SPAZIO
Spacecraft, la Nasa prepara il dopo-Shuttle
— ROBERTO VITTORI

DIFESA
Il Libro bianco si avvicina al traguardo
— ALESSANDRO CORNACCHINI

AVIAZIONE
Registri aerei, operazione trasparenza
— GREGORY ALEGI

AirPress

settembre 2014 48

MENSILE SULLE POLITICHE
PER L'AEROSPAZIO E LA DIFESA

CYBER WAR
La minaccia invisibile

David **Anthony**/ Marco Andrea **Ciaccia**/ Antonio **Colella**/ Alexander **Gamero-Garrido**/ Umberto **Gori**/ Jason **Healey**/ Andrea **Rigoni**/ Jason **Rivera**/ Alessandro **Zanasi**

contributors

MARIO ARPINO
Generale dell'Aeronautica militare, autore di numerosi articoli ed esperto di questioni geopolitiche e militari. È stato capo di Stato maggiore dell'Aeronautica dal 1995 al 1999 e capo di Stato maggiore della Difesa dal 1999 al 2001. Fra i vari riconoscimenti attribuitigli, spiccano la decorazione di cavaliere dell'Ordine militare d'Italia, la Medaglia militare aeronautica di lunga navigazione aerea (Oro), la Legione al merito degli Stati Uniti

ALEX GAMERO-GARRIDO
Ingegnere elettronico. Ricercatore presso il Computer science and a.i. lab e laureato in Technology and policy al Mit. Collabora con il dr. David Clark sul tema della congestione della rete, dell'economia e della politica di Internet. Specializzato in conflitti informatici, ha lavorato per l'Unione internazionale delle telecomunicazioni (Itu), agenzia specializzata delle Nazioni Unite con sede in Ginevra

UMBERTO GORI
Professore emerito, Università degli Studi di Firenze. Già professore ordinario di Relazioni internazionali, Università degli Studi di Firenze. Docente di Studi strategici, Scuola di guerra aerea. Già docente di Relazioni internazionali e Studi strategici, Accademia navale, Marina militare. Già docente di Strategia globale, Scuola di guerra, Civitavecchia. Presidente del Centro interdipartimentale di studi strategici, internazionali e imprenditoriali (Cssii) Direttore, Istituto per gli studi dii previsione (Ispri)

JASON HEALEY
Direttore del *Statecraft cyber initiative* dell'Atlantic council. È stato responsabile per le politiche *cyber* presso la Casa Bianca. Già direttore esecutivo presso la Goldman Sachs Asia, è stato inoltre ufficiale dei servizi segreti della Us Air force. È membro del consiglio della Cyber conflict studies association e docente di Politica informatica

MARCELLO SPAGNULO
Ingegnere aeronautico e dirigente d'azienda. *Consultant and managing associate* presso Extraterrestrials Essentials Llc. Da oltre 25 anni lavora nel settore spaziale - in Italia e all'estero - sia presso aziende private sia presso agenzie governative. Autore di *Lo Spazio oltre la Terra* edito da Giunti-Edizioni e di *Elementi di management dei programmi spaziali*, edito da Springer Italy. Collabora con la rivista *Space Magazine*

ALESSANDRO ZANASI
Ingegnere nucleare. Fondatore della Zanasi & Partners, società di consulenza in materia di sicurezza e co-fondatore di Temis. Professore associato al Wit – Wessex institute of technology di Southampton. Già Security research advisor dell'Esrab e dell'Esrif e docente di Data/Text mining e di Tecniche di intelligence presso l'Università di Bologna. È stato inoltre ufficiale dell'Arma dei carabinieri presso il Centro di investigazioni scientifiche e responsabile dell'Ibm intelligence in sud Europa, Medio Oriente e Africa

Cyber

L'INTELLIGENCE E LA BATTAGLIA DELLE IDEE

ALESSANDRO ZANASI *esperto di cyber-intelligence e fondatore di Zanasi & Partners*

Conoscenza culturale ed efficiente capacità bellica sono legate fra di loro: la *cultural intelligence* è centrale per garantire il successo delle operazioni militari riguardando la capacità di analizzare e sintetizzare informazioni anche dal punto di vista linguistico, socio-economico, consuetudinario e storico-religioso al fine di comprendere, evidenziare le credenze, i valori, le attitudini e i comportamenti di gruppi e individui.

L'elemento di novità degli ultimi anni consiste nell'ampio e ragionato ricorso agli strumenti offerti dal web e in particolare ai *social media*. Questo fenomeno ha aumentato in maniera significativa la velocità e capillarità con le quali un messaggio può diffondersi. Al tempo stesso, sui *social media*, ogni singolo militante o simpatizzante ha la possibilità di rivestire, consapevolmente o meno, un ruolo attivo nella strategia propagandistica del network terroristico di riferimento.

I messaggi vengono ritrasmessi dai singoli utenti, modificati e integrati con nuovi elementi. Il che ha un effetto sull'autorevolezza e veridicità del messaggio stesso, che, nel giro di poche iterazioni, l'utente finale non necessariamente riesce più ad associare all'organizzazione terroristica che lo ha prodotto in origine.

L'Islamic state, che da tempo ha dimostrato di possedere familiarità con le più moderne tecnologie informatiche, unita a una sensibilità non comune nell'utilizzo dei *social media* a fini propagandistici, ha recentemente deciso di alzare il tiro con la diffusione dei filmati relativi alle esecuzioni di ostaggi con l'intento di aumentare la propria credibilità agli occhi del mondo proprio grazie a un sapiente utilizzo del web.

Tale esibizione di forza ha però prestato il fianco a una controffensiva da parte delle agenzie di intelligence occidentali. Sofisticate tecniche di *cyber-intelligence* quali analisi vocale e *video mining* hanno infatti permesso agli analisti di identificare il militante protagonista dei filmati, nonché l'area geografica nella quale i video, o almeno il primo di essi, sono stati girati.

È questa la direzione nella quale l'*intelligence* antiterrorismo dovrà necessariamente concentrare i propri sforzi nel futuro immediato. Sviluppare capacità di monitoraggio e processamento, in quasi *real time*, di tutto il materiale jihadista, testuale, fotografico e video, che circola sul web e sui *social network*. Così come di tutti gli effetti che la fruizione di tale materiale produce "sui cuori e sulle menti" dell'*audience* cui esso è rivolto.

LA CULTURAL INTELLIGENCE
Conoscenza culturale ed efficiente capacità bellica sono legate fra di loro: la *cultural intelligence* è centrale per garantire il successo delle operazioni militari riguardando la capacità di analizzare e sintetizzare informazioni anche dal punto di vista linguistico, socio-economico, consuetudinario e storico-religioso

IL RUOLO DEI SOCIAL MEDIA
I *social media* hanno aumentato in maniera significativa la velocità e la capillarità secondo le quali un messaggio può diffondersi. Attraverso i *social media*, ogni singolo militante, simpatizzante ha la possibilità di rivestire, consapevolmente o meno, un ruolo attivo nella strategia propagandistica del *network* terroristico di riferimento

L'ISLAMIC STATE
L'Islamic state ha dimostrato di possedere familiarità con le più moderne tecnologie informatiche, unita a una sensibilità non comune nell'utilizzo dei *social media* a fini propagandistici. Ciò ha innescato una controffensiva da parte delle agenzie di *intelligence* occidentali che mediante analisi vocale e *video mining* hanno identificato il militante protagonista dei filmati, nonché l'area geografica nella quale le immagini sono state girate

LA GIUSTA DIREZIONE
È necessario sviluppare capacità di monitoraggio e processamento, in quasi *real time*, di tutto il materiale jihadista, testuale, fotografico e video, che circola sul web e sui *social network*. Metodologie d'avanguardia che permettono di automatizzare il più possibile non tanto la raccolta, quanto soprattutto l'analisi delle informazioni, qualitative e quantitative, strutturate e non

L'INFORMATION OVERLOAD
Il rischio è di ritrovarsi una quantità di materiale a disposizione maggiore, di svariati ordini di grandezza, rispetto a quanto sia possibile processarne efficacemente in un contesto di risorse giocoforza limitate.
Il problema è che per essere evitato richiede un massiccio ricorso alle tecniche del *text, data, video mining* e del *big data analytics*

Il rischio più immediato dato dall'adozione di un tale approccio è inevitabilmente quello dell'*information overload*: ritrovarsi una quantità di materiale a disposizione maggiore, di svariati ordini di grandezza, rispetto a quanto sia possibile processarne efficacemente in un contesto di risorse giocoforza limitate. Un problema che per essere evitato richiede un massiccio ricorso alle tecniche del *text, data, video mining* e del *big data analytics*. Metodologie d'avanguardia, già impiegate con successo in vari ambiti, che permettono di automatizzare il più possibile non tanto la raccolta, quanto soprattutto l'analisi delle informazioni, qualitative e quantitative, strutturate e non. Riducendole a un *corpus* di facile gestione e immediata comprensione per l'analista che, sulla base di queste informazioni, deve produrre *intelligence*.
Grazie a Snowden, Assange e ai loro emuli già sappiamo quanto gli Usa e in particolare la loro Agenzia per la sicurezza nazionale stanno facendo in ambito di ricerca e sviluppo in *cyber-intelligence* e *cyber-security*.
Gli investimenti richiesti sono talmente grandi che non solo le organizzazioni private ma neppure uno Stato come il nostro può permettersi una ricerca e sviluppo di livello mondiale se non all'interno della cornice europea che, alla ricerca in materia di *cyber-security*, attraverso i programmi di finanziamento FP7 e Horizon 2020, ha allocato diversi miliardi di euro. Vale la pena ricordare che due progetti di ricerca (*Isar* e *Soteria*) dedicati all'analisi dei *social media* a fini di *search and rescue* e di gestione delle emergenze vedono impegnate svariate organizzazioni di tutta Europa.
Uno dei loro obiettivi è lo sviluppo di tecniche di raccolta automatica di dati e di *social media monitoring* con applicazioni di *data* e *video mining*, *text mining* multilingua e *big data analytics* per la classificazione e il processamento automatizzato del materiale raccolto.
Alcuni progetti si dirigono espressamente alla lotta alla radicalizzazione, ovvero quel fenomeno che porta, ad esempio, un cittadino europeo ad assumere valori e comportamenti sempre più estremistici sino a diventare violento, quali *Safire* e uno, confidenziale e a cui lo scrivente sta collaborando, diretto all'identificazione di potenziali terroristi tra coloro che hanno accesso a infrastrutture critiche.