SPAZIO
I vantaggi dei sistemi di satellite sharing
— ALESSANDRO GOLKAR

DIFESA
L'Italia, la Nato e il valore del dialogo
— SERGIO MATTARELLA

AVIAZIONE
Cosa c'è dietro la pronuncia del Wto contro Ue-Airbus
— G. ALEGI, P. DI PALMA

Airpress

ottobre 2016 71

MENSILE SULLE POLITICHE
PER L'AEROSPAZIO E LA DIFESA

1 triliardo $
spesa cyber-security nei prossimi 5 anni

90%
i dirigenti impreparati a gestire gli attacchi

69%
l'hacker è esterno al sistema violato

64%
furti d'identità

158 mld $
furti ai consumatori nel 2015

25%
attacchi all'internet of things nel 2020 (previsione)

4 su 5
aziende Fortune500 colpite nel 2015

146 giorni
tempo medio di scoperta del danno

Cyber-security
TRA DIFESA E BUSINESS

ALESSANDRO PANSA/ MAURO MORETTI/ KOEN GIJSBERS/ LUIGI REBUFFI

— INVESTIMENTI —

Usa
$19 miliardi nel 2017
aumento del budget del 35%

— INVESTIMENTI —

Uk
piano quinquennale da £1.9 miliardi (circa 450 mln € l'anno)

— INVESTIMENTI —

Francia
piano quinquennale da circa 1 miliardo di euro (circa 200 mln € l'anno)

— INVESTIMENTI —

Germania
circa 66 mln € l'anno dal 2009

— INVESTIMENTI —

Giappone
piano quadriennale da 173 mln € (circa 43 mln € l'anno)

CY4GATE

CYBER EW & INTELLIGENCE
AN ELETTRONICA GROUP COMPANY

THE WORLD IS BECOMING A SMALL PLACE

cy4gate.com

ELETTRONICA GROUP
A FOCUSED GLOBAL LEADER

editoriale

Le bandiere italiane che sventolavano a Washington in occasione della visita di Stato del presidente del Consiglio sono il segno di una novità significativa. Non era mai accaduto che al nostro Paese venisse riconosciuto così platealmente un ruolo decisivo e determinante nelle relazioni fra Stati Uniti ed Europa. Quello che si è celebrato alla Casa Bianca non è stato il rapporto speciale fra Obama e Renzi. Si è consacrata una scelta di lungo termine da parte dei due Paesi che scommettono su una visione condivisa di occidente e lo fanno in una prospettiva che naturalmente va oltre gli attuali inquilini di Casa Bianca e Palazzo Chigi.
Con l'uscita politica del Regno Unito dall'Unione europea, Roma resta il più solido pilastro del ponte che unisce i due lati dell'Atlantico. In questo senso, il nostro impegno in Iraq e nei tanti scenari nei quali siamo protagonisti con la Nato è certamente una ragione di orgoglio. Siamo ancora lontani dagli obiettivi minimi di investimento sulla difesa (*target* europeo fissato al 2% del Pil) ma quest'anno in legge di bilancio registriamo un segnale positivo di inversione di tendenza, pur concentrando l'incremento del *budget* nella spesa per il personale. D'altra parte, il versante industriale potrà beneficiare delle misure contenute nel piano Industria 4.0 predisposto dal ministro Calenda e approvato dal governo. Il contesto politico si presenta quindi in una condizione più favorevole rispetto anche al recente passato. E anche la nostra presenza militare nei Baltici da questo punto di vista rappresenta un elemento di chiarezza assai opportuno.
Ora tocca a tutti proseguire in modo consequenziale. Due i punti su cui varrà la pena di concentrare gli sforzi di *policy*: le alleanze industriali e l'impegno a crescere nella capacità difensiva dello spazio cibernetico. È evidente che l'industria della difesa in Italia agisce in una logica di mercato, con società quotate e azionariati privati. Allo stesso modo non si può ignorare che alcune scelte (MBDA, Piaggio Aero e Avio) investono compiutamente l'interesse nazionale e impattano sulle strategie del sistema-Paese, che non sono estranee alle grandi direttrici della nostra politica estera e di difesa. L'appello "unitario" dei ministri Gentiloni e Pinotti non potrebbe essere in alcun modo letto come una resa industriale dell'Italia a favore dei *competitor* "interni" europei. Non è questo l'auspicio dell'autorità politica, anzi. La difesa europea non è una alternativa alla Nato e neppure un ripiegamento sul blocco economico franco-tedesco. Mercato e visione strategica del Paese possono e debbono trovare un equilibrio virtuoso e il settore privato può dare il segno di migliore consequenzialità scegliendo l'opzione del sano e sostenibile protagonismo. Secondo aspetto è quello legato alla quinta dimensione strategica: lo spazio cibernetico. L'Italia è in ritardo, negli investimenti e nella *governance*. Dobbiamo recuperare con rapidità ed efficacia: non possiamo permetterci di essere così vulnerabili. L'*escalation* di accuse a Mosca per i suoi presunti attacchi *cyber* ai danni degli Stati Uniti e dell'occidente sono solo la manifestazione più visibile di dove si sono spostati i confini della conflittualità internazionale. La nostra sicurezza cibernetica non è meno rilevante di quella assicurata dalle "tradizionali" forze armate. I puntini ci sono tutti, ormai. A ciascuno tocca il compito di unirli in un disegno razionale. Quello emerso a Washington ci sembra il migliore.

sommario

RUBRICHE

Airpress
Agenzia stampa aeronautica tecnica politica

Registrazione Tribunale di Roma n. 10311 del 7/4/1965. Registrazione R.O.C. n. 9884

Editore Base per altezza s.r.l.
corso Vittorio Emanuele II, 18
00186 Roma
telefono 06 454 73 850
fax 06 455 41 354
partita iva 05831140966

Rivista fondata da Fausto Alati
Direttore responsabile **Flavia Giacobbe**
Direttore editoriale **Alessandro Cornacchini**
Redazione **Michela Della Maggesa**
hanno collaborato **Stefano Pioppi, Chiara Rossi**
Progetto grafico **Nom de Plume**
Impaginazione e grafica **Essegistudio**

Per comunicati, abbonamenti, pubblicità
redazioneairpress@gmail.com

Consiglio di amministrazione
Presidente **Gianluca Calvosa**
Consiglieri **Giovanni Lo Storto, Chicco Testa, Brunetto Tini**

Recapito a cura di Nexive
comunicazione@nexive.it

Numero chiuso in redazione il 17 ottobre 2016
Finito di stampare il 20 ottobre 2016

Stampato in Italia
da **Rubbettino print**
Viale Rubbettino, 10
88049 Soveria Mannelli

contributors

JONATHAN D. CAVERLEY
ricercatore associato in Security studies e scienza politica presso il Massachusetts institute of technology, è stato *fellow* presso il Woodrow Wilson center for international scholars di Washington. Precedentemente ha insegnato alla Northwestern University, dove ha fondato e presieduto il *working group* in Security studies. È autore di numerose pubblicazioni su temi di politica di difesa, sicurezza internazionale e industria del settore difesa e aerospazio

SERGIO MATTARELLA
dodicesimo presidente della Repubblica dal 3 febbraio 2015. Dal 1983 al 2008 è stato deputato, prima per la Democrazia Cristiana (di cui fu vicesegretario) e poi per il Partito popolare italiano, La Margherita e il PD. Ha ricoperto la carica di ministro per i Rapporti con il Parlamento (1987-1989), di ministro della Pubblica istruzione (1989-1990), di vicepresidente del Consiglio (1998-1999), di ministro della Difesa (1999-2001) e infine di giudice costituzionale (2011-2015)

ALESSANDRO PANSA
direttore generale del Dipartimento delle informazioni per la sicurezza (Dis) dall'aprile del 2016, è stato precedentemente capo della Polizia dal 2013. Laureato in giurisprudenza all'Università di Napoli, è entrato in Polizia nel 1975 fino ad arrivarne ai vertici. Nel 2005 è stato nominato vice direttore generale della Pubblica sicurezza e nel 2007 prefetto di Napoli. Dal 2010 è stato capo del Dipartimento per gli affari interni e territoriali al ministero dell'Interno

KOEN GIJSBERS
general manager dell'Agenzia comunicazioni e informazioni della Nato (Nci agency), è Maggior generale in congedo del Regio esercito dei Paesi Bassi. Con 35 anni di servizio nelle Forze armate olandesi ha servito in missioni europee e internazionali. È stato capo ufficio informazioni al ministero della Difesa e *assistant chief of staff* al C4I della Nato, comando dedicato all'*intelligence* e ai sistemi computerizzati. Dal luglio del 2012 è il primo *general manager* dell'Ncia

MAURO MORETTI
amministratore delegato e direttore generale di Finmeccanica dal 15 maggio 2014. Riveste molti incarichi anche in ambito internazionale: è presidente dell'Associazione europea delle industrie dell'aerospazio e della difesa; è presidente onorario dell'Aiad, la Federazione aziende italiane per l'aerospazio, la difesa e la sicurezza. Laureato con lode in Ingegneria elettrotecnica all'università di Bologna, ha iniziato la sua carriera nel 1978 vincendo il concorso per ruoli direttivi delle Ferrovie dello Stato, di cui nel 2006 diventa amministratore delegato

ESTI PESHIN
direttore dei Programmi *cyber* di Israel aerospace industries (Iai) è anche direttore generale dell'*hi-tech caucus* della Knesset, il Parlamento israeliano. Prima di assumere questi ruoli, è stata *managing* partner di ENP Solutions. Esperta di sicurezza informatica, è stata inoltre *chief executive officer* di Waterfall Security Solutions. Precedentemente ha servito nelle Forze di difesa israeliane all'interno di un'unità di *élite* tecnologica di cui è stata vice direttore

Cyber

USA-RUSSIA E IL RISCHIO DI CYBER-WAR

Il livello di tensione per attacchi cyber raggiunto da Usa e Russia potrebbe spingere i responsabili politici dell'arena internazionale, come avvenuto nel periodo del confronto nucleare, ad adottare iniziative che vadano a governare il domino cyber, a oggi immune da norme condivise tra gli Stati (norms of state behavior) che delimitino il campo di azione dell'uso della forza

LUIGI MARTINO *teaching and research assistant in Ict policies e Cyber-security presso l'Università di Firenze*

La tensione tra Russia e Usa a colpi di *cyber*-attacchi ha fatto ripiombare la comunità internazionale ai tempi della crisi di Cuba, quando il confronto tra le due potenze si spinse a un livello mai raggiunto. Oggi il confronto interviene, per giunta, nel corso della (bizzarra) campagna elettorale per la corsa alla Casa Bianca, nella quale ci si interroga più che mai sulla necessità di una sicurezza cibernetica. La recente notizia di un "imminente attacco *cyber*" dei servizi di *intelligence* americani (in particolare la Cia) contro la Russia, in risposta ai diffusi attacchi *state-sponsored* da parte del Cremlino, ha introdotto un salto di qualità rispetto alla classica dialettica politica da campagna elettorale. Infatti, con l'ordine ufficiale di Obama rivolto ai propri servizi, la questione ha assunto una priorità per la sicurezza nazionale degli Stati Uniti. Allo stesso tempo, si è assistito, per la prima volta, alla dichiarazione ufficiale di un "attacco *cyber*" con sfumature che rinviano alle dinamiche delle azioni militari classiche.

L'accento significativo posto da Donald Trump sul rischio di manipolazione del voto elettronico ha indotto una reazione della candidata democratica Hillary Clinton, che non ha perso tempo a tirare in ballo le "amicizie compromettenti del *Tycoon* con i russi". La questione di fondo rimane sempre la stessa: il sistema di voto elettronico può essere hackerato? Secondo fonti dell'*intelligence* americana e in particolare dell'Fbi esiste un pericolo concreto che i sistemi informatici vengano hackerati.

Ad esempio, si ricorda il recente attacco subito dal sistema elettorale dell'Arizona, preso di mira da un non meglio precisato gruppo di pirati informatici. Lo stesso Federal bureau ha puntato il dito contro gruppi assoldati dal governo russo che, nello specifico caso dell'Arizona, hanno avviato un persistente e sistemico attacco informatico contro l'infrastruttura che gestisce il voto elettronico. La complessità dell'attacco ha fatto pensare agli investigatori che dietro vi fosse uno *sponsor* statale o, quanto meno, un'organizzazione criminale con elevate capacità informatiche.

A fare da eco ai recenti avvenimenti ci ha pensato anche il department of Homeland security, il quale, attraverso una nota ufficiale, ha messo in guardia dai tentativi (reali) di intrusione, esterna e interna, per modificare il voto elettronico degli elettori americani. Si legge infatti nella nota rilasciata da Neil Jenkins, funzionario presso il department office of Cybersecurity and communications:

"Crediamo che il voto *on-line*, in particolare il voto *on-line* su larga scala, introduca un grande rischio nel sistema elettorale, in particolare la minaccia delle aspettative di riservatezza, la responsabilità e la sicurezza del voto degli elettori e fornisce una via per attori malintenzionati di manipolare i risultati delle votazioni".
Ovviamente sia la Clinton sia Trump cercano di politicizzare il rischio *cyber* a proprio vantaggio.
Sul versante della sicurezza nazionale e delle minacce *cyber*, gli Stati Uniti hanno diversi conti in sospeso con la Russia di Putin (solo per citarne alcuni: il caso estone, il caso Snowden, il caso delle centrali elettriche in Ucraina, il persistente e continuo *cyber-espionage*, il tentativo di manipolazione del voto elettronico, ecc.). D'altro canto, con l'ordine diretto alla Cia, la quinta dimensione della conflittualità entra ufficialmente nei domini bellici e assume caratteristiche proprie, con elementi di deterrenza e di rappresaglia militare. Non a caso, sempre gli Stati Uniti, nella loro ultima *cyber-strategy* hanno espresso a chiare lettere che "di fronte a un attacco *cyber* si può reagire con un attacco militare proporzionale, di tipo informatico e/o classico". La stessa Nato, nel suo ultimo concetto strategico, ha dichiarato che il domino cibernetico deve essere inteso come il quinto domino militare. In altre parole, la militarizzazione del *cyber-space* non solo è avvenuta, ma adesso è anche operativa. Rimane un solo aspetto di non poco conto: l'assenza di norme condivise tra gli Stati (*norms of state behavior*) che, alla base del diritto internazionale, vadano a delimitare il campo di azione dell'uso della forza e creino un *framework* condiviso sulle regole del gioco. A oggi non sono presenti norme condivise di questo genere nel dominio *cyber*, forse perché l'errore di fondo che ha caratterizzato tutte le iniziative, giuridiche e politiche, fin qui portate avanti dalla comunità internazionale, sono state interessate da analisi di tipo tecnologico, ponendo l'accento, ad esempio, sul problema dell'attribuzione, senza analizzare piuttosto l'elemento politico del *cyber-space.* Infatti, questo dominio non vive di vita propria, ma è calato nel più ampio concetto di *warfare*.
Forse, il salto di qualità avvenuto di recente, potrebbe spingere i responsabili politici dell'arena internazionale, come avvenuto nel periodo del confronto nucleare, ad adottare iniziative che vadano a governare un domino ad oggi immune, almeno in via ufficiale, dalle coercizioni del diritto internazionale.

COOPERARE PER ASSICURARE LA RESILIENZA

La minaccia è sempre crescente, ma allo stesso tempo la conoscenza cambia alla velocità della luce. Il problema è che dobbiamo costruire un sistema resiliente con queste dinamicità. Si tratta dunque di innovazione permanente, ma anche di trovare il modo di potenziare la nostra burocrazia affinché le cose siano fatte più rapidamente

KOEN GIJSBERS *general manager dell'Agenzia comunicazioni e informazioni della Nato – Ncia*

Se mi chiedessero in che modo la Nato affronta il *cyber*-dominio, la mia prima risposta sarebbe: non solo cooperando con i Paesi membri, ma anche difendendoli. L'Agenzia comunicazioni e informazioni della Nato (Nci) rappresenta il classico esempio di un'organizzazione internazionale: conduciamo operazioni in 35 luoghi, in oltre 13 nazioni e in missioni come in Afghanistan o per la difesa missilistica. E vi posso assicurare che siamo sotto costante attacco.

Inoltre, l'attuale contesto di sicurezza non fa che peggiorare le cose. La risposta della Nato è cooperare per assicurare resilienza. Se infatti pianifichiamo di difendere i nostri Paesi e tutto il contesto atlantico con l'*Information technology* (IT) e con qualunque strumento digitale, la resilienza è l'elemento indispensabile per assicurare che tutti i sistemi funzionino sempre e in ogni circostanza. In questo senso non ammettiamo compromessi. Non c'è compromesso possibile sulla sicurezza nella Nato.

La minaccia è sempre crescente, ma allo stesso tempo la conoscenza cambia alla velocità della luce. E il problema è che dobbiamo costruire un sistema resiliente con queste dinamicità. Si tratta di innovazione permanente, ma anche di trovare il modo di potenziare la nostra burocrazia affinché le cose siano fatte più rapidamente. Il nemico non ha questi problemi. Attacca al punto di sutura tra due organizzazioni, tra due *network*, tra governi e industrie, proprio dove siamo più deboli. Queste debolezze richiedono collaborazione politica e *partnership*, e su questo la Nato sta lavorando.

La mia agenzia è responsabile per la fornitura di tutti i servizi alla Nato, dall'Afghanistan agli Stati Uniti, e tra essi gli elementi *cyber* rappresentano una priorità. Disponiamo di capacità di *cyber*-risposta centralizzate, in stretta *partnership* con le industrie (di cui Leonardo-Finmeccanica è un esempio), al fine di garantire la sicurezza dell'Alleanza. Infatti, il *cyber*-spazio non è solo una mia priorità, è una priorità della Nato. E se si considera il Summit di Varsavia dello scorso luglio, è possibile evidenziare tre importanti decisioni prese dall'Alleanza.

Prima di tutto, la Nato ha dichiarato il *cyber*-spazio un dominio operativo. Ciò comporta alcune rilevanti conseguenze. Fino a ora, il settore cibernetico era considerato un argomento di natura puramente tecnica. Oggi, dopo questa decisione, è ancora legato alla tecnologia, ma è anche integrato nel *business*, nei nostri scenari operativi e nelle modalità con cui operano i governi. A Varsavia si è presa una decisione politica corretta, al più alto livello possibile, per essere sicuri di cooperare. L'attribuzione di dominio porterà, infatti,

CYBERTECH EUROPE 2016
Cybertech ha scelto Roma per il suo debutto europeo. Il 29 settembre, Cybertech Global Events, in collaborazione con Leonardo, ha organizzato presso il Palazzo dei congressi l'evento che aveva riscosso ampi consensi nelle passate edizioni in Israele, Singapore e Nord America. In conferenze, tavole rotonde e incontri *b2b*, hanno partecipato rappresentanti dell'industria, della ricerca e delle istituzioni, tra cui il ministro Alfano, il direttore del Dis Alessandro Pansa e il *general manager* dell'agenzia Nci della Nato Koen Gijsbers

il *cyber*-spazio a un'integrazione ancora maggiore con l'ambito operativo e questo, per noi, è un passo molto importante.
In secondo luogo, i 28 capi di Stato e di governo hanno stabilito che ogni Nazione rafforzerà la propria *cyber*-resilienza. La nostra forza comune sarà possibile solo quando gli Stati raggiungeranno questo obiettivo. E ogni due anni, durante i *summit*, la Nato verificherà come siamo andati avanti collettivamente.
La terza decisione del Summit di Varsavia è stata il Cyber defence pledge: i Paesi membri hanno concordato di condividere le informazioni per migliorare la comprensione delle minacce cibernetiche. L'obiettivo dell'accordo è rafforzare l'interazione tra i rispettivi *stakeholder* nazionali impegnati in *cyber*-difesa, e approfondire la cooperazione e lo scambio delle *best practice*. I progressi saranno valutati attraverso un'analisi annuale basata su indicatori condivisi e verranno poi rivisti durante i *summit* dell'Alleanza.
Questi tre elementi stanno cambiando fondamentalmente il modo con cui operiamo. Ma quali sono le implicazioni per la Nato e l'industria? Prima di tutto, tecniche: stiamo costruendo un'architettura più resiliente e implementando nuovi strumenti. Sicuramente, come singoli attori, non possiamo affrontare le minacce cibernetiche individualmente. Credo che i Paesi membri debbano cooperare con l'industria per l'innovazione che l'attuale contesto di sicurezza richiede. Nella Nato abbiamo otto *cyber partnership* con il comparto industriale, sin dal 2014. In due anni abbiamo sperimentato una buona collaborazione; abbiamo prodotto alcune applicazioni arrivando a comprendere come innovare. Ho inaugurato un Business executive group con gli amministratori delegati delle industrie e lo considero molto importante per capire come lavorare insieme. Non è facile, poiché ognuno conserva i propri interessi. Abbiamo registrato alcune difficoltà nell'ottenere i soldi che avremmo bisogno di spendere, a usarli per ciò di cui abbiamo bisogno e ad avere un buon processo di selezione per il miglior prodotto e la migliore industria. Non è facile, ma è già operativo: la Nato sta lavorando sui passi successivi. E con i passi successivi intendo che abbiamo bisogno di comprendere minacce che prima non conoscevamo, che abbiamo bisogno di un buon sistema decisionale, di una maggiore consapevolezza dell'ambiente *cyber* e di una migliore resilienza nelle nostre risposte. L'unico modo per andare avanti è lavorare insieme, con industrie e governi, per ottenere più velocemente innovazione e mettersi al sicuro.

Traduzione di Stefano Pioppi

UNA RIDEFINIZIONE DELLA SICUREZZA NAZIONALE

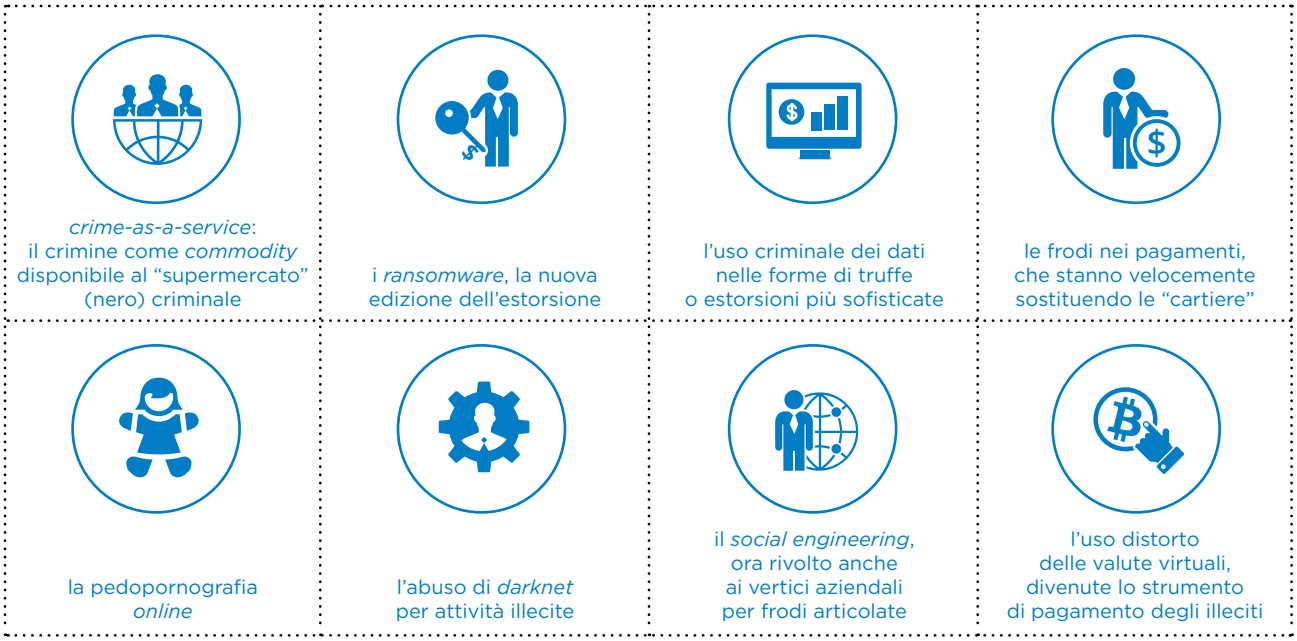
L'innovazione digitale richiede alle comunità di intelligence uno sforzo d'immaginazione senza precedenti, mentre entriamo in un futuro permeato di tecnologia. In questo nuovo mondo, l'intelligence dovrà essere in grado di comprendere, prima ancora degli attori ostili, come una nuova tecnologia possa essere sfruttata per finalità che possono mettere a rischio la sicurezza nazionale

ALESSANDRO PANSA *direttore generale del Dipartimento delle informazioni per la sicurezza*

La crescente mole di dati – raccolti in maniera massiva e riferiti a qualità personali, abitudini, stili di vita e preferenze di consumo – diviene un serio onere per l'impiego da parte di chi li detiene e, allo stesso tempo, rappresenta un obiettivo ambito e altamente remunerativo per chi vuole impossessarsene illecitamente. Occorre acquisire piena consapevolezza degli interessi che entrano in gioco, quando ci confrontiamo con la minaccia *cyber*: l'integrità fisica dei nostri cittadini, l'integrità economica collettiva e delle nostre imprese, le funzioni fondamentali dello Stato, i diritti dei singoli, lo stesso diritto alla libertà. Rispetto a questi valori e a questi interessi, occorre ponderare la modifica delle regole, l'eventuale parziale compressione delle libertà e/o dei diritti dei cittadini in un delicato equilibrio che, peraltro, va modificandosi continuamente proprio con l'evolvere della tecnologia e della minaccia. È in tale contesto che il Dis ha promosso e sta ancora oggi promuovendo iniziative mirate al consolidamento della *partnership* pubblico-privato – ppp, che si rifanno a un modello *multi-stakeholder*. A partire dal 2013, il Dis ha consolidato un formato di condivisione informativa con i gestori di infrastrutture critiche e altri operatori strategici: tali soggetti, se da un lato notificano al dipartimento volontariamente gli attacchi e altre anomalie registrate sulle proprie reti e sistemi, dall'altro, sono destinatari, da parte del Dis, di analisi e valutazioni della minaccia *cyber*, così da assicurare loro un adeguato livello di sicurezza informatica. La nostra attenzione, oggi, è focalizzata sul furto di dati personali e finanziari, inclusi i dati biometrici, così come di informazioni rilevanti sotto il profilo commerciale e strategico; dobbiamo tuttavia considerare anche l'impatto fisico derivante dalla manipolazione di *software*. Abbiamo già al riguardo degli esempi concreti, come il recente test di *hacking* condotto da alcuni ricercatori su modelli di automobile Tesla, che hanno mostrato vulnerabilità che, se sfruttate, avrebbero consentito a un potenziale attaccante di prendere il controllo, tra l'altro, dei freni del veicolo. Questo test mostra, in modo concreto, come un attacco *cyber* possa causare danni sul piano fisico, anche in termini di feriti e, nel caso peggiore, di vittime. Ciò dimostra l'importanza dei cosiddetti programmi di *bug bounty* come quello, ad esempio, denominato Hack the Pentagon, iniziativa promossa quest'anno dal dipartimento della Difesa Usa, volto a testare la sicurezza dei propri siti *web* con esclusione, tuttavia, dei sistemi informatici criti-

IL TREND DEL CYBER-CRIME

Il rapporto Iocta sugli otto *trend* del *cyber-crime* nel 2016 li ha classificati in



Dati Europol - per tutti questi fenomeni, i trend sono in netto aumento

ci. L'innovazione digitale richiede alle comunità di *intelligence*, a livello mondiale, uno sforzo d'immaginazione senza precedenti, mentre entriamo in un futuro permeato di tecnologia. In questo nuovo mondo, l'*intelligence* dovrà essere in grado di comprendere, prima ancora degli attori ostili, come – da un punto di vista squisitamente tecnico – una nuova tecnologia possa essere sfruttata per finalità che possono mettere a rischio la sicurezza nazionale. Il Paese ha ora bisogno di un progetto nazionale di *cyber-security*, che – in una nuova accezione di sicurezza nazionale – possa confrontarsi con le nuove minacce. Ad esempio, l'affidabilità e la sicurezza di componenti *hardware* e *software* che supportano infrastrutture critiche nazionali e altri attori strategicamente rilevanti, possono essere conseguite solo attraverso la messa in sicurezza di tutti i soggetti della catena del valore, inclusi i produttori di componenti *hardware*, gli sviluppatori di *software* e i fornitori di servizi IT. Una delle priorità della nuova edizione del Piano nazionale potrebbe essere l'implementazione di un laboratorio governativo dove testare i sistemi informatici prima del loro impiego nell'ambito di infrastrutture critiche, sia governative sia private. Tale obiettivo non può essere conseguito senza un approccio *multi-stakeholder* basato sulla cooperazione con il settore privato. Per affrontare la minaccia appare cruciale, da un lato, acquisire e tenere aggiornata una vasta capacità di raccolta, analisi e conservazione dei dati, (i cosiddetti *big data*), al fine di individuare e disarticolare in anticipo la minaccia e, dall'altro, poter contare su nuove sensibilità dei *provider* nel sostenere gli attori pubblici nel loro sforzo di garantire la sicurezza. Il Progetto nazionale di *cyber-security* potrà utilmente beneficiare della dotazione messa a disposizione dalla Legge di stabilità per il 2016. Perché il progetto determini, come risulta ormai essenziale, un effettivo cambio di passo per la capacità di reazione del nostro Paese, sarà altrettanto indispensabile che la costruzione dello stesso avvenga con il contributo delle varie componenti (pubbliche, private e della ricerca) che costituiscono la struttura portante del tessuto *cyber* nazionale. E tutti gli attori chiamati a dare il loro contributo dovranno intervenire con spirito indipendente, con posizioni coerenti, con una visione naturalmente rivolta al futuro, tale da porre la sicurezza nazionale al di sopra degli interessi settoriali.

www.sicurezzanazionale.gov.it

IL RUOLO DELL'INDUSTRIA NEL MONDO CONNESSO

All'accelerazione della crescita dei dispositivi connessi e delle applicazioni IoT *seguono questioni di interoperabilità e di sicurezza. Potrebbe essere utile ragionare, in sede europea, su come riordinare gli standard e come rendere i requisiti di cyber-security vincolanti. Del resto, la digitalizzazione è un processo che deve essere protetto e accompagnato da una strategia di cyber-security specifica e aggiornata*

MAURO MORETTI *ad e dg Leonardo-Finmeccanica*

Nel pur difficile contesto macroeconomico, l'industria della sicurezza si è affermata come un'area di prosperità: anche in prospettiva, il settore manifesta un notevole potenziale di crescita, in grado di creare nuovi posti di lavoro altamente specializzati.

Per garantire la prosperità dell'industria della sicurezza, è necessario affermarsi a livello globale, oltrepassando la dimensione europea: non basta superare la frammentarietà del settore industriale della sicurezza e soddisfare la domanda interna; bisogna conquistare nuovi mercati internazionali e, contemporaneamente, proseguire gli investimenti nella ricerca. Una parola-chiave è "condivisione": è necessario che a livello internazionale, nei vari settori, riguardo alla *cyber-security* aumentino gli sforzi per condividere obiettivi, prospettive, *standard* e risorse. Quanto agli obiettivi, in Europa sarebbe opportuno concretizzare una difesa comune: la *cyber-security* rappresenta al tempo stesso una nuova esigenza e una possibile soluzione in vista dell'armonizzazione. I diversi Paesi hanno elaborato strategie specifiche, dotandosi di proprie strutture di *governance* e sviluppando diverse capacità difensive. Bisogna ricercare una maggiore coerenza organizzativa e operativa, e coinvolgere l'industria della difesa per stabilire le future capacità. La *cyber-security* richiederà nuove tecnologie e nuove competenze. Sia i Paesi sia i settori economici e industriali saranno chiamati a sostenere sforzi ragguardevoli per adeguare gli approcci difensivi e disporre delle capacità difensive più appropriate a fronteggiare le minacce e le vulnerabilità tecniche. Allo scopo, sarebbe conveniente promuovere delle forme di specializzazione. Circa le prospettive, ci troviamo già nella quarta rivoluzione industriale, che annuncia un'importante digitalizzazione dei processi di progettazione e produzione. In particolare, il programma Industria 4.0 vuole modernizzare ulteriormente il settore manifatturiero, affrontando anche alcune questioni legate alla sicurezza dei processi di automazione e alla resilienza delle tecnologie coinvolte. Questo, in prospettiva, coniuga la *cyber-security* con il concetto di *cyber-resilience*.

Infatti, la trasformazione dei settori industriali, in particolare quello manifatturiero attraverso l'integrazione dei sistemi di automazione con quelli IT, segnerà un profondo cambiamento che richiederà innovazioni nelle infrastrutture di connettività, nei dispositivi intelligenti collegati via IP, e nelle differenti applicazioni *software* in grado di elaborare e creare valore dai dati, con

Alcuni momenti di Cybertech Europe 2016. Foto in alto a sinistra: il ministro dell'Interno, Angelino Alfano, l'ad di Leonardo, Mauro Moretti e Alessandro Pansa, direttore generale del Dipartimento delle informazioni per la sicurezza.
Nella foto in alto a destra, Marco Carrai. Nella foto in basso, un momento dell'evento

nuovi requisiti sia di *safety* sia di *security*. La convergenza tra mondi fisici e mondi virtuali trova altre manifestazioni oltre il manifatturiero avanzato. Ci sono diversi settori (energetico, dei trasporti e sanitario) che stanno predisponendo infrastrutture di *cyber-security* adeguate. Ci stiamo avviando verso un mondo sempre più connesso. Secondo McKinsey, nel 2025 potrebbero esserci tra 70 e 100 miliardi di dispositivi IoT (*Internet of things*) collegati e l'impatto economico globale delle applicazioni IoT potrebbe raggiungere il valore di 10 miliardi di dollari. E proprio la regione europea guiderà questa affermazione, perché i livelli di crescita annuale potrebbero rimanere costantemente alti per tutto il periodo, superiori a quelli stimati per il Nord America. All'accelerazione della crescita dei dispositivi connessi e delle applicazioni IoT, unitamente alla confluenza di diverse tecnologie e alla loro integrazione, seguono questioni di interoperabilità, di sicurezza e di affidabilità. In passato, nei diversi ambiti applicativi. le tecnologie ICT sono state sviluppate all'interno di architetture particolari. Questa diversità da settore a settore, si riverbera anche nella pluralità di norme tecniche e *standard* altamente contestualizzati. Potrebbe essere utile ragionare, in sede europea, su come riordinare gli *standard* e come rendere i requisiti di *cyber-security* vincolanti. Del resto, dato che la digitalizzazione consente la creazione di nuovo valore – economico, occupazionale e sociale – è un processo che deve essere protetto e accompagnato da una strategia di *cyber-security* specifica e aggiornata.
Infine, occorre stanziare cospicue risorse per proteggere in modo adeguato e appropriato le infrastrutture critiche, che impiegano tecnologie sempre più complesse, integrate e interoperabili. Per assicurare ai diversi settori il giusto livello di *cyber-security*, bisognerebbe anche considerare delle nuove forme di cooperazione e ripartizione dei costi. La *cyber-security* ha un ruolo di fondamentale importanza nelle infrastrutture critiche: deve essere presente sin dalle fasi di progettazione delle architetture dei sistemi di supervisione e controllo, per essere più efficace e consentire di predisporre delle misure di resilienza; rappresenta un baluardo per contrastare – e se possibile prevenire – le minacce, attraverso i progressi della *cyber threat intelligence* e infine migliora la consapevolezza delle minacce e delle vulnerabilità nei diversi utenti dei sistemi critici, contribuendo ad aumentare in loro il rispetto delle politiche di sicurezza e a migliorare la loro condotta nelle eventuali situazioni di emergenza.

L'EUROPA PUNTA SU PARTNERSHIP PUBBLICO-PRIVATE

A partire dalla creazione del mercato unico digitale, sono state identificate una serie di azioni a livello europeo per alimentare la complessiva sicurezza online in Europa, compresa la creazione di un partenariato pubblico-privato guidato dall'industria. In questi termini, l'Ecso ha siglato un accordo con la Commissione europea nell'ambito del programma Horizon2020

LUIGI REBUFFI *segretario generale dell'European cyber security organisation – Ecso*

Il *cyber*-spazio rappresenta la colonna portante della società digitale e della crescita economica, con ben 315 milioni di utenti al giorno in Europa in ogni settore: sanità, *e-commerce*, mobilità, energia, finanza, *Internet of things*. Esso è, per sua natura, senza confini. Ciò significa che qualsiasi minaccia o incidente di *cyber-security* può avere effetti devastanti in molti settori dell'economia e della società. Con minacce in crescita e in evoluzione continua, la protezione del *cyber*-spazio è di primaria importanza. La domanda che dobbiamo porci è: come può un mercato europeo pesantemente frammentato per prodotti e servizi ICT (*information and communication technology*) supportare adeguatamente la protezione di uno sconfinato *cyber*-spazio? Oggi, la sopravvivenza di una solida industria europea di *cyber-security* e la protezione della crescita del mercato digitale sono prioritarie.

A partire della creazione del mercato unico digitale, sono state identificate una serie di azioni a livello europeo per alimentare la complessiva sicurezza *online* in Europa, compresa la creazione di un partenariato pubblico-privato (ppp) guidato dall'industria in *cyber-security*. Per questo, il 5 luglio 2016, l'Organizzazione europea per la *cyber-security* (Ecso), ha siglato un accordo (la *contractual* ppp) con la Commissione europea che pone tre principali obiettivi. Primo, creare e rafforzare la cooperazione tra *stakeholder* pubblici e privati del settore nelle prime fasi del processo di ricerca e innovazione, al fine di permettere ai cittadini di accedere a soluzioni europee innovative e affidabili che prendano in considerazione il rispetto per la *privacy* e la protezione dei dati personali. Secondo, stimolare l'industria della *cyber-security*, allineando domanda e offerta e permettendole di ottenere i futuri requisiti per gli utenti finali e per settori che usufruiscono di soluzioni in sicurezza cibernetica, come il comparto energetico, dei trasporti, manifatturiero o finanziario. Terzo, coordinare le risorse industriali in Europa.

In questo contesto, l'Ecso supervisiona lo sviluppo e l'implementazione dell'Agenda strategica per la ricerca e l'innovazione, parte del programma Horizon2020 e del proprio impegno contrattuale con la Commissione europea. L'Ecso affronta, attraverso gruppi di lavoro, anche altri aspetti politici legati allo sviluppo di un'industria europea per la *cyber-security* e di soluzioni Ue affidabili. In particolare, contribuisce alla definizione di *standard*, test, certificazioni europee, *best practice* e progetti pilota per elementi innovativi della catena di distribuzione. Assicura inoltre l'apertura del mercato a prodotti ICT affidabili, alimenta gli investimenti e offre coordinamen-

to con Paesi terzi. Come Ecso, cerchiamo poi di facilitare la condivisione delle informazioni tra amministrazioni nazionali, *cert* e utenti con l'obiettivo di migliorare il processo di monitoraggio e fornire pareri sulle possibili minacce. Sviluppiamo soluzioni per infrastrutture vitali e fornitori di servizi, in particolare lì dove l'Europa può avere un vantaggio competitivo (sanità, energia, trasporti, sicurezza interna, *e-government*, Industria 4.0, ecc.). Stiamo cercando di incrementare l'uso di soluzioni di *cyber-security* nei differenti mercati e applicazioni, attraverso progetti pilota per l'implementazione di soluzioni prossime alla commercializzazione che dimostrino l'impatto potenziale della sicurezza cibernetica nei diversi settori. Ci poniamo così l'obiettivo di sostenere la crescita delle piccole e medie imprese, accelerando l'ecosistema con un particolare *focus* su *start up* e imprese a crescita rapida. C'è poi l'educazione, altro elemento centrale. Promuoviamo la formazione dei cittadini e dei professionisti affinché vi sia una consapevolezza diffusa delle minacce e delle capacità necessarie per un uso sicuro delle soluzioni informatiche. Infine, stiamo cercando di sostenere l'occupazione nei settori della *cyber-security*.

Tutto ciò richiede fiducia e confidenza nella sicurezza informatica. Questo significa investimenti finanziari, tecnologici e umani. La Commissione europea ha deciso di investire fino a 450 milioni di euro in questo partenariato, all'interno del programma di ricerca e innovazione di Horizon2020 per il periodo 2017-2020. In cambio, si attende che i *player* del comparto investano tre volte tanto nei prossimi anni, per un totale di 1,8 miliardi di euro. In questo modo, stiamo oggi costruendo il futuro della *cyber-security* in Europa. Sin dalla sua creazione, l'Ecso ha acceso la scintilla dell'industria europea dell'Ict. Con 160 membri, è già una delle *partnership* pubblico-private più ampie in Europa, con una *governance* unica. Gli amministratori locali, regionali e nazionali degli Stati membri, i Paesi associati a Horizon2020, all'Eea o all'Efta, possono diventarne membri. Possono partecipare attivamente a tutti i gruppi di lavoro, alle attività e alle strutture decisionali proprio come le grandi società, le Pmi, le *start-up*, i gruppi di ricerca, le università e i *cluster* nazionali o europei. Ognuno con le proprie prospettive e i propri bisogni operativi, e sostenendo l'implementazione dell'Agenda strategica per la ricerca e l'innovazione. Speriamo di portare ancora più *stakeholder* nell'Ecso e di costruire insieme un ecosistema armonizzato e paneuropeo di *cyber-security*.

Traduzione di Stefano Pioppi

PERCHÉ OCCORRE UNIRE LE FORZE

Con il crescente interesse per l'Internet of things, la mole di dati sta crescendo a ritmi allarmanti senza segnali di rallentamento. Siamo a un livello di rischio senza precedenti: un milione di cyber-attacchi vengono sferrati ogni giorno. È necessario tutelarsi facendo sì che la sicurezza metta al sicuro le informazioni personali e di business contro chi vorrebbe danneggiarci

ANDY WATERHOUSE *direttore prevendita Europa, Medio Oriente e Africa di RSA*

Perché occorre unire le forze? Nell'era digitale, la tecnologia avanza a ritmi esponenziali, cambiando le modalità con cui oggi lavoriamo e viviamo. La tecnologia è il motore del progresso umano, ma anche il motore del cambiamento. La nuova era digitale è realmente la quarta rivoluzione industriale, che trasforma vita e lavoro a velocità impressionanti, creando un mondo in cui tutto è interconnesso e generando una grossa mole di dati e di diverse visioni. Le nostre aspettative sono cambiate. La nostra capacità di attenzione si è ridotta. Perfino i pesci rossi hanno oggi un'attenzione più lunga rispetto agli esseri umani a causa dell'impatto che la tecnologia ha su tutti noi. Prima dell'ingresso degli *smartphone*, la nostra capacità di attenzione era di 12 secondi. Ora, è di soli 8. Ci piace avere informazioni e riceverle in tempo reale. Ne generiamo così tante che il 90% dei dati a livello mondiale è stato creato negli ultimi due anni. E tutto questo è stato principalmente guidato dell'incremento esponenziale dell'uso di dispositivi mobili. E con il crescente interesse per l'IoT, la mole di dati sta crescendo a ritmi allarmanti senza segnali di rallentamento. Alcuni di questi cambiamenti spaventano. Siamo a un livello di rischio senza precedenti: un milione di *cyber*-attacchi vengono sferrati ogni giorno. É per questo che dobbiamo tutelarci facendo sì che la sicurezza metta al sicuro le informazioni personali e di *business* contro chi vorrebbe danneggiarci.

In RSA ci siamo relazionati con molti *chief information security officer* (ciso) e *team* di sicurezza per comprendere cosa stesse accadendo nel mercato. Abbiamo compreso due aspetti su tutti. In primo luogo, ci confrontiamo con avversari creativi, pazienti, persistenti, imprevedibili e dotati di moltissimi strumenti a disposizione. Perseverano nelle loro campagne fino a quando non raggiungono l'obiettivo in una superficie d'attacco che cresce come risultato del *cloud*, del *mobile*, dell'IoT. Il perimetro di attacco di un'impresa nell'era moderna è illimitato. In secondo luogo, di conseguenza, non c'è da stupirsi che il 70% delle organizzazioni riportino di aver subito un incidente di sicurezza che ha negativamente impattato sul *business* negli ultimi 12 mesi. Il 90% delle aziende non è soddisfatto del tempo utilizzato per identificare e investigare un attacco. Come risultato, abbiamo stimato che l'80% dei ciso stanno completamente rivedendo la propria strategia di sicurezza. Nel corso degli anni,

LO SCENARIO PREOCCUPANTE
Sono stati cancellati i perimetri con nuove tecnologie come il *cloud*, il *mobile* e l'IoT. Il numero di *device* connessi alla nostra rete cresce di giorno in giorno, con previsioni di oltre 50 milioni di *device* connessi entro il 2020. E la forza-lavoro ora richiede un accesso 24/7 alle risorse aziendali da qualunque luogo, da qualsiasi *device*

IL PROBLEMA DEL GAP OF GRIEF
Ai ceo e al *board* non importa se un *breach* sia stato causato da un *angler toolkit* sfruttando le vulnerabilità di Explorer. Quello a cui sono interessati è l'impatto sul *business*. Diventa per questo sempre più necessario spiegare i dettagli della sicurezza in questa lingua e l'incapacità di farlo è ciò che noi chiamiamo *gap of grief*

LA STRATEGIA DI RSA
La *business-driven security* di RSA fonde il concetto di sicurezza con il contesto di *business* e crea un legame esplicito tra ciò che la sicurezza ci dice oggi e ciò che significa in termini di rischi. Il tutto attraverso tre elementi: *response & detection* rapide, controllo a livello degli accessi utente e gestione del rischio di *business*

per tenere i *bad guys* lontani, molte aziende hanno stratificato con livelli multipli gli strumenti di prevenzione. Siamo partiti con tecnologie statiche, *signature-based*, come i *firewall*, Ids/Ips (*Intrusion detection system/Intrusion prevention systems*) e gli *anti-virus*. Alla maggior sofisticazione delle minacce si sono aggiunti *next-generation firewall*, *sandboxes*, e altre soluzioni per le minacce avanzate. Il problema con questa strategia di "nuova minaccia, nuovo box" è che ha creato una complessità crescente lasciando *gap* nelle coperture e visibilità che gli attaccanti possono sfruttare.
In un *patchwork* di strumenti puntuali, ciascuno offre informazioni limitatamente alla propria area di competenza. Tutti generano *alert* quando qualcosa non funziona nel modo corretto. Ma siccome non sono connessi e non correlano i dati, i *team* di sicurezza si ritrovano in un mare di *alert* da gestire. Alcuni sono reali, ma moltissimi sono dei falsi positivi che esasperano il problema. Senza informazioni sul contesto, non si può determinare se un'attività anomala è benigna o maligna, non si possono connettere una serie disparati di *alert* a una singola campagna di attacco, e non ci si può focalizzare solo su quegli *alert* che potrebbero avere un impatto maggiore sul *business*.
Ciò che è stato costruito nel tempo crea oggi molta complessità, nessun contesto di *business* tra le diverse isole e infine un'inabilità a comprendere se si è implementata una strategia di sicurezza con un impatto significativo. Complessivamente, si è creato un perfetto *habitat* per i *bad guys* che cercano di entrare. Cosa è necessario fare per gestire tutto ciò? Acquisire una visibilità onnicomprensiva che sia più veloce attraverso migliori capacità analitiche e di *detection*. Occorre aumentare la comprensione del contesto di *business* in cui è avvenuto l'incidente e definire attività di risposta più veloci ed efficaci. Infine, occorre migliorare le abilità nel collegare la strategia di sicurezza con le priorità di *business*.
In questo senso, la strategia di RSA fonde il concetto di sicurezza con il contesto di *business* e crea un legame esplicito tra ciò che la sicurezza ci dice oggi e ciò che significa in termini di rischi economici. Il risultato finale è ciò che chiamiamo *business-driven security*. Si tratta di abilitare i tre elementi più critici di una strategia di sicurezza: *response & detection* rapide, controllo a livello degli accessi utente e gestione del rischio di *business*.

NELL'ERA DEL CYBER-ILLUMINISMO

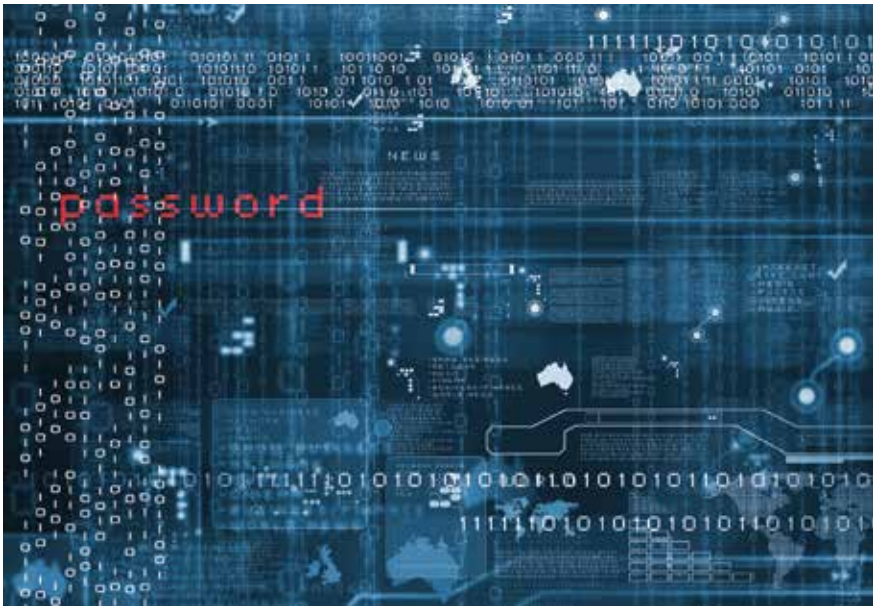
Le nuove tecnologie dovranno rendere sempre più difficile la vita dei cyber-criminali, compiendo un cambiamento nel settore IT al fine di rendere meno vulnerabile un mondo interconnesso che entra nell'era del cyber-Illuminismo. Il futuro sarà sviluppare nuovi sistemi da zero, partendo dal concetto che hackerarli dovrà essere più costoso rispetto ai possibili profitti

MORTEN LEHN *general manager Italia di Kaspersky Lab*

La quantità e le dimensioni degli attacchi informatici sono in costante aumento. Nonostante gli sforzi del mercato, i danni causati da intrusioni e violazioni dei dati sono in crescita. Ogni giorno si registrano più di 300mila attacchi informatici e la situazione è destinata a peggiorare ulteriormente. Alcuni di questi attacchi sono così massicci da minacciare la pace e la sicurezza a livello globale, mentre gli esperti di *cyber*-sicurezza stanno lavorando per garantire la riservatezza, l'integrità e l'accessibilità dei dati all'interno dei sistemi che non sono stati progettati considerando l'eventuale possibilità di un attacco.

Nel prossimo futuro assisteremo allo sviluppo di tre nuovi *trend* nell'ambito della *cyber-security*. In primo luogo, ci saranno più attacchi *cross-border* mirati alle istituzioni finanziarie e, in particolare, alle banche. È lì che si trova il denaro, e hackerare le banche è ormai diventata un'attività criminale redditizia. Temo che ci saranno sempre più attacchi di questo tipo, alcuni di livello molto elevato, altri meno complessi. Alcuni saranno di alto profilo, come nel caso Carbanak, in cui venne rubato un miliardo di dollari da diverse banche, o come l'attacco alla Banca centrale del Bangladesh, durante il quale gli *hacker* riuscirono a sottrarre più di 80 milioni di dollari. In altri attacchi, probabilmente i criminali cercheranno di essere più cauti e rubare somme di denaro più modeste a seconda dei singoli casi, in modo da rimanere nell'ombra e non diventare bersaglio di indagini su larga scala. Nel complesso, le banche, e gli istituti finanziari in generale, sono molto preoccupati per questo tipo di minacce e stanno già lavorando duramente per rinforzare le proprie difese. In secondo luogo, mi aspetto una crescita significativa degli attacchi che riguardano l'*Internet of things*. Abbiamo, infatti, già rilevato casi in cui gli *smart connected device* sono stati infettati per farli diventare parte di *botnet* (una rete infettata) e di attacchi DDoS (*Distributed denial-of-service*), e ritengo che ci saranno molte altre tipologie di infezioni *malware*, magari tramite *ransomware* finalizzati al ricatto. Infine, gli *hacker* svilupperanno metodi per attaccare sistemi industriali e infrastrutture critiche: non ce ne saranno molti di questo tipo, ma saranno quelli più pericolosi.

Alla luce di queste nuove previsioni, è sicuramente importante implementare approcci condivisi, ma anche nuove logiche per contrastare e vincere



GLI STATI UNITI LANCIANO IL PORTALE CYBER.GOV

Greg Touhill, primo capo della sicurezza informatica degli Stati Uniti ha annunciato la prossima apertura di uno sportello *online* dedicato a linee guida da seguire in tema di *cyber-security*. "Cyber.gov – questo il nome del portale – sarà un raccoglitore di *best practice*", ha detto durante un *summit* a Washington il *chief information security officer* (ciso) federale. "Ci siamo focalizzati sull'attuazione di buone pratiche all'interno delle organizzazioni", ha aggiunto. Lo *staff* di Touhill sta ancora lavorando, ma il sito dovrebbe essere *online* entro un paio di settimane

un fenomeno che rischia di creare danni enormi a livello globale. Dal punto di vista normativo, la direttiva europea Network and information security (Nis) rappresenta un passo avanti nella giusta direzione: introduce i requisiti delle indagini sui *cyber*-incidenti e facilita lo scambio di dati nell'Unione europea, rendendo l'Ue e i singoli Paesi più sicuri. Nonostante la sua grande importanza, questa direttiva è solo una legge quadro. È necessario fare qualcosa a livello nazionale. Innanzitutto, i Paesi dovrebbero identificare quali siano effettivamente le proprie infrastrutture critiche, e poi i governi dovrebbero aiutare le imprese basate su queste infrastrutture a capire e misurare il panorama dei rischi e delle tecnologie di protezione, sviluppando guide di *best practice*.

Nel complesso, quindi, il mercato della *cyber*-sicurezza registrerà una crescita: tutto sta diventando sempre più digitale e le infrastrutture IT delle società saranno sempre più complesse, con un numero maggiore di nuovi dispositivi e sistemi. Una quota crescente dei *budget* delle grandi imprese per la *cyber*-sicurezza verrà destinata a diversi servizi e nuove tecnologie. Le grandi aziende spenderanno di più per le piattaforme specializzate nella rilevazione di attacchi mirati nascosti e si assisterà a una crescita del mercato della sicurezza della tecnologia operativa e della protezione dei sistemi industriali computerizzati e connessi. Anche le altre tecnologie emergenti registreranno una crescita sana. Le aziende continueranno a spendere nelle soluzioni di *endpoint-security*, ma con una maggiore enfasi sulle nuove tecnologie. Proprio queste nuove tecnologie dovranno rendere sempre più difficile la vita dei *cyber*-criminali ed è assolutamente necessario un cambiamento nel settore IT al fine di rendere meno vulnerabile un mondo completamente interconnesso e la necessità da parte del mercato della sicurezza IT di entrare in una nuova era di *cyber*-Illuminismo.

Il futuro sarà sviluppare nuovi sistemi da zero, partendo dal concetto che hackerarli dovrà essere più costoso rispetto ai possibili profitti. L'idea è quella di un sistema completamente nuovo con una logica differente rispetto a quelli attuali, in cui si combinano le funzionalità dei sistemi in base agli usi che se ne devono fare.

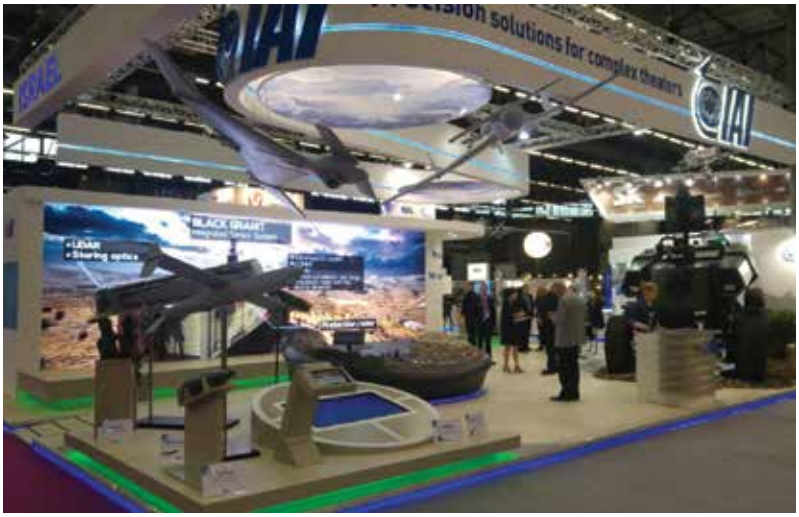
IL RUOLO DI ISRAELE NELLA SFIDA CIBERNETICA

Secondo il Global competitiveness report 2014-2015 del Fondo monetario internazionale, Israele è il terzo Paese al mondo per innovazione. Tra i driver innovativi c'è prima di tutto la crescita dei requisiti cyber; ci sono più minacce, più dati, accessi migliori e dunque un maggiore bisogno di innovazione

ESTI PESHIN *direttore Programmi cyber di Israel Aerospace Industries – IAI*

Le minacce stanno aumentando esponenzialmente. Il mondo *cyber* e quello fisico stanno diventando interconnessi e abbiamo bisogno di un approccio interdisciplinare per contrastare i pericoli moderni. Minacce di livello nazionale richiedono soluzioni di livello nazionale. Come aziende, infrastrutture critiche, governi, o consumatori, facciamo tutti ricorso al *cyber*-spazio. E quando faccio riferimento ai consumatori, porto generalmente l'esempio di mia madre. È una donna abile, che ha lavorato per il governo israeliano per anni, eppure non capisce niente di *cyber*. Nonostante ciò, mia madre fa uso di *social media* e di sistemi di *e-banking*, e necessita dunque di protezione attraverso molteplici soluzioni applicabili: antivirus, *firewall* e intere strutture protettive. E questo è il livello dei consumatori. Quando invece parliamo di sfide di livello nazionale, di protezione di Paesi, di infrastrutture critiche, di sistemi di trasporto globale, tutto ciò richiede soluzioni di livello nazionale. Se prendiamo in considerazione la prospettiva delle infrastrutture critiche, infatti, non possiamo separarla dalla prospettiva di difesa. Gli eserciti e le forze dell'ordine, ad esempio, non possono operare senza alcuni dei servizi offerti dalle infrastrutture critiche. Dall'altra parte, se si danneggia un'infrastruttura critica, si può paralizzare, o quanto meno indebolire. uno Stato nazionale. Questo tipo di sfide sono di grado nazionale e richiedo una soluzione di livello nazionale.

Prendiamo ad esempio in considerazione l'aviazione civile. Al giorno d'oggi, gli aerei sono, in sostanza, dei *data center* volanti con a bordo un mucchio di sistemi computerizzati. Di conseguenza, ci possono essere due tipi di minacce: quelle fisiche (dirottamento, sabotaggio, attacco missilistico, eccetera) e quelle *cyber* (*spoofing* dei sistemi di navigazione, interruzione del servizio, *input* non autenticati, eccetera). Nell'aprile del 2015, un *hacker* di nome Chris Roberts, come riportato dai *media*, è salito su un volo della United. Avrebbe dovuto tenere una conferenza a San Francisco (Stati Uniti), invece prese il volo e twittò che, poiché l'aereo era dotato di *wi-fi*, avrebbe causato la caduta delle maschere per l'ossigeno. Chris è stato bandito a vita dai voli United. Può apparire una punizione eccessiva per quello che sembra uno scherzo, ma Chris è stato in seguito arrestato e interrogato. Nel testo dell'interrogatorio reso pubblico, ha affermato di aver hackerato aeromobili più di venti volte nel corso di due



L'IAI

L'Israel Aerospace Industries (IAI), di proprietà esclusiva del governo israeliano, è la più grande società del Paese nel settore difesa e aerospazio. Fondata nel 1953, ha avuto uno sviluppo parallelo a quello dello Stato di Israele con una particolare attenzione al settore ricerca e sviluppo, a cui sono dedicati dal 2013 cinque centri nel mondo

L'IC3

Il consorzio israeliano delle *cyber* aziende riunisce le maggiori industrie del settore, al fine di individuare soluzioni di interesse nazionale. Oltre alla Iai, azienda leader, figurano Check Point, Verint, ECI, Bynet, Clearsky e CyberX. L'idea di mettere insieme i maggiori fornitori del Paese è nata nel 2011 su iniziativa del governo israeliano in un'ottica collaborativa e strategica

anni. Ha anche ammesso di esserci riuscito penetrando i sistemi avionici attraverso il sistema di intrattenimento *on-board*. La storia è vera o no? L'industria resta un po' perplessa.

In ogni caso, il *cyber*-spazio è in continua evoluzione; oggi assistiamo a un numero sempre maggiore di Paesi che lo percepiscono come un ambito d'interesse nazionale mentre recentemente è stato definito un dominio di battaglia. In questo modo, il mondo sta andando avanti nel riconoscimento del dominio cibernetico. Molta enfasi è posta sulla collaborazione, che è di per sé estremamente importante, ma anche sulla regolamentazione di emergenza. Credo fortemente, dunque, che una delle cose più importanti da fare sia proprio giungere a regole stringenti, per assicurare che il *cyber*-spazio sia più sicuro per tutti noi. C'è inoltre un *focus* sempre crescente sul tema dell'innovazione. Nel mercato, si notano molti attori e una crescente competizione tra un numero sempre maggiore di aziende che acquisiscono competenze cibernetiche. Stanno emergendo anche aziende locali, in grado di fornire soluzioni al proprio Paese. Si assiste, dunque, a un mercato estremamente attraente per gli investitori. Ed è in questo contesto che Israele è considerato un *top innovator*. Secondo il Global competitiveness report 2014-2015 del Fondo monetario internazionale, è il terzo Paese per innovazione. Tra i *driver* innovativi in Israele, c'è prima di tutto il fatto che i requisiti *cyber* siano in costante crescita: ci sono più minacce, più dati, accessi migliori e dunque un maggiore bisogno di innovazione. Israele è così considerato il centro dell'eccellenza internazionale, con un gruppo particolarmente talentuoso in termini di *cyber-capability* e un enorme ecosistema di *start up* di ogni specializzazione.

In questo panorama, l'Israel cyber companies consortium (Ic3) è stato creato al fine di riunire intorno a un tavolo la miglior tecnologia che Israele possa offrire, dalle *start up* alle aziende più grandi. L'Israel aerospace industry è la compagnia leader dell'Ic3, composta poi per la maggior parte da altre sei aziende: Check Point, Verint, ECI, Bynet, Clearsky e CyberX. Il consorzio presenta il meglio del meglio di quello che Israele ha da offrire, con l'obiettivo di garantire soluzioni di livello nazionale a *cyber*-sfide di livello nazionale.

Traduzione di Stefano Pioppi

Maurizio Mensi
avvocato e docente presso la SNA
e la Luiss Guido Carli di Roma

Il riconoscimento facciale in giro per New York

Il 6 ottobre scorso il governatore dello Stato di New York, Andrew Cuomo, ha dichiarato che, per ragioni di sicurezza, intende installare sensori in grado di leggere le targhe delle auto e *software* per sistemi di riconoscimento facciale, da collocare agli incroci stradali e in prossimità di punti sensibili come *tunnel* e ponti fuori Manhattan. Il che, ha immediatamente suscitato polemiche e riportato al centro del dibattito le delicate implicazioni di una tecnica, quella dell'identificazione biometrica e in particolare facciale, che appare destinata a un sempre maggiore utilizzo e che evoca le suggestioni di *Minority Report*, film di successo di qualche anno fa, ove la polizia riusciva a prevedere i reati prima che fossero commessi.

Secondo quanto rivelato dal *New York Times*, in occasione dei giochi olimpici di Sochi del 2014, grazie a una tecnologia chiamata *VibraImage* – simile a quella di una società di Chicago che sta brevettando un sistema che consente, mediante algoritmo, di prevedere il comportamento basandosi sull'espressione, la condotta tenuta e quanto detto da chi è protagonista di video già disponibili in rete – è stato possibile scansionare il volto di milioni di visitatori, così da consentire ai servizi di sicurezza russi (Fsb) di individuare coloro la cui espressione facciale rivelava uno stato di agitazione mentale, tale da far presumere un'imminente minaccia. Il governatore Cuomo ha sostenuto che occorre proteggere le strutture vulnerabili senza precisare peraltro quanti impianti conta di utilizzare, dove collocarli ma soprattutto come saranno trattate e in quali banche dati allocate le immagini raccolte per mettere a confronto i volti dei milioni di automobilisti che ogni giorno arrivano a New York. In realtà, è proprio in base alle concrete modalità e condizioni di utilizzo che può verificarsi la legittimità di una tecnica che presenta rilevanti e delicati implicazioni per la *privacy*, come dimostrato dal rigore sul tema da parte delle varie autorità per la *privacy*. Dalla capacità di prevedere il comportamento degli individui a quella di orientarlo il passo non è troppo lungo e non sono soltanto le forze di sicurezza e i soggetti pubblici a poter fare uso di tali tecniche.

Risulta che l'Fbi disponga di una banca di dati biometrici poderosa, progettata per contenere svariati milioni di immagini di volti, per lo più di cittadini che non sono mai stati sospettati di un crimine, e che il dipartimento per la Sicurezza e altre agenzie Usa non solo si scambino fra loro dati e confrontino le immagini dei sospetti, ma siano già in possesso di tecniche avanzate di riconoscimento facciale. Lo stesso Fbi, a maggio, ha chiesto di essere esonerato dall'obbligo di rivelare chi si trovi nel *database* e di poter custodire senza limiti di tempo tali dati, così da essere in grado di prevedere futuri crimini. Insomma, il tema è quanto mai scottante e sembra destinato ad alimentare con vigore l'annoso e dibattuto dilemma *privacy versus* sicurezza.

Andrea Margelletti *— presidente del CeSI*

Più made in Usa per Israele

Dopo diversi mesi di trattative, Stati Uniti e Israele hanno trovato l'intesa per il rinnovo dell'accordo di assistenza militare che Washington si impegna a garantire a Tel Aviv per i prossimi dieci anni. Il percorso politico e diplomatico che ha portato alla sigla del Memorandum of understanding (Mou) tra i due Paesi è stato segnato da alcuni contrasti relativi all'ammontare degli aiuti, a talune disposizioni che regoleranno le modalità di utilizzo degli stessi e alle recenti politiche di *export* degli armamenti che Washington sta attuando in tutto il Golfo Persico.

Nel dettaglio, il valore del finanziamento ammonta a 38 miliardi di dollari, otto in più rispetto al precedente accordo del 2007, ma due in meno rispetto a quelli ritenuti necessari da Israele per mantenere un adeguato livello di superiorità militare (Qualitative military edge – Qme) nella regione. Si porrà gradualmente fine alla clausola che da circa trent'anni permette a Tel Aviv di destinare poco più di un quarto di questi aiuti alla ricerca, sviluppo e produzione di sistemi d'arma interamente nazionali: per i primi cinque anni, infatti, potrà essere convogliato in questa direzione il 26% dei finanziamenti e, a partire dal sesto anno, tale percentuale diminuirà a poco a poco sino a estinguersi del tutto nell'ultimo.

Quest'ultima disposizione, in particolare, segna un duro colpo per l'industria della difesa israeliana che verrà quindi privata di ingenti risorse per ricerca e sviluppo. Fino a oggi, infatti, programmi di successo tra cui l'Iron dome, il David's sling e l'Arrow, sono stati realizzati anche grazie al sostanziale contributo degli Stati Uniti.

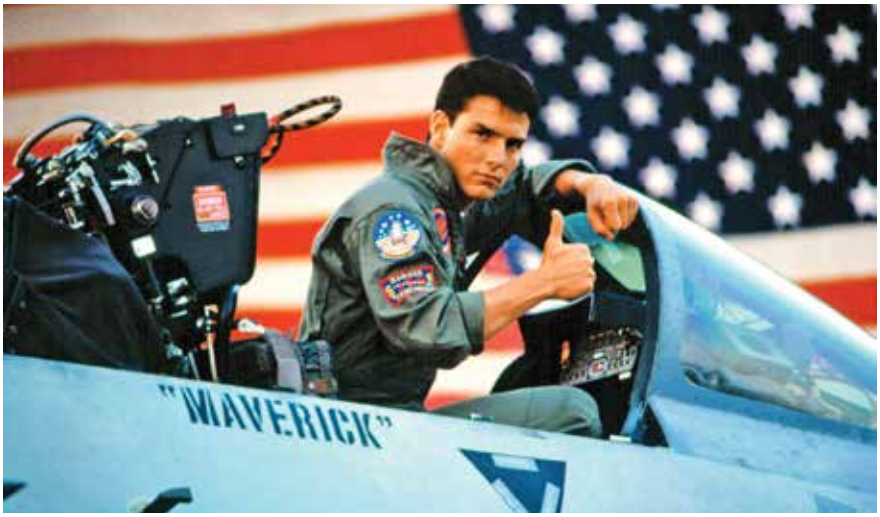
È indubbio che, su questa decisione, abbia pesato il parere dei colossi della difesa americana. Infatti, da un lato l'intesa vincolerà progressivamente Israele a utilizzare il denaro del contribuente americano per acquistare esclusivamente prodotti *made in Usa*, dall'altro limiterà le potenzialità di un concorrente sempre più scomodo nel mercato mondiale della difesa. In conclusione, quindi, il nuovo accordo tra Stati Uniti e Israele in materia di aiuti militari segna sì un incremento di risorse a favore di Tel Aviv nei prossimi dieci anni, ma al prezzo di una maggior dipendenza strategica, industriale e militare da Washington.

PROVE DI CYBER WARFARE MANDANO MAVERICK IN PENSIONE?

Mentre dovremo aspettare qualche decennio per vedere eserciti composti da robot, nel contesto della cyber warfare sono già disponibili sistemi in grado di operare a una velocità impossibile all'essere umano. Nelle intenzioni del Pentagono si tratta sempre di sistemi che non puntano a sostituire l'uomo, ma a supportarlo in modo efficace

ANDREA MELEGARI *chief marketing & innovation officer – CY4Gate Srl*

Nel mondo militare, e nell'immaginario collettivo creato anche dal celebre film *Top Gun*, interpretato da un giovanissimo Tom Cruise, i piloti di aerei da caccia sono sempre stati descritti come il frutto di una selezionatissima *élite* di *Superman*.
Ma c'è chi mette in dubbio la supremazia del genere umano. In un duello simulato, il colonnello Gene Lee, pilota pluridecorato, istruttore di volo e abituato a confrontarsi ed esercitarsi con simulatori di volo in battaglie virtuali, è stato abbattuto in diversi test da Alpha, un *software* d'intelligenza artificiale sviluppato in Ohio da un piccolo *pool* di imprese e ricercatori universitari.
"Sono rimasto sorpreso dalla reattività e dalla capacità del *software* di anticipare le mie intenzioni e di reagire istantaneamente ai miei cambi di strategia in modo da vanificare le mie manovre e i miei attacchi". Il successo di Alpha s'inserisce perfettamente in un dibattito di grande attualità: quali compiti affiderà il Pentagono ai *robot*?
Il Pentagono, infatti, ha deciso di intensificare gli investimenti in algoritmi d'intelligenza artificiale nel tentativo di colmare un *gap* con l'industria privata, dove i *robot* trovano già grande impiego in molte attività che un tempo costituivano una prerogativa esclusivamente umana.
Come spesso accade oltreoceano, alle intenzioni si affiancano sempre investimenti adeguati che, secondo le dichiarazioni del vice ministro della Difesa americano Robert Work dovrebbero variare dai 12 ai 15 miliardi di dollari nel *budget* previsto per il 2017. Lo sviluppo di nuove forme d'intelligenza artificiale applicate alle tecnologie già in uso è considerato infatti un fattore-chiave per garantire agli Stati Uniti un vantaggio strategico nel dominio militare.
Mentre dovremo probabilmente aspettare qualche decennio per vedere eserciti composti da *robot*, in altri contesti l'intelligenza artificiale e le tecnologie di *machine learning* si evolvono più rapidamente e sono già impiegate.
Si tratta, ad esempio, di *software* in grado di analizzare enormi volumi di dati con l'obiettivo di intercettare segnali di cambiamento sociale e fornire



agli analisti indicatori utili per mitigare il cosiddetto effetto sorpresa. Recentemente, la società italiana Expert System, specializzata nell'analisi strategica di grandi moli di informazioni, aveva anticipato chiaramente il risultato del *referendum* sulla Brexit elaborando automaticamente il contenuto di migliaia di contenuti pubblicati su Twitter. Anche nel contesto della *cyber warfare* sono già disponibili sistemi in grado di operare a una velocità impossibile all'essere umano. Nelle intenzioni del Pentagono si tratta sempre di sistemi che non puntano a sostituire l'uomo, ma a supportarlo in modo efficace. Robert Work ha infatti affermato che "l'intenzione è dotarsi di sistemi che in situazioni di attacco siano in grado di garantire protezione e supporto grazie alla reattività e alla velocita che *software* d'intelligenza artificiale sono in grado di garantire, ma l'uomo rimarrà l'unico a decidere se e quando esercitare la forza letale".
Nonostante queste rassicurazioni, il pensiero torna alla finzione cinematografica del film *Terminator*, dove Skynet, la rete immaginaria composta da super-computer, decide che per adempiere al compito di salvaguardare il mondo, la migliore strategia è l'eliminazione del genere umano.
È comprensibile come questa discussione stia sviluppando un acceso dibattito su impatti e rischi sociali di un utilizzo improprio dell'intelligenza artificiale. Google, in collaborazione con l'Università di Stanford, ha identificato i fattori critici e una serie di raccomandazioni che ogni programmatore dovrebbe considerare quando sviluppa un *software* di intelligenza artificiale, così da evitare la creazione di *robot* che possano essere rischiosi per gli esseri umani.
Ma la vera perplessità è un'altra. Che cosa ci deve preoccupare di più?
Il fatto che un algoritmo di intelligenza artificiale abbia battuto un esperto *top gun* o che questo algoritmo sia stato sviluppato da Nick Ernst, un giovane laureato, fondatore e ceo di Psibernetix, una *start up* con sede in Ohio che nel proprio sito *web*, a oggi, dichiara un *team* di tre persone (fondatore incluso)?

BUSSOLA *del*MESE LOCAL

RINNOVATO IL CDA DI ENAC E PRESENTATO IL BILANCIO STAGIONALE

Palazzo Chigi ha proceduto al rinnovo del consiglio di amministrazione dell'Ente nazionale per l'aviazione civile (Enac): confermato presidente Vito Riggio, mentre entrano nel consiglio Alfredo Pallone, Angela Stefania Bergantino, Manlio Mele e Luisa Riccardi. Presentato anche il bilancio della stagione estiva 2016. Tra gennaio e agosto 2016 sono stati registrati 110.828.632 passeggeri, il 4,3% in più rispetto all'anno precedente. L'incremento è pressoché lo stesso (+4,2%) anche considerando i soli mesi di luglio e agosto.

MBDA ITALIA, PERFETTI LASCIA, NOMINATO DI BARTOLOMEO

Dopo sette anni di attività in MBDA, Antonio Perfetti si è dimesso dalle cariche di *executive group director sales and business development* del gruppo e *managing director* di MBDA Italia. Il successore di Perfetti è Pasquale Di Bartolomeo per MBDA Italia. La notizia arriva proprio quando sembra che Leonardo-Finmeccanica stia considerando seriamente l'opportunità di cedere la propria quota del 25% del colosso missilistico, *joint venture* con Airbus e BAE Systems.

PROLUNGATA LA MOSTRA SU DA VINCI A BARI

Sebastiano Leo, assessore all'Istruzione, alla formazione e al lavoro della Regione Puglia ha comunicato la proroga fino al 30 novembre della mostra "Il volo: dalle Ali di Leonardo... a oggi (1480 – 2016)", attualmente ospitata presso l'aeroporto Karol Wojtyla di Bari. Inoltre, la mostra è stata arricchita con l'esposizione di otto dei dieci Codici vinciani anastatici, che si aggiungono alle 42 macchine di Leonardo già esposte. L'affluenza elevata ha indotto Aeroporti di Puglia a un aggiuntivo sforzo organizzativo per soddisfare le ulteriori richieste pervenute dalle scuole pugliesi.

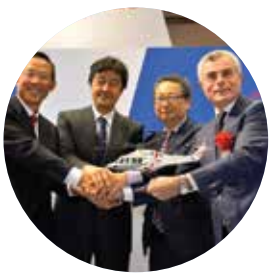
ALITALIA CEDE SLOT DI HEATHROW A ETIHAD

Lo scorso luglio Alitalia ha ceduto a Etihad alcuni *slot* all'aeroporto londinese di Heathrow. Si tratta delle fasce orarie che consentono di decollare e atterrare in un aeroporto. La vendita (60 milioni di euro) da parte di Alitalia al suo azionista è stata necessaria per ridurre le perdite della compagnia. La cessione di alcuni *slot* era già prevista negli accordi iniziali previsti tra le due compagnie.

CARABINIERI, RENZI INAUGURA LA SCUOLA MARESCIALLI DI FIRENZE

È stata inaugurata la scuola marescialli dei Carabinieri Felice Maritano di Firenze. "Nella mia precedente esperienza amministrativa – ha detto il presidente del Consiglio Matteo Renzi presente alla cerimonia – ho sempre sognato di vedere realizzata questa scuola, un'opera imponente che realizza obiettivi strategici". Oltre al *premier*, erano presenti il ministro della Difesa Roberta Pinotti, il capo di stato maggiore della Difesa, generale Claudio Graziano e il comandante generale dell'Arma, Tullio Del Sette.

NUOVI ORDINI PER GLI ELICOTTERI DI LEONARDO



Incetta di ordini all'Helitech di Amsterdam e al Japan Aerospace di Tokyo per gli elicotteri di Leonardo. Dall'Olanda richiesti un GrandNew per la società svizzera Centaurium Aviation, e sei AW169, di cui tre per l'irlandese Lease corporation international, uno per la tedesca HeliService international GmbH, e due (con opzione sul terzo) per Helikore per il debutto coreano del bimotore. A Tokyo, è arrivato un ordine per un GrandNew da parte di un cliente privato e l'annuncio di due lettere di intenti per due AW139 selezionati da Nippon TV e Chukyo TV per Electronic news gathering.

BUSSOLA *del*MESE LOCAL

RR FORNIRÀ A FINCANTIERI I MOTORI PER 7 PATTUGLIATORI

Rolls-Royce fornirà 14 dei più potenti motori diesel Mtu per equipaggiare i sette pattugliatori polivalenti d'altura che saranno costruiti per la Marina militare italiana da Fincantieri. La costruzione dei sette pattugliatori fa parte del piano di rinnovamento della flotta della Marina. I motori ordinati, 20V 8000 M91L, producono ciascuno 10 MW di potenza e saranno consegnati a partire dal 2017. È la prima volta che motori Mtu saranno utilizzati su nuove unità di superficie della Marina italiana. Mtu Italia fornirà, per questi motori, anche assistenza tecnica e supporto logistico.

ACCORDO DI COOPERAZIONE FRA ENAC E REPUBBLICA DEL CONGO

Il direttore generale dell'Ente nazionale per l'aviazione civile (Enac) Alessio Quaranta ha firmato un protocollo di cooperazione con l'Autorità per l'aviazione civile (Anac) della Repubblica del Congo, rappresentata dal direttore generale aggiunto Marcellus Boniface Bongho. Il protocollo riguarda specificatamente la sorveglianza su elicotteri della società Inaer che opereranno in Congo per assicurare il servizio *offshore* per conto di Total E&P Congo e ENI Congo S.A. Questa prima e limitata cooperazione potrebbe portare a un potenziamento successivo.

IL MINISTRO PINOTTI IN OMAN PER RAFFORZARE LA COOPERAZIONE

Il ministro della Difesa Roberta Pinotti ha visitato il sultanato dell'Oman per una serie di incontri mirati al rafforzamento delle relazioni bilaterali e in particolare della cooperazione militare. Durante la visita, il ministro ha assistito insieme al collega omanita Sayyid Badr bin Saud al-Busaidi alla prima edizione di un'esercitazione bilaterale denominata Sun mountain 2016, che "ha coinvolto circa 120 uomini delle Forze armate italiane e si prefigge lo scopo di addestrarsi congiuntamente in ambiente montano e desertico", ha spiegato il ministero in una nota.

PIAGGIO CONSEGNA IL PRIMO AVANTI EVO COSTRUITO AD ALBENGA

L'ad di Piaggio Aerospace – Renato Vaghi – ha consegnato lo scorso 7 ottobre allo sceicco Khalifa Al Saif, ad e fondatore dell'omonimo gruppo, il primo Avanti Evo prodotto nel nuovo stabilimento di Villanova d'Albenga. Lo scorso luglio Al Saif era stato anche designato quale agente per la vendita dell'Avanti Evo in Arabia Saudita, Kuwait, Bahrain, Qatar, Oman e Iraq. Al Saif ha sottoscritto anche un'opzione per l'acquisto di un secondo velivolo per operazioni medevac (*medical evacuation*) che sarà consegnato nel 2017. Questo primo Avanti Evo, in configurazione VIP, sarà invece impiegato per voli *charter* e dimostrativi.

LA SEMESTRALE DI ENAV EVIDENZIA RISULTATI IN CRESCITA

Il consiglio di amministrazione dell'Enav, riunitosi sotto la presidenza di Ferdinando Franco Falco Beccalli, ha approvato la relazione finanziaria semestrale al 30 giugno 2016. Rispetto allo stesso periodo dell'anno precedente, i ricavi sono cresciuti del 4,3%, raggiungendo i 408,9 milioni di euro, mentre il risultato netto si è consolidato in aumento a 22,2 milioni di euro (+41,1%). Il traffico di rotta, in termini di unità di servizio, è aumentato dello 0,7% mentre il traffico terminale, concernente le attività di decollo e atterraggio, è cresciuto ancora di più (+3,1%).

A LEONARDO-FINMECCANICA IL "PREMIO DEI PREMI"

Il colosso italiano della difesa si è aggiudicato il più prestigioso riconoscimento italiano dedicato all'innovazione *made in Italy*. Si tratta del premio nazionale per l'innovazione, meglio conosciuto come "premio dei premi", conferito nel corso di una cerimonia al palazzo del Quirinale, alla presenza del presidente della Repubblica. Leonardo si è aggiudicata la vittoria grazie a un progetto che consente di evitare il rischio di collisioni in volo tra velivoli pilotati e a pilotaggio remoto e garantire la sicurezza degli spazi aerei civili..

BUSSOLA *del*MESE LOCAL

IN VISITA A ROMA IL SEGRETARIO USA PER L'AERONAUTICA

Deborah Lee James, segretario statunitense per l'Aeronautica, è stata a Roma per incontrare alti rappresentanti del ministero della Difesa italiano e visitare il Comando operazioni aeree e il Deployable air command and control centre (Daccc) della Nato a Poggio Renatico. Il segretario, in *tour* in Europa per rafforzare la cooperazione transatlantica in materia di sicurezza, ha detto di aver avuto "un colloquio molto proficuo con gli ufficiali italiani della difesa su quali dovrebbero essere i punti focali della cooperazione tra le nostre forze aeree".

CINQUE AW169 IN BRASILE

Continua a crescere il successo dell'AgustaWestland AW169 in Brasile. Leonardo-Finmeccanica ha annunciato la firma di ordini per cinque nuovi elicotteri da parte di più clienti, *corporate* e privati. Bimotore di grande versatilità, l'AW169 ha incontrato il favore del mercato brasiliano e di quello internazionale. Sale, infatti, a più di venti il numero di AW169 già destinati al Brasile, e a oltre 150 gli ordini (tra cui opzioni e accordi quadro) per questo modello da tutto il mondo. L'annuncio arriva appena dopo la presentazione di fine agosto della nuova configurazione VIP dell'elicottero.

IMMOBILI DELLA DIFESA: A MODENA PROTOCOLLO D'INTESA

Il ministro della Difesa Roberta Pinotti ha firmato un protocollo d'intesa con il comune di Modena e l'Agenzia del demanio per la valorizzazione di immobili non più in uso alla Difesa. Si tratta del magazzino Santa Caterina e della caserma Pisacane, ora a disposizione della collettività. L'accordo si inserisce nel programma di valorizzazione e razionalizzazione degli immobili militari della Difesa fortemente voluto dal ministro. Dal 2014, sono state ridotte le infrastrutture necessarie alle Forze armate, rendendo disponibili, per altre finalità pubbliche, circa 650 infrastrutture.

TELESPAZIO BRASIL PREMIATA PER I SERVIZI DI TELECOMUNICAZIONE

La controllata brasiliana di Telespazio ha ricevuto dalla pubblicazione *Anuario Telecom* il premio "Destaque do ano" per i servizi di infrastruttura di rete. All'azienda del gruppo Telespazio è stata riconosciuta la migliore prestazione in tale categoria nel corso del 2015. I riconoscimenti assegnati da Anuario Telecom, che compila ogni anno la classifica delle maggiori 100 aziende del Paese, premiano sia i prodotti sia i servizi, abbracciando quindi l'intero comparto delle telecomunicazioni. Telespazio Brasil aveva già ottenuto riconoscimenti da Anuario Telecom nel 2011 e 2012.

ANCHE L'ITALIA ALL'EURONAVAL 2016

A Parigi, in occasione dell'Euronaval 2016, il principale salone internazionale dedicato al settore navale, Leonardo-Finmeccanica ha presentato alcune novità della propria offerta. Tra i sistemi esposti, il "*cockpit* navale" per la gestione integrata delle operazioni di conduzione della nave e del sistema di combattimento. Nell'abitacolo, c'è anche il nuovo Combat management system, centro di comando e controllo della nave. Esposti inoltre equipaggiamenti di guerra marina e sottomarina, tra cui il piccolo e potente *sonar* Atas e il cannone navale di grosso calibro 127/64 Light Weight.

L'ITALIA RAFFORZA LA COOPERAZIONE SPAZIALE CON LA RUSSIA

In occasione della 14esima sessione del Consiglio italo-russo per la cooperazione economica, industriale e finanziaria (Circeif) si è riunito alla Farnesina anche il gruppo spazio, presieduto dai rappresentanti delle due agenzie spaziali: Sergey Saveliev, vice presidente di Roscosmos e Gabriella Arrigo, responsabile relazioni internazionali dell'Asi. Al centro del dibattito, i progetti di cooperazione bilaterale, tra cui lo sviluppo di un sistema satellitare di osservazione della Terra geosincrono, il progetto di astrofisica Millimetron, la collaborazione sulla stazione spaziale e la missione ExoMars.

BUSSOLA *del*MESE GLOBAL

AL VIA IL PROGRAMMA DREAM CHASER FOR EUROPEAN UTILIZATION

Il programma Dream chaser for european utilization (Dc4eu) prende ufficialmente il via con la firma di un protocollo d'intesa che ne sancisce l'avvio della fase pilota. A siglare l'accordo sono stati Sierra nevada corporation, Telespazio (Leonardo-Finmeccanica/Thales), Agenzia spaziale europea e OHB System Ag. I partner valuteranno ora la fattibilità e la redditività commerciale delle missioni Dc4eu, in grado di garantire all'Europa un accesso indipendente alle missioni in orbita bassa attraverso uno Space utllity vehicle.

L'ITALIA CONFERMATA NEL CONSIGLIO ESECUTIVO ICAO

La 39sima assemblea generale dell'Icao ha confermato l'Italia tra le nazioni in prima fascia nel Consiglio esecutivo. Il nostro Paese ha ottenuto 166 preferenze (16 in più rispetto al 2013) su 170 votanti, dietro solamente al Brasile. Pochi giorni prima, il direttore generale dell'Enac Alessio Quaranta, a guida della delegazione italiana, era stato eletto presidente della Commissione legale dell'Icao, mentre il nostro Paese era stato premiato dal presidente del Consiglio dell'Icao Olumuyiwa Benard Aliu per gli elevati *standard* raggiunti in termini di sicurezza del volo e del trasporto aereo.

L'ULTIMO SALUTO DI ROSETTA

La sonda dell'Esa Rosetta è scesa sulla superficie della cometa 67P/Churyumov-Gerasimenko, portando a termine la propria missione dopo dodici anni di intensa attività e non prima di aver scattato e inviato le ultime immagini. Partita a marzo del 2004, Rosetta è stata la missione *cornerstone* del programma Esa dedicato allo studio dei corpi minori del Sistema solare. Prima di "accometare", Rosetta ha effettuato tre *flyby* della Terra, uno di Marte, due sorvoli di asteroidi (Steins e Lutetia) e il rilascio del *lander* Philae a novembre 2014, primo veicolo a posarsi su una cometa.

ARIANE 5 EGUAGLIA IL RECORD DI SUCCESSI DI ARIANE 4

Il lanciatore pesante di Airbus Safran Launchers ha concluso con pieno successo la sua quinta missione del 2016, portando in orbita due satelliti per telecomunicazioni: Sky Muster II per l'operatore australiano National broadband network, e GSAT-18 per l'agenzia spaziale indiana Isro. Con la missione VA231, l'ottava dell'anno per l'operatore Arianspace, Ariane 5 (oltre 50 metri di altezza per una massa di 780 tonnellate) eguaglia il *record* del fratello minore: 74 missioni di fila. Ariane 4 ci era riuscito nel periodo 1995-2003.

L'ICAO ADOTTA UNA RISOLUZIONE PER RIDURRE LE EMISSIONI DI CO_2

L'accordo è stato raggiunto nel corso della 39sima Assemblea generale a Montreal. L'Icao ha adottato una risoluzione per il contenimento delle emissioni di CO_2. L'accordo, già definito a febbraio, si suddivide in tre fasi: tra il 2021 e il 2023 la fase pilota; nei successivi tre anni una fase volontaria alla quale partecipano gli Stati già aderenti alla fase pilota; e dal 2027 al 2035 la fase a partecipazione obbligatoria per tutti. Si tratta di un sistema g*lobal market-based* che dovrebbe portare alla compensazione di circa l'80% delle emissioni tra il 2021 e il 2035.

A TERRA PARTE DEI TORNADO TEDESCHI

Viti allentate nell'abitacolo hanno imposto uno stop per oltre trenta velivoli da combattimento Tornado della Luftwaffe. Costretti a terra anche quelli impegnati nelle operazioni contro lo Stato islamico, di base nel sud della Turchia a Incirlik, impiegati per le operazioni di ricognizione e monitoraggio in Siria. La notizia è stata resa nota dall'agenzia di stampa tedesca Dpa. Già l'aggiornamento del *software* sui Tornado tedeschi, a inizio 2016, aveva prodotto un problema di eccessiva luminosità del pannello strumenti dell'abitacolo.

BUSSOLA *del*MESE GLOBAL

ACCORDO DI 40 PAESI SULLA VENDITA DI DRONI ARMATI

Circa quaranta Paesi, tra cui l'Italia, hanno firmato una dichiarazione che intende regolamentare l'uso e la vendita all'estero dei droni armati, con l'obiettivo di non farli cadere nelle mani sbagliate. Il documento rappresenta, secondo gli Usa, un primo passo verso la stesura di una normativa globale sull'uso dei velivoli per uso militare. Russia, Cina, Francia, Israele e Brasile, non hanno firmato l'accordo; sono in parte già esportatori di droni e potrebbero trarre vantaggi dal fatto che gli Usa si impegnano a trattare con maggiore cautela l'esportazione di Uav.

AIRBUS, È INIZIATO L'ASSEMBLAGGIO DEL PRIMO A330NEO

A Tolosa, la compagnia europea Airbus ha iniziato l'assemblaggio finale del suo primo A330neo, un A330-900, con l'integrazione delle ali alla fusoliera centrale. Sia l'A330-800 che l'A330-900 sono dotati di nuove ali ispirate all'A350 con *sharklet* situati alle estremità, di motori Trent 7000 di Rolls-Royce e della nuova cabina AirSpace di Airbus. L'A330neo presenta una riduzione dei consumi di carburante del 14%. A oggi, dieci clienti ne hanno ordinati un totale di 186. Intanto, China Airlines è diventata il nono operato a operare il *widebody* A350 XWB.

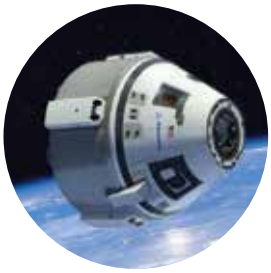
MICIUS IN ORBITA: LA CINA PUNTA SULLA COMUNICAZIONE SICURA

Il satellite cinese QSS, chiamato anche Micius, è apripista e prototipo di una serie di tecnologie dedicate alla comunicazione ottica e in particolare alla sicurezza della comunicazione quantistica (o comunicazione codificata, fondamentale per la sicurezza nazionale e per l'*intelligence*). Pechino ha investito 100 milioni di dollari in questa missione della durata di due anni, il cui obiettivo è trasmettere un segnale ottico attraverso il vuoto spaziale e usare un satellite come ripetitore.

PENTAGONO: OBBLIGO DI NOTIFICA DEGLI INCIDENTI CYBER

La Final rule del programma per la *cyber-security* del dipartimento della Difesa (DoD) americano sarà in vigore dal prossimo 3 novembre. Da quel giorno, tutte le aziende e i loro subappaltatori che svolgano qualsiasi tipologia di attività nei confronti del DoD saranno obbligati a comunicare entro 72 ore ogni incidente informatico occorso ai loro sistemi. In questo modo, la difesa americana obbliga tutte le società con cui collabora alla condivisione rapida delle informazioni relative a eventuali attacchi, rafforzando il sistema di sicurezza nazionale e contrasto alla criminalità informatica.

BOEING RIMANDA DI SEI MESI LO SVILUPPO DELLA CST-100



Il portavoce di Boeing William Barksdale ha annunciato che, a causa di una serie di questioni legate a sviluppo e produzione, l'azienda ha deciso di ridefinire la scaletta per la capsula spaziale CST-100 Starliner. Vengono così riprogrammati i test di volo di un progetto che rientra nel contratto Commercial crew transportation capability stipulato tra la compagnia e la Nasa. In questo modo, scala ad agosto 2018 il primo test con equipaggio (un astronauta Nasa e un pilota Boeing) e a dicembre dello stesso anno la prima missione operativa verso la Iss.

CHRISTIAN SCHERER SARÀ IL NUOVO CEO DI ATR

Christian Scherer sostituirà Patrick de Castelbajac come *chief executive officer* di ATR. Lo hanno deciso Airbus Group e Leonardo-Finmeccanica che possiedono in *joint venture* paritetica il costruttore, stabilendo la durata del mandato pari a quattro anni nel tentativo di garantire stabilità per la nuova gestione esecutiva. Patrick de Castelbajac lascia la carica dopo circa due anni e mezzo; ora sarà *company secretary* e capo dello *staff*. Il passaggio sarà effettivo dal prossimo 1 novembre. Giovanni Tramparulo, è stato confermato per altri quattro anni come *chief financial officer*.

BUSSOLA *del*MESE GLOBAL

MAXI ORDINE PER BOEING DALLA QATAR AIRWAYS

Qatar Airways ha annunciato i propri piani di acquisto da Boeing per trenta 787-9 Dreamliner e dieci *widebody* 777-300Er. A ciò, si aggiunge una lettera di intenti per altri 60 aeromobili B737 MAX 8. In tutto, la maxi commessa ha un valore complessivo, a prezzo di listino, di 18,6 miliardi di dollari. Alla cerimonia per l'annuncio della nuova commessa hanno preso parte il ministro delle finanze del Qatar Shareef Al Emad, l'ambasciatore dell'Emirato presso gli Stati Uniti Mohammed Jaham Al-Kuwari e il vice segretario di Stato Usa Tony Blinken.

ACCORDO GOOGLE-SPACEFLIGHT PER LANCIO DI SATELLITI NEL 2017

I satelliti per l'osservazione terrestre di Terra Bella, controllata di Google, saranno portati in orbita dalla Spaceflight Industries a bordo di un razzo Falcon 9. Secondo il recente accordo, il lancio è previsto per la fine del 2017 dalla base di Vandenberg in California. Oltre agli SkySat di Terra Bella, che raggiungeranno gli altri satelliti della famiglia Google (di cui gli ultimi quattro lanciati da un Vega lo scorso 15 settembre) viaggeranno sullo stesso volo più di venti carichi utili differenti. Sempre nel 2017, altri SkySat saranno lanciati da Orbital ATK a bordo di un Minotaur-C.

AIRBUS CONSEGNA IL SUO DECIMILLESIMO AEROMOBILE

Airbus ha festeggiato la consegna del suo decimillesimo aeromobile. Si tratta di un A350-900 con il logo speciale "10.000th Airbus", che è entrato a far parte della flotta di Singapore Airlines. Tra i nuovi *record* della compagnia francese anche il più elevato livello di produzione di tutti i tempi, con un *backlog* di 6.700 aeromobili (10 anni di produzione). Entro metà 2017 consegnerà il nuovo A350-1000, cui farà seguito la consegna del primo A330neo con alti livelli di riduzione dei consumi e maggiori *comfort*.

AIRBUS E ORBITAL ATK VERSO IL NUOVO EUTELSAT

Eutelsat Communications ha scelto Airbus defence and space e Orbital ATK per la costruzione del suo nuovo satellite, l'Eutelsat 5 West B, che dovrà servire principalmente i mercati video in Europa e Nord Africa. In base ai termini del contratto, sarà Airbus Defence and Space a costruire il *payload* del satellite, mentre la piattaforma sarà prodotta da Orbital ATK. L'Eutelsat 5 West B, il cui lancio avverrà nel 2018, andrà a sostituire il West A nell'intenzione di applicare il principio del *design-to-cost* per la riduzione dei costi e il mantenimento degli elevati *standard* delle *performance*.

LA STAZIONE SPAZIALE CINESE PRESTO VISIBILE DALLA TERRA

Sarà presto visibile dalla Terra la nuova Stazione spaziale cinese, Tiangong-2, lanciata lo scorso 15 settembre con il razzo Lunga marcia 2F, dal centro di lancio Jiuquan. La stazione, che sarà abitata per 30 giorni dagli astronauti Jing Haipeng e Chen Dong partiti il 16 ottobre, orbita intorno alla Terra a una inclinazione vicina ai 42.8 gradi (più bassa rispetto alla Stazione spaziale internazionale) e sarà visibile nell'80% dalle regioni non abitate della Terra. Ma dal 31 ottobre al 16 novembre Tiangong-2 sarà visibile dopo il tramonto negli Usa, Canada e gran parte dell'Europa.

LA SPAGNOLA BINTER ORDINA ALTRI SEI ATR 72-600S

La compagnia aerea spagnola Binter ha firmato un ordine per altri sei ATR 72-600s. Sale così a 18 il numero totale di ordini per l'aeromobile che sta continuando a riscuotere importanti consensi nel mercato europeo. Binter ha tra l'altro già ricevuto quattro ATR 72-600s, e punta a sostituire completamente la propria flotta di ATR 72-500s con i più moderni aeromobili della *joint venture* paritaria tra Leonardo e Airbus Group. Gli aeromobili sostituiti saranno operati dalla sussidiaria Binter CV per il *network* di Capo Verde mentre i nuovi ATR 72-600s serviranno la rete delle isole Canarie.

NOI, LA NATO E IL VALORE DEL DIALOGO

Va affermata con priorità la regola del ristabilimento della legalità internazionale. La via del dialogo rimane centrale, ma presupposto del dialogo è la compattezza e la solidità dell'Alleanza e per questo l'Italia ha risposto nei fatti all'appello degli alleati nordici e non ha mai fatto mancare loro la propria concreta vicinanza

SERGIO MATTARELLA *presidente della Repubblica italiana*

Soltanto una rinnovata prova di unità e solidarietà fra alleati può difendere i valori delle nostre democrazie. Valori che sono alla base del vincolo liberamente assunto tra i Paesi dell'Alleanza, che oggi va rafforzato, alla luce della realtà che viviamo e che ci spinge, ancor più che in passato, a dover superare i confini – o visioni puramente domestiche – perché soltanto insieme potremo essere tutti più sicuri, più forti, più liberi.

L'Italia non ha mai fatto mancare il proprio contributo in termini di visione, prima ancora che in uomini e mezzi, alla famiglia atlantica. Una partecipazione attiva e responsabile fondata sulla solidarietà fra membri. È infatti in questi valori che ancora oggi, a distanza di quasi settant'anni, ci riconosciamo. Quei valori che ci portano oggi a considerare positivamente le richieste di rassicurazione da parte dei nostri alleati dell'est europeo, ma anche a garantire una continuità alla nostra partecipazione alle missioni in Afghanistan e in Kosovo.

Sul piano strategico è vivo il dibattito sulla minaccia proveniente da est. Non è mancato chi ha assimilato le frizioni dell'ultimo periodo a un ritorno alla Guerra fredda. Ma nessuno può riportare indietro la storia, né tanto meno appare sensato riproporre il ripristino di una barriera che rievoca fatalmente quella cortina di ferro che umiliò per tanto tempo le aspirazioni di libertà di interi popoli e per smantellare la quale fu necessaria la determinazione del mondo atlantico e il lungo percorso messo in campo con la Conferenza di Helsinki. È indispensabile che si ponga fine all'irragionevole momento di tensione, la cui pericolosità vivono, quotidianamente, i nostri militari. Le esibizioni di forza, il continuo saggiare le forze, sono solo l'avvio di *escalation* per smontare le quali occorrono poi anni di ripristino di reciproca fiducia. Va affermata con priorità, naturalmente, la regola del ristabilimento della legalità internazionale. La via del dialogo rimane centrale. La convocazione del Consiglio Nato-Russia ha rappresentato un passo nella giusta direzione e ci auguriamo che tale filo non venga spezzato, auspicando che la Russia voglia seriamente collaborare in questa direzione. "Sicurezza militare e una politica di distensione non sono contraddittorie ma complementari" si legge nel rapporto Harmel

STOLTENBERG A ROMA PER I 65 ANNI DEL NDC
È stato celebrato a Roma il 65simo anniversario della fondazione del Nato Defense College, alla presenza dei massimi vertici dell'Alleanza atlantica. Palazzo Baracchini ha ospitato due giorni di *meeting* con il segretario generale della Nato Jens Stoltenberg, il presidente della Repubblica Sergio Mattarella e il presidente del comitato militare, il generale Petr Pavel. Celebrati anche i 50 anni del trasferimento del Ndc a Roma

del 1967. Ma – desidero ribadirlo – presupposto del dialogo è la compattezza e la solidità dell'Alleanza e per questo l'Italia ha risposto nei fatti all'appello degli alleati nordici e non ha mai fatto mancare loro la propria concreta vicinanza.
Identica coerenza e responsabilità occorre avere, naturalmente, nell'affrontare le tensioni presenti nello scacchiere cui guarda il Mediterraneo, per le numerose situazioni di instabilità che si stendono su di un arco che va dall'Iraq e dalla Siria e, passando dalla Libia, giunge sino al Sahel. Terrorismo ed emergenza migratoria e umanitaria i fenomeni che ne emergono. Di queste ultime l'Italia sopporta il peso praticamente da sola per quanto riguarda la rotta mediterranea.
La Nato rappresenta in quest'area un elemento di stabilità e un potenziale moltiplicatore di sicurezza, apprezzata nei vent'anni di cooperazione e dialogo intrattenuti con i Paesi del Medio oriente e nord Africa. Occorre ora rendere concreta la visione affermata dal Vertice di Varsavia, nel momento in cui hanno assunto proporzioni preoccupanti le sfide che da quest'area promanano. La nuova operazione marittima e le iniziative di assistenza alle forze di sicurezza a difesa dei Paesi dell'area, rappresentano tasselli di una strategia di ampio respiro che vede nell'unitarietà dell'impegno e nella complementarietà degli sforzi un distinto valore aggiunto.
L'evoluzione degli scenari sul fianco sud ed est dell'Alleanza mette in evidenza quanto la minaccia si sia arricchita di nuovi volti. Per fronteggiarla occorre anzitutto coesione politica. Quella coesione di valori che ha portato a fare della Nato, in questi decenni, l'asse principale attorno al quale creare quelle condizioni di stabilità e sicurezza presupposti per lo sviluppo di qualsiasi comunità e per la pace. Come ha ricordato il segretario generale Jens Stoltenberg, sono i valori che unirono i dodici membri fondatori dell'Alleanza, determinati a salvaguardare i principi di democrazia, libertà e dello Stato di diritto. È una missione che mantiene inalterata la sua validità e a cui l'Italia continuerà a fornire il suo convinto e attivo contributo.

www.quirinale.it

LA FALSA POLEMICA SUI MILITARI ITALIANI IN LETTONIA

L'intervista in cui Stoltenberg ha citato i 140 militari italiani che prenderanno parte alle missioni Nato in Lettonia, ha acceso una serie di polemiche, nonostante fosse cosa nota dallo scorso luglio. I pompieri sono stati i ministri Gentiloni e Pinotti. Il titolare della Farnesina ha ribadito: "Non è un'aggressione". La Pinotti ha ricordato: "Con la Russia si deve dialogare"

STEFANO VESPA *giornalista*

Non c'è notizia più nuova di una già data. Così, due giorni di dibattito per il 65simo anniversario del Nato Defense College di Roma hanno prodotto confusione politico-mediatica. La "colpa" è dell'intervista del 14 ottobre rilasciata a *La Stampa* dal segretario generale della Nato, il norvegese Jens Stoltenberg, nella quale ha parlato del futuro impegno italiano con circa 140 militari in Lettonia, insieme con altre nazioni e sotto comando canadese forse già nella prossima primavera, e della guida italiana nel 2018 della cosiddetta Vjtf (una forza congiunta di reazione rapida ad altissima prontezza). Solo quest'ultima data era forse una novità, perché nel comunicato finale del Summit Nato di Varsavia dello scorso luglio era già stato annunciato l'impegno italiano in Lettonia e dunque ai confini russi, aggiungendo che alla Vjtf avrebbero concorso sette nazioni, tra cui l'Italia, a rotazione fino al 2022.

Se questa intervista ha causato in Italia un po' di dichiarazioni alle agenzie di stampa, ha consentito a Mosca di continuare nelle stilettate diplomatiche giudicando "l'annuncio" di Stoltenberg come "una politica distruttiva della Nato". I pompieri sono stati il ministro degli Esteri Paolo Gentiloni e quello della Difesa Roberta Pinotti. Il titolare della Farnesina ha ribadito un concetto noto, e cioè che "non è un'aggressione" bensì una scelta "di rassicurazione e difesa dei nostri confini come Alleanza" e che certe decisioni "non influiscono minimamente nella linea di dialogo che l'Italia ha sempre proposto e condiviso con la Nato e che può e deve andare in parallelo con le rassicurazioni ai nostri alleati che si sentono a rischio". Stessa linea del ministro Pinotti: da un lato era già tutto noto da luglio, dall'altro "con la Russia si deve dialogare". Dialogo con Mosca che da sempre è centrale per il centrodestra, mentre Beppe Grillo paventa addirittura venti di guerra e annuncia che con il M5s al governo nessun soldato italiano sarebbe al confine russo. La tensione Nato-Russia è destinata comunque a continuare se Stoltenberg arriva a dire che Mosca "è sempre più assertiva e imprevedibile e ha schierato sistemi missilistici vicino ai Paesi alleati", per cui i membri dell'Alleanza "sono profondamente preoccupati da questo comportamento". Il dialogo è fondamentale perché "dobbiamo evitare azioni e calcoli errati che possono far sfuggire di mano la situazione".

Messa da parte la polemica di giornata, la sessione di due giorni al Nato Defense College (che festeggia anche i 50 anni del trasferimento a Roma)

ha toccato i temi caldi di questi mesi: fronte est e sud dell'Europa, immigrazione, crisi siriana. Nessuna notizia fresca, diverse diplomatiche sollecitazioni affinché le esigenze italiane siano tenute sempre in maggiore considerazione. Il presidente della Repubblica Sergio Mattarella è stato chiaro: all'interno dell'Alleanza atlantica occorre la massima coesione per fronteggiare "l'evoluzione degli scenari sul fianco sud ed est dell'Alleanza". Non solo est, dunque, dove non si deve parlare di nuova Guerra fredda, ma appunto anche sud, dove servono "coerenza e responsabilità" per affrontare le situazioni libica, irachena, siriana e in genere del Mediterraneo e dove, sull'immigrazione, l'Italia "sopporta il peso praticamente da sola". In parole povere, così come l'Italia è in prima linea nell'assumersi compiti e responsabilità in seno alla Nato anche sul fronte russo, oltre che in tante altre missioni, occorre che tutti i Paesi dell'Alleanza si sentano obbligati a ricambiare su quello dell'immigrazione e libico.

È certamente un buon segnale la missione Nato Sea guardian, varata a Varsavia, che dovrà collaborare con la missione europea Eunavfor Med (o missione Sophia) come supporto logistico e di scorta purché "entri in azione senza ritardi" come ha chiesto Mattarella. Lo stesso Gentiloni, nella conferenza stampa finale con Stoltenberg, ha ribadito che "l'impegno strategico Nato nel Mediterraneo è uno dei modi di una crescente cooperazione" augurandosi che la collaborazione tra Sea guardian e Sophia passi da punto di contatto a rapporto reciproco. Un nuovo e importante appuntamento sarà il vertice dei ministri della Difesa dell'Alleanza (il primo dopo Varsavia) in programma il 26 e 27 ottobre a Bruxelles. Sul sistema di difesa comune europea, Stoltenberg ha detto che "il progetto è di grande importanza per la Nato perché 26 dei nostri alleati sono Paesi europei e una difesa europea più forte può dare un contributo al rafforzamento dell'Alleanza, ma occorre evitare duplicazioni", ripetendo ancora una volta quello che è un punto centrale del suo mandato: la necessità che i Paesi membri aumentino la spesa per la Difesa. Da un lato, dunque, l'Ue dev'essere complementare alla Nato, dall'altro il segretario generale rileva che, dopo anni di tagli, la spesa per la difesa torna ad aumentare "anche in Italia, perché viviamo in un mondo più pericoloso con nuove sfide e minacce e dobbiamo adattarci". I vertici militari italiani si augurano di non avere brutte sorprese nella legge di bilancio.

ROMA IN BILICO TRA EUROPEISMO E ATLANTISMO

La Brexit ha il potenziale di danneggiare non solo le relazioni del Regno Unito con l'Europa, ma anche con gli Stati Uniti. Il giusto passo per l'Italia potrebbe essere concentrarsi non sul sostituire il Regno Unito in Europa, ma proprio in America

JONATHAN D. CAVERLEY *ricercatore associato di Security studies presso il Massachusetts institute of technology*

Quando si tratta di politica di sicurezza in generale e di politica industriale di difesa in particolare, l'Italia ha sempre scelto un cammino che bilancia elementi atlantisti ed europeisti. Per esempio, con l'imminente dipartita britannica, l'Italia resterà l'unico Paese dell'Unione europea con legami industriali e operativi sia con l'Eurofighter che con il Joint strike fighter a guida statunitense.

Molti in Italia hanno identificato la Brexit come un'opportunità per approfondire la cooperazione in materia di difesa nel continente. Il Libro bianco della difesa suggerisce che il riorientamento verso l'Europa era già in corso prima del *referendum* britannico. La recente proposta del ministro Gentiloni di una "Schengen della difesa" non fa che confermare questo cambiamento. Tuttavia, la Brexit potrebbe offrire opportunità anche al di là dell'Atlantico, e sarebbe saggio tenerle in considerazione per la comunità strategica italiana. Inoltre, atlantismo ed europeismo non sono gli unici obiettivi in potenziale tensione nel Libro bianco. Gli sforzi tesi a cercare tanto l'*exportability* quanto la cooperazione industriale europea, sono ugualmente in conflitto. L'Italia dovrà scegliere. L'*export* rappresenta la linfa vitale per il settore. L'Italia esporta, difatti, più del doppio degli armamenti usati dalle proprie Forze armate. In più, il Paese dipende ampiamente dalle esportazioni extra-Ue, pari a uno sbalorditivo 43% di tutta la produzione militare domestica (la media europea è inferiore al 30%). Per aumentare le rendite continentali, l'industria della difesa italiana si troverà a competere con fornitori affermati di Germania, Francia e perfino degli Stati Uniti, che saranno riluttanti a cedere porzioni di mercato anche nella forma di *venture* collaborative.

Se anche l'Italia avesse successo nel sostituire il Regno Unito guadagnando una fetta del mercato europeo, le prospettive di un aumento significativo della spesa europea nella difesa rimangono basse. La reale crescita dell'*export* militare si verifica lì dove i Paesi europei non sono ben collocati, come Medio Oriente e Asia. E di sicuro il più grande mercato della difesa al mondo, gli Stati Uniti, resta ben chiuso per le compagnie europee. Collettivamente, l'Unione europea spende circa la metà del *budget* della difesa degli Stati Uniti. Tuttavia, secondo il ceo dell'Agenzia di difesa europea (Eda), il mercato europeo della difesa così frammentato produce solo il 15% rispetto alle capacità di uno sforzo unificato. Le economie di scala massiccia in questo settore lo rendono un *handicap* che nessuna cooperazione riusci-

rebbe a cancellare. In realtà, le economie di scala americane sono solo un primo ostacolo. L'amministrazione Obama, rispondendo alla crescente concorrenza, ha mitigato le restrizioni all'*export* di armamenti per riguadagnare parte del mercato globale. Gli Stati Uniti hanno prodotto Uav (*unmanned aerial vehicle*) per decenni. Anche se avessero accesso a tale *export*, come potranno le versioni europee ancora in fase di sviluppo competere? Il Pentagono sta portando avanti relazioni sempre più strette con la Silicon Valley nella propria Third offset strategy dal valore di 18 miliardi di dollari, uno sforzo incredibilmente ambizioso per il futuro vantaggio tecnologico globale. Qual è l'equivalente europeo della Silicon Valley (anche senza il Pentagono)?

Di certo, c'è ampio spazio per una riforma delle acquisizioni europee ed è innegabile che un progresso ci sia stato, sebbene lento e agitato. Tuttavia, è ugualmente plausibile che le necessarie riforme su larga scala non avvengano mai. Suggerisco, dunque, che l'Italia non abbandoni il proprio approccio bilanciato. Forse ironicamente, la Brexit può danneggiare non solo le relazioni del Regno Unito con l'Europa, ma anche con gli Stati Uniti. Il giusto passo per l'Italia potrebbe essere concentrarsi non sul sostituire il Regno Unito in Europa, ma in America. E gli Stati Uniti potrebbero essere in cerca di un nuovo partner europeo. Nel corso di tutta la frustrazione dei Paesi Ue desiderosi di stabilire una maggiore identità di difesa, il Regno Unito ha svolto il ruolo strategicamente utile, e finanziariamente lucrativo, di fidato interlocutore tra la Nato e l'Europa. La BAE ottiene maggiori guadagni dagli Stati Uniti che dal Regno Unito. In più, la *special relation* con Washington dava a Londra un considerevole potere contrattuale nelle negoziazioni europee, permettendole di minacciare l'abbandono del tavolo delle trattative.

Essere la nuova porta americana sull'Europa potrebbe rendere l'Italia meno popolare tra i propri colleghi europei, ma la politica estera non è un *contest* di popolarità. Essa riguarda trattative basate su interessi e capacità, e l'Italia da sola non ha molto della seconda. Data la modesta spesa, circa la metà di quella del Regno Unito, non è chiaro se l'Italia avrà influenza sul nascente duopolio franco-tedesco. Il destino dell'Italia sarà sempre quello di essere un partner minore. Dovrà dunque scegliere l'alleato che offre maggiore vantaggio strategico e guadagno economico.

Traduzione di Stefano Pioppi

LA POLONIA SGANCIA AIRBUS E SCEGLIE LOCKHEED MARTIN

Sconfessando l'accordo del 2015 con Airbus, Varsavia sceglie i Black Hawk statunitensi per dotare il proprio esercito di nuovi elicotteri da combattimento. Dietro la disputa industriale si nasconde la volontà polacca di prediligere l'atlantismo e il rapporto con la Nato rispetto al progetto, anche francese, di una difesa europea comune

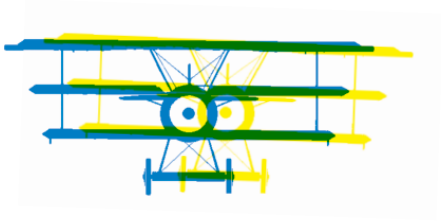
STEFANO PIOPPI

La Polonia ha scelto gli S-70i Black Hawk di Lockheed Martin per il proprio esercito invece dei preannunciati H225M Caracal di Airbus. La notizia era nell'aria, eppure rischia ripercussioni pesanti non solo sul piano industriale, ma soprattutto su quello politico. Ad aprile 2015, infatti, la Polonia aveva preselezionato per il piano di ammodernamento dell'esercito i Caracal di Airbus Helicoptères, che un po' inaspettatamente avevano battuto la concorrenza degli AW149 di AgustaWestland e degli S-70i di Sikorsky, controllata del colosso statunitense. La maxi commessa per 50 elicotteri avrebbe avuto un valore di oltre 3,1 miliardi di euro, la seconda più grande nella storia della Polonia.

E invece, lo scorso 4 ottobre, il nuovo esecutivo targato Diritto e Giustizia, ha chiuso i negoziati con Airbus, per annunciare poco dopo, tramite il ministro della Difesa Antoni Macierewicz, che i primi due Black Hawk arriveranno entro l'anno e altri otto nel 2017. Potrebbero arrivare ordini anche per gli AW 149 di Leonardo-Finmeccanica, presente in Polonia con lo stabilimento di Swidnik. L'annuncio è ovviamente stato accolto negativamente dalla Francia. Possibile il ricorso a un tribunale arbitrale, anche perché l'industria di Tolosa aveva già iniziato a produrre alcuni elicotteri. Il presidente Hollande ha addirittura rimandato la visita a Varsavia in programma per il 13 ottobre con il primo ministro Beata Szydlo, facendo presagire una vera e propria crisi diplomatica.

Dietro le ragioni industriali, infatti, si nascondono quelle politiche. Scegliendo Lockheed Martin, la Polonia ha espresso il proprio scetticismo nei confronti del processo europeo di integrazione della difesa e la preferenza per l'alleato atlantico. Agli occhi di Varsavia, e soprattutto di un esecutivo nazionalista da sempre euro-critico, sono gli Stati Uniti e la Nato a offrire protezione contro la Russia, avvertita come la principale minaccia alla propria sicurezza.

L'ultimo *summit* Nato, non a caso riunitosi a Varsavia, non aveva fatto mancare rassicurazioni in tal senso. I battaglioni a rotazione in est Europa e, ancor prima, l'annuncio dell'installazione del sistema di difesa dai missili balistici Aegis a Redzikowo, sono stati avvertiti molto più rassicuranti e concreti rispetto al dibattito europeo sull'integrazione della difesa. Se a ciò si aggiungono prospettive spesso divergenti tra Varsavia e Parigi su questioni molto delicate come la gestione dei migranti, si delinea che la scelta di prediligere il colosso americano possa essere stata più politica che tecnico-industriale.



Pene di morte giudiziarie ed extragiudiziarie

Francamente, il dibattito sul duello Clinton-Trump non serve a un beneamato nulla, se visto in termini calcistici e il *Lei per chi tifa* è la vacua domanda di chi ha rinunciato a capire e far capire la realtà del mondo. Sotto il diluvio mediatico emergono invece due notizie che interrogano in modo diretto la politica vera e le persone semplici. Su questioni di vita e di morte. Durante la giornata mondiale contro la pena di morte, i vescovi cattolici del Texas, lo Stato con più esecuzioni capitali recenti negli Stati Uniti (più del 30%) e con alcune delle più oscene prigioni private al mondo, hanno diffuso un proclama contro questa pena che, nei Paesi che ascoltano la lezione di Cesare Beccaria, è obsoleta da secoli. Dichiarando la giornata un'espressione a favore della protezione della vita, i vescovi constatano che: la pena di morte colpisce i poveri, le minoranze e gli squilibrati (ma quanti boss mafiosi hanno visto il patibolo?); i costi di un'esecuzione sono tripli rispetto all'ergastolo; la pena capitale non influisce sui tassi di criminalità (come si sa dal 1764, cioè da un quarto di millennio); la morte del criminale non consola le vittime dei familiari, non permette alcuna riabilitazione (è utile rivedere il film italiano *Cesare deve morire*), influenza negativamente l'educazione dei bambini ed esclude compassione e redenzione dalle culture che la praticano. Insomma, perché la morte per iniezione è più civilizzata dello sgozzamento alla Daesh? Quali valori di libertà, eguaglianza, fraternità e democrazia difende? Dall'altro capo dell'oceano Pacifico, invece, si profila una chiesa silenziosa e incerta davanti al massacro extragiudiziale attivamente promosso dal neopresidente Rodrigo Duterte con il tristo primato di 3.600 spacciatori o piccoli criminali uccisi. È difficile non pensare a una Notte dei cristalli o a un *pogrom* prolungati ed è pericoloso, oltre che impolitico, immaginare che alcune vite abbiano meno valore delle altre.

I sondaggi, che mostrano un 76% a favore del presidente massacratore, e un 84% a favore della guerra alla droga (anche se con una maggioranza che prova ripugnanza all'omicidio di massa), rivelano piuttosto a che livello è sceso lo stato di diritto in una democrazia occidentale e quindi la credibilità di uno Stato che elimina i piccoli pesci, ma permette all'impunità, alla violenza e alla contiguità mafiosa d'installarsi nel cuore delle forze dell'ordine. Non ci vuole una scienza infusa per capire che la strada filippina è molto simile a quella messicana, i cui risultati in termini di lotta alla mafia sono, dopo dieci anni, a dir poco deludenti. Se la democrazia vuole vivere deve evitare i silenzi complici sui *killing fields* distanti per circoscrivere e debellare il contagio di una vecchia barbarie con nuovo mascara.

CASA*di*VETRO

Tommaso De Zan e Simona Autolitano
Programma Sicurezza e difesa, Iai

D1

Difesa e Sicurezza Ue

Prorogate le sanzioni Ue per azioni contro l'integrità territoriale dell'Ucraina

Il Consiglio dell'Ue ha prorogato di sei mesi l'applicazione delle misure restrittive per i responsabili di azioni contro l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina. Le misure, originariamente introdotte nel marzo 2014, sono state prorogate fino al 15 marzo 2017. Tali sanzioni prevedono il blocco dei beni e il divieto di viaggio per 146 persone e 37 entità, tra cui le stesse repubbliche separatiste di Donetsk e Lugansk. Si tratta di una delle misure imposte dall'Unione europea in risposta alla crisi in Ucraina, tra cui le sanzioni economiche riguardanti settori specifici dell'economia russa, attualmente in vigore fino al 31 gennaio 2017, e le misure restrittive in risposta all'annessione illegale della Crimea e di Sebastopoli, limitate ai loro territori, attualmente in vigore fino al 23 giugno 2017.

Nuovo pacchetto di aiuti per il Mediterraneo

L'Ue ha stanziato 129 milioni di euro per promuovere la cooperazione regionale nel Mediterraneo e lo sviluppo socio-economico in Egitto e Palestina (Gaza, Area C e Gerusalemme Est). L'assistenza verrà erogata tramite lo strumento europeo di vicinato. Il pacchetto prevede il finanziamento di diversi progetti di cooperazione bilaterale a favore della popolazione egiziana (50 milioni di euro) e palestinese (38,6 milioni). Più di 41 milioni di euro sono invece destinati a programmi di cooperazione regionale a favore dei giovani.

Lotta al terrorismo: sanzioni contro Isis e Al Qaeda

Il Consiglio dell'Ue ha adottato un quadro giuridico che, per la prima volta, consentirà all'Unione europea di applicare proprie sanzioni nei confronti di Isis e Al Qaeda o di persone ed entità a essi associate. Le misure restrittive previste, il divieto di viaggio e il congelamento dei beni, riguardano in particolare i *foreign fighters*, inclusi i cittadini Ue che fanno ritorno in Europa dopo aver sostenuto queste organizzazioni all'esterno dell'Ue. Previo accordo sulle proposte di inserimento da parte degli Stati membri, persone ed entità saranno inserite nell'elenco su decisione del Consiglio.

Aiuti umanitari per Yemen e Iraq

A New York, in occasione dell'all'assemblea generale delle Nazioni Unite, il Commissario europeo per gli aiuti umanitari e la gestione delle crisi, Christos Stylianides, ha annunciato lo stanziamento di ulteriori 70 milioni di euro in aiuti umanitari per lo Yemen (40 milioni) e per l'Iraq (30 milioni). I fondi per lo Yemen si aggiungono agli 80 milioni di euro stanziati dalla Commissione nel 2015 e sono destinati alle agenzie umanitarie che operano nel Paese. Quelli per l'Iraq si aggiungono, invece, ai 104 milioni di euro già stanziati nel 2016.

Colombia: l'Ue sospende le sanzioni contro le Farc

Il Consiglio dell'Ue ha sospeso l'applicazione di misure restrittive nei confronti delle Forze armate rivoluzionarie della Colombia (Farc). Tale decisione fa seguito alla firma ufficiale dell'accordo di pace tra il governo colombiano e le Farc, avvenuta il 26 settembre a Cartagena. L'organizzazione era stata inserita nel giugno 2002 nella lista Ue di persone, gruppi ed entità coinvolti in atti di terrorismo e per questo sottoposta al congelamento dei beni e a misure rafforzate di cooperazione di polizia e giudiziaria in materia penale.

Burundi: proroga di un anno per le sanzioni Ue

Il Consiglio dell'Ue ha prorogato fino al 31 ottobre 2017 le misure restrittive contro il Burundi. Tali misure, introdotte nell'ottobre 2015, prevedono il blocco dei beni e il divieto di viaggio per quattro persone le cui attività compromettono la democrazia o ostacolano la ricerca di una soluzione politica alla crisi attuale, scoppiata a seguito della rielezione di Pierre Nkurunziza alle presidenziali del luglio 2015.

D2

Difesa Nato

Cooperazione per l'addestramento di Forze speciali in quattro Paesi Nato

Bulgaria, Croazia, Ungheria e Slovenia hanno firmato una dichiarazione d'intenti con cui si impegnano a cooperare nell'addestramento di proprie unità di supporto aereo alle operazioni speciali. Tale accordo multilaterale rientra nell'ambito di una più ampia iniziativa di cooperazione dei quattro Paesi Nato, lanciata nel giugno 2015 per creare queste unità militari. L'iniziativa è sostenuta dal quartier generale delle operazioni speciali della Nato e dagli Stati Uniti.

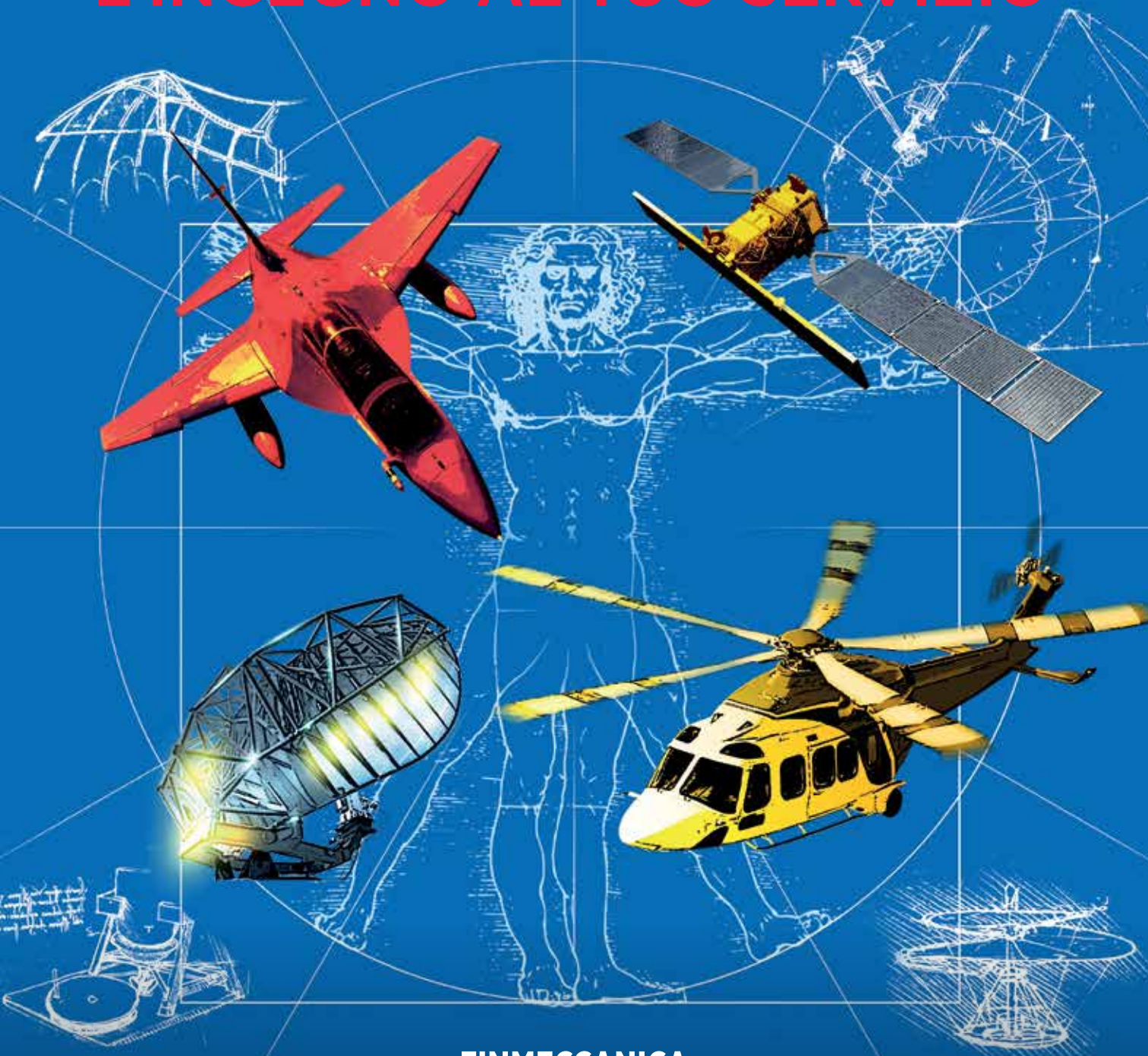
Nato: 4mila uomini nel Baltico entro maggio 2017

I capi di stato maggiore della Difesa dei Paesi Nato hanno discusso a Spalato, in Croazia, il dispiegamento di 4mila militari nella regione baltica, deciso al vertice Nato di Varsavia di luglio. Entro maggio 2017 verrà completato lo schieramento di quattro battaglioni in Polonia, Estonia, Lettonia e Lituania.

La Nato schiererà aerei Awacs in Medio Oriente

L'Alleanza ha annunciato di voler schierare entro ottobre in Medio Oriente i sistemi di aviazione Awacs (*Airborne warning and control system*). Come deciso a luglio al vertice Nato di Varsavia, i velivoli E-3A Sentry della Nato sosterranno gli sforzi della coalizione guidata dagli Usa contro lo Stato islamico. Il vice direttore generale Nato, Alexander Vershbow ha affermato che le informazioni raccolte tramite sorveglianza saranno condivise con i membri della coalizione.

L'INGEGNO AL TUO SERVIZIO



FINMECCANICA
oggi è

LEONARDO

leonardocompany.com

UNA POLITICA INDUSTRIALE 4.0

STEFANO PIOPPI

La rivoluzione digitale non attende nessuno, tanto meno l'industria. Lo ha capito Avio Aero, azienda aeronautica del gruppo General Electric (GE), che ha voluto organizzare a Roma l'evento dal titolo emblematico e augurale "Rinascimento industriale 4.0". Dal dibattito ospitato presso l'aula Adrianea degli Horti sallustiani è emersa chiara un'indicazione: la digitalizzazione dell'industria non è solo una grande opportunità, ma anche una necessità per non perdere competitività in ambito internazionale. In questo senso, l'evento organizzato in collaborazione con *Formiche*, si è inevitabilmente legato alla presentazione, avvenuta solo un giorno prima, del piano del governo Industria 4.0 da parte del presidente del Consiglio Matteo Renzi e del ministro per lo Sviluppo economico Carlo Calenda.
"Vogliamo digitalizzare l'industria non solo perché è necessario, ma anche perché è una grande opportunità. Rinascimento industriale vuol dire mostrare che in Italia si può avere successo, che si può investire", ha spiegato Riccardo Procacci, numero uno di Avio Aero che, come parte del *business* GE, dimostra la capacità italiana di attrarre investimenti. Lo ha ribadito tra l'altro anche Sandro De Poli, ad e presidente del gruppo GE in Italia e Israele, facendo riferimento agli oltre 12mila dipendenti nel nostro Paese per un volume di affari pari a 8 miliardi di euro nel 2015. "L'Italia è tra i primi Paesi al mondo per capacità ingegneristica, una piattaforma fondamentale per lo sviluppo del gruppo", ha ammesso De Poli. Tuttavia, "una buona parte del futuro dipende da quanto e da come riusciremo a digitalizzare le nostre industrie", ha aggiunto.
Oltre alla tecnologia, però, c'è la formazione, indispensabile affinché la prima sia usata correttamente. "Ci troviamo di fronte a una rivoluzione tecnologica e culturale; si tratta non solo di usare nuovi strumenti tecnologici, ma soprattutto di imparare a usarli", ha detto il presidente del World manufacturing forum, professore del Politecnico di Milano Marco Taisch. Gli hanno fatto eco le parole dell'ad di Dallara Automobili, Andrea Pontremoli, che ha voluto richiamare il ruolo sociale dell'azienda. "La chiave di tutto sono le persone che sanno usare le tecnologie, non le tecnologie", ha detto. In questo senso, il ministero dell'Istruzione, dell'università e della ricerca partecipa alla Cabina di regia prevista dal piano Industria 4.0. "Il Miur ha cercato di rispondere alla sfida della digitalizzazione con una visione

L'EVENTO DI AVIO AERO
Il 22 settembre, l'aula Adrianea degli Horti sallustiani a Roma ha ospitato l'evento "Rinascimento industriale 4.0", organizzato da Avio in collaborazione con *Formiche*. Al dibattito, moderato dall'editore Paolo Messa, hanno partecipato (foto in alto a sinistra) i ministri della Difesa e dello Sviluppo economico Roberta Pinotti e Carlo Calenda, il presidente e ad di Avio Aero Riccardo Procacci, il presidente e ad di GE Italia Sandro De Poli. Presenti tra gli altri, l'ad di Dallara Automobili Andrea Pontremoli, il professor Marco Taisch e il consigliere del Miur Mario Calderini

organica che ha al centro le persone, sin dalle elementari, per fornire agli studenti gli strumenti necessari a poter competere e avere successo in questo settore", ha spiegato Mario Calderini, consigliere del ministero per le Politiche di ricerca e innovazione.
Tutto questo si lega alla nuova politica industriale del governo, che i rappresentanti del mondo industriale presenti all'evento sembrano aver accolto con cauto ottimismo. Da parte dell'esecutivo, moderati dall'editore Paolo Messa, sono invece intervenuti i ministri Carlo Calenda e Roberta Pinotti. Il primo ha voluto sottolineare non tanto la dimensione tecnica del piano, riassumibile in 13 miliardi di euro in incentivi fiscali, quanto la visione politica e del mondo su cui esso si poggia. "C'è una base di visione – ha detto Calenda – un disegno che si fonda su una grande fiducia nei confronti delle imprese". Ma c'è di più: la crisi del 2008 ha fatto tramontare il sogno della globalizzazione *win-win* spaccando in due la società. "In Italia il 2015 è stato l'anno *record* per le esportazioni, ma anche per il numero di società chiuse. E l'innovazione – ha proseguito il vertice del Mise – rischia di continuare a dividere tra chi ha successo e chi inevitabilmente non ce la fa". La risposta a questo *digital divide* deve essere politica, deve guardare organicamente a tutti gli aspetti toccati dall'*Internet of things*, dall'educazione all'industria.
Tra i comparti interessati c'è anche quello di difesa e aerospazio, in cui gli investimenti, specialmente in ricerca e sviluppo, hanno sempre dimostrato una ricaduta positiva sul sistema economico nel suo complesso. "La difesa è un settore che ha sviluppato incredibili capacità dall'esigenza di essere autosufficienti e pronti a ogni evenienza in operazioni militari", ha spiegato il ministro Pinotti. In questo senso, il Rinascimento industriale non può di certo escludere il comparto difesa, che anzi si presenta al piano del governo Industria 4.0 con l'assetto strategico offerto dal Libro bianco. "Negli ultimi anni abbiamo osservato tagli complessivi al bilancio difesa del 27%, ora bisogna tornare a investire. Oggi – ha tuonato il ministro – non si può più tagliare; bisogna tornare a immaginare un'attenzione più rigorosa alla difesa del nostro Paese".
Per il comparto difesa, visto l'arco di crisi in cui si trova il nostro Paese, questo sembra necessario. Per tutta l'industria è una grande opportunità per un Rinascimento 4.0.

L'INNOVAZIONE OFFERTA DALLA DIFESA

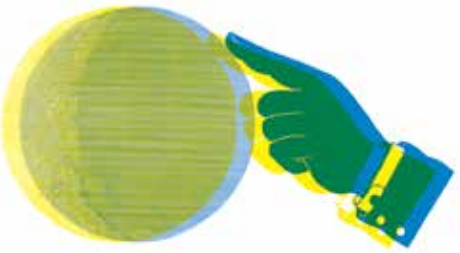
La difesa può offrire alla nuova fase di innovazione tecnologica un importante contributo a livello di qualificate esigenze da soddisfare, sperimentazioni sul campo, inserimento nei più avanzati programmi di collaborazione internazionale. Di qui, un forte e diretto interesse per il programma d'innovazione tecnologica a livello di processi, denominato Industria 4.0

MICHELE NONES *consigliere scientifico dell'Istituto affari internazionali - Iai*

Fra le inevitabili conseguenze della globalizzazione, vi è l'aumento esponenziale della complessità, dovuta anche alla crescente interazione fra i diversi fattori. Persino in un settore apparentemente ben delimitato come la sicurezza e la difesa è, quindi, indispensabile un approccio multidisciplinare, anche in termini culturali, oltre che operativi. Questo è stato esplicitamente indicato nel Libro bianco per la sicurezza internazionale e la difesa presentato dal ministro Pinotti lo scorso anno: "Affrontare in chiave moderna il problema della sicurezza e difesa del Paese richiede un approccio omnicomprensivo e multi-disciplinare. Occorre interrogarsi su come vada sviluppato l'insieme delle differenti capacità che consentono al Paese di essere più sicuro e se sia ipotizzabile un'evoluzione dello stesso concetto di difesa per renderlo più allargato e inclusivo". Questa impostazione comporta che la difesa vada vista come un sistema di cui le capacità tecnologiche e industriali sono una componente essenziale, ma anche che, oltre al settore dell'aerospazio, sicurezza e difesa, tutto il sistema industriale e della ricerca debba essere e sentirsi coinvolto. Di qui, un forte e diretto interesse per il programma d'innovazione tecnologica a livello di processi, denominato Industria 4.0, messo a punto dal ministro per lo Sviluppo economico Calenda. Non va d'altra parte dimenticato che, fra le grandi trasformazioni che stanno caratterizzando gli equipaggiamenti militari utilizzati dalle Forze armate, vi è il sempre maggiore utilizzo di componenti e prodotti civili. E questo vale, ormai, anche per i più moderni sistemi di difesa. La crescita di importanti mercati civili, (trasporto aereo e navale, comunicazioni, informatica, automazione, ecc.) infatti si è basata e ha imposto uno sviluppo tecnologico senza precedenti, anche in termini di velocità dell'innovazione. Questo ha reso disponibili tecnologie, componenti, prodotti altrettanto prestanti e affidabili di quelli militari, ma a un costo nettamente inferiore. Di qui, un utilizzo sempre più ampio nel campo della sicurezza e della difesa, anche per cercare di concentrare le limitate risorse disponibili sulle attività esclusivamente militari. Questo comporta che le Forze armate non possano limitarsi a padroneggiare le tecnologie di loro diretto interesse, ma debbano saper monitorare lo sviluppo tecnologico complessivo per poterne utilizzare al meglio i risultati. In quest'ottica bisogna, quindi, migliorare le competenze tecniche all'interno del mondo della difesa. Secondo recenti studi, le imprese del settore aerospazio, sicurezza e difesa generano

complessivamente, in Italia, 11,6 miliardi di euro di valore aggiunto (0,8% del Pil) e creano direttamente e indirettamente 160mila occupati. Ogni euro di valore aggiunto genera ulteriori 1,6 euro nell'economia e ogni occupato sostiene 2,6 posti di lavoro ulteriori. La spesa per ricerca e sviluppo è di quasi 1,5 miliardi di euro, il 12% di tutta la spesa sostenuta dalle imprese italiane. È, quindi, il secondo settore in Italia per dimensione e per intensità di R&S. Ma la sua importanza è soprattutto sul piano qualitativo, poiché il settore delle tecnologie avanzate è uno dei pochi che il nostro Paese riesca a presidiare. Rappresenta, quindi, un *asset* strategico nazionale. È in questo contesto tecnologico e industriale che va affrontata la nuova minaccia ibrida: alla minaccia classica si somma, da ormai un quindicennio, quella asimmetrica, con l'aggravante che i movimenti terroristici di matrice islamica possono utilizzare, là dove conquistano il territorio, anche forme di minaccia classica, utilizzando la grande quantità di equipaggiamenti militari sfuggiti a ogni controllo durante le recenti crisi nei Paesi della sponda sud del Mediterraneo e in Medio Oriente. Di fronte a questa minaccia ibrida, e con le limitazioni finanziarie imposte da questo periodo di crisi economica, le tecnologie avanzate possono offrire un importante contributo all'esigenza di una maggiore sicurezza e difesa delle nostre popolazioni e territori. Vi sono, dunque, numerose esigenze da soddisfare utilizzando l'innovazione tecnologica: migliorare la protezione per i nostri uomini e le forze locali che addestriamo affinché possano difendere da sole i loro Paesi; incrementare la precisione dei sistemi d'arma in modo da renderli più efficaci, riducendo al minimo errori e perdite collaterali; perfezionare la capacità di raccolta e gestione delle informazioni per contrastare ogni minaccia; potenziare la rapidità dei nostri interventi. Anche per quanto riguarda la manutenzione e il supporto logistico, l'innovazione tecnologica può consentire di raggiungere una maggiore efficienza, migliorando la disponibilità degli equipaggiamenti. Aumentare significativamente il tasso dei mezzi impiegabili, attraverso nuove tecnologie diagnostiche e progettative, potrebbe agire da moltiplicatore di forze, consentendo di avere le stese capacità con un minore numero di mezzi. Nel complesso, la difesa può, quindi, offrire alla nuova fase di innovazione tecnologica un importante contributo a livello di qualificate esigenze da soddisfare, sperimentazioni sul campo, inserimento nei più avanzati programmi di collaborazione internazionale.

Ezio Bussoletti
insegna Fisica e Tecnologie spaziali
presso l'Università Parthenope



Pizza napoletana batte Spazio 1-0

Le attività spaziali con oltre 5mila addetti e su temi che sono punte di eccellenza internazionali necessiterebbero attenzione politica per renderle ancora più competitive in un mercato che vede crescere *competitor* sempre più qualificati e aggressivi. Da molti anni, ormai, si cerca una soluzione per una realtà essenzialmente incentrata sulla sola Agenzia spaziale. A ogni cambio di governo piovono proposte di legge per razionalizzare la situazione rendendola adatta alle nuove sfide. Così è stato anche per l'attuale legislatura con tre proposte (Fi, Pd, Misto) confluite in un unico testo bipartisan *Politiche spaziali e aerospaziali*.

In discussione al Senato, alla commissione Attività produttive in sede referente, il testo si compone di quattro articoli. Le competenze politiche sono trasferite alla presidenza del Consiglio che istituisce un comitato che, a sua volta, riunisce i ministeri interessati alle tematiche spaziali; un coordinamento stretto tra i vari attori nazionali è difatti fondamentale e non più delegabile a una sola amministrazione. Il comitato ha competenze molto ampie tra cui l'indirizzo per la definizione di accordi internazionali, l'approvazione del Documento di visione strategica per lo spazio e la definizione delle linee prioritarie per la partecipazione alle attività dell'Esa. Il ruolo dell'Asi è rimodulato riconoscendo le competenze tecniche senza più compiti politici.

Tra meno di due mesi l'Italia dovrà partecipare alla consueta riunione ministeriale dei Paesi aderenti all'Esa e decidere come e in che misura impegnarsi nei programmi futuri tentando di salvaguardare gli interessi dell'industria nazionale e della ricerca.

Il nuovo assetto, se già operativo, avrebbe potuto ridare nuova forza e credibilità all'immagine di un Paese che contribuisce all'Esa senza avere il ruolo decisionale che gli competerebbe.

Però, a poche settimane dalla riapertura, il Senato stenta a ripartire sul tema mentre è invece affrontata con la dovuta attenzione e priorità la proposta di legge per la qualifica della professione di pizzaiolo accompagnata dall'audizione di rappresentanti delle associazioni di settore. Lo spazio può aspettare... A quando la discussione sui suonatori di mandolino?

Gregory Alegi e Francesca Garello

Bistecche al postbruciatore

Una piuma rossa, lunga e velocissima, accelerò davanti a loro, impennandosi e salendo quasi verticale per trasformarsi in una palla e scomparire nella notte toscana. Neppure il tempo di riprendere fiato e un'altra fiamma si lanciava lungo la pista, con il rumore assordante del postbruciatore. "Il suono della libertà", cercai di dirle, indicando l'adesivo sul paraurti della macchina. Ma il rombo tridimensionale affogava ogni tentativo di conversazione e si avviarono verso l'*hangar* del IX Gruppo, attraversando l'odore acre del cherosene bruciato.

"Insomma, sarebbero questi i famosi notturni?", disse lei, non del tutto convinta.

"Beh, sì", disse lui. "F-104 che decollano di notte, a caccia di stelle, come vuole il loro nome".

Sul prato c'era forse una dozzina di persone in tutto, per lo più piloti e specialisti in tuta, più qualche giovane donna, una delle quali teneva in braccio una bambina che piangeva per lo spavento che chiamava "Papà! Papà!".

"E poi?"

"E poi, finita la missione, tornano e si mangia tutti assieme".

Avvicinandoci al bar in linea di volo, si sentiva sempre più forte il profumo della brace, che alla fine coprì tutti gli altri. Sforzando gli occhi, s'intravedevano in sequenza il bagliore della griglia, il maresciallo che curava il fuoco e un grande mucchio di bistecche.

"Ma quando si mangia?", chiese guardando l'orologio. "Non è che dobbiamo aspettare mezzanotte?".

"Ma no. Lo Starfighter ha pochissima autonomia".

"Avrei dovuto immaginarlo che la spiaggia vicino l'aeroporto nascondeva una fregatura", ribatté senza neppure ascoltare la mia risposta.

Per fortuna lo Starfighter aveva davvero poca autonomia. Gli aerei ricomparvero in un tempo brevissimo, annunciati dal solo rumore, e rullarono velocemente fino al piazzale. I tettucci si aprirono. I piloti scesero. La bambina riabbracciò il padre. La carne maremmana e il Morellino fecero il resto.

"Ma li fanno anche domani, i notturni?", chiese lei.

BISTECCA ALLA GRIGLIA

INGREDIENTI (A PERSONA)

1 costata di manzo di circa 200 gr
oppure
1 medaglione di filetto di circa 150 gr

PER LA MARINATURA

2 spicchi d'aglio
una bella spolverata di pepe
due rametti di rosmarino
mezzo bicchiere di birra
4 cucchiai di olio di oliva
4 cucchiai di succo di limone.
4 cucchiai di miele

PREPARAZIONE

Mescolare gli ingredienti della marinatura, immergervi la carne, coprire con pellicola da cucina e lasciare almeno due ore a temperatura ambiente. Sgocciolare bene, asciugare con carta da cucina, grigliare su una griglia molto calda per circa 2-4 minuti per lato (a seconda del grado di cottura desiderato) e spennellare con la marinatura avanzata. Salare a cottura ultimata e servire subito

Aviazione

BOEING 10-AIRBUS 0. MA IL RITORNO?

L'Ue deve applicare davvero la sentenza che nel 2011 definì aiuti di Stato i contributi per lo sviluppo Airbus. Lo ha deciso il Wto, stabilendo che bisogna compensare agli Usa anche il danno alla concorrenza causato dai contributi erogati in passato. La partita vale 10 miliardi, ma il contenzioso comprende altri due casi, in uno dei quali gli Usa hanno perso in primo grado

GREGORY ALEGI *giornalista e storico*

Il 22 settembre il Compliance panel della World trade organization ha stabilito che "l'Unione europea e taluni Stati membri hanno omesso di implementare le raccomandazioni e decisioni del Dsb per portare le proprie misure in conformità con i propri obblighi in base all'Accordo Scm, ed entro questi limiti, che le raccomandazioni e misure adottate restano operative". Dietro il linguaggio criptico c'è un fatto importante: la partita da 10 miliardi di dollari sugli aiuti di Stato nel settore dei grandi velivoli commerciali si è chiusa con la vittoria definitiva degli Stati Uniti e i perdenti non possono più rinviare le compensazioni. Altre partite restano aperte, ma questa è chiusa (a proposito, attenzione ai paralleli forzati con la megamulta europea alla Apple. Quella è stata comminata unilateralmente dalla Commissione, contro le cui decisioni si può ricorrere; la condanna Airbus nasce da un lungo arbitrato, in cui si sono percorsi tutti i gradi di giudizio).

La vertenza è difficile da riassumere, perché dura da oltre dieci anni, è molto tecnica e molti dati sono omessi in nome della riservatezza commerciale. La disputa era infatti tutt'altro che accademica: Boeing sosteneva – e il Wto le ha dato definitivamente ragione – che gli aiuti europei ad Airbus le hanno fatto perdere vendite in Ue, Australia, Cina, Corea, India, Singapore ed Emirati Arabi. Contratti miliardari e, quindi, danni in proporzione. Il caso DS 316 deciso in settembre era stato aperto l'ormai lontano 6 ottobre 2004 e deciso in primo grado il 30 giugno 2010 e in appello il 18 maggio 2011. In quell'occasione, il Wto concluse che i programmi Airbus A300B/B2/B4/600, A310, A320 e A330/A340 avevano effettivamente goduto di aiuti e finanziamenti al lancio da Francia, Germania, Spagna e (per i soli A320 e A330/A340) Regno Unito, condannando loro e l'Ue a compensare il danno agli Usa. Il punto sotto esame non era però questo, ma se l'Ue avesse fatto quanto il Wto le aveva ordinato di fare.

Il 1° dicembre 2011, l'Ue aveva presentato la lista dei provvedimenti per "rimuovere gli effetti avversi" o "ritirare i sussidi" accertati dal Wto. Lista subito contestata da Boeing, che denunciò come i 36 provvedimenti fossero sostanzialmente vuoti e aggiungendo – per buona misura – che anche i nuovi A380 e A350XWB avevano goduto di vantaggi analoghi a quelli dichiarati illegittimi. Airbus, sempre tramite la Commissione europea, dato che le parti in causa davanti al Wto sono gli Stati, rispose smentendo gli aiuti all'A380/A350 e sostenendo che i sussidi dichiarati illegali per gli altri aerei non c'erano più. Si arriva, così, a oggi.

Cosa c'è dietro la pronuncia del Wto

PIERLUIGI DI PALMA *avvocato dello Stato e presidente del centro studi Demetra*

Ha fatto molto scalpore la decisione con la quale il Wto - l'Organizzazione mondiale del commercio - ha giudicato illegittimi i sussidi erogati, per 22 miliardi di dollari nell'arco di 10 anni, dall'Unione europea e in particolare da alcuni Stati membri (in primis, Francia e Germania) in favore della Airbus, generando, in tal modo, un danno "reale e sostanziale" alla concorrente Boeing.
Numerosi articoli di stampa europei hanno etichettato, in modo alquanto sommario, la "clamorosa" pronuncia del Wto come la "vendetta" americana dopo la decisione della Ue contro Apple.

Tuttavia, a ben vedere, non possiamo ingenuamente accontentarci di credere che la decisione di un'organizzazione internazionale, che è stata istituita allo scopo di supervisionare gli accordi commerciali tra gli Stati membri, con l'obiettivo generale dell'abolizione o della riduzione delle barriere tariffarie al commercio internazionale, pronunciata dopo un procedimento durato anni, sia il frutto di una mera ritorsione.
È da ritenere, piuttosto, che le recenti statuizioni del Wto affondino le loro radici molti anni addietro, nel diverso approccio culturale del governo Usa e dell'Ue rispetto alla liberalizzazione dei mercati mondiali e, specificamente, di quello aerospaziale.
In tale contesto, credo che le valutazioni del Wto, anche se ancora suscettibili di appello e dunque non aventi carattere definitivo, debbano servire da pungolo per le istituzioni comunitarie affinché il mercato dell'industria aerospaziale riceva quello slancio di cui ha bisogno, comprendendo la necessità di abbattere i costi e avviando un percorso di efficientamento che renda il prodotto dell'industria europea di settore più "accessibile" e, dunque, più competitivo.

Sul primo punto il Wto ha deciso che i contributi dei Paesi ad Airbus per lo sviluppo di A380 e A350XWB non sono aiuti di Stato. Ma ha anche stabilito che l'Ue e i Paesi membri coinvolti non hanno rispettato gli obblighi imposti dalla decisione del 2011. Secondo il pannello arbitrale, solo due dei 36 provvedimenti europei "potevano essere davvero definiti come azioni legate al livello di sussidio continuo" dei velivoli Airbus. Peggio, gli altri 34 passi erano semplici argomentazioni per spiegare perché l'Ue ritenesse di non dover fare (o pagare) nulla.
In estrema sintesi, l'Ue sosteneva che i finanziamenti scaduti avevano la stessa capacità di sanare l'irregolarità di quelli ritirati. Allo stesso modo, per l'Ue, un finanziamento scaduto non ha più effetti negativi da sanare e il lungo tempo trascorso fa sì che gli aiuti contestati non siano più una causa genuina e sostanziale di effetti negativi. E se tutto questo era vero, non c'erano passi da adottare o decisioni da applicare.
Un approccio che il Wto ha respinto al mittente, spiegando all'Ue che gli aiuti di Stato devono essere estinti o ritirati prima di giungere alla scadenza"del periodo di applicazione (che, nel caso Airbus, si era concluso prima della decisione del Wto). Nel caso Airbus gli aiuti erano rimasti in vigore fino al termine previsto, senza mai essere stati interrotti o rimborsati in anticipo. "Non si può concludere – spiega il Wto in una sintesi – sulla sola base della scadenza dei sussidi La/Msf e in conto capitale in oggetto che l'Unione europea e taluni Stati membri abbiano *ipso facto* adempiuto all'obbligo di ritirare il sussidio rispetto a tali misure". Conclusione ineccepibile: in caso contrario, il Wto avrebbe di fatto accettato l'aggiramento della decisione di merito raggiunta con tanta fatica.
Tutto finito? No, per almeno tre motivi. Il primo: il caso DS 316 non era l'unico a contrapporre Ue e Usa sugli aiuti di Stato per l'industria aeronautica. Già entro fine novembre 2016 giungerà la prima decisione nel caso DS 487 sugli incentivi fiscali americani, aperto il 19 dicembre 2014, e non è dato sapere chi vincerà. Il secondo: l'appello americano sul caso DS 353, di fatto simmetrico al DS 316, nel quale in primo grado il Wto ha deciso sostanzialmente contro Boeing. Il terzo riguarda ancora il DS 316: la richiesta di rapida applicazione fatta dal presidente Obama lascia intravedere il timore di altre tecniche dilatorie.
Un quadro davvero difficile, in cui gli unici sicuri di vincere sono gli avvocati, che per molti anni ancora continueranno a incassare parcelle milionarie.

LA SICUREZZA AEROPORTUALE E IL MODELLO BEN GURION

Le norme che regolano la sicurezza degli aeroporti si sono evolute sempre in risposta alla minaccia contingente, e troppo spesso solo dopo che la stessa si è manifestata. L'aeroporto Ben Gurion di Tel Aviv, in cui l'analisi dei comportamenti dei passeggeri è ormai parte integrante del sistema di sicurezza, potrebbe rappresentare il modello di riferimento anche per gli scali europei

STEFANO PIOPPI

Nell'era della crescente preoccupazione per il dilagare del terrorismo internazionale, il tema della sicurezza aeroportuale richiama un'attenzione sempre maggiore. Come in qualsiasi schema attacco-difesa, anche per gli aeroporti, gli strumenti di contrasto alla minaccia crescono al suo pari, traendo insegnamento da azioni offensive il cui costo è sempre troppo elevato. Ogni attacco terroristico, tentato o riuscito, ha svelato nuove vulnerabilità negli schemi difensivi, ponendo le basi per una securizzazione sempre crescente ma difatti mai completa. Gli attentanti dell'11 settembre 2001 hanno generato un ripensamento complessivo della sicurezza aeroportuale; si pensi solo alle norme che regolano oggi l'ingresso nella cabina di pilotaggio. Il tanto discusso *body scanner* è stato adottato in molti aeroporti dopo che, il giorno di Natale del 2009, Umar Farouk Abdulmutallab tentò di detonare sul volo Amsterdam-Detroit l'esplosivo nascosto nelle mutande, passando i controlli. Più recentemente, il 22 marzo scorso, l'attacco all'aeroporto internazionale Zaventem di Bruxelles ha riacceso il dibattito sulla predisposizione di controlli a ogni entrata del "lato terra" degli scali europei, cosa che già avviene in molti aeroporti nel mondo. Negli ultimi mesi però, il dibattito sembra descrivere un cambiamento qualitativo della sicurezza aeroportuale, non più legata all'aumento quantitativo dei controlli fisici su passeggeri e oggetti personali, ma piuttosto incentrata sulle misure preventive e previsionali.

Tale passaggio è guidato da Israele, Paese abituato alla necessità di contrastare il terrorismo. Allo scalo Ben Gurion di Tel Aviv, i controlli iniziano prima di entrare in aeroporto sulle macchine in arrivo. Oltre a ispezionare i veicoli, gli agenti rivolgono domande e interagiscono con guidatori e passeggeri al fine di carpire "segnali" di eventuali minacce. Tale controllo comportamentale si esegue anche all'entrata in aeroporto e nei successivi controlli di sicurezza tradizionali, per i quali alla componente tecnologica e fisica (comunque considerevole) si preferisce quella umana, con domande e interrogatori che possono durare dalle poche battute a diverse ore.

L'elemento centrale, e più criticato, di una simile strutturazione è rappresentato dalla selettività dei controlli (o *profiling*). Per un'anziana signora è probabile che i controlli siano molto più rapidi e meno accurati rispetto a quelli effettuati su un giovane arabo che si è presentato particolar-

mente nervoso in aeroporto. È questo il concetto alla base dell'analisi comportamentale: la valutazione accurata di ogni carattere fisico, etnico, e soprattutto di comportamento che possa indicare una minaccia. A Nizza, prima di condurre l'autocarro sul lungomare, Mohamed Lahouaiej Bouhlel ha passato un controllo di polizia interloquendo con agenti che, se preparati, avrebbero forse potuto carpirne le cattive intenzioni. Restano le perplessità legate all'applicazione di tale modello ai grandi scali intercontinentali. Una simile analisi richiede, infatti, personale quantitativamente adeguato alla valutazione di un numero molto elevato di soggetti.

Oltre alla preparazione del personale sull'analisi comportamentale (già prevista nella maggior parte dei corsi offerti da Iata e Icao), una struttura di sicurezza così intesa presuppone un sistema di raccolta, condivisione e analisi dei dati che faciliti le attività di *intelligence* riducendo il numero di soggetti da valutare. La direttiva 681 del 2016 dell'Unione europea getta le basi per la predisposizione di tale sistema, stabilendo l'obbligo per i vettori aerei di fornire alle autorità degli Stati membri i dati del codice di prenotazione (pnr) per i voli in arrivo o in partenza dall'Ue e la possibilità di farlo per i voli intra-Ue. Non è un elemento da poco, soprattutto considerando che i dati pnr comprendono le date di viaggio, l'itinerario, le informazioni relative al biglietto, all'indirizzo e agli estremi dei passeggeri, al bagaglio e alle modalità di pagamento. Tale direttiva permetterà una maggiore condivisione informativa tra i Paesi membri e la possibilità di accedere a dati che, se opportunamente trattati e selezionati, sostengano la prevenzione di atti terroristici. Lo stesso direttore generale dell'Ente nazionale aviazione civile (Enac), Alessio Quaranta, recentemente nominato dall'European civil aviation conference responsabile per la *security*, proprio in rifermento alla direttiva Ue sul pnr, ha ribadito come siano fondamentali la condivisione delle informazioni e l'attività di *intelligence*, in un'ottica non solo nazionale ma anche internazionale.

Aspettando il riconoscimento facciale, considerato dal ministro dell'Interno Alfano "il futuro", e recentemente annunciato dal collega tedesco De Maizière presso aeroporti e stazioni ferroviarie di Germania, il modello israeliano conquista consensi nel dibattito internazionale. L'analisi comportamentale potrebbe essere il nuovo fulcro della sicurezza aeroportuale.

Aviazione

DOVE VA IL POTERE AEREO?

Quali sono le sfide strategiche, culturali e concettuali che devono affrontare oggi le aeronautiche militari e come si presenterà domani il potere aereo? Dall'etica dei droni alle armi ipersoniche, passando per l'evoluzione della dottrina russa, se n'è discusso a Londra. Con una sorpresa: l'interesse per il pensiero aeronautico italiano!

GREGORY ALEGI *giornalista e storico*

In futuro, le aeronautiche militari saranno chiamate ad appoggiare operazioni prevalentemente terrestri (come in Afghanistan) o si misureranno con sofisticati sistemi di difesa aerea? E con quali uomini, aerei e dottrina lo faranno? Attorno a queste domande vertevano le 17 comunicazioni che relatori civili e militari di sette Paesi hanno presentato in due giorni al convegno "Airpower: Now and the Future". Se l'evento organizzato dal Royal air force museum e dalla Royal aeronautical society (che festeggia 150 anni) affrontava temi analoghi a quelli che si dibattono in Italia, il taglio era molto diverso per l'impronta pragmatica e operativa.

Lo si è capito sin dall'intervento d'apertura dell'*air chief marshal* Stephen Hillier, capo di stato maggiore della Royal air force (Raf), che ha declinato il tema del personale come principale risorsa della Forza armata e come necessità di un reclutamento di qualità e dell'offerta di opportunità di carriera e sviluppo personale, in particolare per la nuova categoria dei riservisti sui quali, dal 2015, il modello di difesa fa affidamento per colmare i vuoti creati dai tagli del governo. Altro punto centrale, la formazione tecnica, che fa della difesa un attore di primo piano nel settore sempre meno popolare dello Stem (Scienza, tecnologia, ingegneria e matematica). Allo stesso modo, gli ipersonici della relazione di Mark Hillborne (King's College) andranno a sostituire non gli aerei di linea sulle lunghe rotte intercontinentali, ma i missili balistici. In quest'ottica, le caratteristiche principali dei futuri sistemi, dai propulsori alla manovrabilità, non saranno tecnologiche ma politiche, soprattutto per l'instabilità che si verrebbe a creare dotandoli di testate atomiche.

Rispetto ad altri eventi – come quello del Japcc della Nato, che quest'anno avrà per oggetto la preparazione dell'alleanza alle operazioni aeree congiunte in ambiente degradato – la brevità degli interventi e la maggior laicità, se così si può definire, dell'organizzazione hanno consentito un dibattito vivace e stimolante, anche con critiche aperte alla politica di difesa britannica. Importante anche il tentativo di andare oltre il pur ben rappresentato asse anglo-americano, con contributi sull'evoluzione dell'aviazione militare in India ("l'ultima grande burocrazia dell'epoca vittoriana", secondo il relatore Amin Gupta, Usaf Air war college), l'evoluzione della dottrina so-

vietica dal punto di vista della Norvegia (Paese in prima linea in caso di conflitto, da cui l'interesse per le capacità dell'F-35) e la graduale rinascita del pensiero e delle capacità aeronautiche militari dell'Italia (sintetizzata nell'immagine della formazione della prima traversata atlantica dell'F-35). A colpire, in questo caso, sembrano essere state le considerazioni sulla difesa europea e il potenziale per lo sviluppo di nuovi concetti offerto dalla presenza delle due versioni a decollo convenzionale e corto.

Guardando avanti, in diversi si sono chiesti come la graduale espansione dell'importanza operativa dei velivoli a pilotaggio remoto, ovvero droni, inciderà sulla natura delle forze aeree. Perdere la centralità del pilota che le caratterizza sin dalla nascita (Peter Lee, Università di Portsmouth) e disaccoppiare l'intervento nei teatri operativi dal rischieramento, potrebbero trasformare le aeronautiche in "forze guardiane" (secondo la definizione di Paula Thornhill della Rand) e potenzialmente – com'è emerso dal dibattito – spingere gli avversari a contrastare i droni colpendo le stazioni di controllo dislocate all'interno dei Paesi. Le posizioni più diverse si sono avute sui temi etici: da chi sosteneva che in guerra l'obiettivo è non essere *fair*, cioè equi, a chi ha descritto la campagna aerea contro la Germania come "the bombing of ethics" (la distruzione dell'etica). Non è mancato chi ha sottolineato come gran parte delle azioni più discusse dei droni non siano svolte dalle aeronautiche militari ma dalla Cia, che opera con regole e criteri molto diversi. Qualche incertezza si è notata nell'uso del termine *airpower* che, da un intervento all'altro, passava dal corretto senso di "approccio strategico basato sull'ambiente aereo" a quelli di "mezzo aereo", "operazione aerea" e persino "aeronautica".

Due considerazioni dal punto di vista nazionale. La prima, l'interesse per la prospettiva italiana che, forse perché raramente espressa, è finita su *Flight* quasi in tempo reale. La seconda, l'origine (e in parte lo scopo) del convegno: fornire spunti di riflessione nell'ambito della realizzazione dell'omonima sezione del Raf museum. Una visione dinamica sotto ogni aspetto: non solo perché proietta il museo nel futuro, ma anche perché lo integra nella più vasta e difficile sfida di spiegare alla cittadinanza cosa sono e fanno le sue forze armate.


esa
esa
esa


AVIO
ADVANCED VISION INTO ORBIT
avio.com

MARTE, UNA STORIA LUNGA 20ANNI

VALERIA SERPENTINI

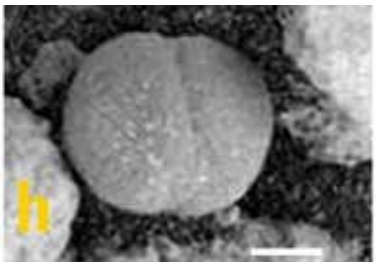
Raggiungere Marte, esplorarne la superficie, comprenderne la composizione e il suo passato, valutare la possibilità di inviare una colonia terrestre, sviluppare tecnica e tecnologia in grado di far viaggiare l'uomo tra i due pianeti. Sono questi alcuni degli obiettivi attorno ai quali si sono sviluppati i principali progetti spaziali degli ultimi decenni. Capire la conformazione geologica del pianeta e studiarne la sua storia fornirà all'uomo importanti informazioni sull'evoluzione di un pianeta che un tempo aveva condizioni ambientali molto simili alla Terra e che oggi risulta essere inabitabile a causa della quasi completa rarefazione dell'atmosfera.

I primi a raggiungere il pianeta rosso, in piena Guerra fredda, furono gli Stati Uniti nel lontano 1976 con le due missioni Viking che inviarono le prime immagini ad alta risoluzione. Per il primo progetto europeo si è dovuto attendere il 1996, anno in cui, ironia della sorte, l'Esa decise di rilanciare gli sforzi europei profusi per la fallimentare missione sovietica Mars 96. Ironia della sorte perché l'attuale missione Exomars – partita come missione congiunta Esa-Nasa – in uno dei suoi momenti più critici di sviluppo, era il 2010, trovò proprio nell'erede dell'Unione Sovietica – la Russia – il partner strategico con cui portare avanti il progetto, dopo l'improvvisa battuta d'arresto dell'agenzia Usa che, per problemi di *budget*, decise di tirarsi indietro, privando la missione Exomars dei due lanciatori, del sistema di atterraggio e della strumentazione necessaria per le attività di orbitaggio.

Nonostante le numerose criticità vissute dal progetto, *in primis* la mancanza di un *expertise* europea per *lander* e *rover* in grado di esplorare la superficie e l'atmosfera marziana, la competenza della comunità scientifica e industriale, soprattutto di quella italiana, ha permesso a Exomars di andare avanti e strutturarsi attorno a due grandi missioni. La prima è partita il 14 marzo 2016 con a bordo il *lander* Schiaparelli e il segmento orbitante TGO (Trace Gas Orbiter). Schiaparelli, costruito nello stabilimento torinese di Thales Alenia Space Italia, è un gioiello della tecnologia nostrana, con al suo interno l'esperimento italiano Amelia per lo studio della parte alta dell'atmosfera, la strumentazione italiana Dreams per lo studio di polvere e meteorologia marziana e il piccolo sistema, sermpre italiano, di retroriflet-

In Italia la prima prova di vita sul Pianeta rosso

Nell'ambito del progetto Discovering Magna Grecia, il ricercatore Domenico Macaluso ha coinvolto l'Università di Cosenza nel rinvenimento in un bacino evaporitico mediterraneo di frammenti di gesso selenitico contenenti microbialiti (piccole formazioni sferiche di 2-3 mm) analoghe a quelle presenti su Marte e rilevati dalle sonde Opportunity e Curiosity. Si tratta delle cosiddette *blueberry*. Un gruppo di scienziati italiani e



statunitensi ha confrontato le rocce della miniera romana di *Lapis specularis* con gli sferoliti trovati su Marte. La perfetta sovrapponibilità delle strutture terrestri e marziane segna un importante passo avanti nella dimostrazione dell'esistenza di vita sul pianeta rosso. Secondo alcuni studiosi, infatti, si tratterebbe di strutture minerali realizzate da microorganismi. Il prossimo passo sarà quello di analizzare i campioni rinvenuti nel Mediterraneo per confermare l'effettiva origine biogenica

tori Inrri essenziale per future attività di misurazione. Il segmento TGO è invece costituito da quattro strumenti (il Nomad e il Cassis europei e l'ACS e il FREND russi) che permetteranno di tracciare la presenza di gas – metano e argon – essenziale per capire possibili attività biologiche e geologiche e comunicare con la Terra. La seconda missione partirà nel 2020 e porterà sul pianeta rosso un *rover* che, grazie alla presenza di una trivella prodotta in Italia, sarà in grado di perforare il suolo fino a due metri in modo da prelevare e analizzare materiale marziano non soggetto alle forti radiazioni che al momento rendono impossibile la vita su Marte.

L'Agenzia spaziale italiana è stata promotrice della missione. Il contributo finanziario italiano si attesta intorno ai 370 milioni di euro (il 33% dell'intera spesa, che è di 1,2 miliardi), il coordinamento generale della missione è stato affidato a Thales Alenia Space Italia e da Torino, più precisamente dal Rover operations control center di Altec, si terrà in contatto con il *rover* che verrà lanciato nel 2020. Grande ruolo, quindi, quello dell'Italia.

Exomars è solo il primo passo di un percorso europeo che in futuro dovrà portare allo sviluppo di strumentazione in grado di effettuare voli di andata e ritorno verso Marte. Le sfide non sono poche e, molto probabilmente, richiederanno approfondimenti tecnologici e puntualizzazioni politico-giuridiche per lo sfruttamento e l'utilizzo delle risorse extra-terrestri.

Avere la capacità di atterrare sul pianeta e ripartire in direzione Terra sarà importante, in un primo momento, per far arrivare nei nostri laboratori dei campioni di suolo marziano da analizzare. È solo dopo la dimostrazione di rientro che si potrà pensare di inviare su Marte i primi coraggiosi esploratori, anche se negli Stati Uniti ci sono già imprenditori visionari, come Elon Musk, che pensano alla colonizzazione del pianeta e alla produzione di navette che tra dieci anni saranno in grado di trasportare in 80 giorni fino a 200 astronauti. Alla fine del XIX secolo, le innovazioni tecnologiche avevano ispirato Jules Verne a scrivere delle avventure del londinese Philae Fogg impegnato nel giro del mondo in 80 giorni. Sono bastati poco più di 100 anni per puntare gli occhi verso nuovi orizzonti. Chi sarà il protagonista del viaggio verso Marte in 80 giorni?

I VANTAGGI DEI SISTEMI DI SATELLITE SHARING

Se Uber ha trasformato il modo di pensare i trasporti pubblici, le architetture satellitari federate potrebbero rivoluzionare l'industria aerospaziale downstream: sistemi osservativi multi-layer in cui piccole e grandi piattaforme satellitari collaborano tra loro configurandosi quali asset di cui sarà possibile usufruire on demand

ALESSANDRO GOLKAR *direttore dello Space center e docente presso lo Skoltech di Mosca*

Piattaforme innovative quali microsatelliti e architetture satellitari distribuite sono sistemi che possono essere concepiti come complementari alle infrastrutture esistenti, tradizionalmente costituite dai grandi sistemi satellitari di osservazione della Terra, telecomunicazioni, e navigazione. Tali concetti innovativi si innestano nel *trend*, che si osserva oramai da decenni nell'industria aerospaziale, del crescente ruolo dei piccoli satelliti e delle piattaforme satellitari distribuite, nonché dei dati e degli annessi servizi da loro abilitati. Una delle grandi sfide odierne dell'industria aerospaziale, e in particolare dell'industria del cosiddetto settore *downstream*, ossia servizi e applicazioni derivanti dall'uso dei dati ottenuti dagli *asset* spaziali, è infatti offrire prodotti a servizio dei cittadini e del settore privato; un settore in grado di fornire nuove capacità per ambiti come la connettività globale, l'agricoltura di precisione, la *business intelligence*, il *real estate* e il mercato assicurativo. Nonostante le esistenti piattaforme satellitari siano gioielli di alta tecnologia, gli alti costi di sviluppo e di lancio fanno sì che le prestazioni, in termini di rivisita temporale delle attuali infrastrutture basate su satelliti monolitici, non possano essere facilmente scalate mantenendo competitività economica sul mercato. Ad esempio, il sistema europeo Sentinel-2 è in grado di offrire un'immagine di un punto situato alle medie latitudini della sfera terrestre ogni due-tre giorni.

Mentre una frequenza temporale dell'ordine di qualche giorno risulta adeguata per una moltitudine di applicazioni scientifiche su scala globale, non consente di studiare fenomeni con dinamiche temporali dell'ordine di ore, se non minuti, quale ad esempio l'evoluzione del traffico cittadino o delle dinamiche di molte delle attività umane. Si pensi alle opportunità che si potrebbero aprire su diversi fronti, nel momento in cui risulti possibile misurare attività afferenti ai diversi settori economici con frequenza nell'ordine di minuti, su scala globale. In un futuro, probabilmente lontano, sarà possibile fruire in tempo quasi reale di tali dati: si pensi a un *Google Maps*, le cui immagini vengono aggiornate ogni ora, disponibile sul proprio *smartphone*.

Innovative architetture satellitari distribuite hanno lo scopo di offrire, tra altri benefici tecnici e socio-economici, capacità di osservazione e di

L'EVENTO AL CENTRO STUDI AMERICANI
Il 10 e 11 ottobre si è tenuta presso il Centro studi americani a Roma la quarta edizione del *workshop* Federalist and fractionated satellite systems, evento che riunisce esperti di sistemi satellitari provenienti da agenzie spaziali (Asi, Esa, Dlr), centri di ricerca e università (La Sapienza, Mit, Skoltech, Cornell University) e industrie (Leonardo, Lockheed Martin, Airbus). Nella foto in alto, da sinistra: Riccardo Grazi (Vitrociset), Alessandro Golkar, Paolo Gaudenzi, Massimo Comparini (ad E-GEOS), Jean Francois Charrier (Airbus - OneWeb Satellites), Mesut Ciceker. Nella foto in basso, da sinistra: Lars P. Dyrud (ceo OmniEarth), Christoph Gunther (German Space Agency), Nicola Zaccheo (ceo SITAEL), Alessandro Golkar, Roberto Capua (resp. Ricerca e laboratorio digitale SOGEI), Daniel Selva (Cornell university), Stefano Santandrea (Esa)

connettività ad alto tempo di rivisita, consentendo lo sviluppo di applicazioni nei settori economici sopra menzionati. È chiaro, tuttavia, che nel momento in cui tali architetture innovative vengano realizzate con piccole piattaforme, non ci si può attendere le stesse prestazioni fornite dai grandi satelliti. Si noti, d'altro canto, che in talune applicazioni l'importanza della risoluzione temporale (ossia il tempo di rivisita) prevale su altre metriche di prestazione come la risoluzione spaziale. Inoltre, si consideri che è altresì possibile concepire sistemi satellitari federati e frazionati basati su grandi piattaforme. Il tema della distribuzione e della piccola scala dei nuovi sistemi satellitari, dunque, non è da confondere. Di fatto, il potenziale maggiore delle nuove architetture distribuite si esplica al meglio nel momento in cui si identificano schemi collaborativi tra satelliti di diverse capacità, strumentazione, orbite e dimensioni.

In questo contesto, le architetture satellitari federate (note nella letteratura scientifica come *federated satellite systems*) sono la trasposizione della *sharing economy* in ambito spaziale, postulando la creazione di sistemi di *satellite sharing* in grado di offrire agli operatori la possibilità di affittare le proprie capacità satellitari quando non richieste dalla propria missione primaria, allo stesso modo in cui Uber ha innovato il settore dei trasporti pubblici in molte città del globo. Si ipotizzano, dunque, sistemi osservativi *multi-layer* in cui piccole e grandi piattaforme satellitari poste a diverse quote orbitali, con strumenti e prestazioni diverse (nonché complementari), collaborano tra loro configurandosi quali *asset* di cui sarà possibile usufruire *on demand*, in modalità di mercato del tutto analoghe a quelle previste dalle future *grid* di distribuzione intelligente dell'energia elettrica.

L'innovazione del settore spaziale *downstream* passa necessariamente per l'innovazione nel settore *upstream*, sviluppando piattaforme satellitari innovative in grado di coniugare e complementare i benefici e le limitazioni di satelliti di diverse capacità e dimensioni, dal grande sistema satellitare geostazionario al nanosatellite in orbita bassa. Il crescente interesse industriale e degli investimenti privati nel settore è testimone di un cambio di paradigma che promette di mutare il volto del settore nei prossimi due decenni di attività.

LA NUOVA FRONTIERA DELLA SILICON VALLEY

Il dipartimento della Difesa Usa si sta aprendo a collaborazioni con innovative aziende californiane che progettano costellazioni di piccoli ma iper-performanti satelliti. Potrebbero svilupparsi small-smart-satellites dalle prestazioni elevate, lanciati a sciami da lanciatori riutilizzabili, dai contorni oggi non definibili, ma che forse sono già nella mente di qualche altro Musk della Silicon Valley

MARCELLO SPAGNULO *ingegnere aeronautico ed esperto aerospaziale*

Tradizionalmente l'industria spaziale commerciale ha sempre posto particolare attenzione al prezzo del servizio di lancio, che è una parte importante del costo complessivo di un sistema satellitare. Allo stesso tempo, però, si è sempre considerato con grande attenzione anche il grado di affidabilità del lanciatore, che è il vero parametro per una realistica valutazione del servizio. Per il settore governativo, e militare in particolare, il fattore economico è invece sempre stato subordinato alla *reliability* del lanciatore.

Si pensi alle attività spaziali del DoD americano. Nel 1995, il Pentagono finanziò il programma Expendable evolved launch vehicles (Eelv) solo per garantirsi l'accesso allo spazio in modo sicuro e garantito, e il prezzo non fu mai un fattore determinante. Infatti nel programma Eelv furono coinvolte, in una sorta di monopolio dedicato, le uniche due aziende statunitensi che realizzavano lanciatori, Boeing e Lockheed, che precedentemente si confrontavano in una sanguinosa guerra commerciale per accaparrarsi il lucroso mercato militare. Quando costituirono nel 2006 la United Launch Alliance (ULA), Boeing e Lockheed non solo erano in competizione per i contratti di lancio, ma erano anche impegnate in una battaglia legale sulla tecnologia missilistica. Per il Pentagono, la *joint venture* fu quindi un modo per risolvere un complesso nodo legale e commerciale tra i suoi migliori – e unici – fornitori di servizi di lancio facendo in modo che entrambi potessero rimanere nel *business*. Tutto ciò aveva un costo che il DoD era pronto a sostenere chiedendo in cambio un'affidabilità quasi totale, che in effetti è stata raggiunta. Dal suo primo lancio nel 2006, la ULA ha effettuato 106 missioni tutte riuscite, e secondo i documenti pubblici avrebbe ricevuto in cambio almeno 15 miliardi di dollari dal governo federale, anche se il valore reale potrebbe essere molto più alto se fossero noti i finanziamenti ricevuti dai *budget* segretati della Cia, della National security agency, del National reconnaissance office e di altre agenzie governative di spionaggio.

Il costo di ciascun lancio della ULA, stimato dal Government accountability office (Gao), è di cir-

ca 350 milioni di dollari. Anche nel caso in cui la *joint venture* non si vedesse assegnato un contratto governativo (ipotesi irrealistica poiché nel 2013 ha avuto un blocco di acquisto di 36 lanci preassegnati), riceverebbe comunque un volume annuale di 800 milioni di dollari per il mantenimento in efficienza operativa del servizio di lancio. Il prezzo dell'affidabilità totale è sempre stato imprescindibile per i militari, mentre per il settore commerciale il giusto *mix* tra affidabilità e costo ha guidato scelte e preferenze.

Per rompere il monopolio della ULA, la SpaceX di Elon Musk ha dovuto praticamente citare in giudizio l'ufficio acquisti del Pentagono, ma alla fine è riuscita ad accreditarsi come fornitore di servizi di lancio e promette di trasportare i satelliti militari nello spazio a meno della metà del costo del fornitore monopolista, calando così il sipario su decine di miliardi di dollari di potenziali risparmi nelle spese militari, o meglio di potenziali diversi utilizzi dei risparmi di spesa. Ecco che si delinea meglio il cambio di paradigma del settore. Dato che SpaceX promette minor prezzo e maggior frequenza di lancio, è lecito ipotizzare che anche il settore militare prenda in considerazione un nuovo paradigma di sviluppo e realizzazione dei satelliti da lanciare. Nello scorso mese di aprile, il capo della US National geospatial-intelligence agency ha dichiarato di voler aprire un nuovo centro della Nga proprio nella Silicon Valley per lavorare in modo più diretto con le *start up* che operano nel settore dello *space-imaging*.

L'idea dell'ente è creare un aggregatore governativo in grado di raggiungere tutti i poli di innovazione della Valley, *in primis* due piccole aziende, ma di alto profilo, la Planet Labs e la Terra Bella (ex Skybox Imaging acquistata da Google nel 2014) che lì hanno sede. Entrambe le società ricordano la SpaceX dei primi anni 2000, quando nessuno credeva nella possibilità di un privato di realizzare un lanciatore innovativo con poco più di un miliardo di dollari, tranne proprio il Pentagono che offrì a Elon Musk il poligono militare di Kwajalein per i primi lanci di prova. Planet Labs e Terra Bella hanno una strategia ambiziosa ma

UN CENTRO NGA NELLA SILICON VALLEY
Di recente, il capo della US National geospatial-intelligence agency ha detto di voler aprire un nuovo centro della Nga proprio nella Silicon Valley per lavorare in modo più diretto con le *start up* che operano nel settore dello *space-imaging*. L'idea dell'ente è di creare un aggregatore governativo in grado di raggiungere tutti i poli di innovazione della Valley, *in primis* due piccole aziende, ma di alto profilo, la Planet Labs e la Terra Bella (ex Skybox Imaging acquistata da Google nel 2014) che lì hanno sede

I MICROSATELLITI
Planet Labs e Terra Bella hanno una strategia ambiziosa ma chiara: realizzare mini e micro satelliti in grado di fornire immagini a elevata risoluzione. L'approccio è completamente diverso dal modello di realizzazione degli attuali satelliti di *imaging*, che costano più di 500 milioni di dollari l'uno, sono grandi come un *suv*, pesano due tonnellate, sono costruiti in cinque anni e operano in orbita per un decennio

LA LEGGE DI MOORE NELLO SPAZIO
Le aziende della Silicon Valley utilizzano componenti *off-the-shelf* e *software open source* per costruire satelliti dalle dimensioni di un frigorifero pesante al massimo 200 kg, così da poter essere lanciati rapidamente e a costi contenuti. Sostanzialmente vogliono portare la legge di Moore nello spazio; un'altra analogia con la SpaceX di Elon Musk, per usufruire di un ciclo di sviluppo più breve, di una maggiore potenza di elaborazione, e di una curva di costo più accessibile

chiara: realizzare mini e micro satelliti in grado di fornire immagini a elevata risoluzione. L'approccio è completamente diverso dal modello di realizzazione degli attuali satelliti di *imaging*, che costano più di 500 milioni di dollari l'uno, sono grandi come un *suv*, pesano due tonnellate, sono costruiti in cinque anni e operano in orbita per un decennio.
Le aziende della Silicon Valley utilizzano componenti *off-the-shelf* e *software open source* per costruire satelliti dalle dimensioni di un frigorifero pesante al massimo 200 kg, così da poter essere lanciati rapidamente e a costi contenuti. Sostanzialmente vogliono portare la legge di Moore nello spazio; un'altra analogia con la SpaceX di Elon Musk (vedasi *AirPress* n° 53 *La sfida di Musk che piace a Google*), per usufruire di un ciclo di sviluppo più breve, di una maggiore potenza di elaborazione e di una curva di costo più accessibile. Magari all'inizio le immagini ottenute non saranno sufficientemente dettagliate per sparare un missile all'interno di una caverna in Afghanistan, ma consentirà comunque di contare le auto in un parcheggio. Però, forse, la seconda generazione di satelliti e sensori raggiungerà le prestazioni degli attuali satelliti spia; in fondo la SpaceX, inizialmente, lanciò nel 2008 il Falcon 1 (700 Kg in Leo), e solo otto anni dopo progetta di lanciare il Falcon 9 Heavy (55 tonnellate in Leo). Certo, il *business* non è semplice: a ottobre un Falcon è esploso sulla rampa di Cape Canaveral durante dei test, ma ciò non fermerà l'avanzamento tecnologico né della SpaceX né di chi progetta futuri satelliti. Ecco perché il dipartimento della Difesa si sta aprendo a collaborazioni con innovative aziende californiane che progettano costellazioni di piccoli ma iper-performanti satelliti, per adottare rapidamente nuove tecnologie da *leading edge*. La combinazione dei nuovi paradigmi di realizzazione e di servizio che gli Usa stanno avviando nel settore dei lanciatori e anche in quello dei satelliti potrebbe, entro pochi anni, mutare profondamente la tipologia degli assetti spaziali.
Accanto ai satelliti convenzionali, al momento imprescindibili per le comunicazioni e l'osservazione, potrebbero svilupparsi *small-smart-satellites* dalle prestazioni elevate, lanciati a sciami da lanciatori riutilizzabili, con un impatto non solo sui costi generali ma soprattutto sulle evoluzioni applicative, governative e commerciali, dai contorni oggi non definibili ma che forse sono già nella mente di qualche altro Elon Musk della Silicon Valley.

Luca Parmitano — astronauta Esa

Esploratori di oggi e di domani

Francesco Sauro è un esploratore: parte, con lo zaino in spalla, e rientra con racconti di avventure, memorie fatte di disegni, mappe e luoghi mai visti prima. Durante Caves 2014 ho percepito la sua passione nel desiderio di trasmetterci le basi di speleologia e geologia, nel trasformarci da semplici spettatori a membri effettivi di una spedizione sotterranea.

Mentre risalgo il letto del fiume che ha scavato, con millenaria pazienza, uno stretto *canyon* nelle Dolomiti, cerco di mettere a frutto gli insegnamenti di quella esperienza, di inserirli nel contesto in cui mi trovo, simile e tuttavia così diverso. Cicatrici pietrificate da tempi lunghissimi (e incomprensibili nella nostra scala umana) ci circondano, le forme scolpite dall'acqua sono un'eco visiva di quelle viste nelle caverne. Studiamo un tratto di parete: sotto è rocciosa, come abbiamo visto finora. In mezzo, è un grezzo mosaico di pietre, di varie dimensioni ma lisce e coese fra di loro, come un muro, ma concavo alla base. Sopra, la parete è ricoperta da terriccio e vegetazione. Ho osservato lo stesso fenomeno nella parete di una valle limitrofa: è lo scheletro del letto di un fiume che, millenni fa, attraversava questo terreno, prima che il *canyon* lo tagliasse in due. Francesco, che ci accompagna e ci guida, conferma la mia intuizione; poi ci mostra gli effetti di quello che, millenni fa, era un antico ghiacciaio. La pietra, grazie a lui e agli altri istruttori del programma Pangaea, acquista una propria voce e racconta la sua storia. I miei colleghi e io non ne parliamo ancora la lingua, ma stiamo imparando a coglierne e distinguerne i suoni – non per partecipare alla conversazione, ma per comprendere, interpretando determinati segnali, quando il racconto è fuori dal comune.

Torneremo sulla Luna, e cammineremo su un asteroide o su Marte: allora dovremo trasmettere informazioni su quei mondi, usando il linguaggio corretto. Dovremo prendere decisioni operative: quali, quanti campioni raccogliere? Cosa raccontano le polveri, le rocce lunari e marziane? Non sarà la mia generazione di astronauti a lasciare quelle impronte ma, quando sarà il momento, dovremo fornire a quei futuri esploratori interplanetari gli strumenti operativi e scientifici per svolgere il loro compito. Pangaea serve allora a preparare gli istruttori del futuro: non per dare risposte agli astronauti, ma per capire quali domande dovranno porsi.

SAVE*the*DATE

8-9 NOVEMBRE

La Best defence conference canadese

La London canadese, in Ontario, ospiterà la Best defence conference, evento dal titolo ambizioso dedicato al comparto della difesa canadese e internazionale. Per due giorni si susseguiranno presentazioni, esposizioni e soprattutto incontri di *business* tesi all'individuazione di *partnership* e contatti commerciali. Parteciperanno industrie ma anche rappresentanti istituzionali e dell'accademia

8-10 NOVEMBRE

Torna in India l'Aeromart Summit

Dopo il successo del 2014, torna a Bangalore in India l'evento dedicato al comparto aerospaziale. La nuova edizione dell'Aeromart Summit punta a coinvolgere oltre 600 partecipanti, 250 aziende e rappresentanti di 20 paesi in più di 5mila incontri *business-to-business* e conferenze. Grande attesa per un evento in un Paese che resta il primo importatore al mondo nel settore difesa e aerospazio

14-15 NOVEMBRE

A Roma una conferenza sulla tecnologia navale

Lo Smi Group, organizzazione specializzata in eventi *b2b*, organizza a Roma la conferenza Naval mission systems technology. L'evento si rivolge agli addetti ai lavori del settore, con l'intenzione di offrire una piattaforma d'incontro tra imprese, investitori e rappresentanti istituzionali. Al centro del dibattito, la nuova generazione di capacità tecnologiche navali

15-17 NOVEMBRE

Il workshop dell'Esa sulla misurazione dei venti

L'Agenzia spaziale europea (Esa) organizza una tre giorni di *workshop* sulle applicazioni scientifiche per la misurazione dallo spazio dei venti oceanici. Il quartier generale del Met Office a Exeter, in Regno Unito, ospiterà numerosi incontri su: monitoraggio ambientale satellitare, strumenti avanzati del settore e modelli e metodi di osservazione

24 NOVEMBRE

Il Cesma discute di reti strategiche

Il Centro studi militari aeronautici Giulio Douhet organizza a Roma, presso la Casa dell'aviatore, l'evento "Le reti di comunicazione strategiche della difesa". Il tema è da sempre al centro del dibattito relativo a ogni tipo di operazione militare, ma ha recentemente acquisito ancora maggiore importanza con l'affermarsi del *cyber*-spazio quale ulteriore dominio operativo

27 NOVEMBRE – 2 DICEMBRE

I materiali avanzati in mostra a Boston

La Material research society, un'organizzazione *no-profit* che riunisce scienziati, ricercatori, industrie ed esperti di tecnologie e materiali avanzati, organizza a Boston il 2016 Fall Meeting & Exhibit. L'evento, rivolto ad appassionati e addetti ai lavori, offrirà quasi 6mila presentazioni in 54 diversi simposi tematici. Tra i temi trattati, la manifattura digitale, le nanotecnologie e l'elettronica

29 NOVEMBRE – 1 DICEMBRE

Il settore dell'aerospazio a Tolosa

L'Aeromart Toulouse 2016 riunirà in Francia il comparto aerospaziale europeo e non solo. Si attende la partecipazione di 1300 società per un totale di oltre 45 Paesi rappresentati. Gli incontri *b2b* previsti sono 15mila, un numero incredibile che conferma l'efficacia dell'Aeromart. All'evento, che mira a superare il successo di due anni fa, parteciperanno tutte le maggiori industrie europee del settore

ENAV. GUARDIAMO IN ALTO.

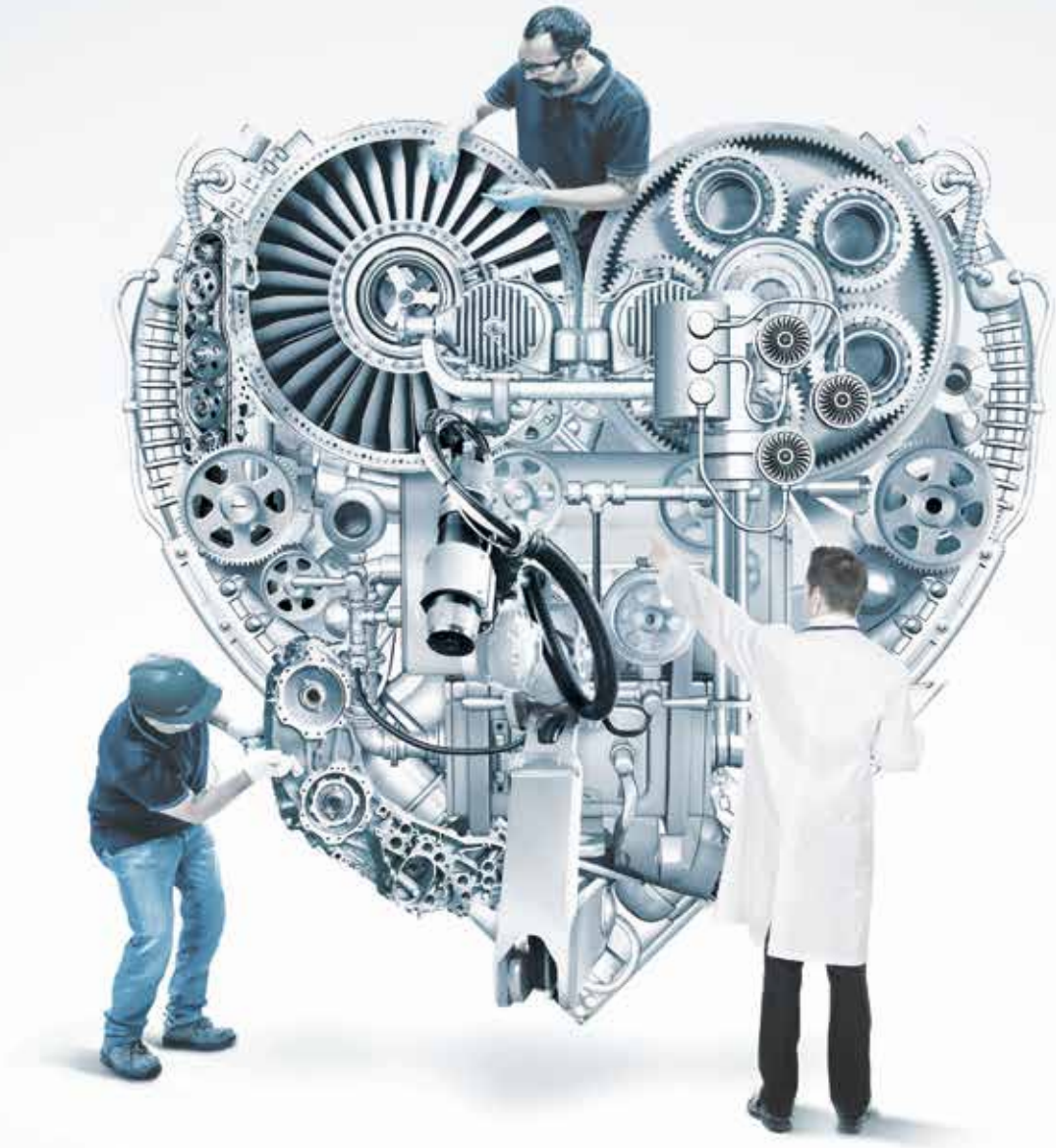
DA 30 ANNI CONTROLLIAMO E GESTIAMO IL TRAFFICO AEREO NEI CIELI ITALIANI.

È COSÌ CHE SIAMO DIVENTATI UNA DELLE SOCIETÀ LEADER DEL SETTORE IN EUROPA.

GESTIRE E CONTROLLARE I CIELI ITALIANI GARANTENDO UN TRAFFICO AEREO VELOCE, REGOLARE E IN SICUREZZA A MILIONI DI PASSEGGERI OGNI ANNO. ECCO COSA SIGNIFICA PER NOI GUARDARE IN ALTO.

enav.it/guardiamoinalto

WE MAKE AVIATION BEAT



GBX
- MECHANICAL POWER TRANSMISSIONS
- ACCESSORY DRIVE TRAINS
- HELO GEARBOXES

LPT
- COMPLETE MODULE OWNERSHIP
- CRITICAL ROTATING PARTS EXPERTISE
- VERTICALIZED PRODUCTION CAPABILITIES

TiAl
ADDITIVE MANUFACTURING
- DESIGN FLEXIBILITY
- ENHANCED MATERIAL PROPERTIES
- NET-TO-SHAPE PARTS CREATION

CRO
- SERVICE EXCELLENCE
- MODULES & COMPONENTS REPAIR TECHS OWNER
- SPARE PARTS PRODUCTION

PRODUCTION
- WORLD CLASS FLEXIBLE MANUFACTURING SYSTEMS
- LEAN & 6SIGMA BASED CONTINUOUS IMPROVEMENT
- SUPERIOR TECH EDUCATION WITH ACADEMIA

NEW TECHNOLOGIES ARE THE HEART OF OUR TRANSMISSIONS AND LOW PRESSURE TURBINES

Driven by innovation we are constantly improving our production standards and competitiveness. **Industry 4.0**, high technology and eco-compatibility for aeronautical engines are our future. This is why we are always challenging ourselves from our commitment to European R&D programs to our leading role among companies driving the **digital industry revolution**.

FOLLOW THE **#ENGINEOFINNOVATION**

DISCOVER MORE ON AVIOAERO.COM

Avio Aero
A GE Aviation Business