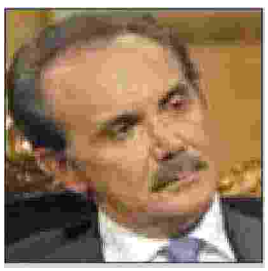
ItaliaOggi
Quotidiano
RUBBETTINO
Data 08-06-2019
Pagina 20
Foglio 1

IL PUNTO DI MAURO MASI*

Una risposta «convenzionale» alla cyberwar

Secondo fonti mediatiche israeliane (la testata *Times of Israel*; dei tweet dell'IDF Israel Defence Forces) nei primi giorni dello scorso mese di maggio il mondo ha assistito al primo caso (noto) di reazione con metodi «classici» a un attacco di cyberwar. Nello specifico, Israele avrebbe reagito ad una pesante offensiva cyber attuata da Hamas con un contrattacco missilistico volto a distruggere (sembra con successo) il quartier generale informatico di Hamas. Un tipico esempio di guerra asimmetrica perché combina in uno stesso contesto «soft e hard power». Ora, in realtà, tutte le guerre sono asimmetriche: negli obiettivi, nelle strategie e nei mezzi (così scriveva Carlo Jean in un suo saggio del 2018). E lo sono da sempre, le uniche novità oggi sono la rilevanza assunta dal cyberspazio e l'utilizzo di Internet e dei social media nella disinformazione, nella sovversione e nell'attacco per indebolire la coesione degli stati e quella delle alleanze con un'efficacia e una capacità prima sconosciute: è ciò che si definisce infowar, una variante della cyberwar.


Mauro Masi

Nel loro bel libro sull'Intelligence Economica (Rubbettino, 2011) ancora Carlo Jean assieme a Paolo Savona danno della cyberwar una brillante descrizione: «La cyberwar è estremamente dinamica, rapida e imprevedibile. Annulla il valore della distanza, del tempo, delle frontiere. Rende possibili sorprese strategiche molto più di quanto esse siano possibili con gli strumenti hard. Può consentire a piccoli gruppi o ad individui singoli collegati in rete di esprimere una grande potenza e di provocare danni disastrosi».

Le nazioni oggi egemoni hanno da tempo capito l'aria che tira e si stanno comportando di conseguenza: negli Stati Uniti già l'amministrazione Obama aveva creato l'Office of cyber security dal quale si è sviluppato l'Office for strategic influence, un ufficio che lavora costantemente sulla rete e sui social utilizzando come consulenti anche alcuni dei più sofisticati hacker americani. Israele, Cina e soprattutto Russia non sono da meno; sono ormai all'ordine del giorno in Occidente le polemiche sulle ondate di «fake news» che sarebbero generate da migliaia di account russi direttamente o indirettamente connessi con istituzioni pubbliche, mentre qualche tempo fa un indagine del *New York Times* rivelò, tra l'altro, l'esistenza di un centro da cui partivano mega attacchi informatici, un palazzone di 12 piani alla periferia di Shanghai quartier generale dell'Unità 61398 dell'Esercito di liberazione popolare dove lavoravano «centinaia o anche migliaia di tecnici con connessioni in fibra ottica ad altissima velocità di tipo militare fornite da China Mobile».

Quindi la infowar o la ciberwar è già ampiamente in corso e ci si sta accorgendo quanto sia difficile la difesa dalle aggressioni cibernetiche che peraltro si dimostrano tanto più devastanti quanto più si rivolgono a nazioni evolute da un punto di vista tecnologico. Hanno invece effetti minori (nel senso che possono produrre forti danni ma non riescono a risolvere i conflitti) quando si rivolgono a paesi più arretrati come dimostra, tra l'altro, l'incapacità degli Stati Uniti di piegare la Corea del Nord anche utilizzando attacchi cibernetici massicci. Forse anche da qui promana la decisione di Israele di rispondere con un attacco «convenzionale» alla ciberwar di Hamas.

*** delegato italiano alla Proprietà intellettuale**
CONTATTI: mauro.masi@consap.it