

# Come fare la guerra cyber a terroristi e hacker

5 **Francesco Bechis** JAMES BOND



Alla base della crociata santa dei terroristi di matrice islamica che fanno tremare l'Europa c'è un clamoroso paradosso: si combattono la globalizzazione e l'Occidente come fossero il demonio, ma la jihad non è mai stata più 'globale' di oggi: i cellulari, il web e i social networks sono le armi che impugnano i nuovi 'soldati di Allah'. Per questo il compito delle forze di intelligence si è fatto più difficile: non basta più intervenire, bisogna prevenire prima che sia troppo tardi. Al Salone della Giustizia dell'Eur mercoledì pomeriggio si è parlato della prevenzione e delle sfide che comporta con esperti militari, giuristi e gli addetti alla sicurezza della **Leonardo S.p.A.**

## **PRIVACY O SICUREZZA?**

L'innovazione tecnologica pone nuove sfide alla prevenzione al terrorismo. Una è di carattere etico oltre che legale: quando l'intelligence deve proteggere il cittadino, può violare la sua privacy o privarlo delle libertà civili? Fino a che punto ci si può spingere? Per **John Mulligan**, vicedirettore del Centro nazionale americano antiterrorismo (NCC), questo *trade-off* non esiste: "Molto spesso le persone parlano della sicurezza e della libertà come di un equilibrio, come se avere qualcosa in più di una volesse dire avere meno dell'altra. Noi del NCC la pensiamo in modo diverso: dobbiamo rafforzare la nostra sicurezza senza venire meno alle questioni della privacy". Ma la realtà mostra che senza intercettazioni ambientali, una chiara invasione della privacy, molti dei piani terroristici non si fermerebbero in tempo. Non che sia facile farlo. "Con le ambientali spesso capita di captare il desiderio di alcuni individui di colpire e punire l'Italia, di colpire i *kafir*, gli infedeli, di fare un gesto eclatante con coltelli o con qualche tipo di ordigno",

spiega **Lamberto Giannini** (in foto), a capo del servizio antiterrorismo del Viminale. Eppure molte delle intercettazioni rimangono solo indizi e non permettono di arrestare queste persone perché mancano le prove necessarie. Il caso recente dell'assassino di Londra, Khalid Masood, è eclatante. Da quando quel tragico 22 marzo ha iniziato a mettere sotto i passanti seminando terrore sul Westminster Bridge con un'auto (affittata legalmente) a quando è stato ucciso sono passati 82 secondi, spiega Giannini: "prima di quegli 82 secondi però non stava commettendo nessun comportamento illegale".

## **IL FATTORE UMANO**

Aumentano le tecnologie, l'intelligence ora ha mezzi che dieci anni fa erano impensabili. L'uomo gioca ancora un ruolo nella prevenzione? **Giuseppe Governale**, il generale al comando del Ros, il nucleo operativo nato negli anni '70 per combattere le Brigate Rosse e ancora oggi in prima linea nell'antiterrorismo, crede che da sola la tecnologia non basti. Certo, senza la partnership con Leonardo S.p.A, la multinazionale italiana della difesa e della sicurezza con cui i Carabinieri hanno messo su una piattaforma di controllo integrato del territorio "che ci invidiano tutte le agenzie europee", il lavoro del nucleo operativo sarebbe più duro. Ma sono gli uomini sul campo a fare la differenza: quando si combatte il terrorismo d'altronde si combattono persone in carne ed ossa. Per questo le indagini sotto copertura del ROS, come quelle durate 6 mesi che hanno portato all'arresto di 17 terroristi proprio la notte del novembre 2015 quando il Bataclan si macchiava di sangue, giocano un ruolo chiave nella prevenzione al terrorismo.

Qual è allora l'apporto delle nuove macchine? Secondo **Andrea Biraghi**, direttore del "Security & Information System" di Leonardo S.p.A, il loro ruolo è quello di supportare le persone che lavorano nell'intelligence, non sostituirle. Biraghi e il suo team non si occupano di terrorismo, ma di difendere il sistema di Leonardo da attacchi cybernetici.

Entrando nel cosiddetto "dark web" però, quello che non è indicizzato nei motori di ricerca, i tecnici si sono accorti che esiste un mondo parallelo di terroristi che si scambiano informazioni sul web. Per fare ordine tra miliardi di messaggi e informazioni inutili, il ruolo delle macchine, spiega Biraghi, è indispensabile: "La macchina aiuta a correlare le informazioni: ad esempio aiuta a scoprire se ci sono due soggetti sospetti provenienti da zone cosiddette 'a rischio' che si incontrano nello stesso aeroporto". Per Biraghi, il motto alla base di un buon lavoro di intelligence, che sia contro i terroristi o contro gli hackers del "dark web", rimane: "learn globally, source carefully, cooperate locally". Che sarebbe a dire: impara dal resto del mondo, scopri le nuove tecnologie e il loro funzionamento a fondo, ma fidati sempre e solo dei sistemi di prevenzione italiani, perché sono "affidabili e non dipendenti da un altro governo".