ELECTRONICS DIVISION

LARIMART
a LEONARDO company

IoT a supporto delle operazioni del soldato sul campo

SEMINARIO CESMA
«IoBT, IoMT - Nuovi scenari per il teatro operativo: dalle infrastrutture critiche alle operazioni militari»

Casa dell'Aviatore
Viale dell'Università, 20

4 Maggio 2022

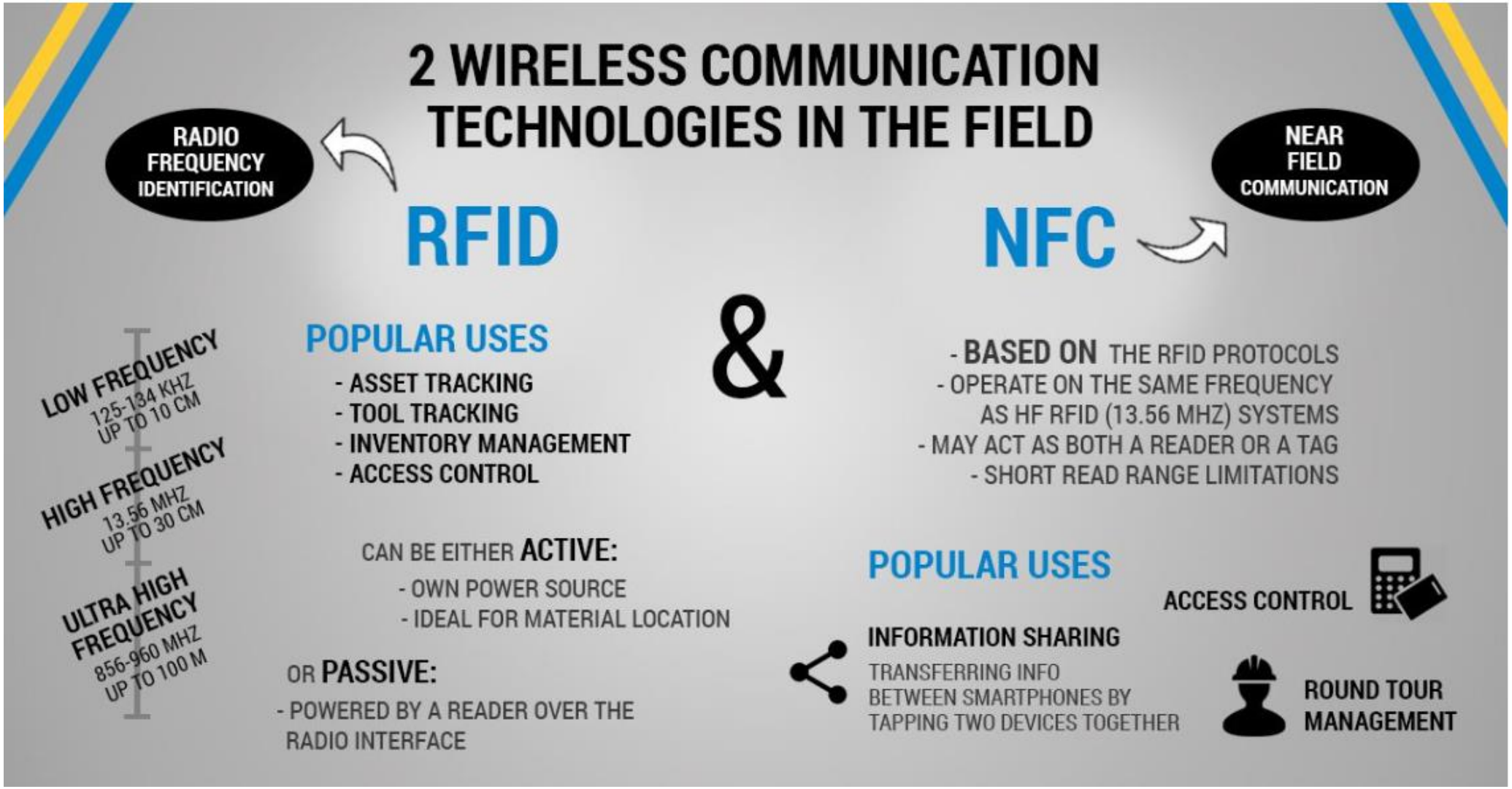
Cinzia Crostarosa

Si è creata l'esigenza operativa di sviluppare le capacità di sistemi connessi all'interno del campo di battaglia, al fine di creare una rete di "cose" (IoT) in grado di adattarsi all'evoluzione della missione.

Il termine **IoT** (*Internet of Things*), sebbene possa sembrare un neologismo, risale al 1999 quando il ricercatore del MIT Auto-ID Center, Kevin Ashton, lo utilizzò in relazione ai dispositivi **Rfid** (*Radio Frequency Identification*), che furono utilizzati durante la seconda guerra mondiale per intercettare gli aerei nemici, si sviluppa poi a partire dagli anni sessanta come derivazione a scopi civili del sistema militare a radiofrequenza di **Identification friend or foe**, ma la sua diffusione è avvenuta principalmente dagli anni novanta in poi.

Con tale locuzione si intende una **rete di dispositivi fisici**, come veicoli, elettrodomestici, telecamere, apparati di fabbrica, in senso più ampio ***smart device***, **integrati con sistemi elettronici, software, sensori, attuatori** ecc., **connessi tra di loro al fine di realizzare la comunicazione tra macchine**, funzionale allo scambio di dati e al controllo remoto.

Illustrazione della gamma di frequenza RFID e NFC e delle differenze



Fonte: ecomx.com/blog/post/rfid-vs-nfc-what-is-the-difference/

MoT – FOC of CIOC

Dopo l'Internet of Things (IoT) arriva anche il Military of Things (MoT). Lo ha spiegato il **generale Francesco Vestito**, comandante del **Comando Interforze per le Operazioni Cibernetiche** (**CIOC**) dello Stato Maggiore della Difesa (SMD) italiano. Lo ha fatto nel suo intervento al **Cyber Day** del **2018**, organizzato dal Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti (SEGREDIFE/DNA), ricordando che "*qualcuno più o meno ogni novembre visita l'Ucraina*" e che "da quelle applicazioni di gaming date ai soldati, è arrivato ai data center. Deviando treni, logistica, carburanti, quindi le azioni umane".

Il **MoT** va al di là di smartphones, frigoriferi smart e sensoristica. "Non ci sono più obiettivi militari o civili, ma obiettivi nel mondo civile – ha ricordato l'alto ufficiale – Noi dobbiamo essere pronti a supportarlo". Con questo obiettivo è nato il **CIOC**. => **Creato nel settembre del 2017, che ha raggiunto la sua Full Operational Capability (FOC) nel 2020.**

Le città quindi, protagoniste dello sviluppo della rete di quinta generazione (5G) e dell'IoT, rappresentano, per il comparto militare, un teatro all'interno del quale l'acquisizione di una completa consapevolezza situazionale (***situational awareness***) è resa più difficile proprio dalla presenza di una ingente mole di smart devices connessi.

Cyberspazio difensivo

Consapevolezza della situazione informatica

Polarizzazione dei Media

Social Media

Cyber Intel

Aspetti legali

Infrastrutture critiche

Cyberspazio offensivo

Guerra Elettronica

Sicurezza della missione

Supporto alle operazioni informative

Sistema d'arma

Effetti Cinetici

Effetti in altri domini

Device connesse per ogni individuo

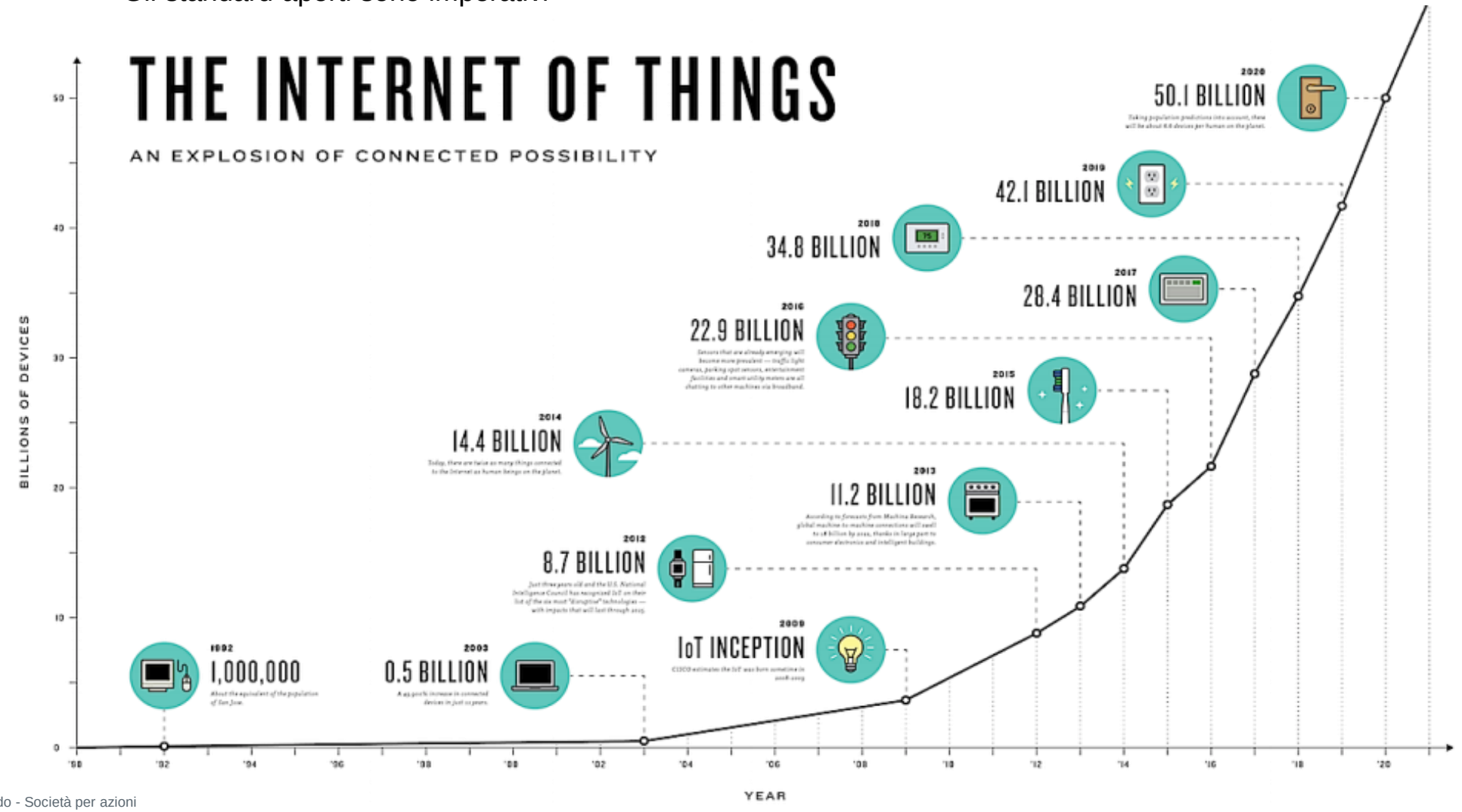
LARIMART

Popolazione	6.3 Bilioni	6.8 Bilioni	7.2 Bilioni	7.6 Bilioni
Dispositivi Connessi	500 Milioni	12.5 Bilioni	25 Bilioni	50 Bilioni

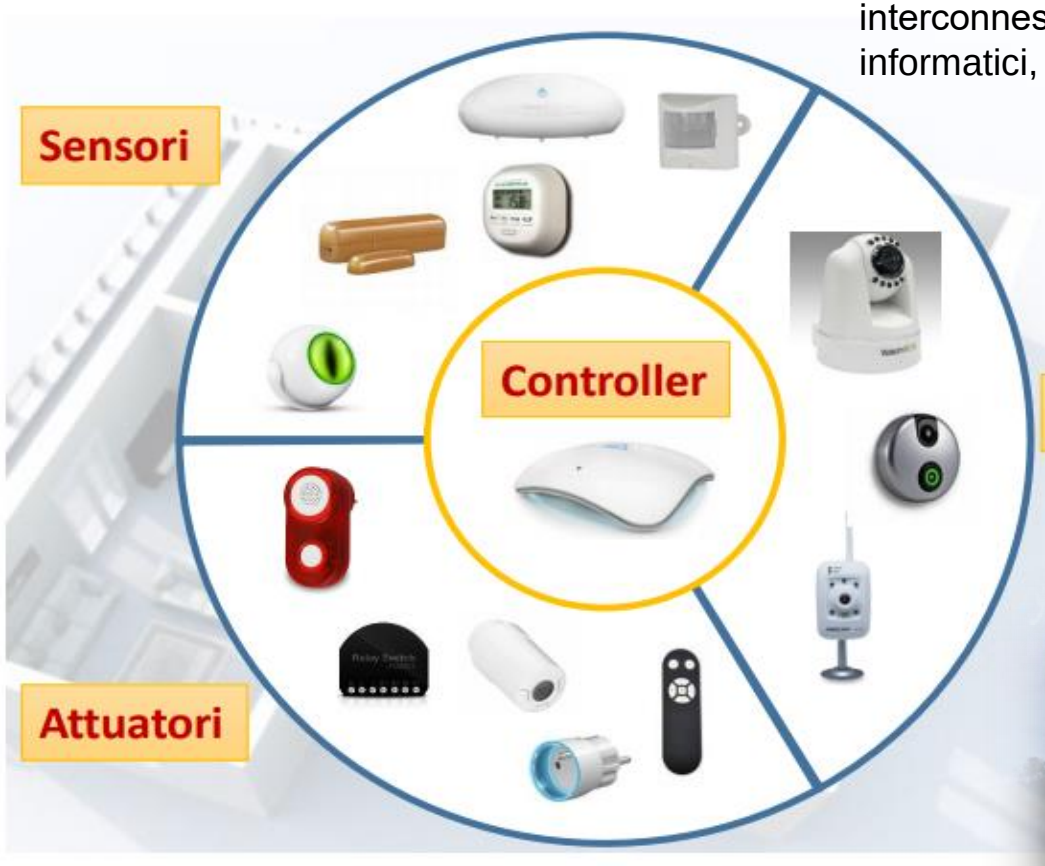
Dispositivi connessi per persona	0.08	#Device > #Persone	1.84	3.47	6.58
	2003		2010	2015	2020

“La diffusione dell'IoT che raggiunge 50 miliardi di dispositivi”

- La connessione e la bassa potenza sono fondamentali
- La distanza è essenziale
- Gli standard aperti sono imperativi



Nel mondo della domotica e dell'internet of things c'è un confine labile tra la programmazione software e il cablaggio fisico di un building, ossia sono due mondi interconnessi, uno è la parte strutturale dei cablaggi e l'altro sono gli algoritmi informatici, che comandano i sensori.



Webcam

Smartphone/Tablet

L'Internet of Things è il futuro, ma è anche la chiave del passato. Sì, la sua funzione principale può essere quella di rendere gli ambienti e gli oggetto più reattivi alle nostre esigenze attraverso l'uso di vari sensori collegati, ma sempre più spesso questi sensori vengono utilizzati per monitorare edifici e strutture.

Smart Home - Ricerca di mercato D-Link in EU

Cosa ci si aspetta da una casa connessa?

1) Protezione della propria abitazione (53%) – Italia (62%)
2) Controllo degli elettrodomestici
3) Controllo dei consumi di energia
4) Multimediale ed intrattenimento (una lieve differenza evidenziata dal campione britannico)

Quali prodotti?

1) Telecamera di sorveglianza IP (74,9%) – Italia (84,4%)
2) Smart plug (56,6%)
3) Sensori di apertura delle porte (55,9%) – Italia (62,9%)
4) Sensori di rilevamento del movimento (54,9%) – Italia (65,1%)
5) Rilevatori di fumo (53,7%)
6) Controllo del riscaldamento (53,2%)

IoT Research Study – 2014 Report by HP Fortify

Privacy	80% raised privacy concerns regarding the collection of data such as name, address, data of birth, health information, credit card numbers
Authorization	80% failed to require passwords of sufficient complexity and length with most allowing passwords such as “1234” or “123456.”
Encryption	70% did not encrypt communications to the internet and local network, while 50% of their mobile application performer unencrypted communications to the cloud, internet and local network
Web Interface	60% raised security concerns with their user interfaces such as persistent XSS, poor session management, weak default credentials and credentials transmitted in clear text
Software	60% did not use encryption when downloading software updates – some downloads cloud even be intercepted, extracted and mounted, allowing the full code to be viewed or modified

L’indagine ha esaminato 10 (*) dei dispositivi IoT più comuni avvalendosi di una combinazione di test manuali e strumenti automatizzati per valutare dispositivi e relativi componenti in base ai criteri Owasp (Open Web Application Security Project) Internet of Things Top 10 e alle vulnerabilità specifiche associate a ciascuna delle 10 categorie principali.

Fonte: https://www.hp.com/us-en/hp-news/press-release.html?id=1744676#.YmqoddpBw2w

(*) Smart Home Speaker: assistenti vocali intelligenti con cui dialogare e svolgere infinite attività. Hanno avuto negli ultimi anni un vero e proprio boom e per moltissimi di noi sono irrinunciabili per gestire in casa l’illuminazione, la climatizzazione, gli elettrodomestici e le attività di routine e di svago.

(*) Smart Car: delle auto in grado di comunicare informazioni in tempo reale, connettersi con altri veicoli e reagire all’ambiente circostante. Semplificano la guida del conducente, prevengono gli incidenti migliorando la sicurezza stradale e riducono i consumi.

(*) Smart TV: un televisore con cui connettersi direttamente alle piattaforme streaming e alle applicazioni, nonché agli altri dispositivi dotati di una connessione a Internet.

(*) Smart Watch: orologi intelligenti da collegare al proprio smartphone per visualizzare messaggi, ricevere ed eseguire chiamate, ricevere informazioni sul meteo, ascoltare musica, registrare le proprie prestazioni atletiche e monitorare sonno e battito cardiaco.

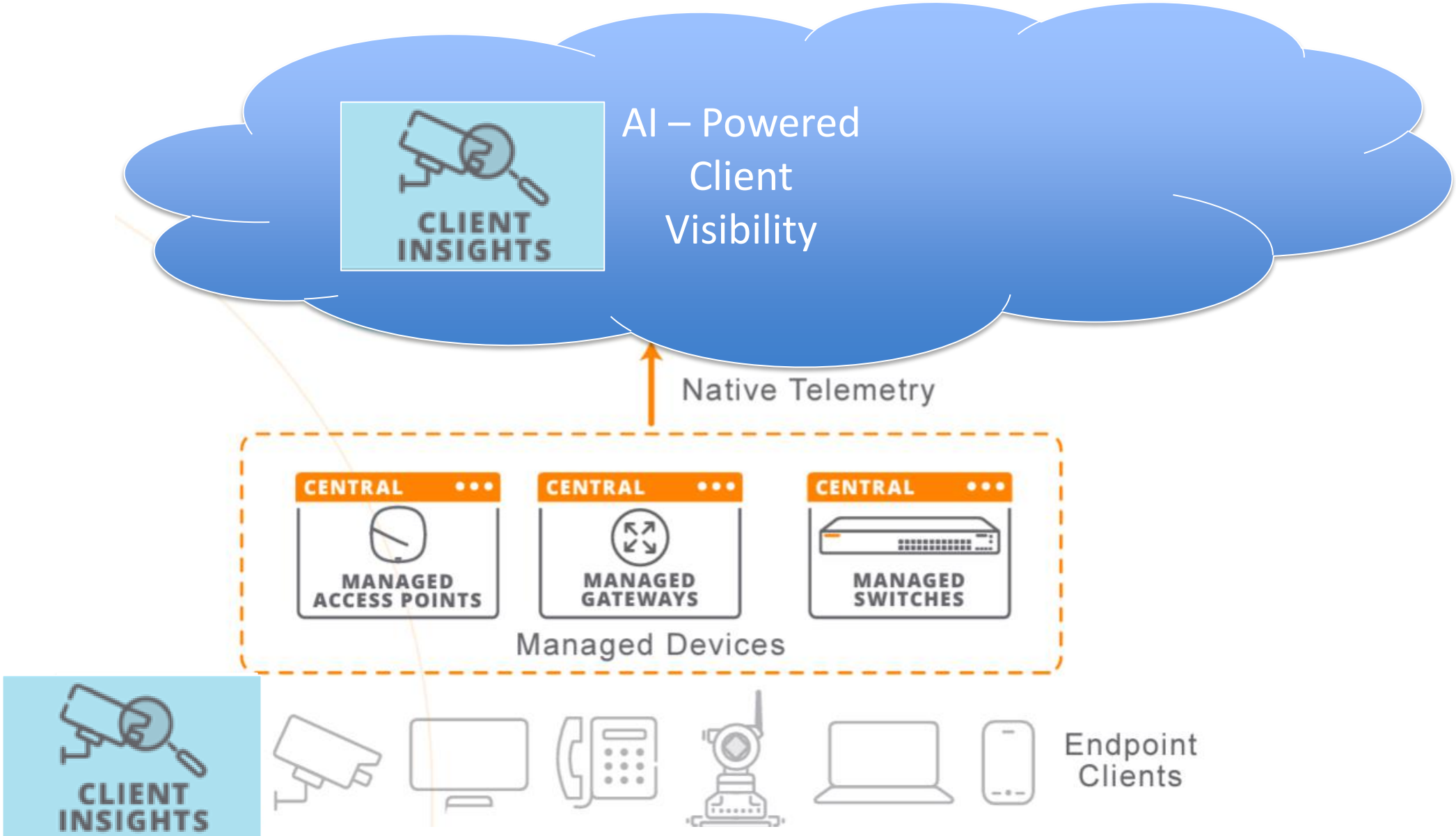
(*) Smart Factory: fondamentale nel settore dell’industria 4.0, consente il controllo dell’avanzamento della produzione, la gestione della sicurezza sul lavoro, la manutenzione, il controllo qualità, la movimentazione dei materiali e la gestione dei rifiuti.

L’addio al portafoglio: ecco come

Rendere o meno disponibile **il servizio chiamato Identity Credential** sui propri prodotti sarà una scelta dei singoli produttori di telefoni, con l’idea però che una caratteristica di questo genere rappresenta un vantaggio competitivo enorme rispetto alla concorrenza, che non l’avrà a disposizione. Come è facile capire dal nostro quotidiano fatto di tante tessere di plastica o addirittura di documenti cartacei, ancora grandemente diffusi in Italia, si tratta di una ***killer application***. Di un servizio talmente **utile da poter essere dirimente all’atto di scegliere un nuovo telefono**. C’è già molto fermento negli Stati Uniti (*dove già esiste l’app Mobile Passport, valida solo in ingresso*), **per l’Europa ci vorrà un po’ più di tempo**. Ma ci arriveremo. Così come arriveremo a legare la validità dei nostri documenti ai **dati biometrici conservati sul nostro telefono**, in modo che non solo i dati sensibili saranno protetti, ma anche la certezza della validità di questi.

Un primo rudimentale esempio è l’ attuale APP IMMUNI, su cui si può caricare il Green Pass.

Esempi di SISTEMI on the shelf dotati di AI



Fonte: https://www.arubanetworks.com/resource/iot-operations-at-a-glance/

Riconoscimento facciale ed Artificial Intelligence

Rischi Cyber: Minaccia e Vulnerabilità

R (rischio) rappresenta il rischio connesso con un particolare attacco in **un determinato luogo**

M (minaccia) rappresenta la probabilità che venga tentato un particolare attacco (1…N) in quel determinato luogo.

V (vulnerabilità) rappresenta la probabilità che una minaccia venga attuata con successo a causa di una debolezza (1…M) nella difesa dell'obiettivo

$$R_{luogo,N,M}(t) = f\left(M\left(\begin{matrix}1\\2\\\dots\\N\end{matrix}\right); V\left(\begin{matrix}1\\2\\\dots\\M\end{matrix}\right); E\left(IC\ \text{☺}\right)\right)$$

E (esposizione) rappresenta il **potenziale** danno dell'attacco, e corrisponde alla porzione delle categorie "Moteff" quantificabile oggettivamente: beni infrastrutturali presenti, popolazione

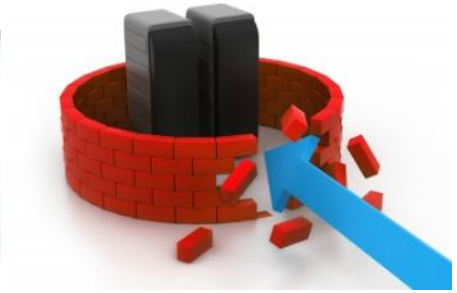
Comprende due aspetti:

Difficoltà di attuazione
- Disponibilità della tecnica
- Costo
- Difficoltà logistica
- Know how
- Motivazione

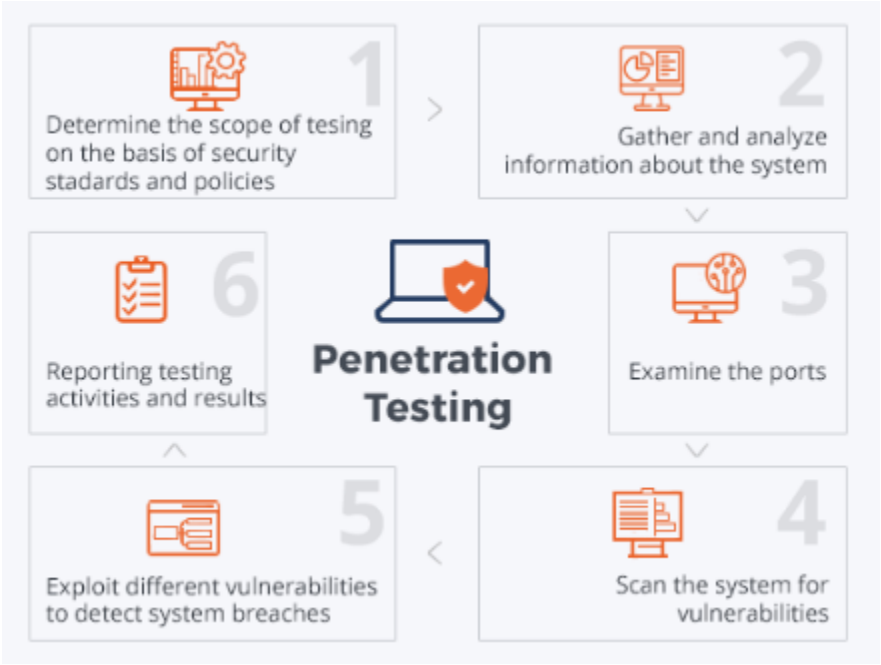
} inerenti all'attaccante

Attrattività dell'obiettivo

Penetration Test



I muri di difesa per quanto possano essere resistenti potrebbero essere aggirati come fecero i greci con il «cavallo di Troia» per espugnare la città.



Si devono determinare per i sistemi le policies di Security sulle quali ci si vuole basare, in modo che si verificano le ***eventuali vulnerabilità***.

Perimetro di sicurezza nazionale

Definizione di infrastruttura Critica

Dalla Direttiva Europea 114/08 CE

«infrastruttura critica» **un elemento, un sistema o parte di questo** ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni;

Le Sale Operative e Posti Comando Militari sono delle Infrastrutture Critiche per il paese

novembre 2019

Disegno di legge: S. 1570. – «Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n.105, recante disposizioni urgenti in materia di **perimetro di sicurezza nazionale Cibernetica»** (approvato dalla Camera e modificato dal Senato)

Per far fronte ai **rischi della sicurezza informatica in Europa**, il 27 giugno 2019 è entrato in vigore il "**Cybersecurity Act**", che è un regolamento che assegna all'agenzia comunitaria per la sicurezza informatica (**ENISA**) nuovi compiti e risorse per proteggere gli utenti dagli attacchi hacker, anche grazie a una *certificazione per gli oggetti connessi.*

CONTROL ROOM

PUBLIC SAFETY

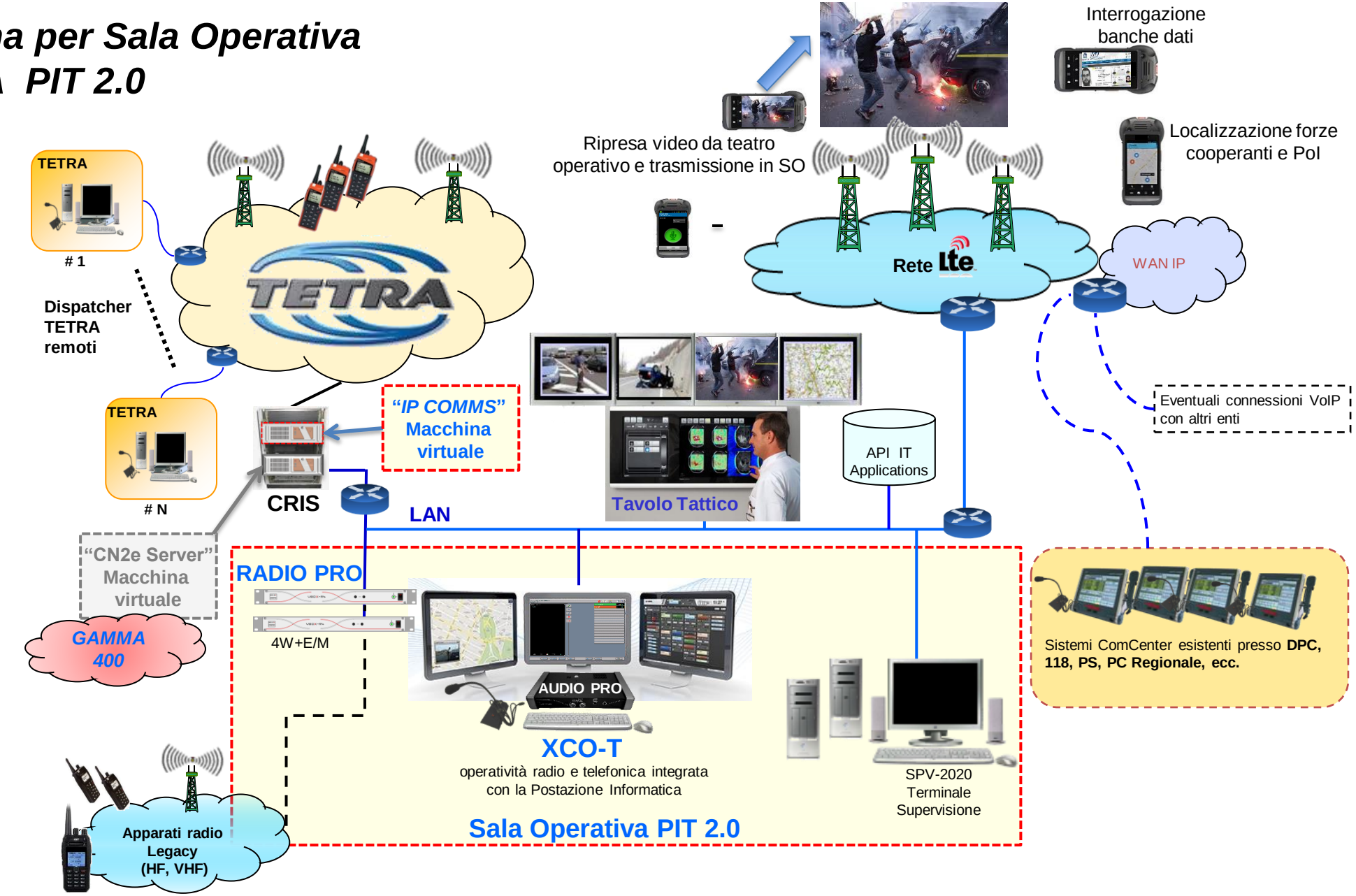
C2 SITUATION AWARENESS

- Autorità
- Governo
- Ambiente
- Difesa
- Sicurezza
- Trasporto
- Energia
- Imprese

RESOURCES

OTHER AGENCIES

Sistema per Sala Operativa TETRA PIT 2.0

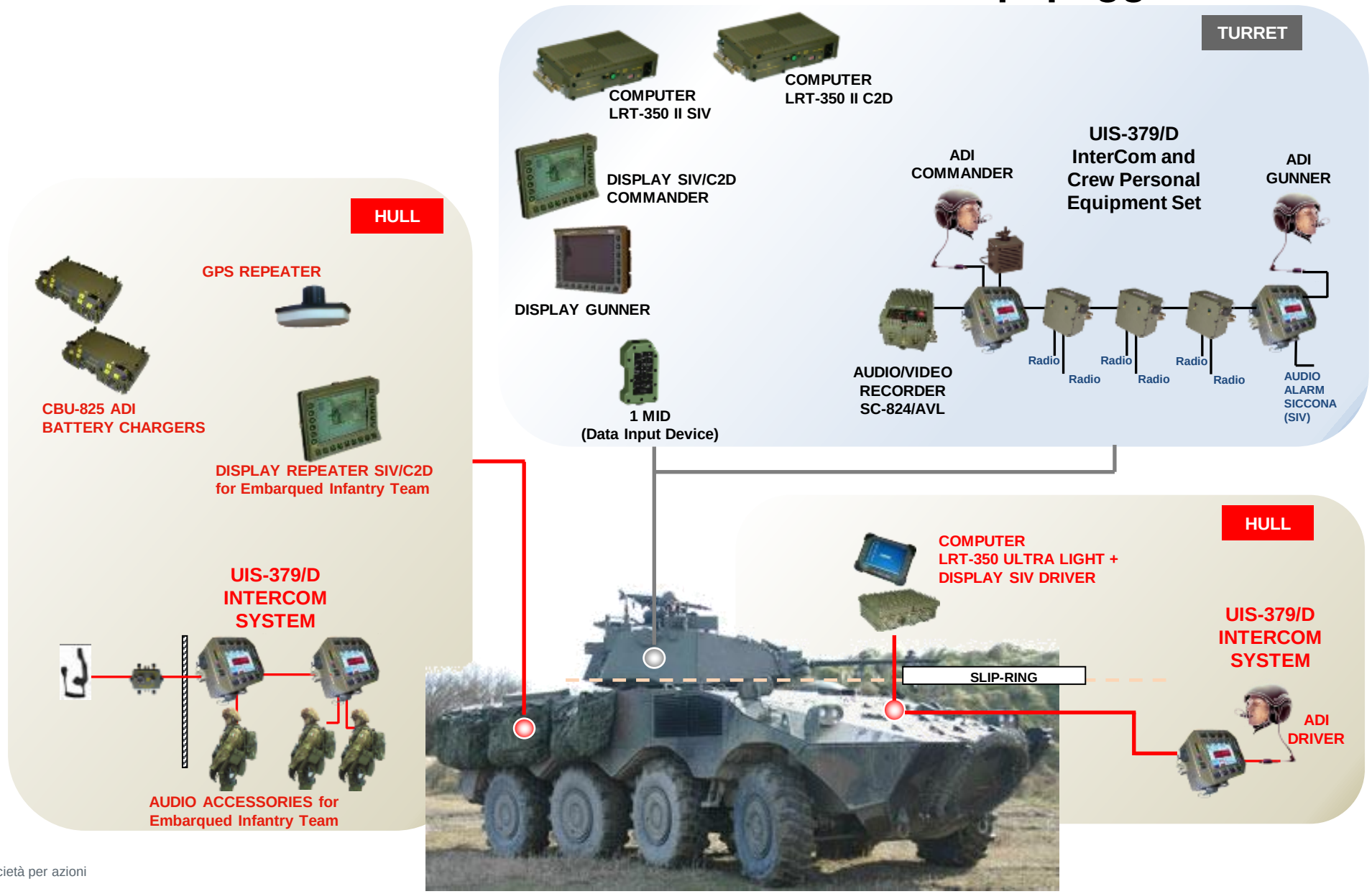


UIS-379/D Digital Intercom System

SC-824/OPRR – Caratteristiche della Radio incorporata della squadra

Platoon

VBM Freccia Combat – Sistemi Larimart di Equipaggiamento



Sistemi Militari IP COMMS

L'IP COMMS è il sistema LARIMART concepito per controllare e gestire le molteplici comunicazioni che avvengono in un Posto di Comando di alto livello.
Il sistema IP COMMS rappresenta un valore aggiunto fondamentale per le esigenze operative di un centro di comando in quanto è in grado di centralizzare tutte le operazioni di comunicazione del singolo utente.
L'architettura IP COMMS progettata facilita l'integrazione con altri sistemi/asset esistenti, aumentando così significativamente l'interoperabilità con il mondo legacy.

Capacità

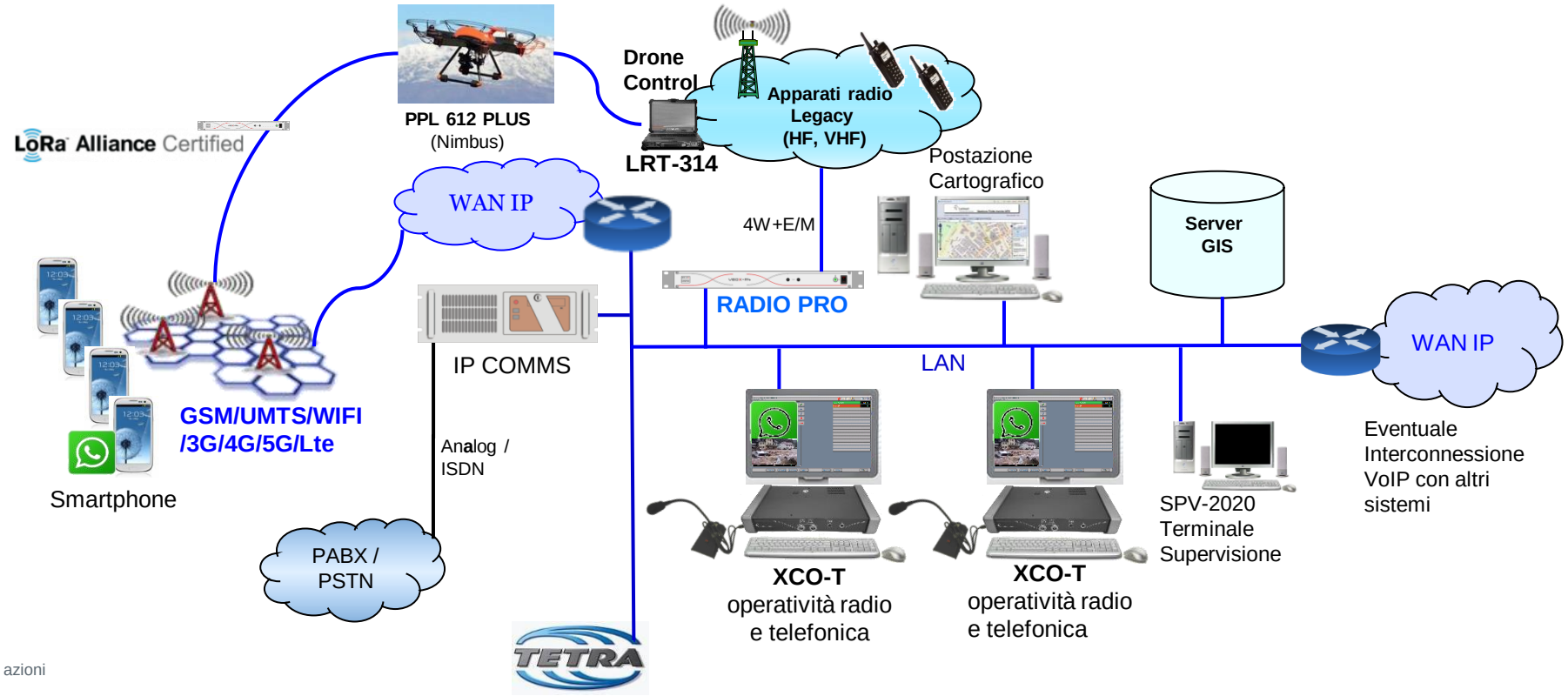
Le caratteristiche principali dell'IP COMMS sono:

- *Centralizzazione delle risorse radio e delle linee telefoniche*
- *Tecnologia Full IP*
- *Architettura scalabile, modulare e flessibile*
- *Registrazione digitale delle comunicazioni che avvengono negli HQ*
- *Console operatore facili da usare e touch-screen*
- *Comunicazioni punto a punto e conferenze multipunto*
- *Comunicazioni simultanee su diversi canali radio*
- *Interoperabilità tra diverse tecnologie radio*
- *Apertura dell'architettura verso miglioramenti/evoluzioni*

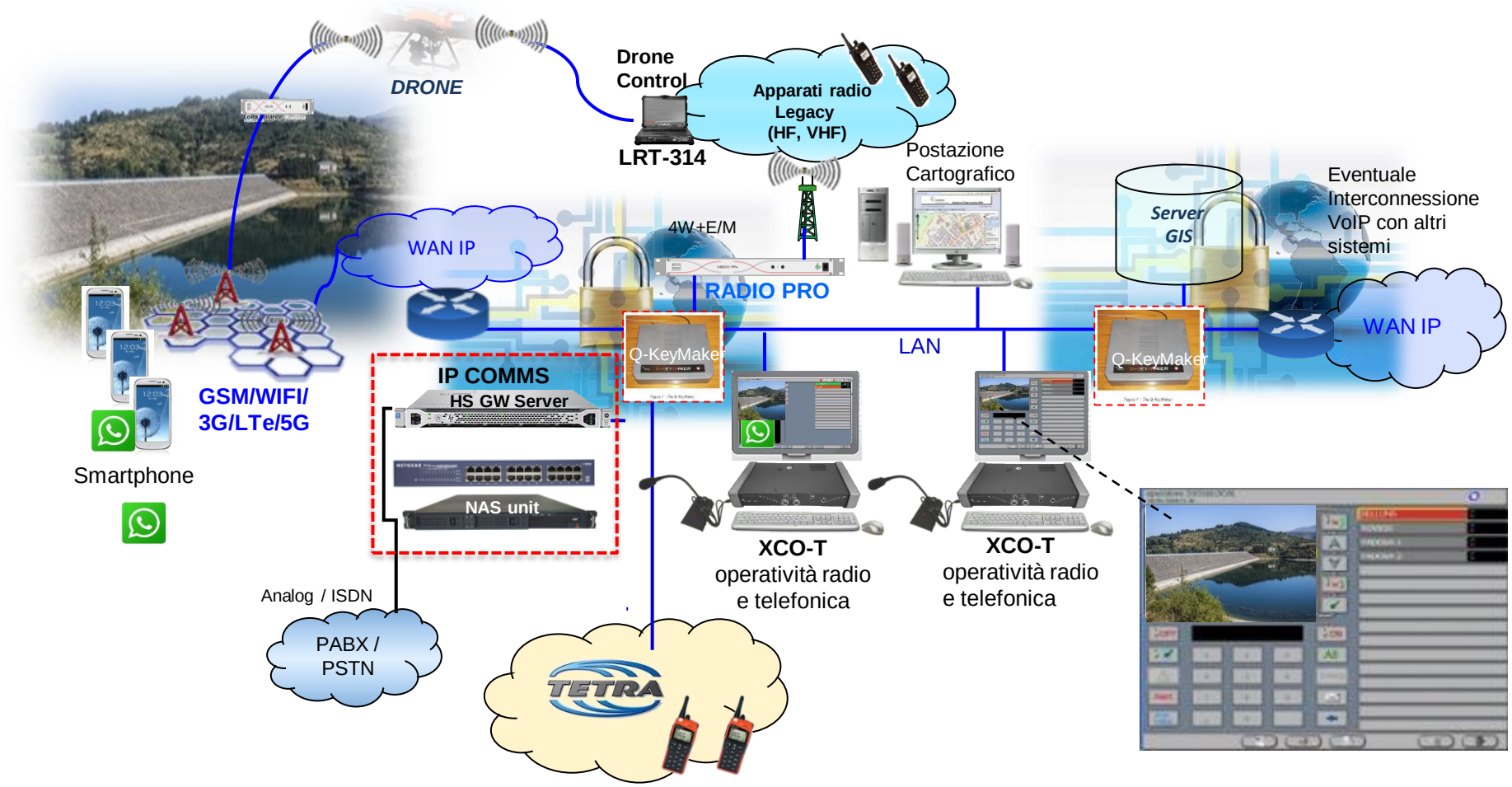
COM CENTER & «Augmented Reality»: esempi operativi con schema di sistema

- Un agente della Forestale vedendo semplicemente tramite gli “Glasses” le fiamme nel bosco può comunicare alla Centrale Operativa l’esatta posizione dell’incendio con una foto (avendo il servizio di «Whatsapp»), in modo tale che possano arrivare il prima possibile i soccorsi.

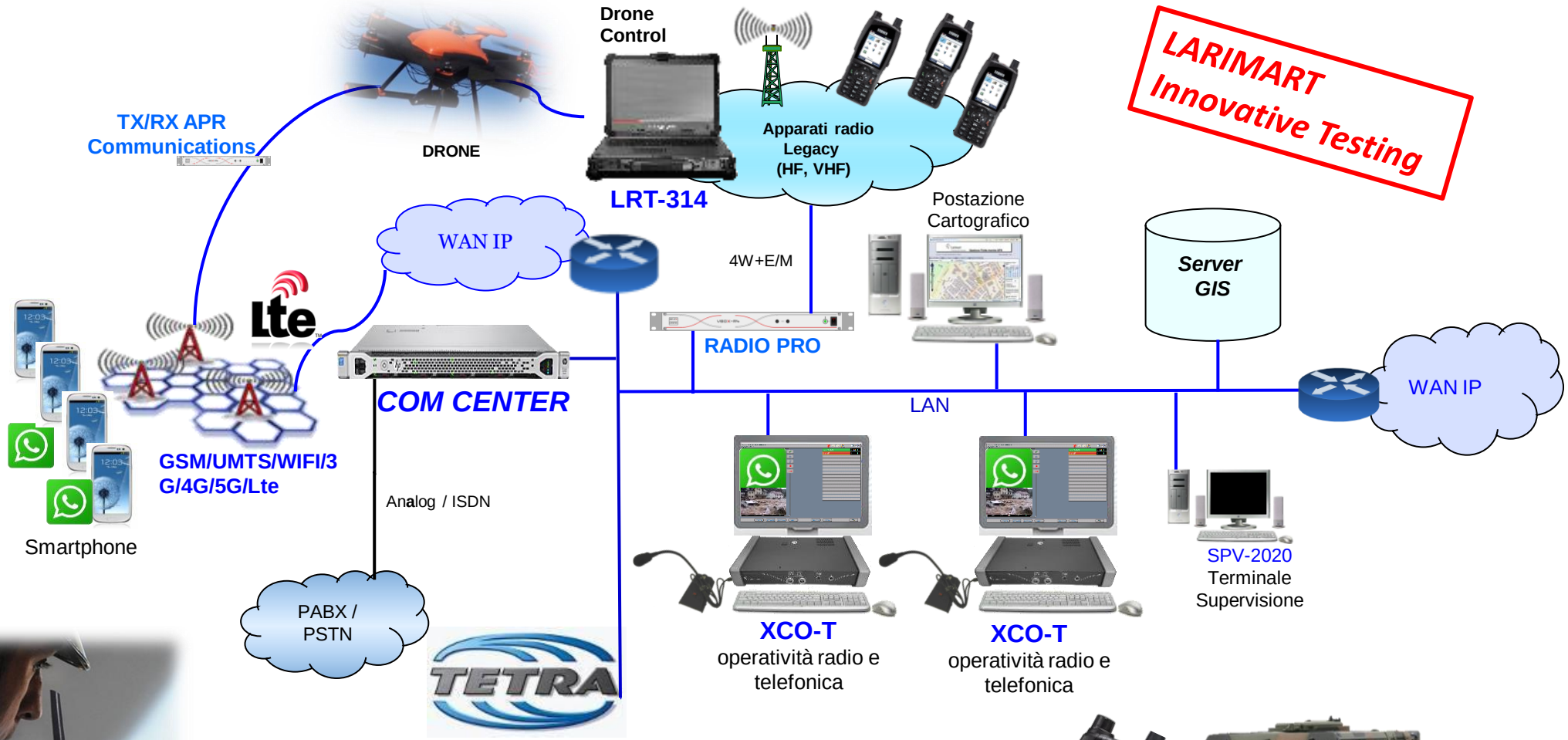
- Un poliziotto ad un posto di blocco sulla strada, vedendo una persona sospetta, con gli "Smart Glasses" può inviare la foto con «Whatsapp», in modo che nella sala operativa possono accedere ai database, così controllano se il sospetto è ricercato dalla Polizia.



Esempio di Sala Situazione per monitoraggio di un sito critico: ad esempio una diga, un cantiere di vaste proporzioni, un sito petrolifero, etc…

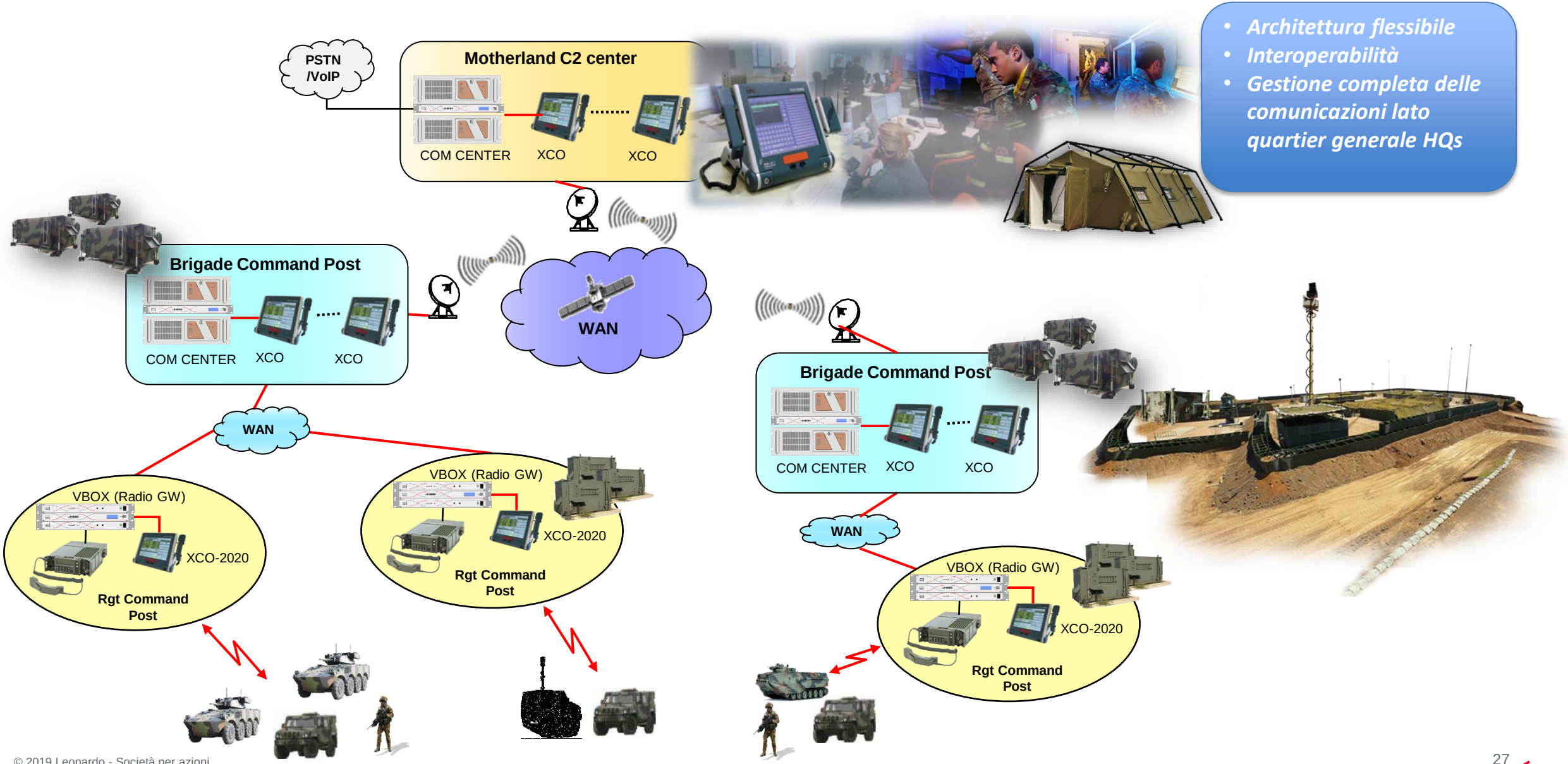


DUAL USE : COM CENTER & Social Networking Apps



«OPERAZIONE STRADE SICURE»

DUAL USE : Sale Operative Militari & Controllo Confini



- *Architettura flessibile*
- *Interoperabilità*
- *Gestione completa delle comunicazioni lato quartier generale HQs*

L'importante obiettivo raggiunto per l'Equipaggiamento del Soldato è il risultato di anni di studi, sviluppi e sperimentazioni condotti nel Programma Soldato Futuro (ora "**Soldato Sicuro**") dall'Esercito Italiano e frutto della consolidata sinergia e la piena condivisione d'intenti tra lo Stato Maggiore dell'Esercito, la Direzione Armamenti Terrestri e l'industria nazionale.

È in tale scenario che si instaura il concetto di **IoMT** (*Internet of Military Things*) o **IoBT** (*Internet of Battlefield Things*) o, ancora più esplicitamente, **l'internet delle cose sul campo di battaglia**.

Tale concetto consiste nella possibilità di **aumentare la consapevolezza situazionale degli operatori impegnati sul campo** fornendo loro, attraverso una rete di sensori e dispositivi interconnessi in grado di restituire dati e informazioni utili all'operazione, una **percezione extrasensoriale dell'ambiente circostante** aumentando così le capacità di intelligence, sorveglianza, ricognizione, implementando contestualmente i sistemi **IFF** (***Identification Friend or Foe***).

Lo **US Army Research Laboratory** e un consorzio di Universita' americane sta sviluppando una ricerca denominata **IoBT REIGN** (***Internet of Battlerfield Research on Evolving Intelligent Goal-Driven Networks***) lo scopo della ricerca è indagare e sfruttare sistemi connessi sul campo di battaglia.

Le reali applicazioni dell'IoBT nell'ambito militare sono diverse:

- Implementazione della capacità **C5ISR (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance)**, al fine di permettere la loro disseminazione a vari livelli della catena di comando e fornire così una **COP** (**Common Operational Picture**) completa.
- Implementare sistemi logistici dove l'impiego una serie di ***sensori montati su aerei, UAV, satelliti e navi*** contribuiranno a *monitorare i movimenti ed i traffici marittimi in ampie aree*.
- L'***Internet of Battlefield Things*** sarà utile anche per ***monitorare le condizioni fisiche dei soldati con sensori incorporati nelle uniformi dei militari***.
- Svolgere attività di *manutenzione predittiva dei vari dispositivi attraverso l'analisi dei big data* relativi alle condizioni delle piattaforme, creando così un vantaggio funzionale ed un importante risparmio di costi.

L'IoBT deve sfruttare adeguatamente tutte le reti: blu, grigia e rossa, ha affermato **Stephen Russell**, **capo** del ramo di elaborazione delle informazioni sul campo di battaglia **dell'Army Research Lab**. In questo costrutto, le reti blu sono sicure e di proprietà militare; le reti grigie sono spesso reti civili dall'affidabilità incerta; e le reti rosse sono reti avversarie.

Russell ha sottolineato che lo sforzo di sfruttare le capacità uniche di un campo di battaglia in rete sarà un **problema interdisciplinare** che riunirà *ricercatori in informatica cyber-fisica, teoria dell'informazione, sicurezza, metodi formali, apprendimento automatico, networking, controllo e scienze cognitive*

Partecipazione a ricerche e studi internazionali

2015

RHEINMETALL DEFENCE
Fraunhofer ICT
DNV·GL
Larimart
A Finmeccanica Company

2016-17

gmv
TNO innovation for life
RHEINMETALL DEFENCE
LARIMART a LEONARDO company

2018-21

RHEINMETALL GROUP
LEONARDO
SAAB
indra
gmv
LARIMART a LEONARDO company
iTTi e-technologies & business
TNO innovation for life
tekever AEROSPACE | DEFENSE | SECURITY
EUROPEAN DEFENCE AGENCY

Equipaggiamento del Soldato

PBI-G12-IT Ballistic Vest and Casco CI-9/89-Evo:

- Il risultato di uno sforzo congiunto tra IT MoD e Industria.
- NIJ-0101.06 e STANAG 2920 completamente conformi
- Attualmente in servizio per l'Esercito Italiano e Forze da Sbarco Italiane.

Werable device integrati con sensori nel Sistema di protezione del soldato per prevenire e/o monitorare :

- **Minaccia CBRN**
- **Funzioni vitali del soldato tramite smartphone oppure smart tessuti per rilevarne stato di salute e prestazioni**
- **Diagnosi e riparazioni da remoto: manutenzione predittiva dei dispositivi**
- **Localizzazione tramite GPS oppure sistemi WI-FI**

Equipaggiamento del Soldato: Soluzioni SIC

Protezioni CBRN

Giubbetto Anti Proiettile PBI-G12-IT (tramite consorzio PBI)

LRT-331 tablet (basato su COTS Panasonic FZ-M1)

Cuffia Acustica Protettiva H-149

Intra Team Intercom (ITI)

(Doppio PTT Radio)

1 USB + PWR

2

3 ETH + PWR

4 PWR

ITA HUB

SDR HH-E (LDO)

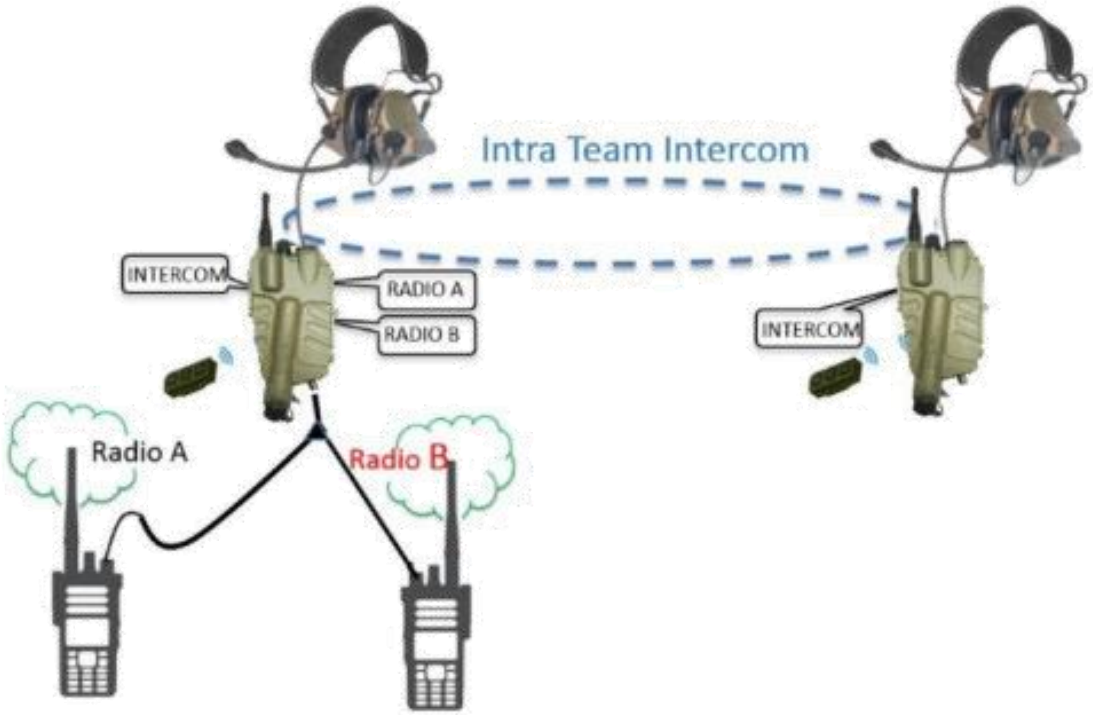
IP CAM

UAV

LINX

GPS SAASM (LDO)

ITI (Intra Team Intercom) Soldier Systems
“Soluzioni personali per i membri dell'equipaggio e dei soldati”



Vista digitale del fucile

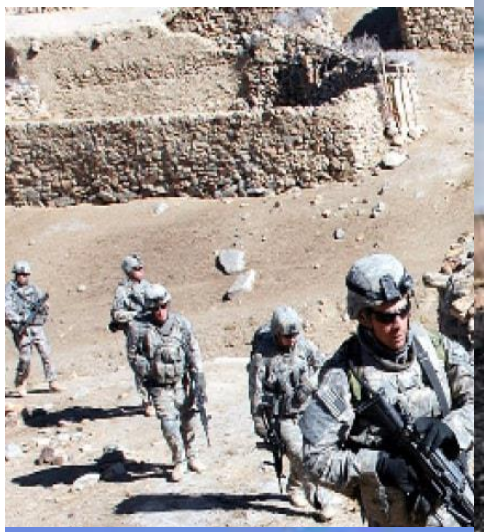
Mentre la nuova tecnologia significava che i soldati avrebbero dovuto trasportare più equipaggiamenti, cosa che di solito non provoca acclamazioni da parte dei soldati, anche se molte delle sue funzioni potrebbero contribuire alla sicurezza.

- Un ***oculare*** pieghevole potrebbe servire come ***monitor di un computer***.
- Il **monitor** potrebbe *visualizzare mappe elettroniche con posizioni amichevoli* chiaramente contrassegnate, che potrebbe anche collegarsi alla **vista digitale del fucile**, permettendo ai soldati di tenere una pistola dietro l'angolo e vedere cosa c'è oltre senza presentare la loro testa come bersaglio.
- La ***vista e il monitor*** potrebbero anche servire da ***potente obiettivo***, fornendo fino a 12 ingrandimenti.

“***Una tecnologia a vibrazione per indicare il giusto percorso alle pattuglie in azione***”

Soldati telecomandati - Per i soldati del futuro gli scienziati americani dell’*Army Research Office* stanno mettendo a punto un nuovo dispositivo tecnologico: una cintura tattica, che include un trasmettitore GPS e indica la direzione ai soldati, consentendo ai comandanti di guidarli sul campo come se fossero telecomandati. Infatti, durante le azioni, è ritenuto pericolo e scomodo cercare la propria posizione su un normale dispositivo GPS dotato di display.

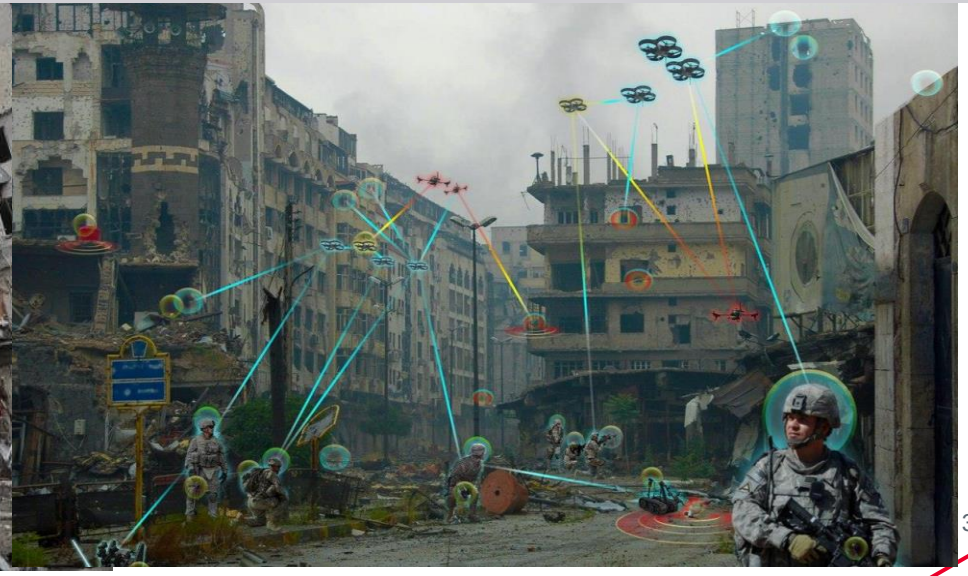
Si segue la vibrazione => **La speciale cintura GPS** include dei motori vibranti che indicano, con una vibrazione da telefonino o da controller per i videogames, la giusta direzione ai *soldati hi-tech*: la cintura ha 8 di questi sensori, con intervalli di 45 gradi, una volta indicato il ***waypoint*** dal comando, il soldato riceve l’input con una lieve pulsazione: andare più a destra, più a sinistra, ad ore 13 e via dicendo.



L'**esoscheletro** leggero può essere realizzato in fibra di carbonio ed è in grado di alleviare efficacemente l'apparato muscolo-scheletrico di un combattente, facilitando il trasporto di carichi fino a 50 kg (equipaggiamento speciale, zaini raider, armi e munizioni). Un tale dispositivo è semplicemente insostituibile quando si effettuano lunghe marce (specialmente su terreni accidentati) o operazioni di assalto.
Esternamente, un esoscheletro passivo è un dispositivo meccanico a cerniera a leva, che imita le articolazioni umane.
Un tale ***esoscheletro*** è chiamato ***passivo***, poiché non ha servi, alimentatori e vari componenti elettronici e sensori nel suo design. Questo rende il design più semplice, affidabile e leggero. L'esoscheletro passivo è facile da usare e completamente autonomo, mentre il peso del kit non deve superare 6,5 kg.
Diversamente un ***esoscheletro attivo*** potrebbe alloggiare dei sensori per rilevare lo stato di salute o affaticamento dei muscoli del soldato.

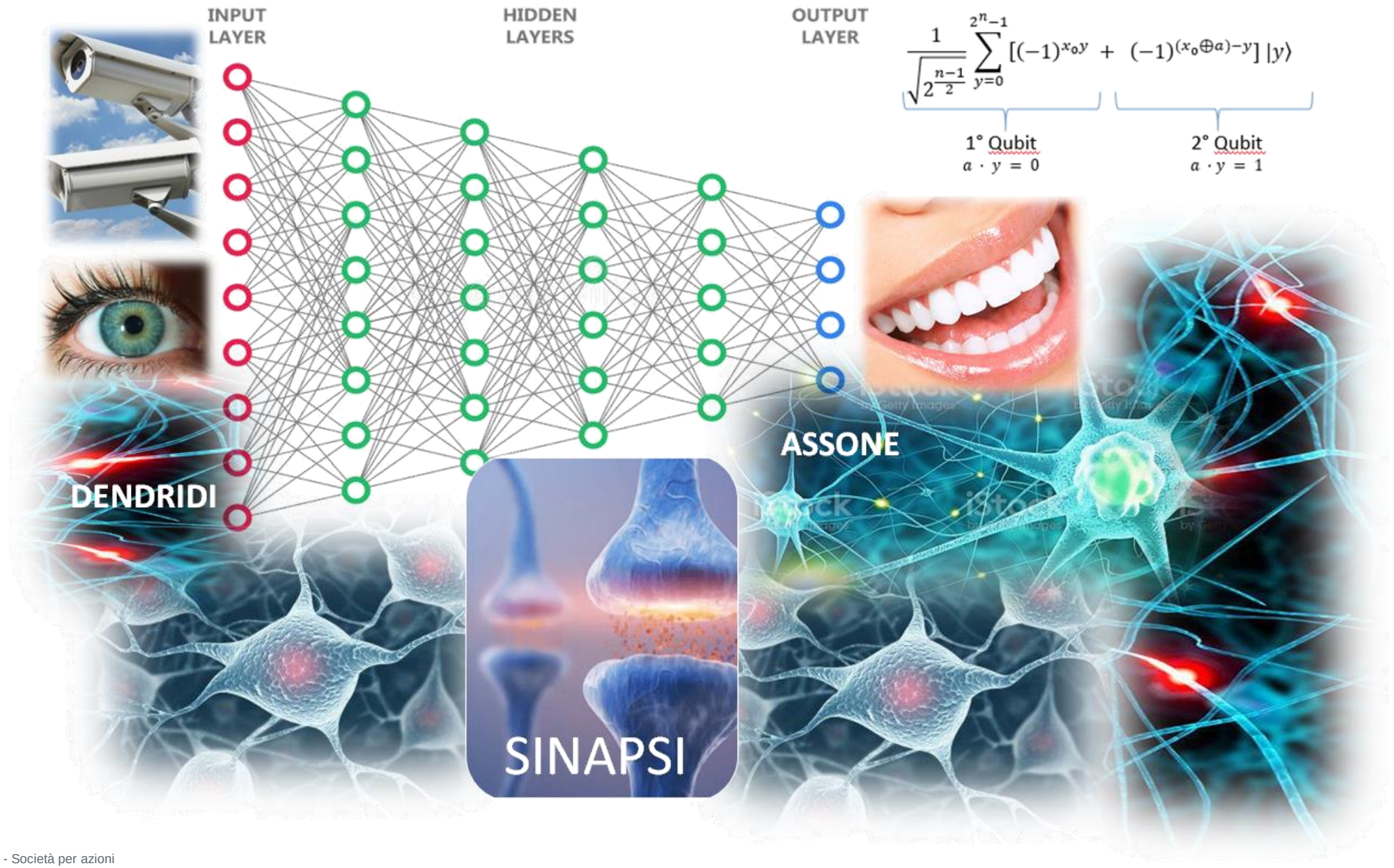
IoT & nuovi teatri operativi urbani

Mentre nulla rimpiazzerà mai le capacità e gli allenamenti nativi di un soldato, ci sono diversi gadget militari destinati a migliorare la sicurezza anche in condizioni di battaglia. E nell'era moderna del combattimento, alcune battaglie sono combattute non su un campo o in trincea ma all'interno di città e paesi, quindi i soldati devono anche considerare la sicurezza dei civili.
Molti dei gadget che portano alcuni soldati sono legati alla raccolta e all'analisi delle informazioni. Usando una combinazione di sensori, telecamere, trasmettitori e display, i soldati hanno a disposizione più informazioni di quante ne abbiano mai avute.
Ma quell'attrezzatura migliora la sicurezza dei soldati e dei civili?
Sorprendentemente, la risposta non è semplice. Nonostante abbia investito più di mezzo miliardo di dollari in un pacchetto di apparecchiature digitali noto come il ***progetto Land Warrior***, l'Esercito degli Stati Uniti ha visto solo un limitato successo nell'integrare sistemi di comunicazione ad alta tecnologia con gadget destinati al soldato medio, *in quanto si deve associare anche il processamento dei dati raccolti tramite reti ad esempio dotate di AI.*



Sebbene la possibilità di connettere una serie di dispositivi ad una rete militare costituisca un vantaggio per le moderne forze armate in termini di gestione informativa, conduzione delle operazioni, logistica, asset management e monitoraggio del personale, sussistono comunque delle problematiche connesse principalmente alla sicurezza della rete in oggetto derivanti da una serie di cyber vulnerabilità come, ad esempio, la possibilità che dispositivi non autorizzati, o non sicuri, si connettano alla rete militare.

I tentativi di intrusione all'interno di reti militari o governative sono tantissimi e in un contesto operativo la possibilità, che le informazioni (spesso riservate) vengano dirottate, le comunicazioni intercettate, o i vari sensori e smart devices sottoposti a cyber attacks, deve essere ridotta al minimo.
Attualmente sono allo studio anche ulteriori sistemi fondati, ad esempio, sullo sviluppo dell'**AI** attraverso algoritmi di apprendimento automatico più robusti basati su **RETI NEURALI** in grado di riconoscere eventuali tentativi di "*deception*" o "resistere" ad attacchi informatici ed exploit, oppure l'avvio di **attacchi** di negazione del servizio (DoS o DDoS).



THANK **YOU**
FOR YOUR ATTENTION

Cinzia Crostarosa
Intl. & Naval & Protection Sales
Larimart S.p.A.
Direzione e coordinamento di Leonardo S.pA.
Via di Torrevecchia 12 – 00168 Roma

tel.: +39 06 30343397
fax: +39 06 30343387
e-mail: cinzia.crostarosa@larimart.it
pec: larimart@legalmail.it
www.larimart.it