a cura del
CeMiSS Centro Militare Studi Strategici

CYBER WARFARE, QUALI REGOLE...?

FRANCESCO LOMBARDI

Se la cyber warfare è "guerra" differenziandosi dalle altre forme di conflitto per strumenti utilizzati e non per principi applicabili, anche la cyber guerra, allora, dovrebbe essere pianificata e condotta nell'alveo di regole generali note ed accettate. Ma essa pare sfuggire a tali principi. Pare estranea al comune sentire in tema di diritto internazionale. Come se il fatto che non siano immediatamente visibili dolore, distruzione e sofferenze che seguono ogni azione bellica faccia sentire meno la necessità di una specifica ed applicabile regolamentazione. Come se la virtualità degli strumenti e delle azioni si trasmetta anche alle norme internazionali di riferimento. Come se le traiettorie lungo cui viaggiano neutroni e bite possano essere svincolate dai principi che, invece, da anni, imbrigliano l'uso e l'abuso delle traiettorie di bombe e proiettili. Regole accettate da Governi, Istituzioni, cittadini e combattenti. A cominciare dall'avvio degli attacchi stessi; possono verificarsi aggressioni informatiche mentre i rappresentanti delle istituzioni coinvolte continuano a sviluppare normali ed apparentemente cordiali relazioni diplomatiche.

La cyber warfare è più presente e più immanente di quanto comunemente si creda. E non solo per gli episodi che, raggiungendo l'onore delle cronache, sono oramai entrati nella letteratura di riferimento: dall'Estonia 2007 in cui gli attacchi assunsero carattere di rappresaglia e di pressione politica o quelli della Georgia 2008 in cui la disarticolazione del dispositivo infrastrutturale precedette le operazioni di terra. Pare oramai acclarato che tra Israele e l'Iran siano in corso conflitti a suon di virus e neutroni con l'intento del Paese ebraico di violare o quantomeno rallentare il programma nucleare di Ahmadinejad. La rilevanza degli effetti realizzabili, anche in rapporto ai costi sostenuti, la difficile dimostrabilità in sedi internazionali o alla pubblica opinione degli attacchi stessi e della loro volontarietà, senza dimenticare la pluralità di bersagli e la possibilità di reiterare gli interventi, rappresentano incentivi ad utilizzare le proprie capacità con meno esitazioni politico-strategiche rispetto a quelle che caratterizzano l'uso degli armamenti tradizionali (ed ancor più nucleari). Lo strumento informatico, poi, a differenza degli armamenti tradizionali, consente di realizzare attacchi senza contiguità territoriale, senza basi di partenza; rende possibili azioni contemporanee da diversi punti del globo; facilita le sinergie tra attori a differente connotazione agevolando la moltiplicazione degli sforzi e sottraendo gli attaccanti da azioni di rappresaglia immediate ed efficaci. Nel nostro paese (e non solo) la tematica non ha ancora trovato una sua compiuta strutturazione. Un buon segnale viene comunque dal fatto che anche la politica ha preso coscienza della pericolosità del fenomeno. Della cosa si è occupato, infatti, il Copasir (Comitato Parlamentare per la Sicurezza della Repubblica) che in una recente relazione riconosce la virtualizzazione delle relazioni internazionali e l'importanza dell'ambiente cibernetico quale nuovo terreno di scontro strategico ed operativo. Anche l'Autorità nazionale concorda sul fatto che le guerre future tra stati o tra attori diversi prenderanno il via con attacchi mirati condotti con strumenti informatici in grado di generare forti criticità all'avversario. Certo che la presa d'atto non è sufficiente; occorrono poi azioni concrete. Ma la consapevolezza è una buona base di partenza. In Italia, come in altre nazioni, mancano regole strumentali ad affrontare tali crisi. Le norme esistenti sono principalmente il frutto della necessità di prevenire e reprimere crimini informatici a sfondo economico, in cui l'aspetto truffaldino è prevalente rispetto a quello politico. Negli USA, in realtà, sono stati approvati provvedimenti che hanno creato un substrato normativo per fronteggiare attacchi del tipo in esame. La possibilità per il Presidente di imporre lo spegnimento dei siti ritenuti strategici, già individuati e censiti dal Parlamento, è l'indicazione evidente dell'estrema pragmaticità che deve improntare le scelte al riguardo ma anche del carattere sinergico col quale va affrontata la materia. Anche l'Europa e l'Italia hanno avviato un dibattito col proposito di perfezionare strumenti normativi e strategie utili, anche se, soprattutto nel nostro paese, la polverizzazione dei centri decisionali e la pluralità dei soggetti coinvolti non agevola l'individuazione di soluzioni valide e condivise. Il gap tecnologico che ancora separa l'Italia da altri paesi avanzati, soprattutto nel settore pubblico, non ci tiene al riparo da attenzioni aggressive. E' vero, come dimostra la pluriennale attività dell'Osservatorio per la Sicurezza Nazionale presso il CeMiSS, che anche il mondo privato, oltre ad autonome strategie di recovery, protezione e backup, è sostanzialmente ben orientato a collaborare per prevenire eventi di tal genere e mitigarne gli effetti. Ma un compiuto sedime normativo per rendere efficaci i confronti in sede internazionale resta necessario ed oramai urgente. La stessa relazione del Copasir dianzi citata, del resto, precisa che "non esistono definizioni condivise di questo nuovo spazio di competizione e potenziale contrapposizione". E non si pensi sia semplice delineare definizioni tanto generiche da essere universalmente applicabili ma tanto concrete per essere effettivamente utilizzabili. Così come è difficilissimo discriminare le responsabilità politiche ed istituzionali in caso di attacchi informatici. Con limpida semplicità, il sottosegretario per la sicurezza e l'antiterrorismo britannico ha dichiarato: "Se bombardo una centrale elettrica di un altro paese si tratta di un atto di guerra. Ma è la stessa cosa se uso un computer per disattivarla?". Ancor più vicino alle nostre realtà, poi, va richiamato l'articolo 5 del Trattato NATO che prevede l'autodifesa collettiva in caso di " attacco armato … contro il territorio,… le forze,… le navi, … o gli aeromobili … di uno degli stati membri". Forse è anche tempo di novellare o quanto meno arricchire il trattato del 1949. La storia mostra come i trattati e le conferenze sul diritto di guerra hanno seguito lo sviluppo delle tecnologie e delle dottrine, quasi mai prevenuto. Sarà così anche stavolta? Chissà se riusciremo a saperlo on line.