risposta. La dà solo a livello cyber?», si chiede Silvestri. Teniamo conto di alcuni aspetti. Primo: il crimine informatico esiste già. Secondo: delle incursioni informatiche è difficile individuare gli autori. Ancora Silvestri: «Nella dottrina della Nato è bandito l' uso di armi chimiche e batteriologiche. Se attaccati con quelle armi, gli Stati Uniti però hanno concepito l' ipotesi di rispondere con armi nucleari. Vale anche per il cyber? In più, importante nelle guerre aeree è la ricognizione che serve a conoscere i danni inflitti. Sulla guerra informatica come si valutano? Ci si fida di ciò che dice il nemico?». A preoccupare Lindley-French è soprattutto la Russia di Vladimir Putin. Tutto questo rende attuali revisioni di dottrine strategiche e contromisure delle quali nel nostro Paese si parla poco. Dal 2018 a Helsinki funzionerà a pieno ritmo il «Centro europeo di eccellenza per contrastare le minacce ibride» voluto dalla Finlandia. Alla sua fondazione hanno aderito dodici Stati, compresi Francia, Germania. L' Italia non ancora. «Minacce ibride» sono le offensive condotte con mezzi diversi, non solo militari. Il ministro finlandese degli Esteri Timo Soini le ha descritte così: «In Europa sono state usate come mezzo sia in conflitti di potere politico sia militari. Sono aumentate attività coercitive e sovversive volte a confondere, complicare e ostacolare i processi decisionali. Durante le crisi migratorie, abbiamo visto elementi di influenza ibrida da attori sia statali sia non. Pilotare i flussi migratori può essere un metodo di pressione politica, e gli organizzatori di attacchi ibridi cercano di radicalizzare i membri deboli della società come loro agenti». Materia sulla quale ragionare. Per innovare dottrine datate.

di Maurizio Caprara