Uso della Forza e Cyber attacks: come far fronte ad una crescente minaccia?

Attribution 2.0 Generic (CC BY 2.0)

L'utilizzo delle tecnologie informatiche e delle telecomunicazioni nello spazio cibernetico per fini paragonabili a quelli bellici è ormai una realtà. Gli attacchi, lungi dall'essere semplici attività di "disturbo", mirano il più delle volte a colpire gli apparati di sicurezza e i settori più sensibili di un Paese. Ciò ha portato gli Stati ad attrezzarsi tecnicamente e giuridicamente per affrontare al meglio tali minacce, prendendo anche in considerazione l'uso della forza armata: il caso dell'UE e della NATO ne sono un esempio.

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems

necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security".

É con queste parole che l'art. 5(1) del Trattato NATO (North Atlantic Treaty Organization 1949) definisce la c.d. "mutual defence clause" ovvero il principio secondo il quale ogni attacco armato contro uno Stato Membro deve essere considerato come un attacco diretto contro l'insieme delle Parti tale da condurre, se le condizioni lo prevedono, anche all'utilizzo della forza armata, individuale o collettiva. L'articolo è tornato alle cronache quest'estate quando, in seguito agli eventi che hanno riguardato la crisi russo-ucraina, il Segretario generale della NATO Jens Stoltenberg ha affermato che anche un "cyber attack" potrebbe innescare l'art. 5 del Trattato nella stessa maniera di un attacco militare convenzionale.

Tale presa di posizione ha portato anche l'Unione Europea a mobilitarsi. Il 19 giugno 2017 infatti, il Consiglio dell'Unione Europea ha adottato il "Cyber Diplomacy Toolbox" (The draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities) il quale, una volta approvato, potrà coordinare le attività di risposta degli Stati Membri dell'UE in caso di cyber attack. Tale Framework prevede inoltre la possibilità per gli Stati, tra le eventuali forme di risposta, che qualora sotto attacco, possano esercitare il loro "inherent right of individual or collective self-defence".

La posta in gioco è estremamente alta. L'eventualità che si possa reagire con la forza armata ad un attacco informatico sembra farsi sempre più concreta in quanto risposta alle

continue tensioni a livello internazionale che vedono un utilizzo sempre maggiore del cyberspazio come mezzo offensivo. Non solo più a fini di spionaggio, ma addirittura per bloccare o paralizzare sistemi strategici per un paese quali aeroporti, siti governativi e sistemi di sicurezza. Tuttavia, anche se il linguaggio giornalistico e politologico fa un ampio uso del termine "guerra" e "attacco" in maniera indistinta, la situazione risulta essere molto più complessa. Il Manuele di Tallin sul Diritto Internazionale applicabile alla Cyberwarfare, descrive il cyber-attack come "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects*". Nello specificio, ciò che più preoccupa attualmente gli Stati è la Cyberwar ovvero l'utilizzo di mezzi informatici che possa indurre al ricorso della forza armato in quanto si configurerebbe come "asymmetric, non-linear and next-generation warfare".

Non tutti i casi in cui sia coinvolto un sistema informatico si possono configurare come Cyberwar. Utilizzare la giusta terminologia è estremamente importante nell'ambito, infatti un suo uso scorretto può portare a gravi distorsioni concettuali e a confondere, per esempio, un atto di guerra con un'attività criminale. Esistono diverse categorie di minacce che possono colpire gli Stati e in dottrina si distinguono a seconda dell'impatto che hanno e degli obiettivi che perseguono: Hacktivism, Cybercriminality, Cyberspionage, Cyberterrorism, Cyberwar sono gli esempi principali. La cyber guerra, data la rilevanza che oggi hanno i sistemi informatici sul sistema-paese, alcuni autori ritengono che debba essere equiparata alle altre tre forme di guerra che tradizionalmente costituiscono la materia, ovvero la guerra terrestre, la guerra marittima e la guerra aerea.

Ammesso tuttavia che ci si trovi di fronte ad un attacco armato, come -ed entro quali limiti-, può reagire uno Stato? Prima dell'istituzione della Società delle Nazioni (1919) gli

Stati beneficiavano di un illimitato *ius ad bellum*, ovvero del diritto di ricorrere alla guerra come mezzo di soluzione delle controversie. Il c.d. *ius in bello* invece, era chiamato a disciplinare le regole del diritto bellico in senso stretto.

La Carta delle Nazioni Unite (1945) tuttavia ha definitivamente abolito la possibilità di muovere guerra. Focalizzandosi sul concetto di "forza" la Carta prevede all'art. 2, par. 4, un divieto generico di ricorso alla forza armata, e all'art. 51 un'eccezione, costituita dalla legittima difesa individuale e collettiva. Ed è proprio nei limiti che pone la Carta nel vietare la minaccia o l'uso della forza armata, che risulta fondamentale capire se l'utilizzo di mezzi informatici, come l'UE e la NATO sembrano considerare dei documenti precedentemente citati, possa configurarsi come una violazione dell'art. 2, par. 4, della Carta.

Ma è proprio la definizione di "attacco armato" a sollevare i maggiori dubbi, specialmente nell'ambito degli attacchi informatici a causa delle difficoltà che si riscontrano nel momento dell'attribuzione della condotta. Chi materialmente lo ha provocato? Uno Stato? Un'organizzazione criminale oppure individui privati? E inoltre, nella definizione del danno causato e dei suoi fini, l'obbiettivo era quello di danneggiare il Paese nel suo complesso o solo alcune parti di esso?

Per quanto sia difficile trovare una risposta univoca, data la molteplicità di tipologie e di forme con cui si caratterizza una attacco informatico, la definizione di "attacco" sembra basarsi sulla dottrina prevalente. Il criterio fondamentale è quello emerso nel famoso caso *Nicaragua v. United States* (1986), nel quale l'ICJ stabilì che per distinguere un attacco armato da un *"mere frontier incident"* bisognasse costatare la *"scale and effects"* del medesimo. Al netto della difficoltà pratica dell'applicazione di tale definizione in caso di attacco da parte di uno Stato, quest'ultima stabilisce tutt'ora un principio cardine, ovvero: "an isolated minor

incident which, by the manner in which it takes place, cannot be mistaken for a threat to the safety of the State would not qualify as armed attack under Art. 51 UN Charter" (Oxford Public International Law).

Tale definizione, per quanto ampia e generica, non è sufficiente a risolvere la questione se ci si trovi di fronte ad un'azione comparabile ad un attacco armato e dunque vietata dall'art. 2, par. 4 della Carta delle Nazioni Unite. Pur rappresentando un importante parametro di riferimento, non prende infatti in considerazione il tipo di arma che viene utilizzata. Successivamente agli attacchi del 9/11, ci si è interrogati molto se le definizioni di arma potesse valere anche per situazioni che fino ad allora non erano ancora state prese in considerazione: come considerare un "highjacked civil airliners"?

Gli attacchi terroristici di New York furono compiuti essenzialmente con questo mezzo che di fatto ebbe il medesimo risultato dell'utilizzo di armi convenzionali quali, bombe o missili. Non è né il normale uso né la destinazione che devono essere prese in considerazione, quanto piuttosto "the intent with which it is used and its effect". Da ciò si deduce che anche un attacco informatico, allorquando soddisfi alcuni condizioni quali una considerevole perdita di vite umane e/o un'estensiva distruzione materiale e fisica, debba essere considerato come un attacco armato. L' "effect based approach" (Roscini, 2010), sviluppatosi sotto l'impulso del terrorismo internazionale, è ad oggi il medesimo con cui si cerca di dare una sistematizzazione alla materia che come si è potuto vedere, soprattutto in ambito di attacchi informatici, risulta ancora molto frammentata e controversa.

Ad esempio, un attacco informatico che pregiudichi il sistema economico-finanziario di un paese, o che danneggi gravemente gli impianti di produzione energetica, dovrebbe essere considerato come una condotta lesiva del principio del non intervento. Al contrario, comporterebbe una violazione

dell'art. 2, par. 4, una manipolazione dei sistemi informatici nel caso in cui comporti il bombardamento di un altro Stato territoriale (Ronzitti, 2014). Ancora, la messa fuori uso dei computer che controllano dighe o invasi artificiali con il fine di provocare la morte di migliaia di persone (Dinstein, 2005), oppure l'accecamento dei sistemi di difesa dell'avversario, situazione che potrebbe rappresentare di per sé un attacco o far presumere che l'attacco sia imminente (Roscini, 2016). In conclusione, come abbiamo precedentemente visto, "l'attacco cibernetico dovrebbe provocare in effetto cinetico, quali la distruzione di beni o l'uccisione/ferimento di persone, per poter essere considerato come una violazione del divieto di ricorso alla forza armata". (Ronzitti, *ibidem*).

I passi intrapresi, da parte sia delle NATO che dell'UE, sono significativi riguardo l'attenzione che su tali questioni è riposta dalla comunità internazionale. La tematiche è estremamente sensibile e di stringente attualità soprattutto dopo le recenti rivelazioni sulle azioni intraprese dalla Russia e dalla Corea del Nord: la guerra cibernetica è così diventata un'ipotesi concreta alla quale far fronte e non solo più il titolo di un film di fantascienza.

Bibliografia

- DINSTEIN Y., *"The conduct of Hostilities under the law of international armed conflict"*, Cambridge: Cambridge University Press, 2004.
- GREPPI E., VENTURINI G., *"Codice di diritto internazionale umanitario"*, Torino, G. Giappichelli Editore, 2012.
- RONZITTI N., "*Diritto internazionale dei conflitti armati"*, Torino, G. Giappichelli Editore, 2014.
- ROSCINI M., "*Cyber operations and the use of force in international law*"; Oxford : Oxford University Press,
- WELLER M., "*The Oxford Handbook of the Use of Force in international law*", Oxford, Oxford University Press, 2015.

Sitografia

- http://www.telegraph.co.uk/news/2017/10/29/eu-governments-warn-cyber-attacks-can-act-war/
- http://www.ecfr.eu/article/essay_getting_the_basics_right
- http://www.latribune.fr/actualites/economie/international/20140904trib0fdbd09da/les-cyberattaques-bientot-considerees-comme-acte-de-guerre-par-l-otan.html
- https://ccdcoe.org/european-union-equipping-itself-against-cyber-attacks-help-cyber-diplomacy-toolbox.html
- https://www.scmagazineuk.com/new-eu-framework-allows-members-to-consider-cyber-attacks-acts-of-war/article/703965/
- https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE