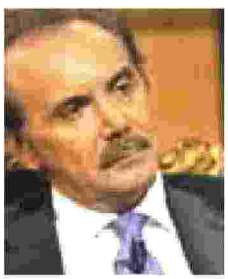
MILANO FINANZA
Settimanale
RUBBETTINO
Data 18-08-2018
Pagina 23
Foglio 1

IL PUNTO di MAURO MASI*

La guerra nel cyberspazio sta proseguendo con altri mezzi

Tutte le guerre sono asimmetriche: negli obiettivi, nelle strategie e nei mezzi (così scriveva Carlo Jean in un suo recente saggio). 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 ed una capacità prima sconosciute: è ciò che si definisce infowar, una variante della cyberwar. 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 a 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 hackers americani. 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 Shangai 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 infowar o la ciberwar sono, di fatto, già in corso e ci si sta accorgendo quanto sia difficile la difesa dalle aggressioni cibernetiche che sono tanto più devastanti quanto più si rivolgono a Nazioni evolute da un punto di vista tecnologico. Possono invece produrre forti danni ma non risolvere conflitti quando si rivolgono a Paesi più arretrati come dimostra l'incapacità degli Stati Uniti di piegare la Corea del Nord anche utilizzando attacchi cibernetici massicci. Il tema riguarda soprattutto la sicurezza tra gli Stati ma è crescente anche la infowar tra privati, capitolo sempre più importante della guerra economica tra le grandi corporation mondiali che, peraltro, da tempo investono miliardi di dollari l'anno per difendersi da attacchi cibernetici. C'è da chiedersi quanto i riflessi di questa guerra, per ora silente ma non per questo meno cruenta, influenzino l'atteggiamento di alcune grandi lobby economiche mondiali (quelle dell'high tech, delle telecom) nei confronti di internet e di una sua eventuale (ma sempre più necessaria) regolamentazione a livello mondiale.

**delegato italiano alla Proprietà Intellettuale*




Dazn si fa largo in Italia