di antenne, beamforming, modulazioni ad alta cardinalità, ecc. Rientrano tra i servizi che beneficiano di questo paradigma i servizi di Fixed Wireless Access (FWA), Virtual/Augmented Reality, di video-streaming ad altissima definizione e di gaming.

La famiglia di servizi di tipo URLLC copre numerosi scenari di utilizzo che hanno requisiti stringenti in termini di interazione in tempo reale, ma necessitano anche di garantire comunicazioni altamente affidabili in termini di disponibilità, robustezza, resilienza e sicurezza. Dal punto di vista architetturale, la riduzione della latenza può essere garantita implementando la parte di processing applicativo in prossimità dell'utente o prevedendo dispiegamenti mirati con logiche di MEC (Multi-Access Edge Computing), dove possono essere istanziate anche parte delle funzionalità applicative necessarie al corretto funzionamento del servizio. Rientrano tra i servizi che beneficiano di questo paradigma quelli di automazione industriale, pubblica sicurezza e i più futuristici servizi di telemedicina e di guida assistita/autonoma.

La famiglia di servizi di tipo mMTC prevede un elevato numero di dispositivi dispiegati in una certa area geografica, che tipicamente sono caratterizzati da requisiti stringenti in termini di elevata durata della batteria ed elevata copertura, ma generalmente statici o nomadici e con ridotta complessità rispetto ai tradizionali dispositivi mobili (e.g. smartphone, tablet, ecc.). Caratteristica predominante di questa categoria è l'elevato numero di messaggi di segnalazione e di controllo dovuta alla numerosità dei dispositivi, mentre in genere non sono richiesti requisiti stringenti in termini di banda e latenza. Rientrano tra i servizi che beneficiano di questo paradigma i servizi di smart city, domotica, sensori ad alta densità per monitoraggio di misure di varia natura e tutti quei servizi legati ai dispositivi wearables.

Le tecnologie fondamentali che hanno permesso lo sviluppo della nuova architettura 5G sono rappresentate da alcune innovazioni di rete, volte a soddisfare requisiti di flessibilità, dinamicità e programmabilità, tra le quali:

- SDN (Software Defined Network), che facilita l'orchestrazione della rete, gestendo in modo automatizzato le attività di provisioning, administration e maintenance;
- NFV (Network Function Virtualization), che consente la virtualizzazione delle funzionalità di rete rendendo le reti più dinamiche e flessibili;
- Network Slicing, che permette di partizionare la rete in "fette" per una gestione flessibile e dedicata dei servizi.

Il 5G, oltre che una piattaforma tecnologica, vuole essere un abilitatore di applicazioni digitali che nascono da un mutuo scambio di know-how tra le aziende operanti nel settore delle telecomunicazioni ed un ecosistema aperto di partner in grado ciascuno di portare del valore aggiunto nella creazione di nuovi casi d'uso utili al mercato ed alla collettività.

IL RED TEAM
Cos'è il Red Team e perché ne abbiamo bisogno

FATA INFORMATICA

Quando si parla di "teams" (squadre) è normale pensare in termini di colori. Tifi per i bianco-celesti, i giallo-rossi, i bianco-neri ecc.?
Nel gioco della sicurezza informatica, si tifa per la Squadra Rossa (o "Red Team" in inglese).
Questo articolo ti aiuterà a capire cosa significa effettivamente il termine "Red Team" e come questo servizio può aiutare le aziende e le organizzazioni di tutte le dimensioni a identificare e affrontare le minacce informatiche. Ci sono svariate strategie che aziende grandi e piccole possono adottare per proteggere le loro reti e i loro dati da eventuali attacchi informatici. Una di queste strategie prevede la verifica delle vulnerabilità di sicurezza in un ambiente aziendale. Per semplificare, è il modo in cui si testa quanto bene un'organizzazione se la caverebbe di fronte a un attacco informatico vero e proprio. Ma poiché i punti deboli in materia di cybersecurity hanno forme diverse, è necessario disporre di un team di sicurezza specializzato che ricerchi in modo completo le vulnerabilità che vanno oltre la semplice valutazione del rischio. Ma che cos'è esattamente il Red Team? Che siano interni o esterni, il Red Team è responsabile dell'esecuzione di attacchi informatici simulati contro la propria azienda (nel caso di un Red Team interno) o altre aziende (nel caso dell'utilizzo di servizi di Red Teaming esterni appaltati) e di stabilire l'efficacia dei programmi aziendali di sicurezza.
È vero che il Red Team utilizza molti degli stessi strumenti e tecniche utilizzati nei Penetration Test o "Ethical Hacking", ma l'obiettivo è diverso. Gli attacchi impiegati dal Red Team sono simulazioni a più livelli, progettate per misurare come le persone, le reti, le applicazioni e i controlli di sicurezza fisica di un'azienda riescono a rilevare, allertare e rispondere a un attacco informatico.
Durante i test del Red Team, esperti professionisti di cybersecurity fanno finta di essere veri e propri cybercriminali e tentano di attaccare le difese informatiche dell'azienda. Gli scenari di attacco che mettono in atto sono progettati per esercitare varie possibilità e identificare preventivamente le lacune nei controlli di sicurezza e nelle successive risposte. Questi attacchi sfruttano una gamma completa di strumenti che hanno a disposizione gli hacker più aggressivi, tra cui il social engineering e i vettori di attacco fisico: dalla creazione minuziosa di e-mail di phishing, ai tentativi veri e propri di violazione sul posto per accedere ai server.

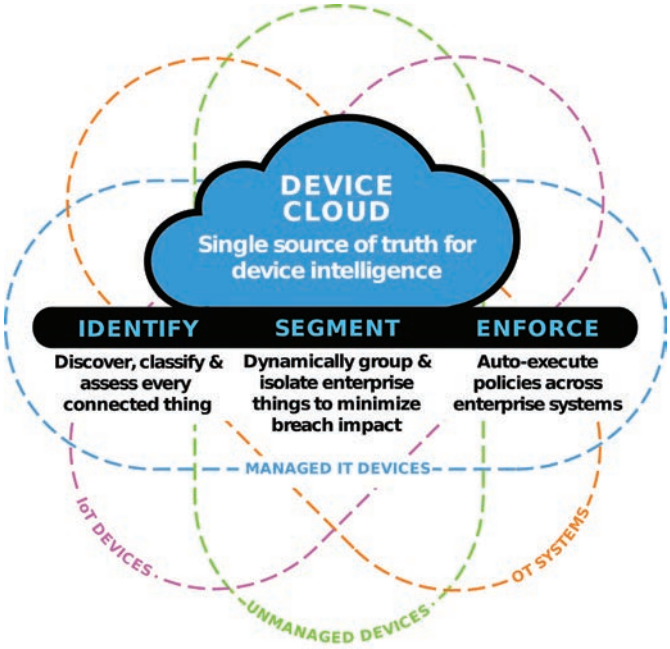
Vantaggi del Red Team Testing

Il Red Team Testing è un potente strumento che aiuta a valutare la capacità di un'azienda di rilevare, prevenire e rispondere a minacce sofisticate e mirate, nonché di identificare e quantificare le lacune di sicurezza già esistenti e migliorare i processi futuri.
Inoltre, contribuisce a definire una base di sicurezza solida, ma che può essere regolarmente rivalutata e riallineata. Di fronte a un crescente panorama di minacce alla cybersecurity, il Red Team Testing aiuta le aziende a identificare i rischi e la suscettibilità di attacco contro le risorse aziendali più importanti.
La premessa del Red Team è paragonabile al vecchio detto sportivo: "L'attacco migliore, è una buona difesa."
Le aziende di tutte le dimensioni -così come i dipendenti- sono vittime di attacchi informatici tutti i giorni!
Il numero complessivo di attacchi DDOS da botnet sta crescendo e aumentando di complessità sempre di più. L'operazione di un Red Team studia l'azienda e quali minacce vengono più utilizzate nello stesso settore e successivamente crea test specifici e mirati da eseguire.
Il Red Teaming non serve solo a trovare le falle di sicurezza delle aziende. Per continuare l'analogia sportiva, un buon utilizzo del "Red Team" fornirà anche strategie per migliorare la difesa in futuro.
Fata informatica opera nel campo della sicurezza informatica dal 1994 e vanta un portafoglio Clienti che va dalla Pubblica Amministrazione Centrale, agli Enti locali ed alle aziende private del settore ICT e di svariati altri settori. I nostri esperti vengono costantemente ingaggiati dai nostri clienti per attività di Red Teaming, Vulnerability Assessment e Penetration Testing.

ACTIVE DEFENSE FOR THE ENTERPRISE OF THINGS

FORESCOUT TECHNOLOGIES

Le sfide legate alla Sicurezza Informatica che si trovano a gestire le aziende e le organizzazioni governative nel mondo sono più complesse che mai, e richiedono soluzioni in grado di rendere sicure le reti di comunicazione, i device ad esse connessi e i dati contenuti nelle varie infrastrutture.
L'esplosione degli apparati connessi, sia in termini numerici che in termini di diversità, rende imperativo per i CISO la creazione di ambienti sicuri nelle rispettive organizzazioni.
Questo comporta la necessità di una completa individuazione dei device connessi, dell'autenticazione dei device e degli utenti che ne fanno uso, e di una analisi accurata del rispetto delle politiche di sicurezza definite dalle organizzazioni.
Inoltre risulta sempre più importante, se non fondamentale, l'automatizzazione delle funzioni di gestione della sicurezza, della bonifica delle situazioni di non rispetto delle politiche di sicurezza e il controllo in tempo reale della situazione nei confronti con quanto richiesto/atteso.
Forescout Technologies è il leader nelle attività di Difesa Attiva della Enterprise of Things.
La difesa attiva è un concetto che parte dalla totale conoscenza dell'ambiente in cui ci si trova ad operare, e quindi si deve basare sulla completa visibilità di ogni device connesso alla rete, sia esso di tipo IT piuttosto che di tipo IoT o OT, indifferentemente da quale sia l'ambiente in cui si connette (Campus, Data Center, Cloud pubblico e/o privato).
La visibilità a sè stante non darebbe particolari vantaggi se non fosse accoppiata ad una classificazione dei device dettagliata e con una conoscenza degli stessi legata al contesto operativo. Solo in questo modo è possibile effettuare una analisi degli ambienti di rete e verificare il rispetto delle politiche di compliancy definite a livello aziendale, di settore o normativo/legale.
La segmentazione in tempo reale di tutta l'infrastruttura di rete dell'azienda, indipendentemente dal fatto che si stia operando sul campus (Wired e/o Wireless), sul Data Center e sul Cloud, realizzata in modalità agentless, e quindi rapida e non invasiva in termini infrastrutturali e operativi risulta ormai fondamentale per ridurre gli effetti degli attacchi informatici che si stanno moltiplicando in modo esponenziale su tutti gli ambienti/mercati con rapidità ed effetti sempre più distruttivi.
L'implementazione di azioni di enforcement automatizzate permette di ridurre i tempi di intervento dei team di gestione della sicurezza, limitando la propagazione degli effetti di malware all'interno della infrastruttura riducendo nel



contempo la possibilità di effettuare errori nella gestione manuale delle attività di dettaglio.
L'integrazione dei sistemi di sicurezza permette di arricchire le informazioni a disposizione dei singoli tool utilizzati e permette di aumentare in modo esponenziale l'efficacia della risposta agli attacchi mettendo a fattor comune informazioni in tempo reale.
Attraverso la piattaforma Forescout, e tramite i suoi moduli Eye Sight, EyeInspect, EyeSegment, EyeControl ed EyeConnect, i nostri clienti sono in grado di attivare velocemente e semplicemente una operatività di Difesa Attiva dell'Enterprise of Things sia in modalità Agentless che in modalità Agent Based basata su tecniche sia attive che passive a seconda delle caratteristiche della infrastruttura di rete aziendale e delle operatività/criticità ad esse collegate riuscendo a incrementare la sicurezza complessiva riducendo nel contempo i tempi di intervento nonché il carico di lavoro e i costi conseguenti delle strutture di Information Security.

L'INTELLIGENZA ARTIFICIALE RIVOLUZIONA LA CYBER SECURITY

FORTINET

L'IA sta cambiando completamente le soluzioni di sicurezza e il modo di lavorare nei Security Operation Center (SOC) e questo beneficio non solo è apprezzabile nelle infrastrutture tradizionali ma anche e soprattutto nelle reti classificate (air-gapped) dove il machine learning può operare localmente senza necessità di avere contatti continui e diretti con cloud esterni.

Una delle rivoluzioni più importanti nella cyber security degli ultimi anni è senza alcun dubbio l'introduzione dell'IA che sta apportando dei benefici importanti, tra i quali:

- Gli algoritmi di machine learning (ML) studiano il traffico dati localmente per determinare "base line" e valutare eventuali difformità, capendo al contempo se le anomalie sono malevole o no. Le signature generiche tendono a creare falsi positivi nei diversi ambienti, mentre le analisi eseguite dal ML localmente determino il traffico ordinario proprio dell'architettura specifica con una drastica riduzione dei falsi positivi.
- L'IA permette di valutare tutte le criticità, generate dalle varie soluzioni di sicurezza presenti nell'architettura, così da far concentrare gli esperti di sicurezza solo sulle anomalie che realmente vale la pena analizzare, con una riduzione importante dell'effort da impiegare nelle analisi e ancora una volta con una netta diminuzione dei falsi positivi.
- Gli algoritmi di Deep Neural Network sono velocissimi nel visionare il traffico e determinarne le irregolarità, non basterebbero decine di migliaia di esperti di sicurezza all'interno di un'azienda per produrre lo stesso risultato in termini di velocità di reazione e prevenzione. Le soluzioni basate su DNN non sostituiranno mai gli specialisti all'interno delle organizzazioni ma possono aiutarli e liberarsi da una serie di attività ormai automatizzare così da ottimizzare tempo e effort.

Nei punti indicati emergono tre fattori chiave, le aziende e gli enti possono vincere le sfide attuali e quelle future nella cyber security grazie all'AI: ridurre al minimo possibile i falsi positivi; ottimizzare l'effort degli specialisti per concentrarli nelle attività realmente necessarie; accelerare l'individuazione e il blocco di una minaccia, oltre che creare misure preventive. Tutti i vantaggi descritti valgono anche per le infrastrutture classificate, solitamente questa tipologia tende a non beneficiare delle novità tecnologiche sempre più interconnesse con cloud esterni, in questo caso parliamo di analisi localizzate nelle infrastrutture specifiche, per cui il concetto di air-gapped non è un ostacolo. È chiaro che in futuro sarà sempre più importante condividere IoC (Indici di Compromissione) con i propri partner/alleati esterni, ma questo può essere fatto a prescindere con software di threath sharing anche nei contesti classificati, seguendo le opportune modalità. Non bisogna dimenticarsi che l'IA nella sicurezza serve a bilanciare l'efficacia dei nuovi attacchi che sfruttano a loro volta l'IA per migliorare le tecniche di attacco e per trovare più rapidamente falle e vulnerabilità. Negli ultimi anni, l'ascesa della "swarm technology", che può sfruttare fattori come il machine learning e l'intelligenza artificiale per attaccare reti e dispositivi, ha dimostrato di avere un nuovo potenziale. I progressi in questo ambito hanno importanti implicazioni in vari ambiti: medicina, trasporti, ingegneria e problem solving automatico. Tuttavia, se utilizzata in modo dannoso, essa può costituire un punto di svolta per gli attaccanti. Se utilizzati dai criminali informatici, gli sciami di bot possono essere sfruttati per infiltrarsi in un network, sopraffare le difese interne e trovare ed estrarre in modo efficiente i dati. Bot specializzati, dotati di funzioni specifiche, sono in grado di condividere e correlare l'intelligence raccolta in tempo reale per accelerare la capacità di uno sciame di selezionare e modificare gli attacchi per compromettere un bersaglio o anche più bersagli contemporaneamente.

Uno degli obiettivi iniziali dello sviluppo di un'intelligenza artificiale "security-focused" era quello di creare un sistema immunitario per la rete simile a quello del corpo umano. La prima generazione di AI è stata progettata per adottare modelli di machine learning per apprendere, correlare e quindi determinare una specifica linea di condotta. La seconda generazione di intelligenza artificiale è stata creata per sfruttare le sue capacità sempre più sofisticate di rilevare pattern ricorrenti, distribuendo diversi nodi di apprendimento in uno specifico ambiente. La terza generazione di intelligenza artificiale è caratterizzata dall'interconnessione dei nodi di apprendimento locali in modo che i dati raccolti possano essere condivisi, correlati e analizzati in modo più distribuito, invece di fare affidamento su un centro di elaborazione statico e centrale, si tratta di uno sviluppo molto importante in quanto le aziende e gli enti puntano sempre più a proteggere i propri ambienti periferici in espansione.

IL NUOVO APPROCCIO ALLA CYBERSECURITY DELLA TECNOLOGIA TRUECDR DI ODIX

Odix è distribuito in esclusiva per l'Italia da Future Time S.r.l.

FUTURE TIME

Gli attori della guerra informatica sono tanto diversi quanto ostili e hanno ormai raggiunto livelli di sofisticazione e tattiche di infiltrazione tali da dover richiedere tecnologie di difesa sempre più innovative e al passo con i tempi.

Nel campo della sicurezza informatica, i sistemi legacy come gli elementi di protezione basati su antivirus o sandbox sono fondamentali per proteggere i dati dalle minacce note, ma non bastano: per contrastare tutti i malware, inclusi quelli che per diffondersi sfruttano vulnerabilità zero-day, cioè ancora prive di patch, è necessario un nuovo approccio che integri i protocolli di sicurezza informatica esistenti.

La tecnologia TrueCDR (Content Disarm and Reconstruction) della società israeliana Odix propone un nuovo approccio alla sicurezza informatica: mentre infatti le tecnologie disponibili sul mercato forniscono soluzioni di rilevamento che controllano la presenza di virus o codici malevoli con lo scopo di bloccare il file che li contiene, la tecnologia CDR sanifica il file stesso e lo restituisce all'utente ripulito da virus o da altro codice non appropriato.

Si tratta di una tecnologia relativamente recente, nata per scopi militari ma molto usata anche per la protezione di organizzazioni operanti in settori critici in tutto il mondo. Sottoposto al processo di Odix, un file viene scomposto nei suoi componenti più elementari che vengono esaminati e sanificati da ogni codice potenzialmente pericoloso. Il file è quindi ricostruito in base alle specifiche del tipo di file originale. Il risultato finale è una copia completamente nuova avente uguale formato e informazioni del file originale, ma priva di contenuti dannosi.

Rimuovendo tutto il codice potenzialmente dannoso, questa tecnologia risulta efficace contro vulnerabilità zero-day, Advanced Persistent Threat (APT), Ransomware e in generale contro qualsiasi attacco basato su file.

I prodotti Odix integrano questa tecnologia in un controllo composto da 4 fasi: applicazione di linee guida stabilite dall'organizzazione, scansione del file usando 5 prodotti anti-malware integrati nel sistema Odix, validazione del tipo di file e infine esecuzione del processo CDR vero e proprio.

A differenza dei tradizionali antivirus, la tecnologia CDR non richiede l'uso di database contenenti informazioni sul malware in circolazione e quindi non dipende dal loro continuo aggiornamento; per sua natura infatti il controllo

CDR è in grado di eliminare file con contenuto pericoloso indipendentemente dal fatto che questo sia conosciuto o no.

La tecnologia TrueCDR di Odix, nata per consentire alle strutture militari israeliane di prevenire le infiltrazioni di malware nelle loro reti protette, è oggi utilizzata da numerose organizzazioni sia pubbliche sia private in tutto il mondo per ridurre in maniera rilevante l'esposizione al rischio di compromissione da attacchi basati sui file in ingresso.

Un esempio di implementazione è quello del Ministero della Salute israeliano, che usa la tecnologia CDR per controllare circa 20.000 file per ora. I file arrivano da vari istituti sanitari per essere archiviati presso il Ministero, provengono da diverse fonti (server FTP, Vault, operazioni batch, ecc.) e sono incanalati verso i server CDR. A causa del carico di lavoro elevato, diversi server CDR Odix sono usati tramite un Load Balancer in modalità Round Robin. Data l'elevata riservatezza dei dati, i server Odix sono configurati per non effettuare alcuna comunicazione verso l'esterno. I file di aggiornamento sono forniti da Odix e caricati sul sistema dagli amministratori della rete.

Future Time S.r.l., azienda romana operante nella distribuzione di soluzioni per la sicurezza informatica dal 2001 e che vanta collaborazioni di successo con le più importanti aziende del settore, ha scelto di credere nell'approccio innovativo alla sicurezza informatica proposto da Odix ottenendo la distribuzione in esclusiva per il mercato italiano. Future Time S.r.l. punta molto su questa partnership in quanto è convinta che una gamma di prodotti tanto all'avanguardia consenta di soddisfare le necessità, sempre in evoluzione, del mercato della cybersecurity offrendo una soluzione complementare alle tecnologie più tradizionali che porterà ad una riduzione drastica della minaccia del malware per le organizzazioni di tutte le dimensioni.

GSTT™ - GMSPAZIO SATELLITE TRACKING TOOLKIT EXECUTIVE SUMMARY

La soluzione al problema della protezione delle missioni spaziali dai rischi di collisione

GMSPAZIO

È innegabile che il genere umano stia vivendo pienamente l'era spaziale. I satelliti in orbita attorno alla Terra rendono disponibili infrastrutture vitali che spesso vengono date per scontate.

Vengono lanciati in orbita quasi settimanalmente gruppi di satelliti facenti parti di nuove costellazioni rivolte a soddisfare le più disparate esigenze come: Telefonia, TV, Internet, mappatura territoriale, navigazione assistita, meteo, ecc.

Attualmente orbitano intorno alla Terra oltre 5.000 satelliti e più di 200.000 oggetti noti come detriti spaziali, le cui dimensioni variano da pochi centimetri a diversi metri. Le velocità di questi oggetti variano da 3 a 7 km al secondo tra le orbite lontane e quelle più vicine alla Terra.

La presenza di così tanti oggetti in un'area così limitata causa collisioni che nel corso del tempo hanno generato e genereranno migliaia di detriti pericolosi che viaggiano a 28.800 km/h nell'orbita terrestre bassa inquinando lo spazio e mettendo in pericolo la sicurezza dei satelliti operativi, ora e per migliaia di anni a venire.

Siamo pertanto difronte ad una scelta epocale: utilizzare lo spazio in modo responsabile e trarne enormi benefici o rischiare di perdere questa risorsa per sempre. Con lo spazio così densamente affollato come possiamo tracciare accuratamente gli oggetti spaziali? Come possiamo prevedere le collisioni in tempo per evitare l'impatto? Come possiamo diventare migliori amministratori della nostra risorsa naturale condivisa dello spazio in modo responsabile e sostenibile?

Sebbene siano previste numerose iniziative per risolvere questi problemi per il momento l'unica soluzione efficace è disporre di strumenti molto precisi che aiutino gli operatori a controllare lo spazio intorno alla Terra per individuare, tracciare, identificare e valutare le minacce provenienti dallo spazio vicino che influenzano le prestazioni delle loro risorse orbitanti.

Le tematiche SSA (Space Situational Awareness) e SST (Space Surveillance & Tracking) per le risorse orbitanti sono quindi cruciali e hanno un impatto diretto sulla sostenibilità e sulla continuità delle operazioni spaziali oltre che verso il segmento terrestre a causa degli eventuali rientri in atmosfera dei detriti generati dalle collisioni.

Nell'ambito del programma specifico per lo spazio di Horizon2020 "la protezione delle infrastrutture spaziali e la creazione di un sistema di sorveglianza e tracciamento spaziale (SST) a livello europeo" è una delle sfide affrontate dall'UE.

In risposta a tali esigenze la GMSPAZIO fornisce una soluzione innovativa, competitiva ed economica denominata GSTT™ - GMSPAZIO Satellite Tracking ToolKit, per il mercato spaziale a livello mondiale. GSTT™ è stato realizzato da GMSPAZIO come soluzione modulare, flessibile e personalizzabile per aiutare gli utenti finali a gestire problemi potenzialmente pericolosi, riducendo drasticamente i costi ed i tempi di avviamento operativo.

GSTT™ è infatti una soluzione operativa in grado di operare integrando qualsiasi tipo di dispositivo di rilevamento e osservazione nuovo ed esistente; l'architettura di GSTT è stata progettata per offrire una soluzione integrata "plug-and-play" completamente personalizzabile capace di offrire agli utenti finali misurazioni precise, elevata reattività ed efficacia operativa.

La personalizzazione del sistema è connessa da un lato all'obiettivo di adempiere al meglio le responsabilità del futuro operatore di sistema e dall'altro all'utilizzo dell'intera infrastruttura esistente con particolare riguardo ai sensori, salvaguardando gli investimenti preesistenti.

In questo ambiente complesso GSTT™ è la soluzione alla necessità di avere un'accurata consapevolezza della situazione spaziale capace di gestire efficacemente i problemi di sorveglianza e monitoraggio dello spazio.

In conclusione il Sistema GSTT™ della GMSPAZIO mette a disposizione dell'utente finale la funzionalità e le capacità indispensabili ad operare una corretta gestione delle risorse spaziali a salvaguardia della comunità umana sia dal punto di vista della fruibilità di funzionalità tecnologicamente avanzate che nel pieno rispetto della sicurezza e della salute pubblica.

HEXAGON & E-GEOS: È INIZIATA LA GUERRA DEI BIG DATA

Come vincerla in scenari operativi con soluzioni di Image Intelligence (IMINT)

HEXAGON

A causa del volume, varietà e velocità di acquisizione di dati geospaziali in ambiente operativo, le organizzazioni governative della Difesa sono sommerse dai 'big data'. Consumare velocemente i dati appena prodotti ed estrarre da questi delle informazioni di valore è diventato ormai quasi impossibile per gli operatori. È questa la realtà che rende così complesso raggiungere un livello di decision-making informato ad ogni livello ed una consapevolezza della situazione in tempo reale, divenute capacità critiche per la sicurezza di un paese. Il vantaggio tattico nel 2021 dipende fortemente dalla capacità di comprendere velocemente ed agire conseguentemente, utilizzando dati in tempo reale provenienti dallo sciame di sistemi a disposizione.

È in tale scenario che le organizzazioni di Difesa ed Intelligence richiedono strumenti per analizzare, visualizzare ed integrare dati provenienti da diverse fonti come satelliti, sensoristica aviotrasportata (sia manned che unmanned) ed altri data set critici per la loro missione; in particolare, all'evoluzione delle prestazioni tecniche delle missioni satellitari di osservazione terrestre fa riscontro il miglioramento continuo delle capacità analitiche delle soluzioni di Image Intelligence (IMINT). Ciò rende fondamentale l'utilizzo di tecnologie geospaziali che permettano di fondere diverse fonti di dati nel loro formato nativo affinché possano essere visualizzati ed analizzati sia in tempo reale che in funzione del tempo, integrando modelli complessi di processamento, modelli simulativi e modelli di Intelligenza Artificiale. È proprio in questo settore che Hexagon, oltre ad essere leader di mercato, sta investendo fortemente (in media circa il 10-12% delle proprie vendite nette) per accelerarne l'innovazione.

Ciò ha spinto e-GEOS a scegliere Hexagon e le sue tecnologie di Real-Time Situational Awareness per migliorare le capacità della propria soluzione per l'analisi IMINT basata su immagini satellitari, sfruttando la modularità della sua piattaforma. Frutto della profonda integrazione tra algoritmi proprietari e pacchetti software "best in class" come la piattaforma Luciad di Hexagon, brAInt™ permette l'esecuzione di flussi di lavoro operativi di IMINT adattabili alle modalità operative dell'utente con cui accedere in modo agevole al contenuto informativo delle immagini satellitari e derivati prodotti a valore aggiunto, attraverso semplici passaggi, il tutto a supporto degli analisti durante ogni fase del ciclo di intelligence.

Concepito come estensione cognitiva al servizio degli analisti, brAInt™ è la piattaforma IMINT modulare di e-GEOS, in cui confluiscono flussi di lavoro operativi per la generazione di report di Imagery Intelligence che vanno dall'analisi dei siti chiave al monitoraggio delle attività a terra, dalla ricerca dei comportamenti anomali alla valutazione situazionale dei danni inflitti e al supporto alla pianificazione delle missioni attraverso un cervello centralizzato che si occupa di orchestrare l'esecuzione dei differenti task siano essi manuali o automatici attraverso le sue diverse componenti operative.

brAInt™ si inserisce nella lunga tradizione delle applicazioni di intelligence e-GEOS ponendosi come soluzione all'avanguardia nella gestione dei flussi di lavoro per il settore Defense & Intelligence. L'esperienza di e-GEOS affonda le radici in molti anni di utilizzo delle immagini satellitari a fini operativi e di addestramento erogato direttamente agli analisti IMINT civili e militari impegnati in prima linea. Grazie a questa interazione stretta con il cliente si è potuto migliorare le capacità funzionali da un lato e dell'altro aggiornare la roadmap dei prodotti, rivolgendo così gli investimenti del cliente in brAInt™.

Abilitata dalla tecnologia Hexagon LuciadFusion, il cui approccio è incentrato sulla fusione dei dati da fonti multiple, braint™ incrementa la frequenza di acquisizione dei dati virtuali. Puntando sull'elevata frequenza di rivisitazione di COSMO-SkyMed e grazie alla tecnologia Hexagon LuciadRIA, braint™ vanta una capacità di analisi di monitoraggio senza confronto, ideale per la valutazione delle attività, obiettivi e comportamenti umani e per la caratterizzazione dei bersagli chiave.

In un unico ambiente brAInt™ semplifica i compiti di raccolta del materiale di origine, relativa archiviazione dei metadati e recupero dei dati da altre fonti e sensori di sorveglianza, quali FMV, sensori in situ, database OSINT, report HUMINT, SIGINT ed ELINT, contribuendo alla ricchezza, alla velocità e all'accuratezza dell'attività complessiva di raccolta e valutazione delle informazioni.

NUOVO SISTEMA D'ANTENNA HF A LARGA BANDA PER COMUNICAZIONI TRA VELIVOLI AD ALA MOBILE E FLOTTE NAVALI

La IES annuncia un innovativo sistema di antenna

IES

A partire dall'esperienza maturata dalla IES nella progettazione e realizzazione di antenne a larga banda per stazioni fisse e relative matrici (antenna/ audio-dati), grazie al prezioso contributo dell'Università Roma Tre, la IES annuncia lo sviluppo di una nuova tecnologia d'antenna per velivoli ad ala mobile.

Lo scopo è di abilitare comunicazioni HF a larga banda per superare i limiti e la potenziale vulnerabilità delle comunicazioni SatCOM. Tale tecnologia permette di effettuare comunicazioni a larga banda, che consentono un trasferimento dati fino a 240kbps, riportando le comunicazioni HF nel loro ruolo chiave di comunicazioni di sorveglianza e/o di backup alla rete Satcom.

Un affidabile sistema di comando e controllo di unità ampiamente disperse in ambienti difficili, come negli scenari tattici, è di fondamentale importanza per massimizzare il successo di una missione. Allo stato attuale, le forze militari fanno affidamento sulle comunicazioni satellitari tattiche che consentono di ottenere ampia copertura sul territorio, flessibilità, buona velocità di trasmissione dati, e capacità di comunicazione senza linea di vista (BLOS - Beyond-Line-of-Sight). Tuttavia, questo può essere oggetto di attacchi elettronici che rendono il nodo satellitare un "single point of failure" del sistema, mettendo a rischio l'intera missione.

I sistemi di comunicazione basati su onde HF (1.5-30MHz) sono noti da tempo per avere maggiore resilienza agli attacchi grazie alla possibilità di creare una rete distribuita di nodi formata dalle unità stesse sul territorio. Sfortunatamente però presentano bande operative significativamente più strette, riducendo la velocità di trasferimento dati a poche decine di kbps. Per questo motivo, negli ultimi anni, gli enti di standardizzazione militare hanno definito un nuovo standard per comunicazioni HF (MIL-STD-188-110 vers.D, Dic. 2017) a larga banda, che consente un trasferimento dati fino a 240kbps, riportando le comunicazioni HF nel loro ruolo chiave di comunicazioni di sorveglianza e/o di backup alla rete satellitare.

In questo contesto si inserisce il nuovo sistema d'antenna proposto da IES.

Un tipico sistema d'antenna a larga banda è costituito da due elementi fondamentali: un radiatore ed un sintonizzatore/ accordatore. Il primo elemento è responsabile della conversione del segnale di potenza proveniente dal trasmettitore nel segnale elettromagnetico irradiato nello spazio. Il secondo elemento, invece, è responsabile della sintonizzazione del radiatore alla frequenza di interesse, che può non coincidere con la naturale frequenza di risonanza dell'elemento radiante. Un accordatore è costituito da una rete circuitale che permette di trasformare il radiatore dal punto di vista elettrico in modo da sintonizzare l'antenna nella sottobanda HF nella quale si vuole trasmettere o ricevere la comunicazione, massimizzando l'efficienza totale del sistema.

La IES nello sviluppo della soluzione tecnologica per varie tipologie di elicotteri, ha considerato radiatori non-risonanti, rendendo la sintonizzabilità nelle sottobande HF di interesse più semplice ed efficiente. Inoltre, ha progettato l'elemento radiante conforme al profilo meccanico o fusoliera del mezzo su cui sono installate (vedi Figura 1).

Figura 1 – Esempio di posizionamento dell'antenna HF conforme alla coda dell'elicottero

Le soluzioni tecnologiche che sono state studiate per il sintonizzatore d'antenna sono quelle che permettono una efficiente e rapida commutazione tra le sottobande HF di almeno 48 kHz. In questo scenario, topologie circuitali innovative basate su componenti a commutazione veloce (es. diodi di potenza e switch all'arseniuro di gallio) sono state investigate e confrontate tra loro al fine di individuarne la migliore configurazione in abbinamento al radiatore a cavità progettato.

La soluzione tecnologica risulta di sicuro interesse nell'ambito di rinnovamento ed efficientamento dei sistemi di comunicazione HF mobili, sia in ambito civile che militare.

REALISMO E ACCURATEZZA NELLA SIMULAZIONE DELLO SPETTRO ELETTROMAGNETICO SOLUZIONI DI ANALISI E SIMULAZIONE DI KEYSIGHT TECHNOLOGIES

KEYSIGHT

Lo Spazio e la Difesa sono la spina dorsale della moderna innovazione commerciale e viceversa.
Internet, le comunicazioni wireless, i satelliti, lo spazio, la navigazione e l'elettrificazione sono in continua evoluzione. Spingere i confini dei limiti tecnici richiede una combinazione di conoscenza approfondita e immaginazione per esplorare nuove possibilità.
Keysight contribuisce fornendo soluzioni con innovazioni tecnologiche all'avanguardia in ambito Spazio e Difesa con hardware e software COTS scalabili e ad alte prestazioni.
Vediamo qualche esempio in ambito applicativo:

LA SFIDA DELLA GUERRA ELETTRONICA

L'evoluzione di radar, guerra elettronica (EW) e contromisure richiedono la generazione e l'analisi di segnali complessi per la simulazione e il test. Di pari passo evolvono le sfide nel rilevare, evitare e contrastare gli attacchi con l'avanzare della tecnologia. In tutti i casi, il test dei sistemi odierni beneficia di apparecchiature di misura ad alte prestazioni: generatori di segnali analogici e vettoriali, analizzatori di spettro, analizzatori di segnali vettoriali, analizzatori di reti vettoriali e altro ancora. Dalle simulazioni di un segnale in arrivo con più emettitori, al test di componenti di precisione in un ricevitore, le soluzioni Keysight sono pronte per gestire la complessità delle applicazioni di test di guerra elettronica (EW).

SIMULAZIONE DINAMICA DI MINACCE AD ALTA DENSITÀ

Le nostre soluzioni vengono costantemente aggiornate a minacce nuove e complesse con la simulazione dei segnali, creando scenari di guerra elettronica (EW) complessi, con una elevata densità di impulsi e con la simulazione simultanea sia dell'angolo di arrivo (AoA) che della cinematica (piattaforme mobili) grazie a generatori di segnali agili e coerenti. La soluzione Keysight è una combinazione di sorgenti di segnale, hardware e software di calibrazione e software applicativo per la generazione di scenari predefiniti o dinamici in grado di simulare un campo di battaglia elettronico con migliaia di emettitori.

REGISTRAZIONE E ANALISI CONTINUA DEI SEGNALI

La verifica accurata dei dati di ingresso e uscita del sistema sottoposto a test è fondamentale per validarne la funzione e le prestazioni. La maggior parte dell'attuale hardware di analisi ha capacità limitate, il che si traduce nella verifica parziale dei segnali, utilizzando analizzatori di spettro o oscilloscopi di fascia alta. L'acquisizione e la registrazione continua dei segnali di interesse per tutta la durata di uno scenario di prova è necessaria per verificare il corretto funzionamento. Keysight offre soluzioni completamente integrate, multicanale, multibanda, con misurazione in tempo reale e riconoscimento degli impulsi, nonché ore di archiviazione dei dati RF registrati. I casi d'uso includono il collaudo dei sistemi di attacco elettronico e la verifica dei sistemi di simulazione delle minacce.

SISTEMI DI COMUNICAZIONE MILITARI

Le comunicazioni militari (MilCom) richiedono prestazioni, interoperabilità e affidabilità in reti che vanno da una copertura ad hoc e locale a un'area più ampia con il supporto dell'infrastruttura cellulare. Molte soluzioni MilCom devono supportare simultaneamente apparecchiature per comunicazioni militari consolidate e tecnologie più recenti. Per fornire una maggiore consapevolezza della situazione, per le MilCom si sfruttano sempre di più tecnologie commerciali come Long Term Evolution (LTE), di quinta generazione (5G) e reti locali wireless (WLAN). Le reti MilCom realizzano anche i vantaggi derivanti dall'adozione di formati di modulazione digitale più recenti.
Le soluzioni di misura devono essere in grado di testare tutti gli aspetti di queste radio versatili man mano che si evolvono con la tecnologia delle comunicazioni. Il nostro approccio di test scalabile e flessibile consente di ridurre al minimo il trasferimento di proprietà intellettuale (IP), accelerare i tempi di produzione, ridurre i costi di ingegneria del test e migliorare la correlazione tra le misure.

I LEONARDO LABS

Un nuovo modello per gli sviluppi futuri delle tecnologie più innovative

LEONARDO - FINMECCANICA

I Leonardo Labs sono gli incubatori di tecnologia destinati a supportare l'azienda nella ricerca di lungo periodo e nello sviluppo delle tecnologie più innovative, in particolare quelle digitali, e delle competenze trasversali alle aree di business aziendali. Ogni laboratorio avrà al suo interno diverse unità di ricerca focalizzate su tematiche quali intelligenza artificiale, sistemi autonomi, big data, calcolo ad alte prestazioni, simulazione e modellazione, tecnologie quantistiche, mobilità elettrica, materiali e strutture. Gli ambiti tecnologici dei laboratori sono definiti all'interno del piano per l'innovazione, uno dei pilastri su cui si fonda la strategia del gruppo.

Queste nuove strutture - alcune realizzate in collaborazione con partner industriali e centri di ricerca leader mondiali nei rispettivi ambiti di competenza – sono e sorgeranno in prossimità dei principali siti industriali di Leonardo in Italia - Cascina Costa (Va), Torino, Genova, Roma, Pomigliano D'Arco (Na) e Grottaglie (Ta) - e negli Stati Unit con l'obiettivo di facilitare anche il trasferimento tecnologico e di massimizzare i benefici per i territori di riferimento, consolidando la collaborazione con le istituzioni locali. I laboratori saranno così fertilizzatori delle realtà locali consentendo al contempo a Leonardo di centralizzare lo sviluppo di tecnologie di frontiera centrate sulla sostenibilità delle soluzioni.

I Labs consentono anche di alimentare un flusso continuo di talenti e di assicurare flessibilità e rinnovamento, sia di capacità sia di competenze professionali: i Leonardo research fellow di provenienza internazionale, inseriti nel network dei Labs, lavorano infatti insieme ad esperti e ricercatori interni alle Divisioni di Leonardo per contribuire ad aumentare la competitività del Gruppo e, ove possibile, anticipare l'innovazione, in una prospettiva crescita sostenibile nel lungo periodo. A giugno 2020 è stato lanciato il bando di reclutamento internazionale che ha portato alla selezione di 72 giovani ricercatori tra oltre 900 candidature.

Un pilastro fondamentale per i Leonardo Labs è il nuovo e potente super calcolatore davinci-1. Il davinci-1 è stato installato a fine 2020, ed è uno dei più potenti supercalcolatori del mondo, posizionandosi all'89esimo posto della classifica TOP500 e al 37esimo posto della graduatoria HPCG500. Tra i supercalcolatori di aziende private, davinci-1 è al decimo posto mondiale, al secondo in Italia e si posiziona subito dopo NASA e JAXA nel settore aerospazio. Il supercalcolatore davinci-1 è una macchina studiata per assolvere più compiti al massimo livello, dalle più esigenti necessità di simulazioni numeriche complesse, come quelle che servono per progettare elicotteri e aerei, al processing di dati, grazie a un enorme spazio di archiviazione, fino allo sviluppo di applicazioni basate sull'intelligenza artificiale e cloud computing – quest'ultimo ambito necessario per l'utilizzo all'interno dei progetti europei, a cui Leonardo ha deciso di aderire, finalizzati alla realizzazione, in ambito europeo, di un market place dove far incontrare domanda ed offerta di servizi cloud. All'interno di questo contesto si definiscono gli standard che verranno adottati in futuro in ambito europeo e questo rappresenta un'ulteriore leva, per Leonardo, per sviluppare la leadership.

Davinci-1 è una delle principali piattaforme di sviluppo dell'attività dei Leonardo Labs in quanto acceleratore di conoscenza e abilitatore nella transizione verso il digitale, consentendo ai ricercatori e agli ingegneri di Leonardo di competere e difendere la leadership aziendale nel mondo. Dalla simulazione all'intelligenza artificiale, infatti, nello scenario di oggi, la creazione di valore si sposta sempre di più dai prodotti fisici a quelli virtuali e davinci1 rappresenta la chiave per abilitare i nuovi servizi virtuali.

In questo contesto storico d'incertezza, Leonardo ha voluto affermare con atti concreti, quali la creazione dei Leonardo Labs e la messa in servizio del Davinci-1, 'importanza d'investire in ricerca, competenze, capacità e infrastrutture, fondamentale sia per rafforzare e consolidare il proprio business e gettare le basi per nuovi prodotti e business ad alto contenuto tecnologico, sia per creare nuovo valore per sviluppare l'azienda in futuro.

RADAR TARGET GENERATION
System-Level Validation for Radar Systems

NATIONAL INSTRUMENTS ITALY

The complexity of modern radar systems and environments in which they operate make it challenging to achieve adequate test coverage to validate system performance. NI radar target generators allow you to simulate real-world test scenarios to efficiently evaluate your radar under numerous conditions, considerably reducing the time spent in costly field trials and flight tests. Unlike target generators built with custom hardware, NI systems are open to the customer, and designed and built upon instrument grade hardware using LabVIEW and LabVIEW FPGA development platforms known for their easy to use data acquisition/generation and analysis capabilities.

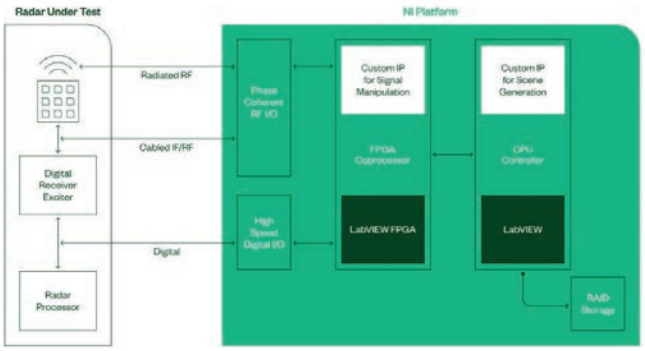
- Simulate multiple targets with individual position, velocity, and attitude
- Apply per-target delay, attenuation, Doppler shift, and RCS modeling
- Implement models for atmospheric propagation, terrain clutter, and multipath
-

NI Solution: Customizable COTS Platform

Phase-coherent multichannel RF acquisition and generation with subnanosecond synchronization on NI Vector Signal Transceivers

Closed-loop, low-latency scenario simulation with real-time signal processing with NI FlexRIO user-programmable FPGA modules

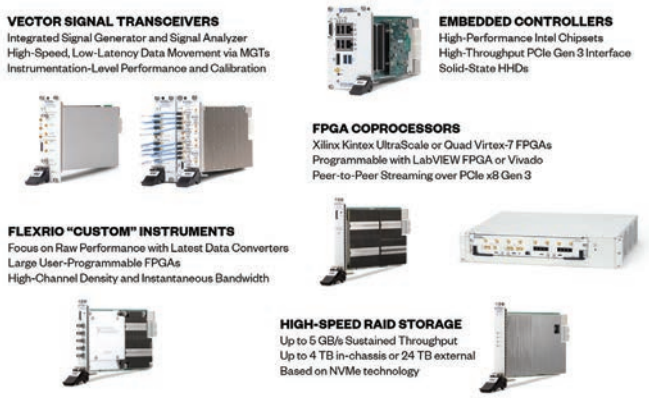
Modular I/O platform provides flexibility to interface at multiple test points: high-speed digital, direct-inject IF, over-the-air RF.



Key Features

- Scale system resources as required to meet the channel count, I/O types, signal processing needs of your application.
- Leverage a proven software and hardware infrastructure to minimize development time and costs.
- Create custom, user-owned IP for target generation, scenario management, signal propagation, and jamming.
- Upgrade software and hardware to add new features when you need them to quickly meet evolving test requirements.
- Record results to the cloud or local RAID as full I/Q spectral data, parameterized results, or measurement metrics

System Components



Key Specifications

Frequency: RF transmit and receive coverage from 9 kHz to 44 GHz

Bandwidth: Up to 1 GHz of instantaneous RF bandwidth

Channel Count: 4 to 34 independent input and output channels per chassis

System Integration on Your Terms

NI offers a variety of solution integration options customized to your application-specific requirements. You can use your own internal integration teams for full system control or leverage the expertise of our worldwide network of Alliance Partners to obtain a turnkey system.

PLANETEK ITALIA: RICERCA ED INNOVAZIONE PER LA GEOINT

Big Data, Intelligenza Artificiale e Blockchain

PLANETEK ITALIA

In un mercato globalizzato le imprese si trovano ad affrontare sfide continue in una competizione ormai internazionale. Questo processo è ancora più vero nel settore ICT e difesa, dove l'evoluzione tecnologica e dei bisogni è rapidissima. In questo contesto, è evidente che le imprese devono dotarsi un una propria strategia di gestione dell'innovazione.

Per questo motivo, nel gruppo Planetek l'innovazione è pianificata in maniera sistematica, coniugando la ricerca orientata ad individuare innovazioni trasformazionali, in grado di garantire vantaggi competitivi di lunga durata, con quella incrementale nell'operatività di breve periodo.

Per governare questo processo, le attività di ricerca sono coordinate dal Design Lab, che indirizza e definisce le priorità di ricerca ed innovazione, e orienta le attività verso lo sviluppo di soluzioni in grado di coniugare la soddisfazione delle esigenze degli utenti, la fattibilità tecnologica e la sostenibilità economica.

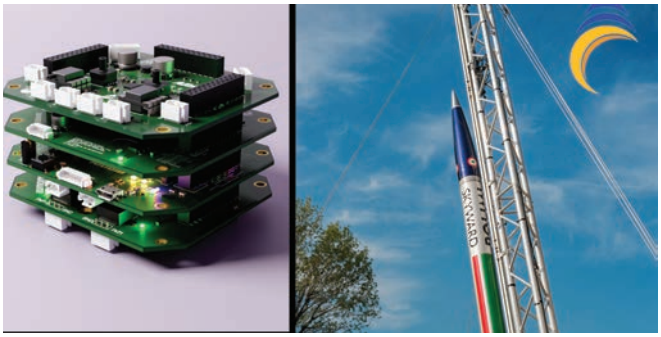
Planetek Italia è attiva in numerosi ambiti di ricerca tecnologica su temi quali: Big Data analytics, Intelligenza Artificiale, BlockChain, Novelty Detection e analisi multi sorgente e multi sensore per applicazioni di GEOINT. L'approccio all'innovazione dell'azienda è orientato anche al cambiamento di approccio nei processi decisionali dei propri utenti, e grandi investimenti sono legati all'adozione del paradigma Info-as-a-Service per i servizi geoinformativi derivati da dati telerilevati: trasformare i dati in flussi continui di informazioni e conoscenza a beneficio degli utenti. I Big Data rappresentano una fonte inesauribile di informazioni che possono fornire conoscenza utile a prendere decisioni rapide e consapevoli. Con il proliferare dei satelliti, oggi, disponiamo di dati giornalieri dell'intera superficie terrestre. Le tecniche di Intelligenza Artificiale (AI) consentono di estrarre dai Big Data conoscenza sotto forma di correlazioni, che altrimenti sarebbe impossibile dedurre con tecniche tradizionali. Tecniche di Deep Learning e Machine Learning applicate ai dati satellitari consentono sviluppare nuove catene di elaborazione automatica per la produzione automatica di conoscenza, anche in termini di report e informazioni di intelligence per la sicurezza. Attraverso procedure semplificate, questi sistemi consentono di effettuare in tempi rapidi l'analisi dei cambiamenti, la target recognition, attraverso analisi multi-sorgente e multi-sensore di sensori satellitari e aviotrasportati di tipo ottico (E.O. ad es. Opsat-3000), iperspettrale (HSI, ad esempio il nuovo satellite iperspettrale italiano PRISMA), multispettrali (MSI), LiDAR e Radar (SAR), come quelli della costellazione italiana COSMO-SkyMed e Cosmo Second Generation, e full motion video. L'innovazione nell'ambito dell'intelligenza artificiale porta anche alla sperimentazione di nuovi paradigmi di interazione uomo-macchina: le tecniche di AI sono state utilizzate per creare chatbot in grado di interagire in linguaggio naturale con banche dati eterogenee. Inoltre, l'intelligenza artificiale associata all'analisi interferometrica di immagini satellitari radar è utilizzata per individuare con accuratezza i punti delle reti idriche e fognarie con situazioni di stress. Le tecniche di AI sono adottate anche per l'analisi di dati disponibili su internet e nei canali social come Facebook, Twitter, Instagram, per arricchire il contenuto informativo dei servizi geoinformativi.

Anche la Blockchain trova ampio utilizzo nella geomatica e nello spazio e in particolare per certificare i prodotti di osservazione della Terra attraverso tutti i passaggi della catena del valore, che vanno dalla acquisizione del dato, alla sua elaborazione, estrazione dei contenuti informativi, fino all'utilizzo di questi in prodotti geoinformativi. In pratica, mantenere la memoria storica di tutte le trasformazioni e manipolazioni a carico di una immagine satellitare fino alla mappa tematica o indicatore di sintesi che viene prodotto dalle immagini. Le tecniche di AI sono anche utilizzate per implementare tecniche di novelty detection per l'analisi dei dati di telemetria e dei dati acquisiti dai sensori di bordo dei satelliti. Queste tecniche sono state utilizzate per rilevare preventivamente eventuali anomalie e malfunzionamenti, prima ancora che possano incidere sulla operatività dei satelliti. Queste tecnologie, sulle quali Planetek Italia lavora ormai da diversi anni, stanno diventando sempre più performanti e affidabili, e svolgeranno sempre di più un ruolo chiave in un settore strategico come quello della Difesa.

Esempio di classificazione automatica di una immagine satellitare tramite algoritmi di Deep Learning Sevmantic Segmentation. Credits: Hexagon

SPAZIO E PASSIONE: POLOMARCONI.IT INSIEME A SKYWARD EXPERIMENTAL ROCKETRY PER UNA SFIDA NEI CIELI

POLOMARCONI.IT



Nonostante lo stravolgimento del mercato causato dalla crisi pandemica del 2020, POLOMARCONI.IT non demorde: grazie agli investimenti aziendali in strumentazione sempre all'avanguardia, continua ad offrire tecnologie innovative e prodotti customizzati al servizio del cliente, mantenendo un ruolo di spicco nel mercato delle telecomunicazioni ad alte prestazioni.

Ma la società si è spinta oltre: si sono infatti avviate collaborazioni per il settore Airborne e Space, dove POLOMARCONI.IT, insieme all'associazione studentesca Skyward Experimental Rocketry, contribuisce al progetto ed allo sviluppo di razzi sperimentali per le competizioni europee e mondiali. Dall'inizio del 2021, la società è divenuta sponsor di Hermes X, nome del progetto del più recente razzo Skyward, il quale punta a superare i 5000 metri di apogeo. L'associazione studentesca, volta alla sperimentazione di razzi suborbitali, comprende tutti i dipartimenti necessari alla progettazione e realizzazione dei prototipi, che prenderanno il volo a settembre 2021 per il test di lancio in Abruzzo, ed il mese seguente nella competizione europea EUROC in Portogallo.

La configurazione RF includerà diverse innovazioni: nel primo prototipo si opterà per un sistema costituito da parti considerate COTS e da parti progettate interamente dagli studenti, mentre per il prototipo LYNX che verrà realizzato per i lanci del 2022 vi è già in corso l'intero design del sistema di telemetria. Nella configurazione del prototipo che verrà lanciato il prossimo anno, i vari dipartimenti dell'associazione stanno da tempo sviluppando un motore ibrido che aprirà la possibilità di competere nelle categorie di lanci fino a 10000 metri di apogeo, oltre ad includere un'aereodinamica nuova, telemetria dedicata e sensori avanzati a bordo razzo al fine di garantire un'estrema affidabilità insieme ad un'elevata quantità di dati trasmessi e raccolti in tutte le fasi del lancio.

Grazie al contributo di POLOMARCONI.IT, il team di Skyward non solo potrà sviluppare l'intero sistema RF, ma avrà anche a disposizione i migliori strumenti di misurazione: analizzatori di spettro per la verifica dei segnali trasmessi, analizzatori vettoriali per le analisi di prestazioni dei circuiti, camere anecoiche e campo di prova per verificare le prestazioni delle antenne, oltre ad una vasta gamma di strumenti per la verifica delle dimensioni meccaniche dei prototipi sviluppati. Il tutto a garanzia di un flusso dati così ampio da poter trasmettere, in tempo reale, il video a bordo razzo con immagini di alta qualità. Trattandosi di un sistema di trasmissione dedicato ed innovativo, sarà inoltre possibile raccogliere in tempo reale un'elevata quantità di dati utili non solo al controllo ed alla verifica dei parametri di volo, ma anche alle fasi successive di analisi di performance del lancio. Nella definizione e sviluppo del sistema RF sono coinvolti diversi membri dei dipartimenti del team di Skyward: elettronica, programmazione e software, strutture, recovery al fine di creare una scheda RF customizzata a tutte le esigenze del lancio. La scheda RF verrà poi inclusa nello stack dell'elettronica di bordo, garantendo una trasmissione adattativa in funzione dei parametri di lancio. Le condizioni operative del lancio, infatti, introducono diversi problemi relativi alle forti accelerazioni, puntamento, rotazioni, richiedendo quindi un sistema di comunicazione solido e che si sappia adattare durante tutto il tempo di volo. Il sistema progettato sarà capace di garantire sia la copertura omnidirezionale che selettiva grazie ad una configurazione simile a quella adottata per il beam-forming. Inoltre, si potrà orientare il fascio d'irradiazione dell'array consentendo il beam-steering man mano che il razzo prenderà quota. Con la presenza di una serie di microcontrollori a bordo verrà selezionata la velocità delle trasmissioni delle informazioni destinate a terra, massimizzando il rapporto segnale rumore del link budget con una tratta fino a 150 Km nel caso di perfetto allineamento tra il fascio d'irradiazione e la ground station.

La parte di comunicazione radio e di telemetria sono prodotte internamente da POLOMARCONI.IT, garantendo eccellenti prestazioni del sistema e lavorazioni di altissima precisione grazie alle macchine CNC per la prototipazione rapida. Gli obiettivi futuri di POLOMARCONI.IT e Skyward sono ambiziosi, ma tutt'altro che fuori portata: grazie allo spirito d'intraprendenza, alla forza di volontà degli studenti ed all'esperienza di un'azienda leader nel settore delle telecomunicazioni, non si potrà che volare in alto.

LA PRIORITÀ È TRADURRE IN SOLUZIONI TECNOLOGICHE IL CONCETTO DI BIODIFESA

È urgente un approccio sistemico ai biorischi

di Massimo Amorosi[1]

RAIT88

Le criticità nella risposta all'attuale pandemia da SARS-CoV-2 ha fatto emergere delle importanti vulnerabilità ai rischi biologici, siano essi di origine naturale o frutto di azioni deliberate. Ad esempio, diversi Paesi non dispongono di capacità necessarie per monitorare le varianti emergenti del virus tramite la sorveglianza genomica - una situazione che potrebbe essere più seria di come appare. Il ricorso al solo strumento vaccinale, al di là della narrativa dominante, non è garanzia di una risoluzione definitiva dell'emergenza pandemica: i mezzi da rendere operativi in termini di sorveglianza, prevenzione e contrasto alle minacce biologiche emergenti devono essere parte di una organizzazione strategica deputata alla biodifesa nazionale.

La redistribuzione globale dei patogeni, dei parassiti , così come delle piante degli animali, dovrebbe essere analizzata nella prospettiva di possibili invasioni di natura biologica e, considerando i comuni aspetti nelle dinamiche spazio-temporali, diventa indifferibile un approccio integrato alla biosicurezza. Per questo motivo, è stato introdotto il concetto di "One Biosecurity", approccio multidisciplinare fondato sulle interconnessioni tra la salute umana, animale, vegetale e ambientale allo scopo di prevenire e mitigare più efficacemente l'impatto delle specie invasive aliene. Le sfide che impongono un radicale cambio di approccio sono molteplici, dalla crescente urbanizzazione e mobilità delle persone fino all'intensificarsi del ricorso alle pratiche agricole e alla persistenza di gap in termini di capacità volte a far fronte a crisi sanitarie ad alto impatto come quella attuale.

Con riferimento alla mobilità delle persone, basti pensare che in Europa, la zanzara è stata responsabile di outbreak di dengue In Francia, così come di chikungunya in Italia e di virus del Nilo Occidentale in Grecia, a seguito del rientro di un soggetto infetto dall'estero il quale ha facilitato in tal modo la trasmissione della malattia. Dal 1970 al 2017, le invasioni di specie aliene sono costate all'economia globale almeno 1,28 trilioni di dollari in termini di danni e di attività finalizzate al loro contenimento, come riportano alcuni ricercatori sulla testata Nature. Con la progressiva interconnessione a livello globale, le specie invasive conquisteranno nuovi habitat facendo lievitare ulteriormente tali costi. Nel complesso, dagli esiti di questa ricerca emerge che compensare i danni causati dalle specie invasive ha un costo che si aggira intorno ai 900 miliardi di dollari, ossia 13 volte tanto l'ammontare di risorse che occorrerebbe per la gestione di queste incursioni.

Grazie al sempre meno oneroso sequenziamento genetico e alle connesse tecnologie diagnostiche e dell'informazione, è oggi possibile creare una mappatura globale dei patogeni in tempo reale nonché una capacità predittiva per certi versi ispirata al modello dei servizi meteorologici. L'impiego combinato di biosensori avanzati e algoritmi di intelligenza artificiale (AI) permetterebbe l'integrazione in modelli epidemiologici allo scopo di prevedere dinamiche evolutive di focolai epidemici significativi imputabili a microrganismi nuovi o emergenti.

L'orientamento della RAIT88 è di investire sempre di più in soluzioni tecnologiche che garantiscano l'attuazione di un approccio sistemico e innovativo alla biosicurezza, nel quadro di una sinergia tra pubblico e privato, come dimostrano gli accordi strategici sottoscritti sia con l'Istituto Zooprofilattico Sperimentale dell'Abruzzo e del Molise di Teramo, sia con il Centro di Competenza per l'Innovazione in Campo Agro-ambientale Agroinnova dell'Università di Torino. Tanto più che, ad oggi al mondo non esistono sistemi di sorveglianza tecnologica integrata che mettano insieme la salute umana, la sanità animale e la sanità vegetale.

A questo proposito, l'Unione Europea ha lanciato nel febbraio 2021 un programma che mira ad allestire un piano di biodifesa per le varianti del SARS-CoV-2, un segnale che le "lessons learned" dell'attuale pandemia cominciano ad essere colte nel Vecchio Continente. In un contesto internazionale in così rapida evoluzione, l'Italia non solo non può farsi trovare impreparata, ma anzi deve proporsi come capofila per l'attuazione di nuovi approcci nel settore rispetto agli altri Paesi avanzati.

[1] *Scientific Secretariat e CBRN Biothreats Specialist presso RAIT88.*

ROHDE & SCHWARZ, UN PONTE TECNOLOGICO DAL PROBLEMA ALLA SOLUZIONE

Per vivere in un mondo sempre più connesso e sicuro

ROHDE & SCHWARZ ITALIA

software defined radio R&S®M3SR

Con oltre 85 anni di esperienza, Rohde & Schwarz sviluppa, produce e commercializza un'ampia gamma di soluzioni per clienti del settore privato e della pubblica amministrazione.
La divisione Test & Measurement offre numerose applicazioni nell'area "Aerospace & Defence" come la strumentazione elettronica a supporto degli sviluppatori, dalla progettazione delle componenti hardware fino al collaudo finale.
Principali applicazioni della strumentazione di misura Rohde & Schwarz:

- Componenti e Antenne dei più moderni Radar multifunzione
- Sistemi disturbatori e di simulazione di scenari elettromagnetici
- Verifica di sistemi di comunicazione analogica e digitale per applicazioni militari e civili
- Sistemi per l'uso in applicazioni tattiche o ferroviarie delle piattaforme 5G / LTE
- Satelliti di comunicazione o satelliti con a bordo radar ad apertura sintetica per lo studio delle mutazioni del territorio
- Sistemi di supporto alla navigazione aerea

Nel settore Homeland Security, Rohde & Schwarz propone un innovativo sistema di scansione del corpo umano "body scanner" basato su onde millimetriche. La soluzione R&S QPS (Quick Personnel Security Scanner), preservando la privacy, permette di individuare qualsiasi oggetto "guardando attraverso" gli indumenti grazie a sofisticate tecniche di acquisizione ed elaborazione del segnale. È un sistema ideale per garantire alti standard di sicurezza presso i punti di "controllo accessi" delle aree aeroportuali o di altre zone sensibili. Le onde millimetriche "superano" infatti lo schermo degli indumenti e consentono al personale addetto alla sicurezza di esaminare i passeggeri senza alcun contatto fisico mantenendo il distanziamento sociale, importantissimo per contrastare la diffusione del SARS Cov 2.
In Europa il sistema QPS è in uso presso i maggiori aeroporti internazionali, in Italia è stato provato con successo presso i principali Hub aeroportuali come efficace risposta al bisogno di sicurezza avvertito dalle istituzioni e dai passeggeri nell'inquieto momento storico che stiamo vivendo!
Ma Rohde & Schwarz non si ferma qui e va oltre, ottimizzando una soluzione dedicata anche ai droni. I droni commerciali rappresentano un potenziale pericolo per il traffico aereo, per le infrastrutture critiche, per eventi politici e sportivi. Pertanto, in un crescente numero di situazioni può essere utile una soluzione che identifichi per tempo la presenza di droni non autorizzati al sorvolo di aree a rischio. Il sistema R&S®ARDRONIS, sviluppato da Rohde & Schwarz, fornisce una completa visione dello spettro elettromagnetico ed allarmi per il personale addetto alla sicurezza, anche prima del decollo dei droni stessi. Inoltre georeferenzia il pilota e può interrompere il controllo del drone. Esso può anche essere equipaggiato con funzioni addizionali per impedire volutamente al drone di essere telecomandato a distanza disturbando i relativi segnali di controllo.
R&S®ARDRONIS blocca le minacce dei droni come unità autonoma o integrata in sistemi di sicurezza più ampi.
Con la sua esperienza tecnologica, leader del settore, Rohde & Schwarz è un partner affidabile per il futuro delle comunicazioni, dell' informazione e della sicurezza. Con la famiglia di Software Defined Radio R&S®SOVERON, R&S è leader anche nel campo delle comunicazioni radio a onde corte. I ricetrasmettitori R&S®M3SR Series4100 della famiglia SOVERON rappresentano una pietra miliare tecnologica. La serie è stata preparata per le forme d'onda HF a larga banda della quarta generazione basate su MIL-STD-188-110D e ALE4G MIL-STD-188-141D.
Sono così possibili collegamenti ad alta velocità tra Unità Dislocate e Comandi delle Forze Armate, della Guardia Costiera e delle Pattuglie di Frontiera permettendo inoltre un significativo miglioramento della shared situational awareness e quindi un processo decisionale significativamente più veloce ed efficace, anche attraverso lo scambio immediato di comandi e rapporti sulla missione.

PROGRAMMA CARE2CONNECT SERCO EUROPA

L'approccio di Serco nella pandemia

SERCO ITALIA

Prima del Covid-19, i nostri oltre 1.000 colleghi in Serco Europa - con sede in Belgio, Lussemburgo, Francia e Guyana francese, Germania, Italia, Paesi Bassi, Spagna e Svizzera - non erano quasi del tutto abituati a lavorare da casa. Tuttavia, quando i rischi sono diventati evidenti, prima ancora che i lockdown nazionali fossero implementati, l'80% della nostra forza lavoro in Europa è stata immediatamente trasferita in modalità smart work.

Tali rapide misure precauzionali hanno ridotto i casi di contagio al minimo. Hanno anche spinto i nostri colleghi in una normalità completamente nuova che ha innescato nuove riflessioni sul lavoro, sulla vita e sul benessere e sul valore del contatto con i colleghi.

"La nostra prima responsabilità è prenderci cura dei nostri team", afferma Gaetan Desclée, Amministratore Delegato, Serco Europe. "Durante il Covid-19, tale responsabilità si estendeva dal tradizionale ambiente di lavoro in ufficio all'ambiente di casa. Il nostro messaggio era - prendetevi cura di voi stessi e dei vostri cari -; la nostra priorità era ridurre la pressione sul lavoro laddove possibile ".

"La nostra filosofia è - Pensa globale, agisci a livello locale ", afferma Francesca Balducci, Direttore Safety,Risk & Compliance. "Per il benessere dei colleghi, questo significa riconoscere che ognuno ha esigenze diverse e fare di più per identificare e supportare quelle esigenze specifiche".

Mentre il lockdown continuava, il nostro leadership team europeo si è reso conto che l'assenza prolungata dalle comunità di lavoro e la mancanza di interazione informale in ufficio stavano avendo un impatto negativo sul benessere mentale delle nostre persone.

Uno dei modi in cui il team ha cercato di aiutare tutti a sentirsi in contatto e rimanere coinvolti è stata la campagna "Care2Connect". Durante la primavera del 2020, tutti i colleghi in tutta Europa sono stati incoraggiati ad intraprendere buone azioni nelle loro comunità locali, per poi condividerle su un'app dedicata in stile social media. Per ogni azione pubblicata, Serco Europa ha donato denaro ad enti di beneficenza selezionati a livello locale, raccogliendo circa 10.000 € in totale e formando una comunità europea molto più forte.

"Prima del Covid-19, le nostre persone, collocate in luoghi diversi ed in diversi Paesi, raramente interagivano tra loro se non per soddisfare le esigenze di lavoro", afferma Francesca. "Care2Connect ha reso popolare un diverso tipo di interazione, incoraggiando i colleghi in tutta Europa a condividere e discutere le esperienze, formando nuove amicizie e nuove reti".

Un' ulteriore campagna Care2Connect, intitolata "tornare alla nuova normalità", durerà per tutta l'estate 2021.

"Uno degli impatti a lungo termine del lockdown è che le persone si sentono meno a loro agio quando lasciano le loro case, al punto che farlo può essere molto stressante", spiega Francesca. "Vogliamo aiutare i nostri colleghi a sentirsi a proprio agio nel reimpegnarsi di persona con il mondo. Allo stesso tempo, vogliamo continuare a far crescere la nostra nuova comunità e le nostre nuove reti internazionali di supporto e collaborazione. Uno dei modi in cui lo faremo è tramite Care2Connect. Un altro modo identificato sara' la trasformazione dei nostri uffici in "hub di collegamento" fisici: spazi sociali ed accoglienti in cui le nostre persone possano connettersi e collaborare ".

Accanto agli sforzi per recuperare ciò che è stato perso, viene prestata grande attenzione a non perdere ciò che è stato guadagnato:

"La partecipazione tradizionale non sarà più richiesta", afferma Gaetan. "Quello che abbiamo imparato prima di tutto è che il nostro personale e' ugualmente efficente in condizioni di flessibilità. La cosa migliore che possiamo fare, sia per i nostri colleghi che per l'azienda, è dare loro il supporto di cui hanno bisogno per vivere bene e la libertà di cui hanno bisogno per lavorare bene. Questa è la nostra opportunità per migliorare la loro qualità di vita aumentando i livelli di produttività ed impegno. È una situazione vantaggiosa per tutti ".

TEMPEST MADE IN SIPAL

Hardware e periferiche TEMPEST made in Italy

di Mariarosaria Mazzacane

SIPAL

Tutela delle informazioni e protezione dei dati, assicurando la difesa dei sistemi informatici e delle informazioni sensibili. Questo l'ultimo traguardo raggiunto da SIPAL che dal 2018 produce hardware e periferiche TEMPEST volti a contenere e preservare le informazioni classificate.

Tutte le apparecchiature elettriche ed elettroniche generano radiazioni elettromagnetiche che possono contenere informazioni, talvolta sensibili. Queste informazioni possono essere facilmente intercettabili attraverso l'interpretazione dei segnali emanati da questi dispositivi.

Un receiver, strumento di laboratorio che misura il campo elettromagnetico, può di fatto interpretare questi segnali in maniera inosservata e senza l'accesso diretto al dispositivo originale.

La metodologia TEMPEST si occupa dunque delle emissioni elettromagnetiche sia radiate – segnali elettromagnetici che si propagano nello spazio – che condotte – emissioni che viaggiano lungo percorsi elettromagnetici conduttivi, come i cavi di alimentazione o cavi dati.

Dalle emissioni eventualmente intercettate e analizzate si può constatare che i campi elettromagnetici irradiati o condotti contengono informazioni, piuttosto che semplicemente "rumore".

A tale scopo, SIPAL si dedica in modo diretto alla difesa dei sistemi informatici e alla protezione delle informazioni classificate. Per cui progetta, certifica e produce apparati TEMPEST secondo i diversi livelli di protezione previsti dalla normativa di riferimento che consentono la salvaguardia delle informazioni sensibili processate sugli apparati informatici.

L'azienda possiede quindi tutte le abilitazioni necessarie alla distribuzione di materiale TEMPEST e, con una consulenza a 360 gradi, supporta il cliente nella scelta dei sistemi più adatti alle singole esigenze.

Grazie al laboratorio omologato dagli enti preposti, ai magazzini COMSEC idonei allo stoccaggio e al personale abilitato per la distribuzione sul territorio nazionale, SIPAL fonde le proprie competenze tecniche e scientifiche nello studio, nella progettazione dei prodotti e nella redazione della documentazione propedeutica all'omologazione dei propri apparati.

La forza di SIPAL è un team con esperienza trentennale nel settore in grado di supportare la propria clientela sia militare che civile, al fine di realizzare reti classificate, siti omologati e sistemi informatici sicuri secondo il livello di classifica richiesto.

Attualmente, infatti, l'azienda ha in catalogo una vasta gamma di prodotti tutti dotati di certificato di omologazione, atti a realizzare un'infrastruttura hardware e software tale da poter costruire una rete classificata per ambienti autorizzati a processare informazioni sensibili.

Di pari passo, SIPAL si occupa di Facility TEMPEST Zoning, procedura che consente di determinare il livello di rischio di un ambiente e che si effettua prima dell'installazione di prodotti TEMPEST. Quest'ultima è un'attività propedeutica al TEMPEST Equipment Zoning che determina il livello di appartenenza del dispositivo da utilizzare in base al grado di attenuazione della zona di pertinenza secondo le normative che regolamentano la materia – attività che si esegue mediante l'ausilio di un Laboratorio TEMPEST omologato.

Pertanto, essendo in linea con le più aggiornate misure di sicurezza e standard adottati a livello internazionale, l'azienda è istituzionalmente riconosciuta come punto di riferimento ingegneristico per la tutela delle informazioni (Nazionale – NATO – UE) e risulta la prima società italiana NATO BOA Partner a far parte dei fornitori certificati TEMPEST del NATO Information Assurance Product Catalogue (NIAPC).

BREVETTI ESSENZIALI PER UNO STANDARD (SEP): CARATTERISTICHE, VANTAGGI E CRITICITÀ ASSOCIATE

Potenziali rischi dei SEP per la libera concorrenza

Ing. Lorenzo SORDINI – Italian and European Patent and Design Attorney, Partner Studio Torta S.p.A.

STUDIO TORTA

Una norma tecnica (chiamata comunemente standard) è un documento che definisce le specifiche tecniche per un prodotto, un dispositivo, un sistema, un'apparecchiatura, un processo o una tecnologia.

Gli standard sono generalmente definiti da enti di normazione (Standard Setting Organizations – SSO) quali, ad esempio, l'Istituto Europeo per le Norme di Telecomunicazione (ETSI) o l'Unione Internazionale delle Telecomunicazioni (ITU).

Un brevetto che protegge una tecnologia essenziale per l'implementazione di uno standard è definito brevetto essenziale per lo standard (Standard Essential Patent – SEP), per cui è impossibile fabbricare, commercializzare o utilizzare prodotti conformi ad uno standard senza fare uso delle tecnologie coperte dai SEP relativi a tale standard.

Tipicamente, la politica degli SSO prevede che siano gli stessi titolari di brevetti a dichiarare i propri SEP relativi a uno standard, senza che ci sia una verifica da parte degli SSO della correttezza di tali dichiarazioni. Il fatto che le dichiarazioni di essenzialità siano basate solamente su un'autovalutazione dei titolari dei brevetti senza alcuna verifica da parte degli SSO può portare a cosiddetti fenomeni di "sovra-dichiarazione". Ad esempio, a novembre 2017 la Commissione Europea ha emesso una comunicazione per illustrare l'approccio dell'UE sui SEP, in cui si richiamava l'attenzione sul fatto che diversi studi condotti su importanti tecnologie oggetto di standard avevano dimostrato che solamente tra il 10% e il 50% dei brevetti dichiarati come essenziali erano poi risultati essere effettivamente dei SEP per tali standard.

I SEP possono conferire notevole potere di mercato a chi li detiene. Infatti, una volta che è stato raggiunto un accordo su uno standard, il mercato è vincolato de facto allo standard e ai relativi SEP. Questo potrebbe indurre un titolare di SEP ad avere comportamenti anticoncorrenziali, ad esempio escludendo i concorrenti dal mercato o richiedendo royalty eccessive. Per cercare di arginare tali comportamenti anticoncorrenziali, molti SSO esortano i titolari di SEP a impegnarsi a concedere in licenza questi ultimi in regime FRAND (i.e., Fair, Reasonable And Non-Discriminatory, ossia equo, ragionevole e non-discriminatorio), in modo tale da cercare di garantire sia l'accessibilità alle tecnologie oggetto di standard da parte di tutti i soggetti interessati, sia un'adeguata remunerazione dei titolari di SEP.

Negli ultimi anni si è avuto un notevole incremento dei contenziosi brevettuali relativi a SEP, in particolare nel settore delle telecomunicazioni in cui le controversie brevettuali hanno coinvolto colossi del settore quali Apple, Samsung, Qualcomm e Google.

Recentemente, inoltre, la battaglia legale sui SEP relativi alle tecnologie di telefonia mobile di seconda, terza e quarta generazione (2G, 3G, 4G) ha cominciato a coinvolgere anche aziende del settore automobilistico (e.g., Daimler e BMW) a seguito dell'uso sempre più esteso di tali tecnologie a bordo degli autoveicoli. In tale ambito, le richieste dei proprietari di SEP, che generalmente cercano di legare l'ammontare delle royalty al valore del prodotto finale, trovano una tenace opposizione da parte delle case automobilistiche che, invece, ritengono che l'ammontare delle royalty dovrebbe riflettere solamente le funzionalità direttamente legate alla connettività 2G/3G/4G e non il prezzo degli autoveicoli (peraltro, notevolmente più alto rispetto a quello di un "semplice" smartphone o tablet).

In un tale scenario, la prossima frontiera per i contenziosi brevettuali basati sui SEP relativi alle tecnologie 3G, 4G e 5G sarà rappresentata, molto probabilmente, dal settore dell'Internet of Things (IoT) laddove, però, le controversie brevettuali non coinvolgerebbero più solamente importanti aziende hi-tech o grandi case automobilistiche, ma potrebbero riguardare, con conseguenze potenzialmente ben più devastanti, le Piccole e Medie Imprese (PMI) che attualmente stanno lavorando e investendo molto sull'IoT e che, ovviamente, hanno a disposizione molte meno risorse per potersi difendere.

In conclusione, quindi, i SEP rappresentano uno strumento estremamente vantaggioso per le aziende titolari che, grazie ad essi, possono ottenere ingenti guadagni, oltre a recuperare gli investimenti effettuati per lo sviluppo di innovative tecnologie oggetto di standard.

Purtroppo, però, i SEP rappresentano anche un potenziale rischio per la libera concorrenza, potendo essere utilizzati per l'attuazione di pratiche anticoncorrenziali volte all'ottenimento di una posizione dominante sul mercato.

T-RACK: IL COMPACT DATACENTER TATTICO DI TELECONSYS

Con la soluzione ingegnerizzata da Teleconsys è arrivato il momento del "Power to the Edge!"

TELECONSYS

La trasformazione delle Forze Armate Italiane rappresenta un'esigenza assolutamente prioritaria per conseguire una adeguata information superiority necessaria per attuare il concetto delle Effects Based Operations caratteristico di gran parte delle attuali operazioni militari.

In uno scenario di crescente complessità, diviene sempre più importante disporre di capacità C2 che operino il più possibile in tempo reale, elaborando le informazioni in prossimità di dove le stesse si generano, al fine di fornire una immediata situational awareness alle forze in campo.

Teleconsys ha realizzato una soluzione compact-datacenter leggera, basata su tecnologie iperconvergenti, semplice da assemblare, trasportare, alimentare e raffreddare: l'HCI Tactical DataCenter, certificato IP66 – MIL-STD810F.

Dalle premesse del documento Future Operating Environment dello SME è nata una soluzione che rivede completamente le capacità di elaborazione negli scenari tattici tanto da permettere il dispiegamento FOE di applicazioni che possono sfruttare risorse e prestazioni simili ai Data Center stanziali.

Nel recente passato, per installazioni in scenari con dispiegamento rapido e outdoor, si aveva una scelta obbligata, quella di trasportare materiale pesante e poco maneggevole oppure sacrificare le capacità di elaborazione e resilienza che normalmente venivano ridotte al minimo.

L'ambiente dei teatri operativi è altamente dinamico e complesso, limitato da condizioni ambientali spesso non favorevoli, da connettività debole e da instabili caratteristiche della rete tattica: questo pone requisiti rigorosi per l'infrastruttura di rete ma, soprattutto, per l'elaborazione sottostante. Nella tecnologia attuale, gli utenti fanno generalmente affidamento su un Data Center capacitivo e condiviso per inviare dati al centro di comando con potenzialità di calcolo elevate. Tuttavia, in condizioni operative, un ritardo di tale backhaul può essere davvero vitale, specialmente quando il throughput di rete è fortemente limitato o le applicazioni degli utenti richiedono performance dedicate come, ad esempio, il Voip e la Video Conferencing. L'utilizzo della capacità di elaborazione disponibili "localmente", comparabili a quelle di un moderno Data Center di medie dimensioni, migliorano significativamente le prestazioni delle applicazioni e riducono il rischio di non ricevere risposte puntuali nel corso delle Operazioni.

Oggi Teleconsys presenta soluzioni Tactical Edge studiate per dimensioni e peso ridotti, consumi elettrici contenuti (SW&P) ma con performance di livello DC, installabili rapidamente e dedicate a supportare carichi di lavoro Enterprise direttamente sul campo o in sedi remote.

Per quanto riguarda la sicurezza della piattaforma è presente l'automazione totale per il controllo in tempo reale delle baseline di hardening STIG e in perfetta conformità con gli standard necessari ai reparti della Difesa. Le tecnologie di Iper-convergenza utilizzate garantiscono resilienza in caso di fault e la possibilità di erogare nativamente tutti i servizi tipici per la fruizione dello storage, anche utilizzando tutto il range di crittografia eventualmente necessario in particolari scenari di dispiegamento. Particolare attenzione è stata dedicata alla Sicurezza di rete, semplificando enormemente le tradizionali operazioni di firewalling interne e/o perimetrali.

In relazione all'interconnessione e alle integrazioni Network è disponibile un'ampia gamma di interfacce "state of the art" adatte a soddisfare e ad operare in qualsiasi condizione.

La soluzione di Compact-DC base offre, nelle dimensioni di un trolley tradizionale e con un peso ampiamente inferiore ai 40kg, la potenza di un cluster a 4 nodi dotato di tecnologia Intel Xeon e NvME, con consumi ridotti e capacità elaborative elevate in condizioni di temperatura esterna oltre i 50°C e senza condizionamento. Le tecnologie e le soluzioni utilizzate garantiscono flessibilità nelle operazioni di trasporto rapido e nelle fasi di installazione in infrastrutture stanziali, la soluzione, infatti, prevede, oltre al dispiegamento stand-alone, anche le opzioni di montaggio in rack tradizionali. Volendo quantificare, l'utilizzo di due moduli base in installazione affiancata, in 5 RU di un rack standard. Soluzione ideale anche per le operazioni di medio e lungo termine. Avere sul campo questo tipo di capacità e prestazioni apre a scenari in cui è possibile ricavare, utilizzare e analizzare una considerevole mole di dati senza la dipendenza da una sorgente remota, abilitando gli operatori con strumenti e dispositivi di ultima generazione.

SPACE SITUATIONAL AWARENESS & SPACE TRAFFIC MANAGEMENT

TELESPAZIO

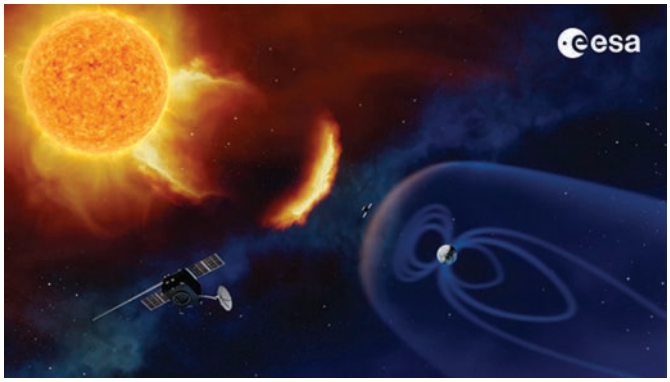
Lo spazio circumterrestre ospita un gran numero di assetti tecnologici sensibili, fondamentali per il benessere e la sicurezza della società odierna. Telespazio è da tempo impegnata sul tema della prevenzione e protezione degli HVSA (High Value Space Assets), supportando il monitoraggio delle potenziali minacce indotte dallo Space Environment e dai Resident Space Objects (RSO) cooperativi e non, e.g. detriti, satelliti inoperativi o ostili. Recentemente, l'ingresso di attori privati nel settore spaziale ha determinato l'incremento repentino del numero di RSO orbitanti, principalmente veicolato dal dispiegamento di Mega-Costellazioni (e.g. Starlink, One Web). In assenza di tecniche di prevenzione e rimozione appropriate e di strategie di mitigazione condivise, l'accesso allo spazio potrebbe essere irrimediabilmente compromesso, determinando un incontrollato aumento degli oggetti in orbita.

A tal proposito, l'Unione Europea (UE) sta adottando sistemi sempre più efficaci per il monitoraggio dell'ambiente spaziale, e.g EUSST. La mitigazione delle minacce poste dal nuovo scenario deve essere gestita migliorando anche la protezione "operativa" degli asset spaziali, ciò implica la necessità di aumentare la consapevolezza spaziale globale. Pertanto, il concetto Space Surveillance & Tracking (SST) deve evolversi, da un lato, verso il concetto di Space Domain Awareness, ma la "New Space" richiede la creazione di un quadro globale di Space Traffic Management (STM), che dovrebbe affrontare sfide tecniche e normative.

Il rafforzamento e consolidamento di tali competenze e sistemi, diviene fondamentale per l'Europa, e ovviamente per l'Italia, anche in considerazione del fatto che lo Spazio è ormai considerato un ambito di confronto militare in cui vanno identificate e neutralizzate le minacce agli HVSA (High Value Space Assets) da parte di satelliti non cooperanti ed ostili.

1. SSA - Miglioramento delle capacità ed evoluzione del servizio

Gli attuali servizi di SSA si basano principalmente sulle capacità di raccolta ed analisi dei dati da parte del SST e SWE. L'aspetto che caratterizza maggiormente questi due settori è la capacità di modellizzare accuratamente la dinamica orbitale degli RSO e gli eventi di fisica solare che intervengono nella descrizione dell'ambiente spaziale terrestre. Il miglioramento di tali modelli, per via diretta (formalizzazione matematica) o indiretta (Artificial



Intelligence) può contribuire maggiormente all'evoluzione dell'SSA.

2. La prospettiva dell'evoluzione dei servizi industriali

Telespazio ha una lunga tradizione nel campo del SST, comprovata dalle numerose attività di supporto alle operazioni per gli HVSA nazionali (e.g. Cosmo-Skymed).

Le principali capacità di prevenzione stanno evolvendo secondo due filoni principali:

- Automazione dei servizi di prevenzione delle collisioni e valutazione dei rischi;
- Prevenzione delle collisioni come servizio (CaaaS).

L'iniziativa CaaaS ha l'obiettivo di supportare i clienti che vogliono affidarsi a servizi professionali, senza la necessità di sviluppare internamente infrastrutture dedicate. Il servizio, basato sull'analisi del Messaggio di Alerting fornito da JspOC/EUSST, mira a ridurre i tempi di valutazione del rischio di collisione e a suggerire un set di manovre che soddisfino i vincoli tecnologici ed operativi della missione. In tal senso la partecipazione di TELESPAZIO all'iniziativa lanciata dalla società NorthStart Earth and Space offre l'opportunità di evolvere ulteriormente l'offerta di servizi in ambito SST ed STM.

3. Integrazione dei dati di sensori spaziali e servizi

L'iniziativa NorthStar, in cui partecipa attivamente la Space Alliance, punta a fornire servizi space-based di SSA. Al fine di fornire una serie di servizi preliminari e valutare le potenziali capacità della missione, Northstar ha pianificato il dispiegamento di una missione precursore che precederà l'intera costellazione di 40 satelliti in orbita eliosincrona.

Il sistema prevede la raccolta di un massiccio volume di dati e mira alla creazione di un catalogo preciso e dettagliato degli oggetti in orbita terrestre. Il database, insieme ad ulteriori osservazioni e misurazioni fisiche, contribuirà alla realizzazione di diversi servizi in grado di prevedere la dinamica orbitale di uno specifico RSO e di caratterizzarne, in termini di assetto, forma e comportamento.

EVOLUZIONE DELL'INFRASTRUTTURA ITALIANA MILSATCOM: L'INNOVAZIONE COLLEGATA AL PROGRAMMA SICRAL 3

Paolo Conforto, Vincenzo Marziale, M. Petrone, F. Finocchiaro, Alessandro Pisano

THALES ALENIA SPACE

L'infrastruttura italiana MILSATCOM sta per essere rinnovata e migliorata nel prossimo periodo. Dopo 20 anni di vita operativa effettiva il satellite SICRAL 1 è stato re-orbitato ed il satellite SICRAL 1B concluderà la sua missione formale nel 2024 lasciando il compito di mantenere il servizio MILSATCOM agli ultimi satelliti lanciati, SICRAL 2 e FIDUS. Di conseguenza una nuova generazione di satelliti SICRAL andrà dispiegata per mantenere e rinforzare il servizio nei prossimi anni.

Il Sistema SICRAL attualmente si basa sull'uso delle frequenze in banda UHF, SHF, EHF fornendo il servizio MILSATCOM in tutta l'area terrestre visibile dai satelliti, rappresentando un asset infrastrutturale di grande pregio per le Forze Armate italiane e più in generale per l'intero Paese. Molteplici innovazioni tecnologiche, sia a livello di piattaforma che a livello di payload, verranno implementate nella nuova generazione di satelliti SICRAL 3 con notevoli miglioramenti relativi al servizio grazie all'uso diffusivo del processing digitale. La propulsione elettrica, l'uso di configurazioni di satellite di piccole dimensioni, l'implementazione di tecnologie di on-board processing nella comunicazione in banda Ka (oltre ai tradizionali servizi di banda SHF e UHF con elaborazione digitale del segnale) e la protezione da interferenze sono alcune caratteristiche di rilievo sviluppate nel progetto del sistema SICRAL 3.

Il progetto SICRAL 3 ha l'obiettivo di realizzare un nuovo asset satellitare che garantisca la continuità dei servizi SATCOM, correntemente forniti dalla costellazione operativa formata dai satelliti SICRAL-1B (lanciato nel 2009) e SICRAL 2 (lanciato nel 2015) e il duale ATHENA FIDUS (lanciato nel 2014), nonché l'aggiornamento tecnologico necessario.

Il SICRAL 1, lanciato all'inizio del 2001, è stato re-orbitato e passivato in questi giorni completando la sua vita operativa dopo vent'anni a fronte dei 10 previsti.

La Difesa italiana sta procedendo con la definizione e lo sviluppo di un Sistema completo che includa il Segmento Spazio (formato da due Satelliti con i due rispettivi Carichi Utili), il Segmento Terra, le attività di Lancio, LEOP e Commissioning/IOT, le attività di ILS&OPS con le opportune soluzioni atte a garantire il richiesto livello di sicurezza nel Sistema. Il sistema SICRAL 3 deve essere progettato in modo assicurare una vita operativa in orbita geostazionaria di almeno 15 anni.

La nuova generazione dei satelliti SICRAL, SICRAL 3a e SICRAL 3b, rappresenta un importante passo avanti nelle tecniche e tecnologie militari relative alle comunicazioni satellitari Militari, Governative e Commerciali.

In primis la piattaforma satellite, tutta italiana, sarà progettata per poter essere lanciata, tra gli altri, con lanciatori di piccolo cabotaggio, come ad esempio le future generazioni del lanciatore italiano VEGA, implementando sistemi di propulsione elettrica allo stato dell'arte e configurazioni meccaniche compatibili con lanci multipli, nel caso di lanciatori di maggiore capacità, determinando un rilevante risparmio nel costo del lancio.

I Carichi Utili di TeleCom rappresenteranno anch'essi un notevole passo avanti per le bande di frequenza utilizzate, come descritto di seguito:

- La banda UHF accrescerà la propria capacità quasi raddoppiandola implementando reti digitali di formazione del fascio irradiato
- La banda SHF e la banda Ka verranno trattate come un unicum permettendo lo scambio di traffico e la sua distribuzione in copertura, fra una banda e l'altra
- Il segmento spaziale, nodo di comunicazione del sistema, sarà equipaggiato infatti per la banda SHF e Ka di un unico processore digitale riprogrammabile secondo innovativi concetti "Software Defined Radio" che consentirà la piena flessibilità nella riallocazione di sotto-canali fra SHF e Ka oltre che all'interno di ogni singola banda di frequenze
- Il segmento spaziale diventerà inoltre il primo elemento di integrazione dell'infrastruttura militare di Telecom con l'Osservazione della Terra; verrà infatti per la prima volta implementata una connessione inter-satellitare ottica LEO-GEO associata ad una connessione RF con la stazione di terra.
- Il segmento spaziale sarà inoltre equipaggiato con innovativi sistemi spaziali di rilevazione minacce e rilevazione danni infrastrutturali, per esempio dovuti a detriti spaziali in linea con la identificazione dell'infrastruttura satellitare come elemento critico nazionale.

Ancora una volta la flotta satellitare SICRAL si presenta come uno degli elementi di maggior prestigio nel panorama spaziale internazionale rinforzando la presenza dell'Italia nel settore dell'alta tecnologia.

LA CYBER THREAT INTELLIGENCE

L'approccio tradizionale alla cyber security è ormai superato e non è più sufficiente: le minacce sono sempre più complesse e gli avversari sempre più strutturati.

TS-WAY

I processi decisionali delle organizzazioni si stanno trasformando radicalmente passando da un tradizione approccio decisionale basato sull'intuito dei decision-maker a quello guidato da un'analisi analitica dei dati e delle informazioni. Questo approccio sta prendendo sempre più piede anche nell'ambito della difesa delle infrastrutture fisiche e logiche delle organizzazioni, oramai sempre più strettamente legate come nel caso della compagnia Colonial Pipeline in cui un attacco ransomware ha messo KO il maggior oleodotto della East Coast americana.

Ad oggi le cyber minacce rappresentano l'aspetto potenzialmente più critico per l'operatività di tutti i giorni dato il loro potenziale impatto profondamente distruttivo sulle organizzazioni, le loro attività e i loro processi. Il tradizionale e ormai superato approccio alla cyber security non è più sufficiente a gestire le minacce altamente sofisticate e strutturate denominate Advanced Persistent Threat (APT) risultando sempre più inefficace nel rilevare gli attacchi complessi.

L'adozione di un approccio strategico alla sicurezza, come quello proposto dalla Cyber Threat Intelligence (CTI), permette di capire meglio gli attori malevoli che hanno preso di mira il perimetro digitale da difendere e di attuare delle misure di remediation degli incidenti più rapide ed efficaci. La CTI è quindi un valido strumento di supporto nel processo decisionale poiché permette di ottenere elementi informativi strategici e di contesto, che inseriscono in una cornice più ampia i dati e le informazioni tecniche generati dagli apparati di difesa perimetrale ed aumentano la consapevolezza interna verso un mondo che, per definizione underground, rimane difficilmente osservabile e spesso incompressibile.

Similmente al ciclo di intelligence, la CTI è un processo "circolare" continuo composto dalle fasi di monitoraggio, identificazione, elaborazione, analisi, disseminazione ed ottenimento del feedback che, spesso, dà il via a nuovi cicli di intelligence. L'applicazione del ciclo può essere tattica, in grado di dare risposte utilizzabili nell'immediatezza, o strategica con l'obiettivo di valutare le possibili linee di sviluppo e supportare le strategie future dell'organizzazione. Attraverso il monitoraggio della rete (clear web, deep e dark web) è possibile tracciare obiettivi, target e interessi degli attori malevoli attivi e conoscerne quindi le armi digitali, le infrastrutture utilizzate, le tecniche e metodologie usate per sferrare i propri attacchi. Nel monitoraggio vengono ricercati gli Indicatori di Compromissione, informazioni particolari che permettono di riconoscere le minacce, che rappresentano vere e proprie "impronte digitali" delle minacce (ad esempio gli IP o gli hash dei malware utilizzati dagli attaccanti).

Per raggiungere questo risultato sono necessarie specifiche tecnologie e processi verticali e una forte verticalizzazione di più competenze tecniche (di contesto, tecniche, investigative). Un'attività efficace di protezione, specialmente di tipo predittivo e preventivo, permette di adottare strumenti di difesa specifici per eventuali attacchi e individuare potenziali nuovi punti deboli all'interno della rete.

In altre parole, l'investire sulla Cyber Threat Intelligence, integrando tecnologie, persone e processi, permette di ottenere un sistema di difesa non solo reattivo, ma soprattutto preventivo e predittivo.

Questo impulso deve partire dai vertici della propria organizzazione che devono farsi promotori stabili di questo cambio di paradigma e supportare la diffusione della cultura della sicurezza, CTI in particolare, all'interno di ogni livello della propria organizzazione.

Va tenuto a mente che il personale già presente potrebbe non aver le capacità, tempo e competenze tecniche per eseguire le attività richieste da questo tipo di incarico e potrebbe non essere né semplice né rapido reperire nel mercato personale senior già addestrato. D'altro canto, delegare questa attività ad una azienda esterna richiede che ci si affidi a professionisti affermati che abbiamo un alto livello di affidabilità e trust da parte sia dei loro clienti sia degli altri attori presenti sul mercato senza cercare di risparmiare qualcosa affidandosi ad aziende o servizi che risiedono in paesi terzi spesso con legami non particolarmente chiari con le agenzie di intelligence locali.

RADAR METEOROLOGICO DOPPLER VAISALA WRS400 IN BANDA X A DOPPIA POLARIZZAZIONE

Misure molto accurate, in tempo reale e ad alta risoluzione

VAISALA

Subito dopo il decollo e durante le fasi che precedono l'atterraggio, gli aeromobili sono particolarmente vulnerabili alle condizioni meteorologiche.

Dopo il decollo, iniziano a salire per raggiungere la quota di crociera – con velocità ancora in aumento e facendo attenzione al traffico aereo presente. In avvicinamento, volano con bassa potenza del motore ed a velocità ridotta (e quindi la loro capacità di risalire rapidamente o regolare la traiettoria è limitata). La conoscenza del quadro meteorologico in atto in queste fasi di volo è fondamentale ed è per questo motivo che molti aeroporti nel mondo hanno iniziato a dotarsi di specifici radar meteorologici in banda X per avere informazioni di dettaglio lungo i sentieri di decollo e atterraggio. Il radar in banda X fornisce importanti informazioni di nowcasting dei sistemi meteorologici in avvicinamento e dei fenomeni ad essi correlati, quali pioggia, neve, grandine, temporali, microburst, etc., consentendo alla torre di controllo e ai piloti di completare il processo informativo delle condizioni meteorologiche in atto o in divenire. Ciò è particolarmente vero per gli aeroporti che si trovano vicino alle montagne e alle zone costiere dove i sistemi meteorologici sono più difficili da rilevare o monitorare. Per questo motivo, Vaisala ha posto grande attenzione nello sviluppare un radar meteorologico in banda X, facilmente integrabile nella rete di sensori di aeroporto.

I dati del radar in banda X possono aiutare a migliorare la sicurezza e l'efficienza delle operazioni, consentendo di monitorare le condizioni meteorologiche sui corridoi di decollo e avvicinamento.

Il radar meteorologico Vaisala WRS400 ha un disegno innovativo ed impiega trasmettitori a stato solido, con un conseguente basso costo del ciclo di vita. I trasmettitori a stato solido hanno il pregio di lavorare a basse tensioni ed inoltre, nel caso di rottura di un amplificatore l'unica conseguenza sarebbe la diminuzione della potenza trasmessa e non il completo spegnimento, come nel caso di trasmettitori di tipo magnetron. L'antenna del radar Vaisala WRS400 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 possano essere fissati vicino al centro di gravità del radar, 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 la cui tensione è mantenuta costante. Questa soluzione è ispirata a principi di bassa manutenzione e non c'è necessità di sostituire olii o lubrificare il piedistallo o, come nei radar tradizionali, le catene di trasmissione.

L'affidabilità del sistema è aumentata da alcune caratteristiche peculiari: la protezione contro i fulmini è integrata nel disegno del radar e le unità di protezione sono costituite da modelli commerciali di alta qualità; il sistema include il BITE di ausilio per una facile ricerca guasti, consentendo anche di fornire anticipazioni sulla degradazione di funzionamento, prima che si verifichi l'effettivo guasto.

Il Vaisala WRS400 è un Radar Meteorologico Doppler in banda X a doppia polarizzazione innovativo e quando utilizzato in combinazione con un Lidar a scansione Vaisala WindCube per il monitoraggio del vento in aria chiara, fornisce uno strumento completo ed affidabile per il monitoraggio di tutte le condizioni meteorologiche, soprattutto per il rilevamento del wind shear, consentendo al pilota di adottare le opportune procedure di volo.

LESSONS LEARNED BY THE ROMAN LEGIONS STILL MATTER FOR TODAY'S DEFENSE IT

and why they still matter for today's Defense IT

VATES

There is a latin word which cannot be easily translated in English nor in many languages today: "Impedimenta". It is roughly translated as "Army logistics" but it really describes the entire resources and logistics of the Roman Army while moving towards the battlefield and on the battlefield.

Romans had learned that logistics is the key to military success. They were not more courageous than others, in fact their first concern was to protect their troops from the ennemy. But they knew that without logistics the best army will break down and lose its best assets. Today, anyone in the military would say the same. But few would also say the same of the Defense IT.

Defense IT not only needs to do its job right, run its operations securely, it also increasingly needs to ensure portability of applications and data. This is true not just between data centers, but also between the theatre of operations and the homeland.

Defense IT faces unique challenges - and several are directly related to the ones faced by armies of all times. The reality is that any IT teams or CIO will face a lot of vendors who will pitch their solutions - be it software, hardware, or cloud services- and hear them describe why each of their offerings matter more than many others. Sometimes, this will be absolutely true, or at least they may have a point. Some other times, whatever is pitched simply will not match the needs and requirements of the Defense Ministry or the armed forces.

But there are a few things that need to be taken care of. Three of them are fundamental: Security, Portability, Efficiency.

Security

Security is a primordial need for people, for organized communities and groups, and therefore for any army. Romans soliders had an excellent reputation no matter what their speciality was - from the simple, light infantry velites to the heavy triarii, but also the auxiliary units and even the frumentarii - logisticians who later became a kind of special field intelligence corps. But few people seem to realize that the first duty of the officers in roman legions no matter what their rank was was to protect the troops and its supply lines. The famous "turtle" formation of legionnaires covering themselves with shields and advancing in square formation was not so much a fearful sight as it was a reassuring, battle proven method aimed primarily at protecting the roman soldiers' lives. There was honour in falling for Rome - but it was better to win and come back alive. In this regard works the same way. It is only really useful if it is secured from hostile actions. Our world has entered a phase where everything is connected, even the battlefield. There is more value to be gained, less resources used and more effects if an ennemy grounds an entire fleet of warships or jetfighters to the ground with a cyber attack than with an actual engagement which is in itself always problematic. Security of the IT systems in a defense context is therefore absolutely crucial and is not just a factor of financial investment. It relies on the right tool for the right job and a proper understanding of the risks and the landscape.

Portability

An idle army is an army waiting to be attacked, especially in a hostile territory. The ability to move to one point to another, and in fact to transport the army and its equipment and resources is another fundamental notion. Defense IT follows the same logic. IT systems must be portable for agility in scaling up and down depending on the circumstances but also for security - the ability to backup entire systems is key. Portability also means the ability to switch supplier and avoid vendor lockdown in case it would become a liability or just to preserve the ability to pick the best solutions over time. Virtualization and containerization are important tools in that regard.

Efficiency

Last but not least, an army, just like IT systems, must be efficient. Efficiency is not only about getting the job done. It's about getting the job done the right way. Scaling up or down through the adequate use of resources and skills is a good definition of efficiency when applied both to military and IT contexts. Efficiency requires planning and a careful understanding of the tools, the environment, the purpose and the teams who will be work towards reaching the purpose. Ultimately efficiency provides the measure for excellence as well as economies of scale, two other notions of paramount importance for IT systems and the military.

A lot of technologies have changed since the times of the Romans - but the imperatives haven't even after 1600 years.

LA DIGITAL TRANSFORMATION È UNA QUESTIONE DI FIDUCIA

Edwin Weijdema, Global Technologist, Product Strategy, Veeam

VEEAM

Oggi più che mai, dipendiamo dalla tecnologia per lavorare, comunicare e divertirci, e proprio per questo motivo dobbiamo riporre la massima fiducia in essa. Quando scegliamo di lavorare da casa invece di andare in ufficio, siamo fiduciosi del fatto che il nostro computer sia perfettamente funzionante, che la connessione Internet sia stabile e che si possa accedere alle applicazioni in cloud di cui abbiamo bisogno. Nonostante ciò, inconsciamente, siamo più preoccupati della connessione o dello stato del nostro computer quando lavoriamo da casa rispetto a quando siamo in ufficio, con un team IT a disposizione nell'ufficio accanto.

Questo perché spesso, avere fiducia nella tecnologia significa affidarsi all'ignoto. Ho abbastanza fiducia in qualcuno o qualcosa da poter superare l'incertezza del risultato? Se non si ha fiducia, non si corrono rischi, non si fa il così detto "salto nel buio", il che significa che non si cambierà mai. Quindi, mentre le aziende continuano il loro percorso di Digital Transformation (DX), come possono assicurarsi che una mancanza di fiducia verso la tecnologia non impedisca loro di prendere i rischi necessari associati a qualsiasi tentativo di avviare il cambiamento?

Per certi versi, il processo che ci porta ad avere fiducia nella tecnologia è molto simile a quello che avviene con un altro essere umano. Abbiamo una serie di strumenti a cui attingere. Il primo è il nostro istinto. Spesso capiamo se possiamo fidarci di una persona in meno di 30 secondi dal primo incontro. E questo avviene anche per la tecnologia. Tutto, dal logo del brand alla prima interazione con l'interfaccia utente, contribuisce alla nostra percezione di un dispositivo, di un sito web o di una comunicazione, ci dice se possiamo fidarci o meno. Diversi studi suggeriscono che siamo più propensi ad accettare telefonate da numeri che riconosciamo. Siamo diffidenti nel fornire informazioni personali su noi stessi quando ci registriamo a un servizio online, mentre non esiteremmo a dare gli stessi dettagli a un addetto bancario o a un consulente finanziario.

Ma il nostro istinto, se da una parte è un alleato molto potente, a volte può deluderci. Nel mondo reale, significa ad esempio credere alla storia che ci sta raccontando un amico per scoprire che in realtà si tratta di uno scherzo o ritrovarci a guidare verso l'ufficio perché è ciò che ci dice il nostro cervello per poi rendersi conto che è domenica. Nella sfera digitale, significa cliccare su link di phishing, compromettere le informazioni sulla sicurezza personale e accettare le fake news come una verità.

Tuttavia, la fiducia non è solo una questione di pancia. La fiducia si guadagna nel tempo attraverso le nostre esperienze, ma anche attraverso quelle degli altri. Quando leggi opinioni condivise da altre persone che non hai mai incontrato, la tua incertezza e la sensazione di rischio diminuiscono. Ti senti più sicuro nel fare quel passo verso l'ignoto. E lo stesso concetto si applica anche alla tecnologia che ci aiuta a ridurre l'incertezza dandoci accesso a un enorme quantità di informazioni. Queste informazioni sono un vero e proprio un abilitatore di fiducia.

La maggior parte degli utilizzatori di tecnologia e dei team IT preferisce aspettare e vedere. Che si tratti di acquistare un nuovo smartphone o di migrare i dati nel cloud pubblico, in molti cerchiamo conferme da persone che l'hanno provato per prima.

Quando si parla di fiducia, uno dei maggiori problemi che le aziende hanno nei confronti delle nuove tecnologie è la loro sicurezza. I dati saranno sicuri e protetti? Vogliono anche sapere cosa succede quando le cose vanno male. Come possiamo riportare i nostri servizi online e recuperare rapidamente i nostri dati? Secondo il Veeam Data Protection Report 2021, il 27% dei business leader europei vede le minacce informatiche come una sfida alle loro iniziative di Digital Transformation nei prossimi 12 mesi. Questa maggiore consapevolezza dell'impatto generale delle violazioni e della cybersecurity peserà molto sulla scelta del partner che li accompagnerà in questa trasformazione.

Per quanto riguarda il livello di successo delle modalità con cui le aziende stanno attualmente proteggendo i dati, i malfunzionamenti e le carenze dei backup stanno lasciando il 58% dei dati potenzialmente non protetti. È chiaro che il rapporto dell'uomo con la tecnologia, che sia un cliente, un decisore aziendale o un dipendente, è tutta una questione di fiducia. Ciò significa che le aziende devono rivolgersi a consulenti tecnologici fidati che possano aiutarle a garantire che il loro percorso di trasformazione digitale sia costruito su basi solide, con una protezione dei dati che sia adatta allo scopo.

TOWARDS URBAN DELIVERY USING A COOPERATIVE FLEET OF UNMANNED AERIAL VEHICLES

W. Matta, S. Mazzaro, A. Antenucci, A. E. Fiorilla

VITROCISET

SWARM concept

The use of air mobility and multi-domain autonomous systems will transform travel, package delivery and other urban activities in ways that would have seemed impossible just a few years ago, by addressing and solving open research issues that are not only and exclusively about the transport domain. Among the advantages of using autonomous aerial systems in urban areas, there is the possibility of monitoring and at the same time trying to reduce city pollution, decongesting traffic in the main urban areas, finally making for citizen workers the habitability of the city a real option. The use of fleets of drones for the delivery of goods will produce further increases in the field of e-commerce, dramatically increasing the profits of many companies. The total economic benefits resulting from the use of air mobility and self-driving systems could be beyond expectations with the emergence of ever new applications capable of increasing efficiency and productivity. First, however, it will be necessary to regulate such activities, making them safe for citizens in the first place and of course for the companies that will benefit from them. We therefore propose a framework based on a Ground Control Station (GCS) developed as part of the Vitrociset R&D project, called SWARM. It is a software capable, through the state of the art of route optimization algorithms, to plan, simulate and validate urban deliveries through drone fleets, also considering the so-called last mile problem, using modern and advanced technologies of Artificial Intelligence (AI) in the field of computer vision, using cooperative COTS multi-mini UAVs, to increase the efficiency of delivery activities by avoiding collisions, as well as to optimize and increase associated services such as urban surveillance and pollution monitoring, with an all-in-one solution. Its strong point is the possibility of using COTS fleets of cooperative and heterogeneous mini/micro UAVs. Relating to the possible delivery of goods in a city environment, the UAVs of the fleet can be equipped with simple commercial effectors for the delivery of packages and with integrated on-board computers (OBC) for the implementation and resolution of the problem of last mile control and precision landing, using advanced computer vision algorithms. The Ground Control Station (GCS) presented here (Fig. 1) allows to control heterogeneous and commercial fleets of drones, using Vertical Take-off and Landing (VTL) mini/micro UAVs, or customized drones based on open or standard communication protocols.

Fig. 1. Real on field tests of the delivery system

Using the internal fleet manager it is possible to plan a mission with different kinds of drones, by choosing the waypoints for each flight plan of each single drone. The flight can be validated by running an instant and on-the-field simulation of the mission, which gives to the operators useful information about the possible success of the operations. Such simulation provides, for example, the percentage of the battery usage (e.g. some paths could be too long for the chosen equipment) or even presence of possible obstacles (like trees or buildings). As part of the enhanced features of its software, the system is particular useful for the delivery domain, for automatic path planning and landing zone search/tracking functionality.

Conclusions

Rapid drone delivery could accelerate the already steep uptick in e-commerce and increase the bottom line at many companies. The overall economic benefits of air mobility could be immense as new applications increase efficiency and productivity. The main barrier to achieve the above impact lies in the combination of two factors: regulation and technology development, in particular there is a need for common rules at national/transnational level for the provision of U-Space services. Industry may be reluctant to invest significant resources in further developing solutions like the one proposed, unless a stable regulatory framework will be able to guarantee that positive market conditions will be maintained throughout the next years.

L'INFORMAZIONE E L'INNOVAZIONE: UN EXCURSUS DALLA DIGITAL TRANSFORMATION AI SOCIAL TARGETS

Un focus sulla comunicazione

WICODE

La "digital transformation" introduce molti cambiamenti che ogni nazione, azienda e popolo è chiamato ad applicare. Ad oggi, lo sforzo più grande è stato il processo di formazione per accogliere la trasformazione. L'intera società subisce l'impatto con il cambiamento dei tempi e ogni uomo cerca di mettersi al passo.

Tutto questo è una necessità per essere coerente con le modifiche sociali ed industriali, e per dare un contributo fattivo ad un auspicabile miglioramento. Viviamo un momento difficile in cui cambiare è essenziale per adattarsi in una società in continua evoluzione.

WiCode è impegnata in progetti di "cambiamento" che vanno dalla certificazione della filiera agro-industriale alla analisi predittiva applicata alla giurisprudenza, dal data protection alla cyber & physical security per contrastare minacce su infrastrutture critiche, inoltre, abbiamo fatto della formazione la nostra pietra miliare.

In questi anni si siamo soffermati sul rapporto tra cambiamento e informazione, intesa come scambio di messaggi relativi a notizie. Questa è stata tra le prime ad essere oggetto di digitalizzazione, trasformazione e ad essere considerata come la possibilità di diffondere e avere accesso al messaggio del cambiamento, nel modo più trasparente e rapido possibile. Frequentemente, l'accesso ai "fatti" è stato più rapido della loro pubblicazione stessa. Questo "fenomeno" è tra i primi in elenco, in termini di violazione, manipolazione e inoculazione di errata informazione. Una volta pubblica, un'informazione può subire una "violenza" che ne provoca un'alterazione, in altri casi è pubblicata volontariamente errata, questo processo lo identifichiamo col nome di disinformazione. La disinformazione è una "minaccia ibrida" che si annida nelle pieghe di ogni "sistema" pubblico/privato e in ogni "dispositivo" (gruppo) umano.

Siamo costantemente impegnati in attività di indagini digitali e riscontriamo che contrastare questi fenomeni risulta difficile quando si perde il controllo o non c'è certezza della fonte. Un fenomeno contemporaneo (contenuto nella disinformazione) sono le "fake news" e "deep fake", questo può provocare l'impossibilità o cattiva gestione dell'informazione pubblica, un fenomeno spesso legato

anche alla scarsa attitudine nel riconoscere l'inattendibilità dell'informazione e alla presenza di poche fonti aperte con cui confrontare la veridicità di un "fatto". Osserviamo da anni le evoluzioni della rete social e pensiamo che la perdita di controllo delle informazioni non genera solo all'obiettivo una "confusione" nel lettore ma tende anche a minare alcune tipologie di "interlocutore target". Uno dei danni che può arrecare la disinformazione è la "manipolazione di massa", infatti attraverso, ad esempio, gli "insights" dei social network è possibile scegliere l'"utente bersaglio" ed iniziare ad agire in modo subdolo e malevolo, costruendo in alcuni casi delle vere e proprie "trappole digitali", generando di conseguenza, una inconsapevole continua diffusione di notizie non vere, questo fenomeno è definito "misinformation".

Stiamo lavorando ad alcuni progetti di ricerca che hanno come obbiettivo la "marcatura indelebile" dell'origine dell'informazione, che abbinata alla successiva certificazione permetterebbe una enorme passo avanti nel contrasto alla manipolazione delle notizie.

La "libera informazione" è la vera vittima dei canali di mediatici non adeguatamente regolamentati e tutto quanto detto rappresenta l'evoluzione digitale degli ultimi 20 anni: l'acquisizione di diritti attraverso strumenti nati come giochi e trasformati in armi da guerra alla portata di tutti.

Concludendo, riteniamo che la convergenza tra privacy, cyber security, strumenti regolatori e regolamentari, tecnici e applicativi, sono e saranno la pietra miliare per la costruzione della gestione "sicura" dell'interscambio comunicazionale ma soprattutto auspichiamo che la velocità di pensiero dell'innovatore non sia troppo disruptive e non crei velocità differenti tra pubblico, privato e cittadini.

EDT (EMERGING AND DISRUPTING TECHNOLOGIES): TECNOLOGIE EMERGENTI E DIROMPENTI PER LA STRATEGIA NATO

Un commento al documento del EDT Nato Advisory Group.

MARCO BRACCIOLI

In un documento recente della Nato, si sono prese in esame quali possono essere le tecnologie emergenti e dirompenti da adottare nella Nato. Le considerazioni tecnologiche di tipo militare avranno comunque impatto sulle società occidentali anche in campo civile, individuando e focalizzando su 5 Domini tecnologici emergenti che hanno rilevanza per l'Alleanza Nord Atlantica.

1. Al primo posto tra le tecnologie d' interesse della Nato, gli Advisor pongono il Machine Learning e l'Intelligenza Artificiale. Su questo tema suggeriscono di sviluppare tale AI come tecnologia abilitante e per lo sviluppo di applicazioni in vari settori, il computing neuromorfico, lo sviluppo di reti neurali per la difesa ed una migliore efficacia per l'analisi dei big data real time and non real time.
2. Al secondo posto lo sfruttamento della Scala Quantistica dal Quantum Computing al Monitoraggio Quantistico dei Big Data al Post Quantum, la Crittografia Quantistica fino allo studio e sviluppo dei materiali innovativi
3. Data Security al terzo posto, lo sviluppo di algoritmi e sistemi di difesa e di attacco, applicazioni avanzate di data storage e data transactions , la crittografia quantistica, le blockchains e tutte le attività di cyber security e di protezione delle supply chains militari/ industriali.
4. Al quarto posto un perimetro di varie tecnologie come quelle orientate alla miniaturizzazione, all Energia (batterie etc), quelle orientate alla difesa dell'infrastrutture critiche, le IoT (internet of things) e la Robotica. Molte di queste tecnologie devono ancora raggiungere una piena maturazione ma la Nato intende mantenere un focus tecnologico su di esse.
5. Chiude la lista delle priorità Materiali Biologici sintetici con la relativa progettazione, sintesi e manipolazione dei materiali al livello atomico e molecolare per innovazione a livello mesoscopico e macrosopico. Questa sezione riguarda i settori della bioingegneria, dell'ingegneria chimica, la genetica, i nuovi metodi di produzione e progettazione.

È chiaro che il mondo dati e ciò che gira in torno ad esso diventa una nuova dimensione di stress nella battaglia per le risorse mondiali che fino ad ora vedevano nelle risorse classiche come l'acqua, il cibo, l 'energia le materie prime i drivers di conflitto, il mondo dati e le nuove tecnologie creano nuove asimmetrie geopolitiche modificando talvolta gli equilibri di potere. Questi conflitti sono quelli dello spazio Cyber dove predominio e Sovranità digitale vanno affermati in una guerra digitale in tempo di pace.

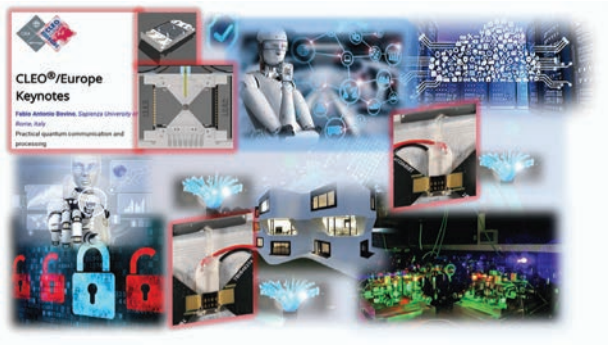
Non meno strategica delle 5 aree tecnologiche per la Nato è la STEM B (Scienza, Tecnologia, Engineering, Matematica e Business), ciò la ricerca e lo sviluppo delle risorse umane che possano sviluppare le aree di interesse strategico. Non meno importanti sono i settori dello Spazio, della Comunicazione Multi dominio e del volo ipersonico dove la Nato dovrà sviluppare una propria postura tecnologica per aumentare la competitività e la Resilienza del Blocco Atlantico nei confronti di potenze globali e regionali.

QUANTUM COMPUTING, INTELLIGENZA ARTIFICIALE, ROBOTICA CHIAVI DI VOLTA DEL PROSSIMO FUTURO POST-PANDEMIC

"Machine Learning" versus "Deep Learning": Reti Neurali

CINZIA CROSTAROSA

Nell'epoca covid con distanziamento sociale, siamo in uno scenario in cui la tecnologia e le connessioni sono gli strumenti per sostenere l'economia globale. Si dovranno potenziare i processori, che abbiamo a disposizione, anche se in realtà siamo arrivati allo stato dell'arte del computing, per cui non si può progredire in modo consistente, come si evince dalla legge di Moore. Per il salto tecnologico si deve ricorrere ad un modo nuovo di studiare la realtà della fisica, che non è più quello del silicio e del transistor. Si deve verificare se i nuovi hardware fotonici corredati di software legato alle reti neurali siano in grado di fornire dei risultati concreti e necessari per il nostro futuro. Sarà una nuova elaborazione in parallelo e non più sequenziale. Non si dovrà trascurare l'aspetto cyber security, basato su tecnologie Quantum, come la QKD (Quantum Key Distribution) Infrastructure. La Fisica Quantistica è un nuovo modo di leggere la Natura, con un potenziale dirompente e rivoluzionario, che permette di costruire device, che influenzeranno profondamente la nostra vita, come ha affermato F.A. Bovino durante una CLEO/EUROPE Plenary Session a Monaco nel 2019. I settori maggiormente interessati saranno Difesa, Aerospazio, Energia e Telecomunicazioni. La Quantum Information Technology può supportare modalità nuove nel campo dell'elaborazione delle informazioni, che si basano sui Qubit. I progressi nello sviluppo di tecnologie per realizzare l'elaborazione di informazioni quantistiche sono incastonati in una gara a livello globale tra i laboratori di ricerca internazionali. Alla fine del 2019 è stata annunciata la Supremazia Quantistica di Google e sembra arrivata la possibilità concreta di avere personal computer, che sfruttino la tecnologia dei Qubit, per cui l'Europa e di conseguenza l'Italia sono in corsa per affermarsi in tale ambito, con strategie diverse. Ancora in emergenza pandemica, l'Italia sarà presente al CLEO®/Europe 2021 https://www.cleoeurope.org/keynote/, per esporre i nuovi traguardi, in un ambito complesso, ma cruciale per i destini delle nazioni. Sarà presentato il nuovo processore quantico (vedi figura), nodo della Quantum Internet del Dipartimento di Scienze di Base e Applicate per l'Ingegneria dell'Università



Sapienza, in figura gli schemi del Quantum Entangler e del Dispositivo Plug and Play per Quantum Internet, PNRM COPERNICO finanziato grazie al Ministero della Difesa italiano. Nel marzo 2011 all'Associazione AFCEA Capitolo di Roma si aprirono sessioni di lavoro in merito alla Teoria della distribuzione quantistica delle chiavi Network QKD ed alla necessità della loro validazione sperimentale, anche per la comunicazione spaziale. Nello scenario di utilizzo dei Big Data sicuramente è importante che siano potenziati i collegamenti con banda ultra larga, tramite i cablaggi in fibra ottica, anche per far fronte all'emergenza COVID. L'Intelligenza Artificiale (AI) si inserisce in modalità disruptive nel tessuto tecnologico, in più ambiti della Robotica, ad esempio il settore dell'automotive, l'ambito biomedicale o quello finanziario. Con lo sviluppo di veicoli a guida autonoma serve un AI, che sappia prendere decisioni in modo trasversalmente più complesso rispetto ad un sofisticato software, che si implementa sulla base di algoritmi a logica booleana. In ambito sicurezza si ricorre all'AI per modalità applicative, come sistemi antiintrusione o antiincendio, che sono governati da software di nuova generazione, che rilevano tramite sensori, valutano tramite algoritmi di Machine Learning (ML) e agiscono autonomamente in base a meccanismi di autoapprendimento del software. La tecnica di AI maggiormente in crescita è il ML, che richiede una significativa quantità di dati archiviati, che spesso non sono liberi ma detenuti da soggetti, come le piattaforme on- line definite superstar firm, vedi Facebook e WhatsApp. Le dimensioni delle imprese superstar sviluppano conseguenze rilevanti per l'AI, dato che possiedono i dati, che è il materiale su cui sviluppare il ML. Nessuno può eguagliare la disponibilità dei dati del settore privato, per cui combinando tale realtà con la tecnologia quantistica, si ha il salto tecnologico dell'era del Quantum Computing e delle reti neurali di tipo deep learning, che promettono un tipo di funzionamento vicino alle sinapsi del cervello umano. Infine per proiettare nel futuro gli ambiti: AI, Big Data e Quantum Information governati dalle STEM, Science, Technology, Engineering and Mathematics, è doveroso introdurre la diversità di genere minacciata dai bias cognitivi.

Soci
Corporate

ALMAVIVA. Leader italiano nell'Information Technology, AlmavivA accompagna la trasformazione digitale nei settori chiave per l'economia del Paese.
La presenza in Italia come riferimento di valore. E da solide competenze Made in Italy, unite alla capacità di integrare culture, intelligenze ed esperienze diverse, è nato un network globale. Protagonista della trasformazione digitale. Tecnologie AI-driven «made in Italy» basate su Machine Learning, Deep Learning e Natural Language Processing. La Digital Transformation disegnata sulle frontiere dell'innovazione.
www.almaviva.it/it_IT

ASC27 è una società innovativa con sedi a Roma ed a Bologna. Lavoriamo nei settori dell'Intelligenza Artificiale e della CyberSecurity. ASC27 coniuga la ventennale esperienza maturata nel mondo Cyber, con le sue spiccate e peculiari competenze nel settore dell'AI. L'azienda, totalmente privata ed indipendente, sviluppa soluzioni ad ampio raggio per la Sicurezza Fisica, Cyber e cyber Fisica impiegando tutto il proprio know-how maturato in 4 continenti ed introducendo l'Intelligenza Artificiale come elemento permeante e distintivo all'interno delle sue soluzioni. Cosa contraddistingue la nostra Società? Diciamo spesso: <<noi non affittiamo AI (dal Cloud), noi sviluppiamo Intelligenze Artificiali>>. Motto aziendale: <<We Build Knowledge>>.
www.asc27.com

ASCITAL è una Società Consortile a r.l. costituita nell'anno 2003 e che, al momento, comprende 10 PMI consociate, tutte italiane, operanti nei settori dell'ICT, della Sicurezza globale, degli Impianti tecnologici, dei Sistemi integrati di automazione industriale e dei Lavori infrastrutturali, potendo annoverare le abilitazioni di sicurezza per la trattazione di informazioni classificate e svariate certificazioni ISO e SOA. Il Mercato di Riferimento riguarda: Cyber Security, Ingegneria dei Sistemi, System Integration, Automazione, Schermatura di ambienti, Networking, Videosorveglianza, Prodotti ed impianti di fonia, Cabling ed impianti elettrici, Opere Civili, schermatura di ambienti, prove Tempest.
www.ascital.it

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

Core Sistemi, sul mercato ICT dal 2005, è specializzata nello sviluppo di soluzioni ICT per aziende e pubbliche amministrazioni, con un'attenzione particolare al mondo della Difesa. Il core business dell'azienda si basa su tre business units: Cyber Security: prevede un approccio che va dall'analisi del rischio, alla definizione, implementazione e gestione di infrastrutture di sicurezza tailor made; Managed Services & Solutions: gestisce proattivamente lo stato di salute dei sistemi installati, con lo scopo di fornire una risoluzione di fronte a malfunzionamenti o problemi tecnici; Data Center: lo sviluppo dei Data Center ha permesso di espandere le capacità elaborative, dando vita a nuove applicazioni. Core Sistemi ha assecondato queste evoluzioni fornendo un ampio ventaglio di soluzioni per la progettazione e la realizzazione di Data Center di nuova generazione.
www.coresistemi.it

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

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.
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

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

Elettronica - ELT (a.k.a. ELETTRONICA) Group is a global leader in the business of Electromagnetic Warfare/Electromagnetic Defence with a complete portfolio of state-of-the-art solutions to satisfy the most challenging requirements of modern operational scenarios.
ELT is an Italian Company, established in 1951, share-held by Leonardo, Thales and, for the majority, by a private owner, with an order book of 1.2 B€ and revenues of 250+ M€ per year.
The solutions designed and manufactured by ELT cover a wide range of applications and missions: Intelligence-Surveillance-Reconnaissance, Electronic Warfare, Cyber Electromagnetic Activity, Homeland Security and Border Surveillance
ELT solutions are integrated in several kind of platforms (aircrafts, helicopters, fighters, UAVs, Surface ships, underwater vessels) and manage information in air, land, sea and cyber domains. The record include military, military supported and intelligence missions where the Company solutions have been tested and proven in operations by European and non-European Countries worldwide.
ELT widen its competence and offers by means of two sister Companies:
ELT GmbH, which is a Centre of Excellence in Homeland Security, Test Validation Systems and Video Digital Boards Design and Production
CY4GATE, which provides Governments with software and hardware solutions to support the full cycle of intelligence and to succeed in Cyber operations in the electromagnetic environment, communications, operating systems and wired networks.
www.elt-roma.com

ENAV, 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, Official Distributor di Esri per il mercato italiano, è l'azienda leader nelle soluzioni geospaziali, con sedi a Roma, Milano e Cagliari. 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, fondata nel 1961, opera nel campo della progettazione, integrazione, vendita, installazione, assistenza tecnica, consulenza e formazione nell'ambito della Meteorologia e delle Scienze Atmosferiche, introducendo in Italia tecnologie innovative in vari settori applicativi. Sin dal 1979 è Rappresentante per l'Italia del gruppo Vaisala, per tutte le applicazioni di Meteorologia e dal 2011 Partner Tecnico Certificato. Da Novembre 2018 fa parte del gruppo Vaisala anche Leosphere, azienda già rappresentata da Eurelettronica Icas. E', inoltre, Distributore Esclusivo in Italia di: Kipp&Zonen, Totex, Millard Towers, Acams, Jotron. Tra i clienti: Aeronautica Militare, Esercito Italiano, Enav, ARPA Piemonte, ARPA Campania, ARPAE Emilia Romagna, ARPA Veneto, ENI Taranto, Autovia Padana, Autostrade per l'Italia, Iride Energia, ACTV,GDF Suez, JFCNP (NATO).
www.eurelettronicaicas.com

Eurolink Systems dal 1993 fornisce soluzioni tecnologiche ad alto grado di affidabilità e innovazione nei due settori: Schede di acquisizione e processing e/o subsistemi integrati per applicazioni radar, sonar, High Performance Reconfigurable Computing. Server rugged e server sicuri conformi alla norma DoD 5200.44 contro Cyber attack. Mini e micro sistemi a pilotaggio remoto, aerei e terrestri autonomi ed a sciame. Ha sviluppato una famiglia di robot terrestri (Leopardo), un filoguidato VTOL (Cobra), co-sviluppato un mini UAV Bramor con operazioni >3ore di endurance e >35Km LOS. Tra i clienti: Gruppo Leonardo; MBDA; Elettronica; Nato, Centro di eccellenza training e simulazione; NURC; Esercito Italiano; Aeronautica Militare Italiana; FF.AA. straniere; Istituti di ricerca.
www.eurolinkssystems.com

Eustema fornisce avanzati servizi di Consulenza e Ingegneria del Software dal 1989.
In questi trent'anni di attività ha valorizzato e capitalizzato, unica in Italia, il retaggio di innovazione della Olivetti, sviluppando soluzioni ICT all'avanguardia che rendono i nostri Clienti sempre più competitivi e favoriscono la digital transformation del Paese
In particolare le attività core di Eustema si focalizzano sulla progettazione, realizzazione e gestione di soluzioni innovative in ambito digital trasformation, digital media solutions microservices architecture , cloud application and IT trasformation, Data Analitycs, data governance & Quality, Enterprise e Content Management, Security and Privacy. Attraverso il proprio Centro R&S, focalizza l'attenzione della propria attività di ricerca su machine learning, blockchain, IOT, big data.
Principali clienti sono: INPS, INAIL, MEF, MiSE, Dipartimento della Protezione Civile, Poste Italiane, RAI, Sogei; Ministero Difesa, Capitanerie di Porto, ENEL, TERNA, FS, AdR, ANAS, Comune di Milano, Infocamere.
www.eustema.it

Fabaris. Fondata nel 1996, Fabaris SpA da oltre 20 anni opera nell'ambito ICT, con una forte focalizzazione nel settore Aerospazio e Difesa. Vanta tra i suoi clienti aziende della pubblica amministrazione e dei servizi (Energia, Telco, Trasporti, Gaming).
Specializzata in Cyber Security, Infrastrutture di rete, Data Center e produzione di Soluzioni Software, negli anni ha ampliato la propria offerta commerciale, realizzando sistemi e progetti di Modeling & Simulation
Referenze: Stato Maggiore della Difesa, Presidenza del Consiglio, Esercito Italiano, Aeronautica Militare, Marina Militare, Carabinieri, Guardia di Finanza, SACT NATO, Leonardo, Almaviva, MBDA, ESA.
www.fabaris.it

Fastweb offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese.
Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultralarga.
Fastweb ha sviluppato una rete nazionale in fibra ottica di 45.600 chilometri e oggi raggiunge con la tecnologia fiber-to- the-home o fiber-to- the- cabinet circa 7,8 milioni di abitazioni e aziende.
Entro il 2020 Fastweb raggiungerà con la rete ultrabroadband 13 milioni di famiglie (ovvero il 50% della popolazione), di cui 5 milioni con tecnologia Ftth e velocità fino a 1 Gigabit e 8 milioni con tecnologia FttCab e velocità fino a 200 Megabit per secondo.
La società offre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G e 4G Plus. Entro il 2020 il servizio mobile verrà potenziato, a partire dalle grandi città, grazie alla realizzazione di una infrastruttura di nuova generazione 5G con tecnologia small cells.
La società fa parte del gruppo 18Swisscom dal settembre 2007.
www.fastweb.it

Fata Informatica 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 è il leader della sicurezza per l'Enterprise of Things. Offriamo l'unica soluzione scalabile che difende attivamente l'Enterprise of Things identificando, segmentando e imponendo la conformità di ogni dispositivo connesso alla rete eterogenea del cliente. Forniamo la possibilità di integrare la nostra piattaforma con una vasta pletora di tecnologie di sicurezza già in uso presso il Cliente al fine di incrementare il livello di sicurezza ed il valore complessivo degli investimenti fatto nell'ambito della sicurezza informatica. La piattaforma Forescout viene distribuita in modo rapido nell'infrastruttura esistente senza richiedere necessariamente l'installazione di agent, l'aggiornamento dei sistemi né modifiche alla rete. Forescout da oltre venti anni non ha mai venduto un semplice prodotto, ma ha sempre venduto il successo e la soddisfazione dei Clienti.
www.forescout.com

Fortinet protegge le principali aziende, service provider ed organizzazioni governative di tutto il mondo, offrendo ai clienti la piena visibilità e il controllo rispetto a superfici d'attacco sempre più vaste, oltre alla potenza necessaria per soddisfare i requisiti prestazionali in continuo aumento generati dalle reti borderless – oggi e in futuro. L'architettura Security Fabric di Fortinet offre sicurezza senza compromessi per rispondere alle più delicate sfide di security e proteggere i dati lungo l'intera infrastruttura digitale, in ambienti di rete, applicativi, multi-cloud o edge. Fortinet si classifica al primo posto tra i sistemi di sicurezza forniti a livello mondiale e oltre 500.000 clienti si affidano all'azienda per proteggere la propria attività. Come Tech e Learning company, il Fortinet Network Security Expert (NSE) Training Institute vanta uno dei più importanti e ampi programmi di training sulla cybersecurity nel settore.
www.fortinet.com

Future Time, Future Time, azienda attiva nella distribuzione di soluzioni per la sicurezza informatica, nasce nel 2001 dalla sinergia di due preesistenti realtà attive in questo campo.
Forte della profonda conoscenza di un mercato in continua evoluzione e della competenza tecnica dei propri esperti, Future Time propone un'offerta completa di soluzioni di sicurezza dedicate al mondo enterprise e collabora con aziende leader di settore tra cui Trend Micro, Stormshield, Wozon, Avast, Positive Technologies, Acronis; inoltre è distributore esclusivo di Odix per il mercato italiano. Punto di forza di Future Time è la solida rete di partner estesa a tutto il territorio nazionale, consolidata nel corso dei vent'anni di attività.
www.futuretime.eu

GMSPAZIO opera nei settori Difesa, Aerospazio e Homeland Security offrendo ai propri interlocutori soluzioni integrate e personalizzate in ambito: Modeling & Simulation, Space Surveillance & Tracking e Space Situational Awareness, Satellite Constellation Design & Operations, Border Patrol Control, Missile Defense Analysis, Sistemi Unmanned e Sistemi per il controllo del traffico aereo degli UAV. Distribuisce prodotti AGI (M&S), Orbit Logic (Collection Planning), Phoenix Integration (MBSE), PACSESS (NDT), Kratos (SATCOM), microdrones (UAV), Kanguru (Secure Storage). I principali clienti di GMSPAZIO sono: AIRBUS, ALTEC, ASI, ASTRIUM, CIRA, DLR, ELV-AVIO, ESA, EUSC, INAF, Ministero Difesa Italiano, Ministero della Difesa Spagnolo, Leonardo, MBDA, NATO, OHB, PolSA, RUAG, Space Engineering, Telespazio, Thales Alenia Space Italia.
www.gmspazio.com

Hexagon è un leader globale nella fornitura di sensori, software e soluzioni ad alto valore aggiunto. Poniamo i dati dei nostri clienti al centro di ogni progetto, per aumentare l'efficienza, la produttività e la qualità nelle applicazioni industriali, produttive, infrastrutturali, di sicurezza e di mobilità. Le nostre tecnologie permettono di modellare e governare gli ecosistemi urbani e produttivi per diventare sempre più connessi ed autonomi, garantendo scalabilità e sostenibilità. La divisione Geospatial di Hexagon sviluppa piattaforme tecnologiche software, applicazioni e soluzioni leader per visualizzare, analizzare e generare informazioni dettagliate basate sulla posizione geografica.
Unendo i mondi Geospaziali ed Operativi, facilitiamo i nostri clienti ad utilizzare la " Location Intelligence 5D" per risolvere le nuove sfide del mondo reale e di "mission-critical".
www.hexagongeospatial.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

IES Fondata nel 1990, è composta da un team di esperti nel campo dei sistemi di telecomunicazione per applicazioni civili e militari, negli ambiti terrestri, avionici, navali e ferroviari. La professionalità, la competenza e l'esperienza del proprio staff fanno della IES un interlocutore di primo piano, che la rendono fortemente competitiva nei settori strategici di prestigiosi enti pubblici, privati ed internazionali (NATO). Le attività principali riguardano: progettazione e realizzazione di innumerevoli prodotti (amplificatori RF, matrici Audio/RF, filtri, antenne), installazione e manutenzione di sistemi di comunicazione, con particolare attenzione allo sviluppo di specifici progetti per infrastrutture critiche ad alto livello di sicurezza.
http://www.iessrl.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 2020, Keysight ha realizzato un fatturato di 4,2 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

Leonardo è un player globale ad alta tecnologia nei settori dell'Aerospazio, Difesa e Sicurezza. La Società progetta e realizza prodotti, servizi e soluzioni integrate per Governi, Forze Armate, clienti civili e istituzionali, coprendo ogni possibile scenario d'intervento: aereo e terrestre, navale e marittimo, spazio e cyberspazio. Leonardo, con sede in Italia, ha circa 50 mila dipendenti, una consolidata presenza industriale in quattro mercati principali (Italia, Regno Unito, Stati Uniti e Polonia) e un importante network di collaborazioni strategiche nei principali mercati mondiali ad alto potenziale. Ogni anno Leonardo investe in Ricerca e Sviluppo circa il 12% dei ricavi.
www.leonardocompany.com

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 di sviluppare 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. Sedi: Verona, Bergamo, Trento. Collabora con istituti di ricerca e eccellenze universitarie nazionali ed internazionali. In particolar modo, con Polito, CNR e Links, si è aggiudicata un importante bando ESA per la ricerca. Principali clienti: produttori di radio, organizzazioni governative, system integrators. Settori: R&D PROJECTS al servizio di progetti customizzati per i clienti, ATC, LAND & NAVAL, TRANSPORT, PMR, DAS & 5G, M2M e MICROWAVE. Combinatori multicanale automatici, filtri, multi accoppiatori amplificati per la ricezione, duplexer, multiplexer, antenne e sistemi di antenne sono i prodotti di punta per le installazioni terrestri, aeree e navali. President & CEO: Domenico Zanin
www.polomarconi.it

RAIT 88 è HUB strategico e sistemico per la Difesa e la NATO su: Progettazione, Ricerca, Sviluppo, Integrazione, Riparazioni, Gestione e Soluzione dell'Obsolescenza, divenendo l'unica società in Italia a lavorare in assenza di documentazione fornendo prodotti FFF. RAIT88 è riferimento nei settori della Robotica, Realtà Virtuale e Artificial Intelligence, che le consentono di partecipare ai PNRM, investendo in tecnologie Quantistiche come il Quantum LiDAR/Quantum Radar e in Sensoristica Avanzata per l'aiuto al Soldato. RAIT88 rientra nei 40 fornitori strategici del programma Elite Leonardo Lounge. RAIT88 è stata pluripremiata ai "Le Fonti Awards®" come: Eccellenza dell'Anno Innovazione & Leadership Sistemi Informativi Sanitari ed Eccellenza dell'Anno Innovazione & Leadership Electronic Supply Chain, con lo sfidante obiettivo di supportare il Sistema Paese.
www.rait88.com

Rohde & Schwarz. Da più di 80 anni, Rohde & Schwarz è sinonimo di qualità, precisione e innovazione in tutti i campi delle comunicazioni wireless. Presente in Italia dal 1947, Rohde & Schwarz produce, progetta e mette a punto, sul territorio nazionale, soluzioni di comunicazione e di misura ad elevato contenuto tecnologico. Tra i suoi clienti figurano le più significative aziende private, enti pubblici e forze armate. Strutturata in tre divisioni, due dedicate alla vendita e una interamente dedicata ai servizi tecnici, Rohde & Schwarz Italia promuove, inoltre, la ricerca di soluzioni di comunicazione e di misura, economicamente accessibili anche alle piccole e medie imprese, rendendo disponibile l'alta qualità dei suoi prodotti ad una vasta fascia di mercato.
www.rohde-schwarz.it

Serco Italia S.p.A. è la filiale italiana di Serco group Plc con sede nel Regno Unito ed è 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, per entrare nel gruppo FININC nel 1988. Con un know-how storico nel Supporto Logistico Integrato SIPAL si rivolge oggi al mercato civile e militare, con uno staff di oltre 400 professionisti ad altissimo tasso di specializzazione. Con 12 sedi in Italia e un'esperienza di oltre 40 anni, SIPAL lavora con flessibilità, rapidità e competitività, personalizzando in ogni dettaglio i servizi offerti.
Dal 2018 SIPAL produce hardware e periferiche TEMPEST e di recente è diventata NATO BOA Partner; possiede altresì le abilitazioni necessarie per operare ai più elevati livelli di segretezza, supportando il cliente 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

Studio Torta. leader nella consulenza della Proprietà Industriale, 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 59 professionisti, alcuni dei quali di madrelingua cinese, giapponese, tedesca e francese, specializzati per i mercati internazionali e 131 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 2020 ha generato un fatturato di 540 milioni di euro e può contare su 3000 dipendenti in nove Paesi.
www.telespazio.com

Thales Alenia Space. Da oltre quaranta anni Thales Alenia Space progetta, integra, testa e gestisce sistemi spaziali innovativi ad alta tecnologia per telecomunicazioni, navigazione, osservazione della Terra, gestione ambientale, ricerca scientifica e infrastrutture orbitali. Governi e industrie privati fanno affidamento su Thales Alenia Space per la progettazione di sistemi satellitari che provvedono in ogni luogo e in ogni momento alla connessione e al posizionamento, al monitoraggio del mostro pianeta, all'incremento delle sue risorse e all'esplorazione del nostro Sistema Solare e oltre. Thales Alenia Space vede lo spazio come un nuovo orizzonte, aiutando a costruite una vita migliore e più sostenibile sulla Terra. Una Joint Venture tra Thales (67%) e Leonardo (33%), Thales Alenia Spaces Thales insieme a Telespazio forma la partnership strategica "Space Alliance", in grado di offrire un insieme completo di servizi. Thales Alenia Space ha un fatturato consolidato di 2,15 miliardi di euro nel 2019 e 7.700 dipendenti nove paesi.
www.thalesaleniaspace.com

TS-WAY. Anno di fondazione 2010, un expertise in cyber threat intelligence unica nel panorama italiano, TS-WAY sviluppa sistemi e tecnologie finalizzati alla produzione informativa per una difesa intelligence-driven. TS-WAY produce informazioni validate di tipo strategico, tattico, operativo e tecnico, consentendo alle organizzazioni di risparmiare tempo e risorse, anticipare le minacce complesse e gli avversari strutturati, comprenderne la portata e la natura, potendo contare su un partner affidabile in caso di incidente informatico. Un approccio alla sicurezza preventivo ed estremamente completo a garanzia e tutela dei beni e della continuità del business delle organizzazioni clienti.
www.ts-way.com

Vaisala, con più di 80 anni di esperienza, sviluppa e produce un'ampia gamma di sistemi, da sensori e stazioni meteorologiche automatiche, a sistemi di radiosondaggio e radiosonde, radar meteorologici in banda C e banda X, sistemi AWOS e Wind Shear. Grazie all'acquisizione di Leosphere, Vaisala è leader nel campo della fornitura di Lidar in diverse applicazioni. L'acquisizione dei servizi meteorologici B2B di Foreca rafforza lo sviluppo delle soluzioni nel campo digitale. Consistenti sono gli investimenti nello sviluppo delle tecnologie: Vaisala investe ogni anno fra il 10 e il 12% dei ricavi. Innovazioni sostenibili e basate sulla scienza sono valori fondanti. Vaisala è il partner ideale fornendo tutti i mezzi e gli strumenti affidabili e di alta qualità indispensabili per conoscere e gestire i fenomeni meteorologici e per sviluppare processi industriali sempre più sostenibili, assicurando la massima efficacia e sicurezza delle proprie attività.
www.vaisala.com

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

Veeam® è leader nelle soluzioni di backup, recovery e data management che abilitano la Modern Data Protection. Forniamo un'unica piattaforma per ambienti cloud, virtuali, SaaS, Kubernetes e fisici. I nostri clienti sono certi che le loro applicazioni e i loro dati siano protetti e sempre disponibili grazie alla piattaforma più semplice, flessibile e affidabile del settore. Veeam protegge oltre 400.000 clienti nel mondo, tra cui l'82% delle aziende Fortune 500 e il 69% delle aziende Global 2000. L'ecosistema globale di Veeam include oltre 35.000 partner tecnologici, rivenditori, service provider e alleanze partner. Veeam ha uffici in oltre 30 Paesi.
www.veam.com

Vitrociset, azienda del Gruppo Leonardo, fornisce soluzioni di "Sustainment" e Training" nei mercati della Difesa, Sicurezza, Spazio e dei Trasporti, attraverso l'integrazione delle più avanzate tecnologie in ambito ICT, sicurezza e simulazione. Vitrociset offre ai suoi Clienti un ecosistema di prodotti, soluzioni e servizi nel campo della "Smart Logistics", garantendo i più elevati standard di qualità, sicurezza e affidabilità. I prodotti e servizi nascono per rispondere con puntualità anche alle più specifiche esigenze, creando valore per i propri Clienti e garantendo piena compatibilità operativa con sistemi preesistenti e di prossima implementazione.
www.vitrociset.com

WiCode S.r.l. è un'azienda Italiana fondata nel 2015. In pochi anni ha raggiunto numerosi traguardi offrendo servizi e prodotti ad aziende pubbliche e private. Oggi è un punto di riferimento per la Cyber & Physical Security, CyberSpace, Social Resilience e Data Protection. Si avvale di professionisti specializzati e riesce a ricoprire ruoli sempre più all'avanguardia e complessi. Ha comprovata expertise nella progettazione, gestione e auditing in ambito Cyber & Physical Security nel settore ferroviario e infrastrutture critiche in genere. WiCode attraverso i suoi Partner è presente in varie Nazioni Europee, negli USA e in America Latina. Aree di Intervento: Ricerca e Sviluppo; Cyber Risk Assessment; Data Protection Plan; Social Engineering; Open Source Intelligence & Cyber HUMINT; ICT Resilience Auditing; Project Management; Blockchain; Virtual & Augmented reality; Smart Working
www.wicode.it

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: