Data di pubblicazione: 5 settembre 2017

Diritto e guerra cibernetica

di Saverio Setti

Abstract

La possibilità che l'uso della forza nelle relazioni internazionali coinvolga il cyberspazio è divenuta una realtà concreta. Ciò crea interessanti interrogativi in merito all'inquadramento del cyberwarfare all'interno del vigente sistema di relazioni interstatuali. Cosa accade nel momento i cui attori esteri minano la stabilità interna ovvero orientano il risultato elettorale di uno Stato attraverso l'uso del computer? È possibile una reazione armata nei confronti di una intrusione non autorizzata nei sistemi posti a difesa degli interessi politici, militari, economici, scientifici ed industriali di un Paese? Oggetto del saggio è una prima individuazione dei principi normativi che oggi possono applicarsi alla guerra cibernetica. Dopo una prima ricognizione sulla definizione di cyberwarfare, si analizzerà la definizione di uso della forza nelle relazioni internazionali, per cercare di comprendere se ed in quale modo sia lecito per uno Stato reagire ad un attacco cibernetico.

Profilo dell'autore

Saverio Setti è Capitano RN dell'Esercito impiegato in *electronic warfare*. Formatosi all'Accademia militare di Modena, ha conseguito la laurea magistrale in Scienze strategiche e quindi proseguito gli studi all'Università di Torino laureandosi in Relazioni internazionali. Nel 2014 ha partecipato alla missione in Afghanistan. Ha completato gli studi con il terzo titolo di laurea presso la facoltà di Giurisprudenza dell'Università di Verona. È consulente scientifico ed autore di vari saggi.

Keyword cyberwarfare, diritto e relazioni internazionali

Sommario

1. Attacco cibernetico: una definizione

È, ormai, riconosciuto da a parte degli stessi Stati belligeranti, che gli strumenti cibernetici[1] costituiscano una 'nuova linea di combattimento'[2]. Ciò premesso, è di fondamentale importanza ricercare un'esatta descrizione di questo fenomeno sia sul piano legale che tecnico informatico, al fine di valutarne i riflessi sul piano delle relazioni internazionali.

Un attacco cibernetico consiste in un'azione posta in essere per mezzo di una rete di computer[3] al fine di disarticolare, distruggere, degradare o impedire l'accesso a computer e reti, ovvero alle informazioni ivi contenute[4]. Emerge da questa definizione un punto di grande interesse: sia l'arma che l'obiettivo dell'attacco sono le reti di computer e le informazioni ivi residenti. Questa caratteristica è sufficiente a distinguere gli attacchi cibernetici dalle più tradizionali forme di guerra elettronica, anch'esse orientate contro i *network* avversari, ma condotte a mezzo dell'energia elettromagnetica. In estrema sintesi, infatti, un attacco di guerra elettronica si serve di impulsi per disturbare o distruggere una qualche rete di comunicazione *wireless*[5].

L'attacco cibernetico, invece, si serve di un algoritmo codificato a mezzo di un computer per diffondere degli effetti pregiudizievoli, estremamente variegati, a seconda della tipologia di attacco o del sistema bersaglio[6] di questo. In effetti, il termine attacco cibernetico ricomprende una vasta gamma di tecniche ostili attuabili attraverso un codice. Tra i vari tipi di strumenti, uno dei più utilizzati è il *malware*[7], ovvero un programma avente lo scopo di cagionare danni diffusi, quali il disturbo del funzionamento di una rete, la sottrazione di informazioni, l'accesso non autorizzato a reti o sistemi[8]. Altro esempio di strumento di attacco è il DDoS (*distributed denial of service*[9]), meno sofisticato del *malware*, ma non meno efficace. Trattasi di un attacco il cui scopo è impedire a un sistema (*server*) di erogare i servizi di competenza ai sistemi richiedenti (*client*)[10]. Porre in essere un attacco DDoS è relativamente semplice, essendo sufficiente, ad esempio, una generazione massiccia di *e-mail*, magari con pesanti allegati, di per sé idonea a comportare il blocco di un sito *web*[11].

Gli obiettivi di un attacco cibernetico possono essere due: le informazioni e/o la causazione di un danno fisico.

Nonostante una parte isolata della dottrina abbia posto in dubbio che un attacco *cyber* possa rivolgersi direttamente contro un'informazione[12], la gran parte degli autori ritiene che, se si interpreta in maniera estensiva il termine, l'informazione ben possa essere oggetto di attacco cibernetico. In termini informatici, concretamente, un'informazione è ogni dato che riduca l'incertezza in ordine allo stato di un sistema[13]; ciò significa che il sistema operativo di un computer, i suoi processi automatizzati, le sue applicazioni (così come i *file* ivi contenuti) sono classificabili quali informazioni.

Un attacco cibernetico può, poi, cagionare un danno di natura fisica. Come accaduto nel caso Stuxnet[14], un programma malevolo può colpire sistemi che regolano le infrastrutture più critiche delle società tecnologicamente avanzate: questi sistemi dirigono il traffico aeroportuale, la distribuzione di gas o petrolio, la centrali nucleari e chimiche, le aperture delle dighe, solo per porre alcuni esempi.

Un attacco cibernetico può porsi in essere isolatamente o a supporto di un attacco convenzionale, al fine di semplificarne il compimento ovvero di massimizzarne gli effetti. Un *malware* può, ad esempio, essere utilizzato per disabilitare i sistemi di difesa antiaerea di uno Stato, onde consentire una più efficace penetrazione delle forze aeree dell'attaccante[15].

2. Legge di guerra nell'era di internet

Come già notato dalla dottrina più attenta[16], ogni controversia inerente il cyberspazio[17] si sviluppa su un duplice piano. Una prima considerazione inerisce la scelta delle disposizioni di legge che, nate per il mondo reale, debbano applicarsi allo spazio cibernetico. Una seconda considerazione impone di analizzare i valori che sono posti alla base di queste regole, per trarne un basamento idoneo a sostenere un sistema di norme per un mondo interconnesso[18].

Per quanto qui di interesse, dunque, è necessario porre attenzione al vigente diritto dei conflitti armati e cercare di trarne profili normativi applicabili agli attacchi cibernetici, legittimati, in questo, dalla c.d. clausola Martens[19]. Secondo questa disposizione, in attesa di una completa codificazione del diritto di guerra, «le popolazioni e i belligeranti restano sotto la salvaguardia e sotto l'imperio dei principi del diritto delle genti, quali risultano dagli usi stabiliti fra le nazioni civili, dalle leggi di umanità e dalle esigenze della coscienza pubblica». Questa clausola è finalizzata a valutare la liceità di armi non specificamente previste dal diritto internazionale pattizio ed è preordinata ad impedire l'interpretazione secondo cui ciò che non è espressamente vietato è permesso. La clausola Martens ha il vantaggio di convertire regole metagiuridiche, derivanti dai principi e dai valori comuni dell'umanità e della coscienza pubblica, in principi giuridici.

L'art. 2, par. 4, della Carta delle Nazioni Unite dispone un divieto generale di ricorso alla forza ed alla minaccia di uso della stessa[20] nelle relazioni internazionali, fatta salva l'eccezione del 'diritto naturale' alla legittima difesa individuale e collettiva[21].

Occorre dunque accertare, soprattutto ai fini di questo scritto, l'esatta definizione del termine forza, al fine di comprendere se essa debba necessariamente qualificarsi quale armata o se possa ricomprendere altri tipi di coercizione[22]. La dottrina maggioritaria[23] ritiene che la 'forza' di cui all'art. 2, par. 4 debba qualificarsi come armata, militare o, almeno, violenta[24].

Ci si è chiesti se l'impiego di mezzi informatici contro uno Stato possa essere considerato come una violazione dell'art. 2, par. 4. La dottrina del nostro Paese non ha, ancora, analizzato la questione a fondo. Si è argomentato, *passim*, che il *cyberwarfare* riguardi il metodo di combattimento, piuttosto che il ricorso alla forza armata; ciò premesso, un attacco cibernetico di per sé sarebbe lesivo del solo principio di non intervento e non dell'art. 2 par. 4[25].

Più approfondita è, in merito, la ricerca anglosassone[26]. Essa propone[27] un test di sette requisiti per determinare se un attacco costituisca o meno un uso della forza sul piano delle relazioni internazionali:

1. *gravità del danno*: la causazione della morte di persone ovvero di estesi danni alle cose è indice di uso della forza militare
2. *immediatezza delle conseguenze dell'attacco*: qualora gli effetti dell'attacco si producano in un lasso temporale limitato[28] l'operazione è probabilmente di tipo militare; qualora l'effetto si produca in settimane o mesi, è più probabile che l'azione sia di tipo economico o diplomatico
3. *immediatezza del nesso causale*: se l'azione intrapresa è la sola ed unica causa del risultato, è assai probabile si tratti di un azione militare; più degrada la stretta correlazione causale, meno probabile è la qualificazione dell'atto quale uso della forza;

4. *violazione di un confine statale*
5. *misurabilità del danno*: se gli effetti possono esse quantificati con immediatezza con scarso o nullo processo valutativo che si rivolga a elementi soggettivi[29], l'attacco ha carattere militare
6. *legittimazione presunta*: si presuppone[30] che un'azione di forza cinetica sia portata a compimento da uno Stato, in quanto detentore del monopolio dell'uso della forza legittima[31]. Altri tipi di attacchi non cinetici, come quelli condotto nel cyberspazio, non si presumono[32] posti in essere da attori statuali
7. *responsabilità*: ove uno Stato si assuma la responsabilità di un atto distruttivo, questo deve inquadrarsi in una operazione militare tradizionale.

Questa ricostruzione ha, senz'altro, il merito di fornire una griglia di determinazione *post-factum* dell'uso della forza, per verificare se il divieto di cui all'art. 2 par. 4 possa dirsi violato. Si deve, tuttavia, evidenziare che taluni requisiti rivestono, alla luce dell'odierno stato tecnologico, meno importanza di altri: ad esempio, il criterio di violazione del confine perde rilevanza nel contesto della guerra aerea o marittima.

3. Caratteristiche degli attacchi cibernetici

Il problema dell'inquadramento dell'attacco *cyber* nel sistema della Carta dell'ONU è ovvio: al tempo della stesura di questa, l'informatica non era in grado di rappresentare una minaccia. È tuttavia, ricercando i singoli connotati di un attacco cibernetico, è possibile confrontarli con i principi dello *ius in bello* in vigore e trarre una disciplina unitaria.

Come ricordato nel §1, gli attacchi cibernetici possono concretamente declinarsi in un larghissimo *range* di azioni, che possono, però, presentare quattro peculiarità comuni[33], idonee a distinguerli dagli attacchi convenzionali: mediatezza, intangibilità, localizzazione e risultato.

3.1. Mediatezza

Nonostante gli attacchi cibernetici diretti siano certamente possibili[34], nella maggior parte dei casi un attacco manipola un sistema per innescare una reazione a catena che porti all'evento dannoso desiderato dall'attaccante. Si pensi ad una modifica malevole dei dati di controllo trasfusionali di un ospedale militare, che comporta trasfusioni errate, dunque dannose, nei confronti dei nemici feriti, oppure si ipotizzi la manipolazione del *downlink* del GPS[35] finalizzata a modificare la traiettoria di un missile.

Questa caratteristica non presenta particolari problemi sul piano del diritto internazionale. È stato, infatti, stabilito per via giurisprudenziale[36] che l'uso indiretto della forza può integrare una violazione dell'art. 2 par. 4 della Carta dell'ONU.

3.2. Intangibilità

La seconda caratteristica dell'azione di attacco cibernetico è l'intangibilità, problema che, legalmente parlando, esiste su tre piani distinti. *In primis*, l'obiettivo dell'attacco potrebbe non esistere nel mondo fisico, trattandosi di informazioni (v. *supra* §1) contenute in un *server*.

Secondariamente l'arma stessa è intangibile, perché trattasi di un codice binario. In terzo luogo, intangibile può essere il tipo di danno dell'attacco.

Con riferimento all'obiettivo dell'attacco, nessun problema si pone nel caso in cui questo sia un obiettivo appartenente al mondo fisico. Questioni più complesse emergono allorché l'obiettivo sia l'informazione (nel senso visto più sopra) e, particolarmente, quando l'atto ostile non miri a distruggere l'informazione, ma a danneggiarla, modificarla ovvero degradarla in qualche modo. Allo stato, l'unica teoria valida è stata proposta dalla dottrina anglosassone[37] e si basa sul risultato realmente prodotto dall'attacco (*results-based theory*). Esemplificando, nel momento in cui un attacco cibernetico (prescindendo dalle modalità dello stesso) possa porre in serio pericolo l'incolumità di cose o persone, rientra nella definizione di forza di cui all'art. 2 par. 4.

La seconda questione proposta riguarda la possibilità di definire 'armata' la forza di un attacco posto in essere per mezzo di ciò che, sostanzialmente, è codice binario[38]. Anche in questo caso occorre rifarsi alla teoria orientata al risultato. Si è, correttamente, osservato che: «la coercizione armata non è caratterizzata dal fatto che sia impiegata od emessa energia cinetica, ma piuttosto dalla natura del risultato che si intende ottenere, nello specifico un danneggiamento fisico ovvero una aggressione alla vita umana»[39]. In effetti la definizione corrente di arma, anche nel nostro Paese, è un qualunque dispositivo, strumento meccanico ovvero elemento di natura chimica, nucleare o elettromagnetica che venga utilizzato allo scopo di offendere oppure sia utilizzato per la difesa personale dell'utilizzatore[40].

3.3. Localizzazione

Gli attacchi cibernetici sollevano problemi assai rilevanti in merito alla localizzazione sia dell'aggressore che del bersaglio. È bene premettere che, nonostante una violazione di confine sia un indice chiaro e spesso inequivocabile di applicabilità del diritto internazionale ovvero del diritto di guerra, la legge internazionale non richiede il superamento di un confine per la qualificazione di un atto come uso della forza. Si pensi all'intervento (anche armato) messo in atto da un Paese per salvare i cittadini all'estero[41] che, nella dottrina e nella prassi internazionale, sembra sempre più affermarsi quale autonoma eccezione al divieto generale dell'uso della forza nelle relazioni internazionali[42].

Il problema principale si incontra allorché si debba localizzare, con un certo grado di probabilità, il luogo fisico da dove è partito l'attacco. L'attuale tecnologia, unita all'abilità di quanti utilizzano la rete per scopi malevoli, consente di occultare con efficacia non solo la propria identità, ma anche il luogo di partenza dell'attacco, instradando questo in un elevato numero di sistemi (*server*) nei più disparati Paesi del mondo[43] prima di colpire il bersaglio. Parte della dottrina ha sostenuto che le azioni di guerra cibernetica si combattono nel cyberspazio, luogo ove le leggi internazionali non valgono[44]. Si tratta di una tesi da rifiutare, poiché, come già espresso più sopra, se l'attraversamento di un confine è di per sé una prova dell'uso della forza internazionale, non è richiesta una violazione del confine per considerare un dato attacco come un uso della forza. Sul piano concreto il problema della localizzazione dell'attaccante attiene all'aspetto tecnico-operativo, più che a quello legale.

Sul piano giuridico basti osservare che, nel caso di un conflitto armato in essere, la dottrina[45] sostiene che il belligerante non possa effettuare operazioni cibernetiche in territorio neutrale e

precisa che il neutrale ha il dovere di impedire ai belligeranti l'uso di strutture cibernetiche localizzabili nel suo territorio.

3.4. Risultato

Come accennato, assai varie sono le tecniche attraverso cui è possibile attuare un attacco cibernetico, dalla semplice negazione del servizio ad una più sofisticata manipolazione di un *server*; innumerevoli sono le tipologie di risultato ottenibile: dalla creazione di meri inconvenienti a danni catastrofici a cose o persone.

L'indeterminabilità *ex ante* del risultato di un attacco cibernetico è la caratteristica che, forse, rende più incerta l'integrazione dell'uso della forza internazionale e, conseguentemente, l'applicabilità del diritto di guerra[46].

Un attacco *cyber* può essere diretto non a cagionare un danno, ma a degradare un servizio o una funzione, al fine, ad esempio, di forzare la comunicazione su un canale meno sicuro[47]. Il punto centrale del problema è comprendere se un attacco di questo tipo possa sussumersi nel concetto di uso della forza.

Anche in questo caso è necessario, per evitare interpretazioni successive sempre più estensive, rifarsi al modello del risultato realmente ottenuto, sostenendo che un attacco cibernetico debba mettere in pericolo o ledere cose o persone per sussumersi nel concetto di uso della forza. Gli attacchi che producano altri risultati, ad esempio danneggiamenti della proprietà intellettuale, costituiscono certamente interferenze violatrici del principio di non intervento, fonte di responsabilità per gli Stati, ma inidonei a qualificarsi come uso della forza internazionale.

Ovviamente, nel caso in cui un conflitto armato sia già in essere tra legittimi belligeranti, un attacco informatico di ogni tipo, indipendentemente dal risultato, è un atto permesso dal diritto internazionale dei conflitti armati, sempreché non integri un atto di perfidia[48].

Stante quanto sopra riportato, si può giungere ad una prima riassuntiva conclusione: qualora un attacco cibernetico, direttamente o indirettamente, cagioni una conseguenza fisica, cioè una distruzione, dispersione, deterioramento o inservibilità totale o parziale di cose mobili o immobili, ovvero una lesione o la perdita di vite umane, costituisce un uso della forza ai sensi dell'art. 2 par. 4 della Carta dell'ONU[49].

Conseguentemente, nel caso n cui un attacco cibernetico non si manifesti nella sfera fisica, ovvero colpisce solo informazioni, ovvero comporti danni fisici estremamente irrisori, non si potrà parlare di uso della forza, ma di altra, se il caso illecita, condotta, da cui può derivare una responsabilità internazionale.

4. Attacco cibernetico: risposta armata?

Come ricordato, una delle eccezioni al generale divieto di uso della forza è stabilito nell'art. 51 della Carta dell'ONU, che prevede il diritto naturale alla legittima difesa individuale e collettiva. È appena il caso di ricordare che l'esatta definizione di 'legittima difesa' è una delle questioni più

divisive del diritto internazionale[50]. Particolarmente complesso è, allora, applicare questo concetto di difesa all'attacco cibernetico, perché si tratta di risolvere tre fondamentali questioni:

8. *An*: una data azione cibernetica può ingenerare una risposta in legittima difesa?
9. *Erga*: nei confronti di quale soggetto si deve dirigere la risposta?
10. *Quomodo*: in che modo è lecito rispondere?

L'analisi sull'*an* può iniziare da una situazione paradigmatica, ovvero il caso astratto in cui un attacco cibernetico cagioni danni paragonabili a quelli che avrebbe causato un attacco convenzionale[51]. In questo caso uno Stato è in linea di massima titolare del diritto di risposta, anche armata, in legittima difesa. Lo stesso dicasi per un'azione cibernetica congiunta ad altri tipi di attacchi, sempreché il risultato sia il medesimo.

Assai controverso è il caso di un attacco *cyber* sia diretto contro una infrastruttura informatica che contenga informazioni critiche per la sicurezza nazionale. Parte isolata della dottrina[52] ritiene che un'azione di questo tipo possa innescare una risposta armata da parte dello Stato, poiché – si argomenta – le caratteristiche della società contemporanea e la sua dipendenza dall'ICT[53] rendono questa assai vulnerabile agli attacchi cibernetici, da cui ci si deve difendere con ogni mezzo.

A mente di chi scrive trattasi di interpretazione eccessivamente estensiva. Non solo giacché, s'è sopra argomentato, per una risposta armata è necessario un danno di natura fisica, ma anche perché, nei contesti di combattimento odierni, l'azione cibernetica si risolve, concretamente, in manovre aventi carattere ancillare rispetto alla condotta delle operazioni di guerra che restano, per la gran parte, di natura convenzionale.

Profilo più problematico della questione in discussione riguarda la configurabilità della legittima difesa preventiva in un contesto *cyberwarfare*.

La posizione della dottrina italiana[54] è di generale riconoscimento dell'esistenza di un diritto alla legittima difesa preventiva, in conseguenza delle moderne tecniche di armamento[55], idonee di per sé a rendere impossibile l'esercizio della legittima difesa *post factum*. In estrema sintesi è lecita una reazione in legittima difesa non solo successivamente all'attacco, ma anche quando questo sia stato sferrato, ma non abbia ancora colpito il territorio altrui[56], o, ancora, nell'imminenza dell'attacco[57].

La legittima difesa preventiva può riguardare riguarda il contesto cibernetico poiché questo ne può essere il prodromo, cioè può essere indice di un imminente attacco convenzionale: in questo caso, al fine di una attivazione in legittima difesa, dirimente è l'obiettivo dell'attacco. Se l'attacco informatico è diretto contro sistemi di difesa missilistica, comunicazioni militari, sistemi di risposta all'emergenza, radar o satelliti, è altamente probabile che uno Stato possa giudicare l'attacco cibernetico come il prodromo di un attacco convenzionale ed agisca in legittima difesa[58]. La dottrina ritiene che un attacco *cyber* ad altri tipi di infrastruttura, ad esempio il sistema di scambio finanziario, in sé solo considerato non possa legittimare lo Stato colpito ad una reazione armata in legittima difesa[59].

Una volta definito che una certa azione cibernetica può originare una risposta in legittima difesa da parte dello Stato, si pone il secondo problema: nei confronti di quale soggetto si deve dirigere la risposta (*erga*)? Come riconosciuto dalla dottrina[60], il problema dell'imputabilità certa (o

quantomeno molto probabile) dell'azione in capo ad un soggetto è, sul piano tecnico-informatico, una delle questioni chiave. Nella maggior parte dei casi[61], infatti, gli attacchi sono lanciati in maniera anonima, sfruttando particolari tecniche che consentono di mascherare non solo l'identità di chi pone in essere l'atto ostile, ma anche il suo punto geografico[62]. In questo modo è possibile non solo nascondere l'autore dell'attacco, ma attribuire falsamente questo ad altri.

Il problema dell'imputabilità, oltre che il piano prettamente informatico, inerisce anche l'ambito legale. Si deve, infatti, notare che, così come accade nel caso di un attacco convenzionale, anche nel caso di un'azione cibernetica ostile è assai improbabile che uno Stato si assuma formalmente la responsabilità dell'atto, per quanto esistano evidenze che questo ospiti organizzazioni terroristiche. Per poter vantare il titolo di azione in legittima difesa, lo Stato vittima di attacco dovrà dunque, stabilire una connessione tra il soggetto che ha posto in essere l'ostilità e lo Stato contro cui viene diretta la difesa[63].

La questione qui, deve scindersi in due temi distinti.

Su un primo piano deve verificarsi la possibilità di risposta in legittima difesa nei confronti di un attore non statale. Il testo della Carta non fornisce una risposta univoca, poiché l'art. 51 si limita a disporre la liceità della difesa 'nel caso che abbia luogo un attacco', senza specificare la provenienza di questo. Il problema si è posto dopo gli attentati al *World Trade Center* ed al Pentagono del settembre 2001, cui gli Stati Uniti hanno reagito in legittima difesa contro l'Afghanistan (operazione *Enduring freedom*[64]). Questa azione è stata legittimata dalle ris. 1368 e 1373 dell'ONU, nel preambolo delle quali si fa esplicito riferimento al diritto alla difesa legittima[65]. Concorde è la posizione della dottrina[66], secondo cui una risposta armata ad un attacco condotto da un'entità non statale è consentita, per quanto in termini restrittivi. Legittimo è l'uso della forza contro lo Stato territoriale qualora l'entità non statale abbia agito su istruzione, direzione o controllo di questo Stato. Qualora l'attacco provenga da un area non sottoposta alla giurisdizione di alcuno Stato, si potrà reagire contro l'entità non statale nell'area in questione.

Su un secondo piano deve rilevarsi che gli attacchi cibernetici di maggior pericolosità sono solitamente posti in essere da due o più persone, spesso site in Stati diversi, ed aventi connessioni assai labili con il Paese (ove ce ne sia uno) che trae un vantaggio dall'attacco[67]. In materia mancano diretti riferimenti giurisprudenziali o dottrinali, per cui ci si deve riferire alla regola generale sopra riportata. È, dunque, chiaro che uno Stato non deve assicurare alcun contributo necessario o agevolatore materiale o morale nelle fasi ideativa, preparatoria o esecutiva dell'attacco. Se così non fosse, il Paese si esporrebbe ad una reazione in legittima difesa da parte della vittima che, però, ha l'onere della prova[68].

Tutte le risposte agli attacchi, che siano cinetici o elettronici, sono soggette a due requisiti che precisano il *quomodo*: necessità e proporzionalità[69]. La dottrina[70] ha affermato che la forza può essere esercitata quando sussiste una necessità di legittima difesa urgente, irresistibile, tale da non lasciare la scelta dei mezzi ed il tempo di deliberare. Nella sostanza il requisito della necessità è integrato tutte quelle volte in cui la repulsione della forza attaccante debba essere immediata e non vi sia tempo per preavvisare il Consiglio di Sicurezza per l'avvio delle procedure di rito[71]. La necessità è tangente all'immediatezza, questa da considerarsi in maniera elastica: una reazione

tardiva da parte dello Stato vittima di attacco si configura più come una rappresaglia che come un esercizio di legittima difesa.

Il secondo requisito è la proporzionalità tra attacco e legittima difesa. È bene sottolineare che questo criterio non deve intendersi in termini quantitativi, non essendo richiesta una perfetta simmetria tra azione e reazione[72]. Certamente lo Stato attaccato può portare la sua reazione in profondità, al fine di indurre l'avversario a cessare la sua azione lesiva. Illecita sarà, però, una risposta che arrechi mali non necessari o comunque non proporzionali ai vantaggi militari che possono derivare dal suo compimento[73]. L'obbligo di ponderazione dei vantaggi militari rispetto all'entità dell'attacco è di condotta e non di risultato, poiché la effettiva portata può essere valutata solo dopo l'inizio dell'attacco.

Quanto considerato porta ad un interessante interrogativo sulle possibilità che uno Stato reagisca in legittima difesa in maniera cinetica, quindi con un attacco armato, contro un uso illegittimo della forza a mezzo di una azione cibernetica. La risposta è certamente affermativa[74]. Come ricordato, il requisito della proporzionalità non implica necessariamente una risposta *in kind*, né che l'azione di risposta sia limitata al territorio dello Stato che oppone la difesa. Ne consegue che la vittima di attacco cibernetico legittimamente può usare le armi a sua disposizione per respingere l'attacco, fintantoché la difesa sia proporzionata all'offesa. La proporzionalità, dunque, deve valutarsi in ordine all'obiettivo dell'azione di risposta, ovvero quello di respingere l'attacco ovvero prevenirne la venuta in essere. Tutto ciò che è necessario per raggiungere questo obiettivo deve ricomprendersi all'interno di proporzionalità della legittima difesa, dunque coperto da liceità internazionale. La dottrina unanime riconosce come lecito un attacco convenzionale in risposta ad un'azione cibernetica finalizzata a preparare il campo di battaglia per l'uso della forza militare[75].

5. Altre azioni di riposta: le contromisure

Ove l'attacco cibernetico non integri gli estremi di una violazione dell'art. 2, par. 4 della Carta dell'ONU, lo Stato vittima può disporre comunque adeguate contromisure, concordemente con quanto previsto dai trattati internazionali.

Tra le contromisure di natura restrittiva, la prassi internazionale porta ad analizzare le sanzioni economiche, ovvero quelle restrizioni di natura patrimoniale, commerciale ed economica da parte di uno o più Stati verso un paese ritenuto colpevole di una condotta internazionale illecita[76]. Assai varie sono e tipologie di misure sanzionatorie, da embarghi su specifiche merci[77] a restrizioni di natura finanziaria quali il blocco dei conti correnti.

L'Unione europea[78] prevede la possibilità di applicare sanzioni economiche e finanziarie sia per la difesa dei valori comuni, che per il rafforzamento della sicurezza nell'Unione in tutte le sue forme[79].

Ci si chiede se sia possibile una risposta *in kind*, ovvero rispondere ad un attacco cibernetico che non integra l'uso internazionale della forza con lo stesso mezzo. La risposta può trovarsi nella giurisprudenza[80], che propone tre requisiti di liceità della contromisura. Primo: l'azione deve essere intrapresa in risposta ad un illecito internazionale posto in essere da uno Stato e deve essere contro questi rivolta. Secondo, lo Stato vittima dell'atto illecito deve aver intimato la cessazione

dell'azione lesiva ovvero chiesto il ristoro dei danni. Terzo, gli effetti della contromisura devono essere proporzionati al pregiudizio effettivamente subito.

Ciò premesso e considerata la massima versatilità delle azioni cibernetiche, è possibile affermare che queste, forse ancor più delle sanzioni economiche, possono atteggiarsi a strumento di contromisura paradigmatico ed estremamente efficace per rispondere ad illeciti internazionali che non costituiscano una violazione dell'art. 2 par. 4 della Carta dell'ONU. Si pensi, ad. esempio, che una serie di *black out* di strutture non essenziali di uno Stato può essere una adeguata misura coercitiva in risposta ad un atto illecito da questo posto in essere. Paradigmatico, in tal senso, è il caso *Floodnet*. Nel 1998 un gruppo di attivisti[81] lancia un attacco DDoS[82] contro il sito internet del Dipartimento della Difesa degli Stati Uniti. Gli specialisti *cyber* del Dipartimento compilano un programma che identifica il computer da cui viene lanciato l'attacco e risponde a questo con un DDoS (assai più efficacie poiché diretto contro un sistema *consumer*) ponendo fine all'attacco originario. Nonostante taluni limitati rilievi sul piano legale, appare condivisibile l'opinione che la risposta degli Stati Uniti possa considerarsi una contromisura appropriata[83], in particolare nei confronti di un attore non statale. Questo approccio, definibile difesa attiva, non è, comunque, esente da rischi, poiché in grado di ingenerare una *escalation* di attacchi, astrattamente idonea ad avere ricadute di natura cinetica. La scelta oggi adottata pare più rivolta alla costruzione di solide strutture di difesa passiva[84], in grado di respingere o di annullare gli effetti degli attacchi.

Ulteriore opzione per lo Stato vittima dell'azione lesiva è l'attivazione del sistema di sicurezza collettivo, previsto dal Capitolo VII della Carta dell'ONU, agli artt. 39 ss.

Il Paese oggetto dell'attacco può denunciare questo al Consiglio di Sicurezza, che ha competenza esclusiva in materia di mantenimento della pace e della sicurezza internazionale, e trasmettergli tutti gli atti ritenuti necessari. Il Consiglio, una volta accertata l'esistenza di una minaccia ovvero di una violazione della pace o di un atto di aggressione, dispone misure coercitive[85] che involgano o meno l'uso della forza.

Il Consiglio di sicurezza può raccomandare o decidere l'adozione di misure coercitive non comportanti l'uso della forza armata. Ai sensi dell'art. 41, queste possono comprendere un'interruzione totale o parziale delle relazioni economiche e delle comunicazioni ferroviarie, marittime, aeree, postali, telegrafiche, radio ed altre, e la rottura delle relazioni diplomatiche.

Una misura del Consiglio potrebbe, dunque, imporre una limitazione degli accessi ad internet, fino a giungere alla estrema misura della totale disconnessione di un Paese[86]. Taluni dubbi possono esprimersi in relazione a quest'ultimo tipo di decisione. In considerazione dell'elevata dipendenza delle strutture economiche e produttive degli Stati più avanzati, una disconnessione della rete mondiale potrebbe comportare conseguenze certamente paragonabili all'embargo, al blocco di un porto o all'istituzione di zone interdette al volo, ricadendo nell'uso della forza autorizzato da Consiglio, ma al di fuori del disposto dell'art. 41. Trattasi di un problema che, però, ha portata sostanzialmente teorica, poiché non si è mai realizzata un'ipotesi di completa disconnessione e perché questa misura sarebbe assai complessa da attuare.

Normalmente tali misure non hanno un termine finale e posso essere sospese o revocate con una decisione del Consiglio.

Simili misure di natura difensiva possono essere stabilite dagli Stati che concludano patti militari per l'organizzazione della difesa collettiva[87], legittimi purché conformi agli obblighi di cui all'art. 51 della Carta dell'ONU.

Note

(ultimo accesso ai link indicati: 1 settembre 2017)

[1] Ovvero tutti quei dispositivi che «contengono organi sensoriali, effettori, e l'equivalente di un sistema nervoso per il trasferimento dell'informazione dagli uni agli altri», N. WEINER, *La Cibernetica - Controllo e Comunicazione nell'animale e nella macchina*, Il Saggiatore, Milano 1968, p. 71.

[2] D. Sanger, *U.S. Cyberattacks target ISIS in a new line of combat*, The New York Times, 24 aprile 2016, p. A1. V. anche K. Breene, *Who are the cyberwar superpowers?*, in World Economic Forum, <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>, P. ROSENZWEIG, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and the world*, Praeger, Santa Barbara, 2013 e U. GORI, S. LISI, *Cyber warfare 2014*, Franco Angeli, Milano 2015.

[3] In questo testo si adotta una definizione di computer estremamente ampia, intendendo con esso una macchina automatizzata idonea ad eseguire calcoli matematici complessi ovvero altri tipi di elaborazione dei dati (cfr. P. CERUZZI, *Storia dell'informatica. Dai primi computer digitali all'era di Internet*, Apogeo, Milano 2006, pagina 9). In questo senso, quale *computer* deve intendersi non solo il classico *personal computer* (fisso o portatile), ma altresì lo *smartphone*, il *tablet*, lo *smartwatch* ed ogni dispositivo computerizzato installato in veicoli, aeromobili e natanti.

[4] Dipartimento della Difesa degli Stati Uniti d'America, *Dictionary of military and associated terms*, 8 novembre 2008, v. voce *cyberwarfare* (t.d.A.).

[5] Altre forme di attacco elettronico includono un utilizzo a larga gamma dello spettro elettromagnetico, come le onde radio, radar, microonde ed anche spettro ottico (strumenti laser ed infrarosso). Le tecniche di guerra elettronica possono consistere nell'intercettazione passiva delle comunicazioni avversarie, nella sorveglianza dello spettro elettromagnetico, nell'inganno del traffico radio e radar come il *jamming* e l'interferenza. Cfr., in merito, R. HEICKERÖ, *Electronic warriors use mail order equipment*, in «Framsyn Magazine», aprile 2005.

[6] Ovviamente il bersaglio di un attacco cibernetico non può che essere un computer (nel senso visto in nota 3). Tuttavia è possibile una diversificazione dell'obiettivo dell'attacco sotto due aspetti. Un attacco può colpire direttamente un *software* (ad esempio crea una copia occulta del contenuto del disco fisso del bersaglio e invia il tutto al pc attaccante o ad altro) oppure può colpire indirettamente l'*hardware* attraverso il *software* (ad esempio è possibile modificare il programma d gestione del disco fisso ovvero dell'impianto di raffreddamento del pc per creare danni fisici). Naturalmente si può diversificare l'effetto dell'attacco a seconda che questo sia condotto contro un sistema in uso a un privato o una famiglia o contro computer privati in uso a dipendenti di imprese o dello Stato o, ancora, contro *mainframe* (grandi computer costituiti da una potente unità centrale di elaborazione dati capace di gestire molti programmi contemporaneamente, alla quale sono collegati numerosi terminali) aziendali o statali.

[7] Abbreviazione per *malicious software* (programma dannoso).

[8] La pericolosità di questa tipologia di codice è moltiplicata dall'inserimento del *malware* all'interno di un programma non malevolo. Il *maleware* si nasconde come all'interno del cavallo di Troia (prendendo, appunto, il nome di *Trojan*) e viene avviato inconsapevolmente dall'utente insieme al programma non malevolo. Una volta lanciato, il *maleware* è in grado di rimanere in esecuzione a prescindere dalla volontà dell'utente, di moltiplicarsi e di diffondersi all'interno della rete. Per un caso di studio si veda U.S. CERT,

An Undirected Attack Against Critical Infrastructure, settembre 2005, <https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf>.

[9] Negazione diffusa del servizio di rete.

[10] Si pensi, ad esempio, ad un attacco DDoS diretto contro una società emittente carte di credito. Negando il servizio di questa, ogni transazione monetaria dei clienti sarebbe impossibile. Questo potrebbe determinare i fruitori del servizio a recedere dal contratto di carta di credito, con danno per l'impresa oggetto d'attacco.

[11] Assai interessante, in merito, E. TIKK, K. KASKA, L. VIHUL, *International cyber incidents: legal considerations,* Centro di eccellenza e cooperazione di difesa cibernetica della NATO, 2010, p. 112, <https://ccdcoe.org/publications/books/legalconsiderations.pdf>.

[12] Y. DINSTEIN, *Computer network attacks and self-defense*, in M. SCHITT, O. DONNELL*, Computer network attack and international law*, Naval War College, Newport 1999, p. 102.

[13] H. DINNISS, *Cyberwarfare and the laws of war*, Cambridge University Press, New York 2014, p. 4. Questa definizione include assai più del tradizionale significato di informazione quale fatto o conoscenza richiesti affinché un essere umano possa formarsi o modificare un'opinione

[14] Un programma malevolo avente lo scopo di rendere inutilizzabili le centrifughe della centrale nucleare di Natanz in Iran, impendendo la rilevazione dei malfunzionamenti. Il codice consentiva di alterare la programmazione logica dei sistemi di controllo industriali operanti su sistema operativo Windows (ad esempio, i gasdotti, i sistemi di trattamento delle acque eccetera). Ad oggi sembra sia stata de-compilata (tramite il *reverse engereering*) e resa pubblica una parte del sorgente di Stuxnet, un *rootkit*, ovvero uno strumento in grado di garantire l'accesso (ed il controllo) ad un utente non autorizzato.

[15] Questa situazione astratta si è realizzata il 6 settembre 2007, allorché la Forza aerea israeliana ha eluso le difese antiaeree siriane per colpire un sospetto sito di produzione nucleare nei pressi di Dayr az-Zawr (cfr. L. FLORIDI, M. TADDEO, *The Ethics of Information Warfare*, Springer, Londra, 2014, p. 77).

[16] R. KU, *Foreword: A Brave New Cyberword*, in «Thomas Jefferson Law Review», 125 (2000), p. 125, <http://heinonline.org/HOL/LandingPage?handle=hein.journals/tjeflr22&div=11&id=&page>.

[17] Felicemente definito come «*spazio concettuale* dove le persone interagiscono usando tecnologie per la comunicazione mediata dal computer», R. FIDLER, *Mediamorfosi. Comprendere i nuovi media*, Guerini e Associati, Milano 2000, pp. 89-90.

[18] Nella considerazione che, ove le fattispecie non sia normate, è necessario rifarsi al procedimento analogico, applicabile, però, al solo diritto consuetudinario. Fattispecie nuove, non espressamente regolate, potranno essere disciplinate da norme preesistenti, purché si tratti di fattispecie che presentano caratteri analoghi.

[19] Contenuta nel preambolo della IV Convenzione dell'Aja, nelle quattro Convenzioni di Ginevra, nell'art. 1 par. 2 del I Protocollo addizionale e nel preambolo della Convenzione sulle armi inumane.

[20] Ad esempio un ultimatum, ma non la 'corsa agli armamenti' (Corte internazionale di Giustizia, *Reports*, 1986, 135, par. 269), né il mero possesso dell'arma nucleare (Corte internazionale di Giustizia, *Reports*, 1996, 246-247, parr. 47-48).

[21] Art. 5. Altre eccezioni riguardano l'uso della forza autorizzato dal Consiglio di Sicurezza, l'ormai desueto intervento contro stati ex nemici (artt. 53 e 107), il consenso dell'avente diritto. Non unanimemente accettate sono le eccezioni all'uso della forza che si basano sull'intervento a protezione dei cittadini all'estero e l'intervento d'umanità.

[22] Si noti come nel testo della carta in alcuni casi il termine 'forza' e qualificato dalla precisazione 'armata' (*ex multis* 6° considerando del preambolo), mentre in altri esso appare non meglio qualificato (es. art. 44).

[23] *Ex multis*, N. RONZITTI, *Diritto internazionale dei conflitti armati*, Giuffré, Milano, 2014, pp. 29-30.

[24] Si è notato che, nei lavori preparatori, varie sono state le proposte di qualificazione del termine forze. In particolare, il ministro degli esteri del Brasile propose di ricomprendere anche la coercizione economica,

ma quest'emendamento fu respinto (2 voti a favore della proposta e 26 contrari, cfr. *Summary report of eleventh meeting of Commitee I*/1' Doc. 215, I/1/10, 6 UNCIO [6 maggio 1945] 334, 559). Ulteriori tentativi successivi alla redazione della Carta non hanno avuto successo. Nella Dichiarazione sulle relazioni amichevoli (ris. ONU 265-XXV), la coercizione economica è ricompresa nell'ambito del principio di non intervento. L'art. 3 della risoluzione sull'aggressione (ris. ONU 3314-XXIX) non menziona la coercizione economica tra gli atti di aggressione

[25] Ronzitti, *Diritto internazionale* cit., p. 33.

[26] Degno di nota è il *Manuale di Tallin sul diritto internazionale applicabile alla guerra cibernetica*, (M. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2012), redatto nel contesto di una serie di studi condotti da un gruppo di giuristi internazionali presso il Centro di Eccellenza e Cooperazione di Difesa Cibernetica della NATO. Non si tratta di un codice avente forza di legge, ma è una raffinata ricerca accademica indipendente.

[27] M. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in Columbia Journal of Transnational Law, Vol. 37, 1998-99, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993>.

[28] Si pensi all'esplosione di un ordigno ovvero all'immediato *jamming* di una rete di comunicazione.

[29] Si pensi alla distruzione di un edificio, valutabile immediatamente in modo oggettivo. Meno immediata e oggettiva è la valutazione degli effetti che può avere una 'guerra valutaria'.

[30] *Iuris tantum*.

[31] A. DE SIMONE, B. ACCARINO. L. ALFIERI, *Diritto, giustizia e logiche del dominio*, Morlacchi, Perugia, 2007, p. 125. Trattasi di un concetto ora in erosione, cfr. sul punto A. TORRE, *Costituzioni e sicurezza dello Stato*, Maggioli, Sant'Arcangelo di Romagna 2014, p. 384.

[32] Fatta salva ovviamente prova contraria.

[33] Cfr. Dinniss, *Cyberwarfare*, cit., p. 65 e ss.

[34] Si pensi ad un *malware* che disattiva il sistema di controllo di una diga, cagionando un'inondazione.

[35] Ovvero la modifica dei dati che il sistema di posizionamento satellitare globale invia ad un sistema ricevente.

[36] Corte internazionale di giustizia, Caso delle attività militari e paramilitari in e contro il Nicaragua (Nicaragua c. Stati Uniti), sentenza di merito del 27 giugno 1986, par. 205.

[37] I. BROWLIE, *International law and the use of force by States*, lavori per la lezione al Graduate Institute of International Studies, Ginevra, 1 febbraio 2001, <http://www.europaeum.org/files/publications/pamphlets/IanBrownlie.pdf>.

[38] Trattasi di una serie di zero ed uno (*bitstream*) che consente al computer di eseguire alcune operazioni; può trattarsi di operazioni relativamente semplici (come un attacco DDoS basico ovvero un attacco a forza bruta [*bruteforce*: un programma che tenta di ottenere una *password* inserendo a gran velocità tutte le parole presenti in un vocabolario finché la parola chiave non viene 'indovinata']), ma anche assai complesse, ad esempio il citato Stuxnet, che conteneva, al suo interno vari *malware*.

[39] Schmitt, *Computer Network Attack and the Use of Force in International Law*, cit., t.d.A.

[40] R. BUSETTO, *Dizionario militare*, Zanichelli, Bologna 2004, p. 71. Da un punto di vista di normativa interna si suole operare una suddivisione tra armi proprie ed improprie. Le prime sono oggetti progettati e creati appositamente per essere usati come armi, mentre le armi improprie sono oggetti originariamente destinati invece ad altra funzione, che in un determinato frangente vengono usati come armi. Nel nostro ordinamento interno manca una norma penalistica o di pubblica sicurezza che dia una definizione ontologica dell'arma; la tecnica del nostro legislatore è piuttosto di indicare gli strumenti che sono armi o debbono essere intesi tali (es. art. 585 c.p. e art. 4 della l. 110/1975). Per un approfondimento si veda F. CARINGELLA, A. IANNUZZI, L. LEVITA, *Manuale di diritto di pubblica sicurezza,* Roma, Dike, 2013, pp. 463-568.

[41] Nel caso in cui questi versino in pericolo di vita e lo Stato territoriale non sia in grado o non volesse (ad esempio, per complicità con un gruppo terroristico) disporre adeguate misure per la loro protezione.

[42] Ronzitti, *Diritto internazionale*, cit., p. 48.

[43] Particolarmente quelli che hanno legislazioni sulla riservatezza in rete assai rigide.

[44] S. KANUNK, *Information warfare: new challenges for public international law,* in «Harvard International Law Journal», 1996, p. 272, citato in A. STRATI, M. GAVOUNELI, N. SKOURTOS, *Unresolved issues and new challenges to the law of the sea*, M. Nijhoff Publ., Leiden 2006, p. 134.

[45] Manuale di Tallin, art. 92 e 93.

[46] Concorda sul punto Dinniss, *Cyberwarfare*, cit., p. 72.

[47] Si ipotizzi un disturbo su una cella telefonica per forzare il *downgrade* delle comunicazioni da 4G a 3G.

[48] Ovvero un atto «che fa appello, con l'intenzione di ingannarla, alla buona fede di un avversario per fargli credere che ha il diritto di ricevere o l'obbligo di accordare la protezione prevista dalle regole del diritto internazionale applicabile nei conflitti armati»; la definizione (ed il divieto) è contenuta nell'art. 37 del I Protocollo addizionale.

[49] Concordi anche Schmitt, *Computer Network*, cit., p. 928 e Dinniss, *Cyberwarfare*, cit., p. 74.

[50] P. BARGIACCHI, *Orientamenti della dottrina statunitense di diritto internazionale*, Giuffrè, Milano, 2011, p. 113 e ss., M. MANCINI, *Stato di guerra e conflitto armato nel diritto internazionale*, Giappichelli, Torino, 2009, p. 226 e ss., AA. VV., *Istituzioni di diritto internazionale,* Giappichelli, Torino, 2016, p. 321 e ss. Per una breve ricognizione di Scienza politica si veda M. DELLI SANTI, *Il nuovo terrorismo: questioni giuridiche e scelte politico-militari nelle misure di contrasto*, in «Informazioni della Difesa», 6/2014, pp. 48-67, <http://www.difesa.it/InformazioniDellaDifesa/periodico/periodico_2014/Documents/R6_2014/48_67_R6_2014.pdf>.

[51] Ovvero eccedenti rispetto a quelli di un semplice incidente di frontiera, cfr. N. RONZITTI, *Introduzione al diritto internazionale*, Giappichelli, Torino 2016, p. 434.

[52] W. G. SHARP, *Cyberspace and the use of force*, Ageis Research Corp, Falls Church 1999, p. 129.

[53] Le tecnologie dell'informazione e della comunicazione (*Information and Communications Technology*).

[54] *Ex multis*, A. SINAGRA, P. BARGIACCHI, *Lezioni di diritto internazionale pubblico*, Giuffrè, Milano 2009, p. 329, V. CANNIZZARO, *Diritto internazionale*, Giappichelli, Torino, 2016, p. 50, Ronzitti, *Introduzione al diritto*, cit., p. 432, S. MARCHISIO, *Corso di diritto internazionale*, Giappichelli, Torino, 2014, p. 343.

[55] Illogico ed irragionevole sarebbe richiedere ad uno Stato di essere colpito da un'arma nucleare per legittimarne la reazione.

[56] Si pensi all'attacco giapponese a Pearl Harbour.

[57] Il concetto dell'imminenza deve, necessariamente, intendersi in maniera restrittiva per evitare abusi. Non è imminente una minaccia latente, ad esempio la mera connivenza dello Stato con un gruppo terroristico. Di questo tipo di minacce deve occuparsi il Consiglio di Sicurezza. Non corrispondente al diritto internazionale è, tuttavia, la cosiddetta dottrina Bush, secondo cui, per far fronte alla minaccia terroristica ed alle armi di distruzione di massa, gli Stati potrebbero intervenire anche nel caso in cui lo 'Stato canaglia' ospiti organizzazioni terroristiche o possegga le suddette armi e sia pronto ad usarle, cfr. Ronzitti, *Diritto internazionale*, cit., p. 37.

[58] Si pensi, ad esempio, ad un *malware* che consenta un accesso ad un utente non autorizzato sfruttando una vulnerabilità non nota (*backdoor*) di un sistema di difesa missilistico. Il *malware* ben potrebbe, poi, essere in grado di propagarsi all'interno di tutta la rete e prendere il controllo dei sistemi ad essa connessi (il fenomeno prende il nome di *botnet*), risultando così il pieno controllore (*root*) dell'intero *network*.

[59] A partire dal 27 aprile 2007, l'Estonia fu soggetta ad un una serie di attacchi cibernetici diretti contro varie infrastrutture del Paese, incluso il Parlamento, alcuni ministeri ed il sistema di scambio finanziario elettronico, ma non è stato attivato il meccanismo della legittima difesa.

[60] J.L. RICHET, *Cybersecurity policies and strategies for cyberwarfare prevention*, Information Science Reference (IGI Global), Hershey, 2015, p. 32, J. DEVER, *Cyberwarfare: Attribution, preempion and national self defense*, JLCW, Vol. 2, Iss. 1, 2013, p. 37, J.R. VACCA, *Computer and information security handbook*, Morgan Kaufmann, Burlington 2009, p. 341.

[61] Tra i pochi casi in cui un programma malevolo consentiva (probabilmente per un errore del programmatore) di risalire all'ideatore si ricorda il *malware* 'ILOVEYOU', un *file* compilato in Visual Basic che, nel maggio del 2000, cagionò rilevanti danni a servizi di posta elettronica.

[62] Una delle tecniche più usate è il c.d. *IP spoofing*, che modifica l'indirizzo IP (un'etichetta numerica che identifica in modo univoco un dispositivo connesso ad una rete) del mittente. Assai interessante, nel merito specifico, è S. LINTA, R. KHAN, *Today's impact on communication system by IP spoofing ad its detection and prevention*, Grin, Norderstedt, 2011, p. 14 e ss.

[63] Sulla stessa posizione è la Corte Internazionale di Giustizia nel parere consultivo relativo alle *Conseguenze giuridiche derivanti dalla costruzione del Muro dei Territori palestinesi occupati* del 9 luglio 2004.

[64] A quest'operazione ha preso parte anche in nostro Paese dal 15 marzo al 15 settembre 2003. A seguito di autorizzazione parlamentare del 2 ottobre 2002, prendeva avvio la missione di circa mille uomini, inquadrati nella *Task Force* 'Nibbio'.

[65] Su questa posizione si è allineata la NATO che ha considerato l'attacco terroristico come idoneo ad attivare i meccanismi di cui all'art. 5 del trattato istitutivo.

[66] *Institut de droit international*, sessione di Stantiago del 2007.

[67] Una moltitudine di attacchi cibernetici sono stati post in essere a danno della Georgia durante la seconda guerra in Ossezia del Sud, tra cui vari DDoS contro *server* bancari e di telecomunicazioni georgiani. Si noti che era possibile, da parte di chiunque, registrarsi presso il dominio <stopgeorgia.ru> e scaricare gratuitamente alcuni programmi che consentivano a chiunque di unirsi all'offensiva cibernetica (cfr. J. CARR, *Inside Cyber Warfare: mapping the cyber world*, O'Reilly, Sebastopol, 2012, p. 106). La posizione russa è stata di completa negazione di queste attività cibernetiche e non si è provata una diretta connessione tra la Federazione e gli attacchi.

[68] Assai interessante, sul punto, è A. MAUGERI, *La responsabilità da comando nello statuto della Corte Penale Internazionale*, Giuffrè, Milano, 2007, p. 360.

[69] Tali condizioni non sono espressamente previste dall'art. 51 della Carta dell'ONU, ma appartengono al diritto consuetudinario e sono state riaffermate nella sentenza Nicaragua vs Stati Uniti.

[70] Facendo riferimento al celebre caso Caroline (1937).

[71] Si pensi alla necessità di rendere inoffensiva una fregata che ha lanciato un primo missile contro un porto e che si prepara a lanciarne altri.

[72] Ronzitti, *Diritto internazionale*, cit., p. 40. La cosiddetta reazione *in kind.*

[73] Fatte salve le rappresaglie lecite.

[74] Dinniss, *Cyberwarfare*, cit., p. 104.

[75] Lecito sarebbe, ad esempio, sottoporre a bombardamento un edificio utilizzato per lanciare attacchi elettronici finalizzati a paralizzare i sistemi di difesa antiaerea di uno Stato.

[76] J. HAIDAR, *Sanctions and Exports Deflection: Evidence from Iran*, Paris School of Economics, University of Paris 1 Pantheon Sorbonne, Mimeo, 2015.

[77] Da non confondersi con il blocco di un porto, che costituisce uso della forza.

[78] E, conseguentemente, il nostro Paese che agisce nel contesto della politica commerciale comune (art. 207 TFUE) e della politica estera e di sicurezza comune (Titolo V TUE).

[79] Documento sulle sanzioni del Consiglio UE, 15 settembre 2009, <http://eeas.europa.eu/archives/docs/cfsp/sanctions/docs/index_it.pdf>.

[80] Caso riguardante il progetto Gabčíkovo-Nugymaros, Corte Internazionale di Giustizia, 25 settembre 1997, <http://www.icj-cij.org/files/case-related/92/092-19970925-JUD-01-00-BI.pdf>.

[81] Nello specifico, chi, usando reti e computer in modo creativo, mette in discussione l'operato di governi e multinazionali organizzando petizioni online, virus benevoli, siti web di controinformazione è chiamato *hacktivist*, neologismo che unisce le parole *hacking* (l'insieme delle operazioni e delle tecniche usate per gli attacchi cibernetici) ed *activism*. Cfr. A. DI CORINTO, *Un dizionario hacker*, Manni Editori, S. Cesario di Lecce 2014, p. 54. Nel caso specifico il gruppo prende il nome di *Electronic Disturbance Theater*.

[82] Nello specifico si tratta di un *malware* detto *Floodnet*, dal funzionamento assai semplice. Utilizzando un programma di piccole dimensioni (*applet Java*) che invia ininterrottamente, ad un sito bersaglio, la richiesta di caricare una pagina ogni 6-7 secondi. Maggiore è il numero di computer attaccanti, esponenziallmente più alto è il numero di richieste: diecimila pc connessi simultaneamente generano circa centomila richieste al minuto. Il sito (o il *server*) non è un grado di gestire questa improvvisa mole di richieste e si blocca, negando il servizio. In merito vedasi M. DESERIIS, G. MARANO, *Net.art – l'arte della connessione,* Shake, Milano, 2008, pp. 150 – 151.

[83] Cfr. Dinniss, *Cyberwarfare*, cit., p. 108.

[84] Cfr. Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf>, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, dicembre 2013, <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf>, *Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali*, marzo 2017, <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf>. In merito si veda il DPCM 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali

[85] Altrimenti può adottare raccomandazioni, non giuridicamente vincolanti, o decisioni, obbligatorie.

[86] Dal *world wide web*, giacché sarebbe estremamente complesso vietare effettivamente la costituzione di reti locali.

[87] Ad esempio l'Organizzazione del Trattato del Nord Atlantico (NATO), il cui *casus foederis* è specificato all'art. 5 del Trattato istitutivo.