"SECURITY & SISTEMI DI DIFESA ELETTRONICA

A. BRANCALEONI (Elettronica SpA)

A.C. BOSCARINO; C. DI VIRGILIO; M. MAZZELLI

INTRODUZIONE

- La spinta maggiore nello sviluppo degli APR è stata fin qui data dal loro sempre crescente impiego in situazioni di conflitto, con scelte tecnologiche ed architetturali figlie di questo impiego prevalente

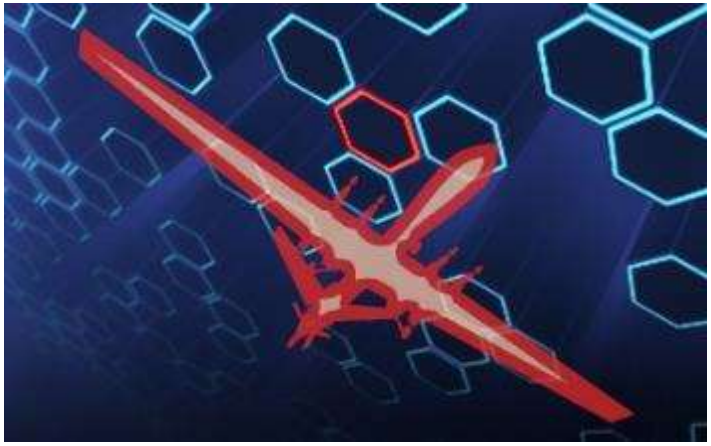
- L'impiego duale degli APR in spazi aerei non segregati rende necessario:
  - Analisi dell'affidabilità e dell'interoperabilità richiesta ai diversi e nuovi sistemi ed operatori coinvolti
  - Analisi dei requisiti in termini di security e di safety, della capacità di handover del pilota e di connessione con l'ambiente ATM
- E' prevedibile che l'impiego duale degli APR in ambienti non segregati comporterà una particolare attenzione a tutti gli aspetti inerenti la Cyber Security, sia per il segmento di bordo che per quello di terra
- E' prevedibile un impiego duale di payload di Difesa Elettronica per missioni di sorveglianza dello spettro elettromagnetico

IL TEMA DELLA SECURITY

- Il tema della security rappresenta la vera sfida per un impiego duale degli APR in tutte le classi di spazio aereo perché diverse e tante possono essere le fonti di rischio (fisico, elettronico, cyber, etc) che possono compromettere la sicurezza del volo e quindi del velivolo, del personale impiegato, degli altri utilizzatori dello spazio aereo e di tutte le terze parti
- Alcuni eventi occorsi negli ultimi anni hanno mostrato il grande impatto mediatico, economico e politico che possono avere le minacce alla sicurezza di sistemi critici, militari e non (p. es. Stuxnet, incidenti su Lockheed Martin RQ-170 Sentinel, Camcopter, SkyNet)
- Le minacce sono sempre più *blended*, mischiando attività condotte su reti *wired* e *wireless* utilizzanti dunque lo spettro elettromagnetico a radiofrequenza.
- Il 2012 ha riproposto un concetto già sviluppato anni prima noto come Cyber Electronic Warfare, che mescola elementi proveniente dalla Electronic Warfare tradizionale con quelli delle Computing Network Operations
- Con riferimento agli APR va sottolineato che, salvo alcune eccezioni come le comunicazioni di comando e controllo tipiche degli APR, tale sfida trova forte comunalità e grande possibilità di trasferimento tecnologico dall'aviazione *manned.*

SECURITY PER GLI APR

- A causa della loro intrinseca natura *war-oriented* e il loro impiego in scenari *uncontested*, gli APR presentano problemi di sicurezza rilevanti, legati a possibili interferenze e disturbi intenzionali sui link di comando e controllo tra la piattaforma e la GCS, nonché attacchi cyber portati contro la piattaforma APR, al suo SW di comando, ai sistemi di navigazione (GPS) o contro la infrastruttura di controllo di terra (GCS)



- Un APR completamente operativo presenta tre componenti fondamentali:
  - l'elemento umano
  - l'hardware sia del APR e il GCS (o qualsiasi altro elemento di controllo)
  - il software che funge da interfaccia tra l'HW e l'elemento umano e rende possibile operare con la piattaforma APR
- L'interazione tra questi tre fattori è particolarmente delicata quando si parla di effetti di attacchi condotti contro tali piattaforme.
- Si rende dunque necessaria definire una strategia di protezione dell'intera infrastruttura di rete (*wired* e *wireless*) che supporta le missioni degli APR.

LO SPETTRO ELETTROMAGNETICO

- Lo spettro elettromagnetico è un mezzo che offre diversi vantaggi a sistemi che vogliono comunicare senza essere vincolati da un collegamento cablato
- Svantaggi: l'ambiente elettromagnetico è accessibile liberamente, a meno di attuare delle misure di sicurezza per proteggere l'accesso al canale a radiofrequenza
- I sistemi che comunicano attraverso lo spettro elettromagnetico sono suscettibili a differenti tipi di minacce:
  - **Accidentali**: sono minacce ai sistemi/reti che avvengono in modo casuale (e.g., eventi naturali, fallimento di un sistema dovuto ad un problema hardware) o causate da errore umano
  - **Intenzionali**: sono quelle azioni causate da un attore con l'intento di rappresentare una minaccia al corretto funzionamento del sistema/rete
- Nell'ambito delle minacce intenzionali, gli attacchi possono essere raggruppati nelle seguenti famiglie:
  - danni fisici o compromissione di servizi essenziali
  - disturbi dovuti a radiazioni (EMP)
  - attacchi di rete
  - compromissione di un nodo

CARATTERISTICHE DEI LINK RADIO DEGLI APR

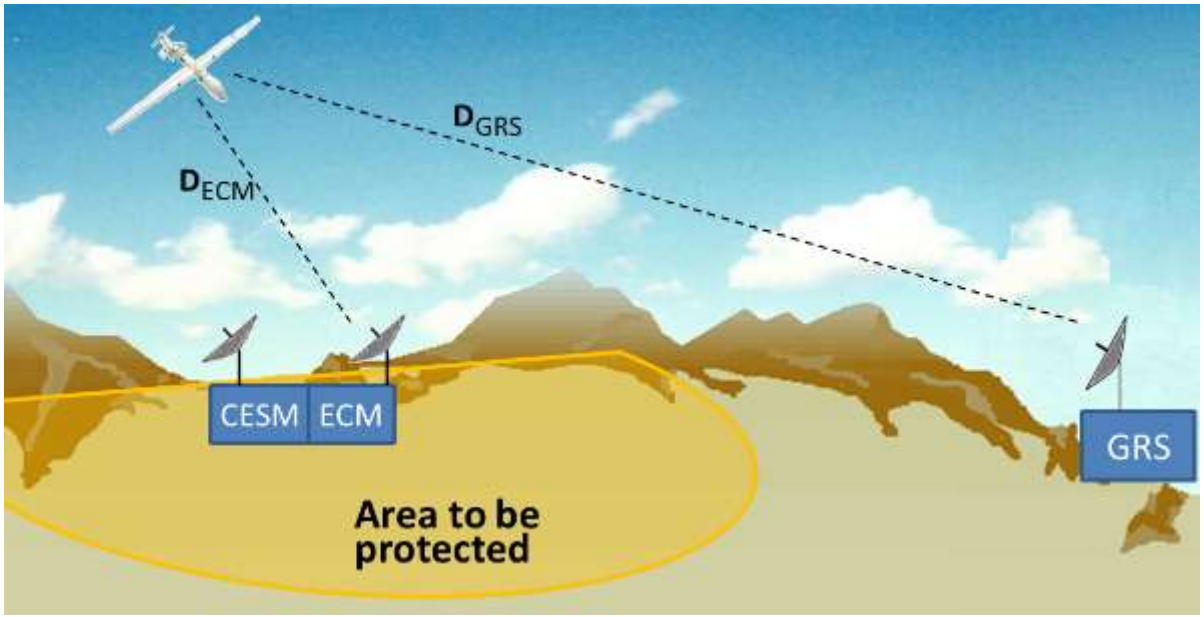
- Uno degli aspetti più critici nel "Sistema APR" è costituito dalla necessità di un controllo, costante, attraverso due collegamenti radio:
  - UP-LINK, utilizzato per trasmettere i segnali di comando, controllo e guida dell'APR dalla Ground Remote Station (GRS)
  - DOWN-LINK, per trasmettere verso la GRS:
    - Dati di volo dell'APR
    - Segnali video , data-stream elaborati dai vari sensori on-board (LIDAR, SAR, sistemi di sorveglianza elettromagnetica ELINT/COMINT)

UP-LINK		DOWN-LINK	
Band	% using	Band	% using
VHF	13%	VHF	0%
UHF	32%	UHF	17%
L	6%	L	19%
S	11%	S	13%
C	21%	C	23%

Fonte: Jane's

- Normalmente, gli APR utilizzano collegamenti radio in LOS (Line of Sight) per operare in un range compreso tra 50 e 150 km (dalla GRS).
- Per distanze superiori si utilizzano trasmissioni in BLOS (Beyond Line of Sight) mediante uso di satelliti o relay di comunicazione *airborne*

APR: ANALISI DELLE VULNERABILITA'



- Il down-link è il target preferito per la scoperta ed allarme della presenza di un APR
- Disturbo intenzionale sugli up-link, oscurando la ricezione da parte dell'APR dei segnali di comando provenienti dalla GRS
- Disturbo intenzionale sul segnale GPS (GALILEO)
- Ulteriore step: utilizzo di un cyber attack sul segnale GPS (spoofing coordinate)

ESEMPIO 1: RQ-170 Sentinel - 2011

- UAV Lockheed Martin RQ-170 Sentinel catturato dalle forze Iraniane
- Venne utilizzato:
  - Disturbo a radiofrequenza al link LOS tra GCS e APR per forzare la modalità auto-pilota
  - Cyber attack condotto mediante l'iniezione di un segnale GPS fake per ingannare il sistema automatico di guida

Effect: "The operators of the UAV lost control of the aircraft and had been working to determine its status."

[source NATO - International Security Assistance Force in Afghanistan]

ESEMPIO 2: SCHIEBEL CAMCOPTER - 2012

- Uno Schiebel S-100 Camcopter cadde sulla sua GCS nei pressi di Incheon (South Korea)
- I tecnici persero il controllo del velivolo, a causa dell'assenza del segnale di posizionamento GPS
- 1 vittima, 2 feriti
- Ipotesi: segnale di disturbo al GPS indirizzato dalla North Korea

Effect: "The initial investigation proved the fact the system lost its GPS – we don't know why it lost its GPS other than the only time we have seen it lose GPS is when it is jammed but I can't go any deeper than that statement.'"

[source: Neil Hunter – managing director at Schiebel]

SISTEMI DI DIFESA ELETTRONICA PER APR

- Il paradigma del Network Centric Warfare ha introdotto nuovi livelli di capacità dei sistemi di Difesa Elettronica, migliorando la cooperazione e la sincronizzazione dei sistemi interconnessi in rete, velocizzando la risposta delle catene di comando e controllo e migliorando il contenuto informativo delle missioni ISTAR

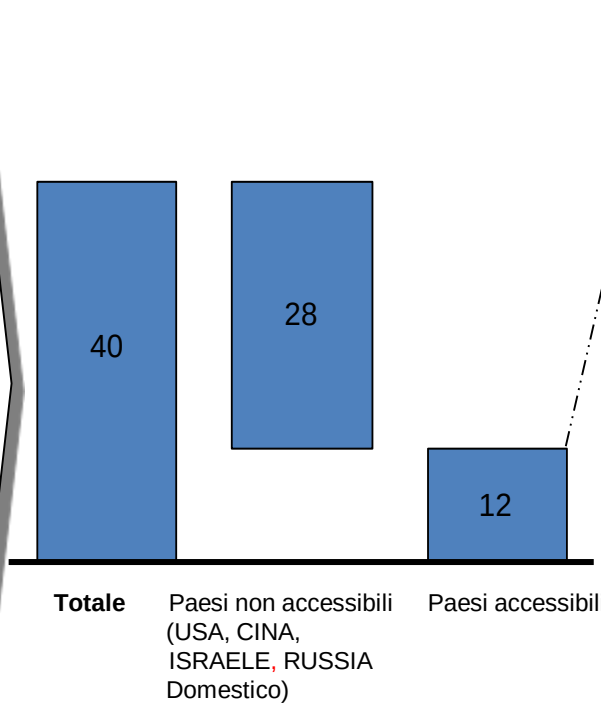
- I sistemi di Difesa Elettronica stanno assumendo una sempre maggiore importanza nell'ambito delle applicazioni di *Homeland Security, Maritime Surveillance*, *Law Enforcement*

- La sorveglianza dello spettro elettromagnetico, risorsa scarsa e dunque preziosa, rappresenta uno degli aspetti vitali per la sicurezza di una nazione

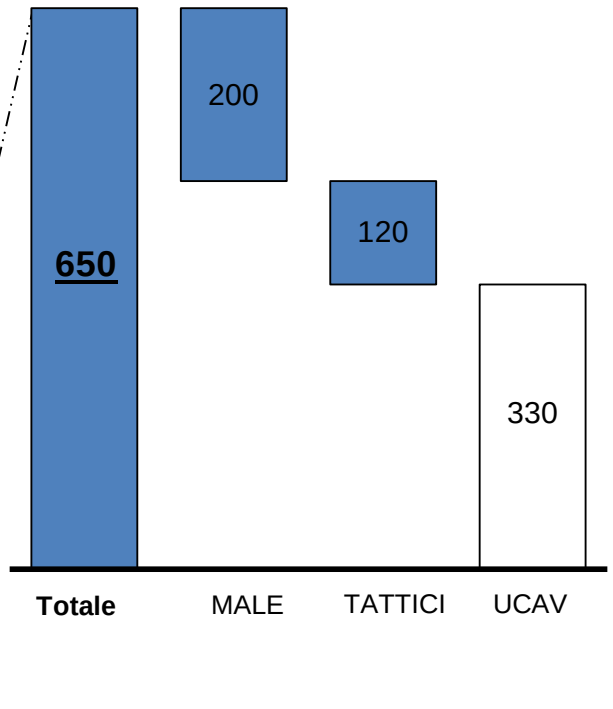
Centro Studi Militari Aeronautici 'Giulio Douhet'

PANORAMICA SUL MERCATO APR

① Composizione Mercato APR (prossimi 5-10 anni) B€



② Mercato APR - PAYLOAD EW accessibile (prossimi 5-10 anni) M€



	MALE	TATTICI	UCAV
Prezzo payload EW (M€):	0,7-1	0,8	0,6-1,4
Richiesta di payload EW:	50%	30%	100%

①

- Il mercato APR mondiale è in netta crescita e rappresenta un Business di 40 B€ nei prossimi 5-10 anni
- Il mercato totale accessibile (esclusi Usa, Cina, Israele e Russia) è nell'ordine di 12 B€

②

- La stima del mercato potenziale ed accessibile del payload EW per UAV è di circa 650 M€ in 5-10 anni sulle piattaforme MALE, Tattici e UCAV.
- La piattaforma HALE non è stata considerata in quanto il trend di mercato vede una riduzione forte del segmento HALE a favore del segmento MALE

Fonte: Elaborazione dati Marketing intelligence ELT su dati JDF

TABELLA COMPARATIVA PAYLOAD

Sensor capabilities	Collection	Detection	Recognition	Surveillance	Target Acquisition
TV FMS	Poor	Poor	Excellent	Excellent	Excellent
IR FMS	Medium	Medium	Good	Excellent	Excellent
ESM	Excellent	Excellent	Medium	Medium	Poor*
Achievable via synergy	Excellent	Excellent	Excellent	Excellent	Excellent

INTEGRAZIONE PAYLOAD DIFFERENTI

EW payload

- In grado di detettare automaticamente le emittenti a RF (Radar e Comunicazioni)
- Effettua l'assessment delle emittenti
- Estende il range di sorveglianza dei sistemi EW di bordo

EO/IR payload

- Viene indirizzato sul target rilevato dal EW payload, riducendo notevolmente:
  - Il tempo di ricerca
  - Il tempo per la geolocalizzazione delle emittenti
- Optimum: effettuare poi l'osservazione del comportamento del target

Vantaggi in ambito Sorveglianza Marittima

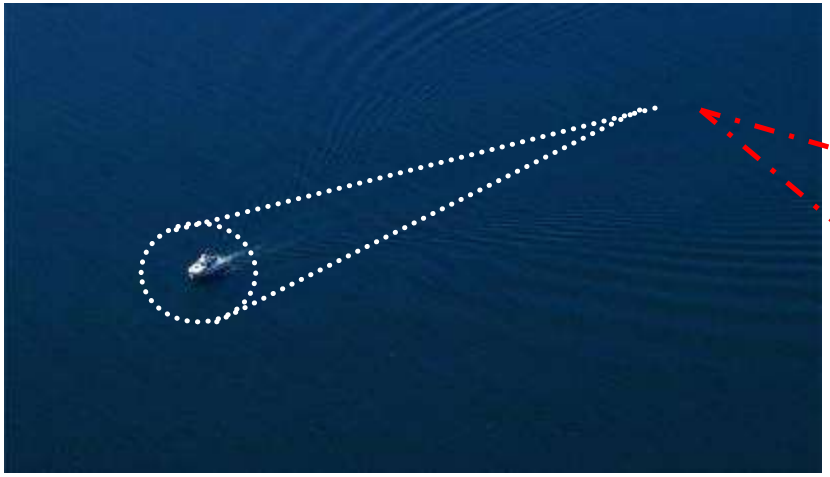
- Aumento della capacità di riconoscimento dei sistemi EW di bordo:
  - Estensione oltre l'orizzonte EM
  - Correlazione delle informazioni tra il payload dell'APR e i sistemi EW imbarcati sulla nave
- Mission Planning
- Mission Preparation
- Mission Execution

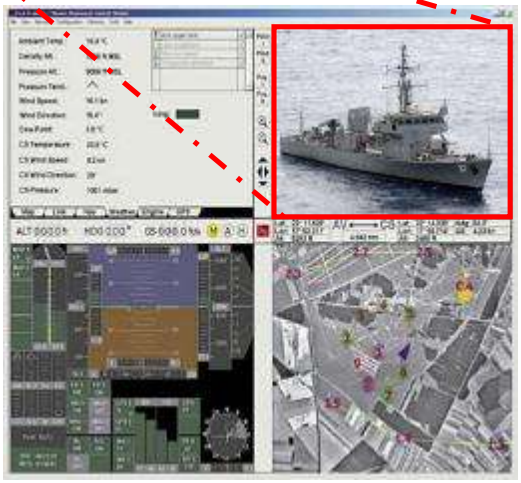
PIATTAFORME DI INTERESSE ELT

LIGHT EW PAYLOAD

APR: MISSIONE CON ESM PAYLOAD

- APR decolla per detettare l'emittente grazie al suo EW payload
- Dati dell'emittente e direzione sono trasmessi alla GCS
- Sulla HMI di controllo presso GCS l'emittente è rappresentata con direzione e cono di accuratezza DF





- L'operatore invia l'APR verso l'emittente sulla base delle info elaborate dal EW payload
- Il payload EO/IR acquisisce il video che viene inviato a GCS per l'identificazione del target

CONCLUSIONI

- A causa della loro intrinseca natura *war-oriented* e il loro impiego prevalentemente in scenari operativi *uncontested*, gli APR presentano problemi di sicurezza rilevanti
- Il tema della security rappresenta la vera sfida per un impiego duale degli APR in tutte le classi di spazio aereo perché diverse e tante possono essere le fonti di rischio (fisico, elettronico, cyber, etc)
- Alcuni eventi occorsi negli ultimi anni hanno mostrato il grande impatto mediatico, economico e politico che possono avere le minacce alla sicurezza di sistemi collegati in rete
- Le minacce agli APR saranno sempre più *blended*, mischiando attività di disturbo tradizionale con quelle più sofisticate di cyber-attack (spoofing), condotte sui sistemi di comunicazione, comando e controllo e navigazione
- Si rende necessario definire una strategia di protezione dell'intera infrastruttura che supporta le missioni degli APR
- I futuri payload di Difesa Elettronica, integrati con quelli "tradizionali" (EO/IR, SAR), assumeranno una sempre maggiore importanza in ambito Homeland Security, Border Surveillance, Maritime Patrol, Law Enforcement, …

SPARE: SECURITY IN AMBITO CIVILE