Milano Finanza

diffusione:35538
tiratura:54755

IL PUNTO DI MAURO MASI*

La guerra cibernetica era già cominciata da tempo

Tra gli aspetti della drammatica guerra che il mondo sta vivendo in questi giorni c'è anche il capitolo, forse meno appariscente ma non per questo meno importante, della guerra cibernetica. Soprattutto i russi – finora considerati maestri in questo settore – si stanno accorgendo di come gli attacchi di questo tipo possano essere duri e severi: in questi giorni il traffico ferroviario negli snodi di Minsk e Orsha è completamente impazzito a causa degli hacker ucraini e bielorussi. Anonymus ha attaccato e messo fuori combattimento per lunghe ore le agenzie di stampa russe (ad iniziare dalla Tass) e i siti dei principali quotidiani (ad iniziare da Izvestia). La cyberguerra, peraltro, esiste da tempo con episodi in quasi tutti gli scenari bellici mondiali anche se non sempre sono riconosciuti come tali. Ad esempio, secondo alcuni media israeliani nel maggio 2019 il mondo ha assistito al primo caso di reazione con metodi «classici» ad 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 con la guerra russo-ucraina. 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 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. Tutto ciò viene definito info-war, una variante della cyber-war. Nel bel libro Intelligence Economica (Rubbettino, 2011) ancora Jean assieme a Paolo Savona danno della cyber-war una brillante descrizione: «E' 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». Negli Usa, di cyber-war si occupa l'ufficio per la Cybersecurity and unfrastructure security agency; Cina e 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 il New York Times rivelò 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. Quindi la info-war o la cyber-war erano già ampiamente in corso ben prima del conflitto russo-ucraino; ora tutto il mondo si sta accorgendo quanto sia difficile la difesa contro questa minaccia. (riproduzione riservata)