*di Cristiana Era*Nell'era post-moderna il concetto di conflittualità si è esteso anche alla quinta dimensione, il cyberspazio. Dopo qualche anno di colpevole ritardo, il tema ha finalmente attirato l’attenzione anche dei media - complici soprattutto gli attacchi hacker ai siti di alcune delle testate internazionali più importanti (quali il New York Times e il Washington Post) – e delle istituzioni nazionali che, pur partecipando al dibattito nazionale, solo recentemente hanno ovviato all'inerzia burocratica con l’approvazione del decreto della Presidenza del Consiglio del 24 gennaio 2013, con il quale l’ex Premier Mario Monti lanciava l’allarme sulla minaccia cibernetica nel nostro Paese. Il nuovo DPCM rappresenta indubbiamente un primo passo in avanti verso la definizione di una strategia di difesa che a tutt'ora manca in Italia. Ma, come è stato rilevato da autorevoli esperti del settore, la strada da percorrere è ancora molto lunga.
Per molto tempo la discussione accademica si è focalizzata sulla determinazione di concetti quali spazio cibernetico, attacco cibernetico, guerra cibernetica e relative implicazioni. Ma dopo un anno disastroso come quello del 2012, in cui il cyber crime è aumentato a livello esponenziale - in Italia, come nel resto d’Europa e del mondo - il grido di allarme lanciato dagli specialisti ha trovato orecchie più attente in diversi ambienti istituzionali, compreso quello militare. Da un quadro generale di descrizione di minaccia cibernetica si è passati, così, all’analisi delle possibili contromisure. In altre parole, il dibattito si sta spostando dallo studio del fenomeno in generale all’esame di una strategia di difesa di cui c’è urgente bisogno. Nel DPCM, infatti, sono riportati sei concetti principali di riferimento: lo spazio cibernetico, la sicurezza cibernetica, la minaccia cibernetica, l’evento cibernetico, l’allarme e la situazione di crisi. Sono, questi, elementi portanti nella definizione della “cyber dimension”, senza però rappresentare una lista esaustiva di tutti i fattori. Del concetto di “cyber protection”, infatti, manca una chiara precisa definizione.
E in realtà, è proprio sul concetto di protezione – di protezione delle infrastrutture critiche, per essere più precisi – su cui deve fare perno una qualsiasi strategia di cyber security. Da questo punto di vista l’Italia, rispetto ad altri Paesi più tecnologicamente avanzati, è molto indietro. Le infrastrutture critiche sono quelle che, se colpite, possono paralizzare le attività e le istituzioni di un’intera nazione. Considerando che molti dei sistemi che regolano il funzionamento quotidiano del Paese sono in parte o del tutto informatizzate (si pensi, ad esempio, alle reti ferroviarie e di trasporto in generale, alle centrali energetiche, alle reti informatizzate della pubblica amministrazione, ma anche all’intero sistema industriale e finanziario), il nostro Paese risulta particolarmente vulnerabile, anche a causa di una marcata disattenzione e disinteresse, fino ad ora, da parte di tutti: istituzioni, aziende e privati cittadini. Sono queste le conclusioni, ben poco incoraggianti, evidenziate recentemente dal Clusit (Associazione Italiana per la Sicurezza Informatica). E a rimarcare l’emergenza “rischio attacco” è anche un rapporto della Maglan Group, che rivela come ben il 90% delle società italiane quotate in borsa sia a rischio cyber spionaggio.
Il quadro così delineato è preoccupante nella misura in cui il rischio “virtuale” è reale, concreto ed immediato. Se ne è avuta dimostrazione pratica a marzo di quest’anno, quando i principali siti di informazione della Repubblica Ceca sono stati paralizzati da un attacco di hacker non meglio identificati, e quando si è avuta un primo esempio di conflitto cibernetico fra gruppi di hacker malesi e hacker filippini, conflitto parallelo e concomitante a quello terrestre in atto nel Borneo nordorientale. Da questi eventi si possono trarre alcune conclusioni sia di natura interna, sia relative ad un quadro generale di politica internazionale. Innanzitutto la cyber criminalità (che può avere fini di natura eversiva/terroristica, economica o politica) è già in grado

di colpire con effetti dirompenti sul sistema Paese: per ora si tratta di “prove tecniche di trasmissione”, un po’ come i test nucleari. Ma le suddette prove sono andate a buon fine: cyber spionaggio cinese all’interno di siti americani; blocco della rete informatica dei mezzi di comunicazione in Europa; per non menzionare il caso dell’attacco all’Estonia del 2007, ormai diventato un riferimento da accademico citato in tutti i convegni sul tema e che ha costretto un’organizzazione regionale di difesa all’avanguardia quale la NATO a correre ai ripari e ad accreditare un centro di eccellenza che si occupa di cyber security proprio a Tallin.
Quello che si auspica da tempo è un migliore coordinamento tra Paesi alleati, una maggiore collaborazione tra settore pubblico e settore privato e una diffusa information-sharing, quest’ultima invocata a gran voce ma poi largamente disattesa proprio da quelle istituzioni che per prime se ne dovrebbero fare carico, a riprova di un malcelato timore di condividere informazioni “sensibili” che in qualche modo possano avvantaggiare una ipotetica concorrenza (sia economica che politica). Pertanto è facile individuare le difficoltà primarie di far fronte a questa nuova tipologia di minaccia e/o di conflitto. La quinta dimensione è per sua natura fluida, dinamica , con barriere di accesso pressoché nulle che annientano i rapporti di forza fisici: pochi individui ben organizzati e tecnicamente preparati possono arrivare a danneggiare un intero sistema nazionale non sufficientemente protetto. I costi relativi ad un attacco cibernetico sono minimi, non vi è bisogno di una struttura gerarchizzata, è veloce e con poche possibilità di rappresaglia, con l’enorme vantaggio di garantire quasi totalmente l’anonimato del suo autore. Come è stato più volte rilevato non esiste una protezione che garantisca l’inviolabilità totale, ma vi può essere però una strategia difensiva che miri a prevenire ed eventualmente a ridurre il numero dei danni e la loro entità. Non si tratta semplicemente di una questione tecnica: a monte ci deve essere una precisa politica programmatica e di indirizzo. E in Italia siamo, purtroppo, ancora molto indietro. Il nuovo DPCM ha il merito di aver preso coscienza ufficialmente di una minaccia effettiva e delle vulnerabilità nazionali. Ma non è riuscito a rendere meno farraginoso e meno burocratico un eventuale sistema di prevenzione, azione e reazione, preoccupandosi di far salve, invece, le competenze di vari uffici ministeriali o pubblici in generale. I continui tentativi di difesa di prerogative istituzionali mal si conciliano con le esigenze di snellezza e di risposta pronta ed immediata ad una eventuale emergenza cibernetica. Per non parlare del primo elemento di una qualunque strategia difensiva: la prevenzione. Nella quinta dimensione prevenire diventa infatti elemento di primaria importanza: una capace opera di intelligence può ridurre l’effetto di un attacco se non addirittura il blocco dello stesso. Perché quello che manca è il tempo di comprensione di ciò che è avvenuto e di reazione. Sapere in anticipo in cosa consiste l’attacco dà dunque il vantaggio del tempo. In un sistema nazionale i tempi di approvazione di qualunque decisione di rilievo sono generalmente molto lunghi. Per poter mantenere un equilibrio di forze nella quinta dimensione è indispensabile avere degli organismi snelli con un certo grado di autonomia, del personale professionalmente all’avanguardia, procedure veloci e poca burocrazia, oltre alle risorse necessarie a riqualificazioni sia strutturali che umane. Non solo una questione tecnica, dunque, ma una nuova politica. Perché gli hacker solitari, i terroristi e la criminalità cibernetica hanno già capito come si fa.