Cyber attacchi. Della Morte (Università Cattolica): "Ancora complesso applicare il diritto internazionale"

Se uno Stato subisce un attacco armato da un altro Stato, la reazione per legittima difesa è prevista e codificata dal diritto internazionale. Ma nel caso in cui l'attacco colpisca i server delle forze armate o della sanità, si può rispondere ricorrendo all'uso della forza "tradizionale" (ovvero cinetica e non cibernetica)? L'interrogativo è fortemente attuale oggi che assistiamo agli attacchi di cyber terrorismo in vari scenari di crisi. Prima per il conflitto in Ucraina, poi per quello in Medio Oriente, la guerra ha assunto nuove connotazioni che provocano comunque dei danni, mantenendo nascosti i responsabili e i loro mandanti. Al Sir, il professor **Gabriele Della Morte**, ordinario di diritto internazionale e membro dell'Humane Technology Lab dell'Università Cattolica di Milano, spiega come sia una materia in cui le variabili da valutare sono tante e complesse. **Professore, i cyber attacchi prima per il conflitto in Ucraina e poi in Israele come vengono definiti dal diritto internazionale?** Il cyber attacco è un'operazione digitale che produce effetti assimilabili a quelli cinetici, ovvero la distruzione di obiettivi o comunque la *diminutio* della forza nemica nel contesto di un conflitto fra due parti. La più precisa definizione di cyber attacco non è ancora codificata da convenzioni internazionali ma da uno studio, il cosiddetto manuale Tallin, redatto da un gruppo di ricerca finanziato dalla Nato che si è interrogato su quali fossero le frontiere riguardo ai mezzi (armi) e ai metodi di guerra (tecniche e strategie) cibernetiche. Ai sensi del manuale, un cyberattacco consiste in un'operazione cyber, di carattere offensivo o difensivo, che può ragionevolmente causare la morte o danni a persone o cose. In altri termini, esistono situazioni in cui delle tecnologie che possono avere un uso civile in un contesto di pace potrebbero avere invece un uso militare in un contesto di guerra. Per fare qualche esempio, disattivare le comunicazioni radio o internet della parte nemica, sabotare una diga o una centrale nucleare, ha un'incidenza su una strategia di conflitto. Ed è in questi casi che si pone il dilemma se le tradizionali categorie del diritto internazionale possano essere adattabili anche in un contesto non cinetico. **Non c'è ancora chiarezza al riguardo?** Davanti a noi abbiamo due aspetti del problema. Il primo è quello dello *jus in bello,* che pone il quesito se le Convenzioni dell'Aia e di Ginevra – il cosiddetto diritto umanitario – trovino applicazione in un contesto non cinetico. Il secondo, quello dello *jus ad bellum,* concerne la possibilità di adoperare la forza in risposta ad un attacco armato per legittima difesa. Se si subisce un attacco armato tradizionale (così come previsto dall'articolo 51 della Carta delle Nazioni Unite), si reagisce per legittima difesa. Ma nel caso in cui l'attacco sia cibernetico si può rispondere con la forza? **Ed è possibile rispondere a queste domande?** È ancora molto complesso. Nel primo caso, il diritto internazionale umanitario trova applicazione per limitare gli effetti della guerra. Le norme infatti sono costruite intorno a due poli. Il primo è il principio di distinzione, che impone di discernere tra obiettivi legittimi perché militari, da un lato, e illegittimi perché civili, dall'altro. Il problema di applicare queste norme, nel caso in cui venga praticato un attacco cyber, è che la tecnologia può avere effetti sui militari ma anche sui civili. L'altro polo è il principio proporzionalità. Nel caso di forza cinetica è facile valutare la proporzionalità, ma nel caso di un cyber attacco, come per esempio un malware che impiega anni a causare tutti gli effetti dannosi, come è possibile applicare il principio di proporzionalità? Rispettare i principi di distinzione e proporzionalità può rivelarsi in tali contesti un'operazione molto complicata. **E quanto alla legittima difesa, è possibile ricorrervi in caso di cyber attacco?** Ci sono diverse questioni che si accavallano. In primo luogo, qual è la soglia di gravità che occorre superare per qualificare il cyber attacco quale attacco armato e quindi consentire di agire in legittima difesa? Altro problema è: a quali parametri si può fare ricorso nell'attribuzione di un cyber attacco a un determinato Stato? Per fare un esempio, potrebbe essere arduo dimostrare che un gruppo di cyber-warriors, come Anonymous, agisca sotto il controllo di un determinato Stato e quindi rispondere per legittima difesa secondo le norme tradizionali del diritto internazionale. Anche perché i cyber attacchi possono essere ubiqui, provenire cioè da diversi posti diversi. **L'Italia come**

ha regolato finora queste eventualità? Il tema è molto attuale. Nel 2021, il ministero della Esteri, in collaborazione con la Presidenza del consiglio dei ministri e il ministero della Difesa, ha prodotto un *position paper* che dà delle indicazioni ma lascia ancora degli spazi aperti. Inoltre, la direttiva Nis II dell'Unione europea, che è stata appena approvata e deve ricevere applicazione in Italia entro l'ottobre 2024, impone la messa in sicurezza di tutta una serie di strutture strategiche contro possibili cyber-intrusioni. Ci si rende conto che ormai alcune questioni di sicurezza hanno a che fare anche con la sicurezza numerica e non solo tradizionale.

Elisabetta Gramolini