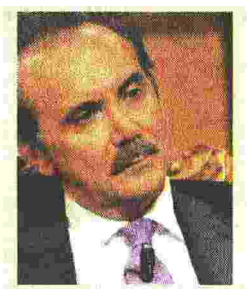
MILANO FINANZA
Settimanale
RUBBETTINO
Data 25-01-2020
Pagina 25
Foglio 1

IL PUNTO di MAURO MASI*

Dagli Usa alla Russia, da Israele alla Cina: la cyber-war è già in corso

Secondo alcuni media israeliani lo scorso maggio il mondo ha assistito al primo caso di reazione con metodi «classici» a un attacco di cyber-war. Israele avrebbe reagito a un'offensiva cyber di Hamas con un contrattacco missilistico volto a distruggere il quartier generale informatico del movimento palestinese. Si tratta di un tipico esempio di guerra asimmetrica perché combina «soft e hard power»; tema quest'ultimo di scottante attualità nel contesto venutosi a creare dopo l'eliminazione del generale iraniano Suleimani. Tutte le guerre in realtà sono asimmetriche negli obiettivi, nelle strategie e nei mezzi (così Carlo Jean in un suo saggio del 2018). Lo sono da sempre; le uniche novità oggi sono la rilevanza assunta dal cyber-spazio e l'utilizzo di Internet e social media nella disinformazione, nella sovversione e attacco per indebolire la coesione degli Stati e quella delle alleanze con efficacia e capacità prima sconosciute. Tutto ciò viene definito info-war, variante della cyber-war. Nel bel libro *Intelligence Economica* (Rubbettino, 2011) ancora Jean assieme a Paolo Savona danno della cyber-war una brillante descrizione: «La cyber-war 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 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 Usa già l'Amministrazione Obama aveva creato l'Office of Cyber Security, dal quale si è sviluppato l'Office for Strategic Influence, ufficio che lavora costantemente su Rete e social utilizzando come consulenti anche alcuni dei più sofisticati hacker americani. Negli Usa di cyber-war si occupa anche l'ufficio per la Cybersecurity and Infrastrutture Security Agency oggi diretto da Chris Krebs, uno dei maggiori esperti mondiali del settore. 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 il *New York Times* rivelò 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 al altissima velocità di tipo militare fornite da China Mobile». Quindi la info-war o la ciber-war sono 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 tecnologicamente evolute. Hanno effetti minori quando si rivolgono a Paesi più arretrati, come ha dimostrato l'incapacità degli Usa di piegare la Corea del Nord utilizzando attacchi cibernetici. (riproduzione riservata)

**delegato italiano alla Proprietà Intellettuale*




Intrappolata nella rete

Dagli Usa alla Russia, da Israele alla Cina: la cyber-war è già in corso