CYBER VADE MECUM

VIII parte

Raffaele Azzarone

L'articolo conclude il Cyber Vademecum finalizzato a illustrare i molteplici aspetti di un fenomeno la cui incontrollabile espansione in tutti gli ambiti della nostra vita quotidiana costituisce motivo di elevata preoccupazione. Nel nostro excursus ci siamo già soffermati su attori, malware, contromisure, normative nazionali e internazionali, evoluzione della minaccia e aspetti economici. In questa circostanza sono forniti cenni in materia di diritto internazionale. La mancanza di specifiche norme pone seri interrogativi nell'affrontare, in particolar modo, le tematiche delle Cyber war e della legittima reazione di uno Stato a un attacco informatico. Solo recentemente, da parte di Organismi internazionali sono state avanzate interpretazioni sulla possibilità di applicare il vigente diritto internazionale al dominio cibernetico.

1. L'autore ringrazia Stefano Mele per i preziosi contributi forniti in tema di legittima reazione di uno Stato a un attacco informatico.

CENNI DI DIRITTO INTERNAZIONALE

Cyber crime, cyber terrorism e cyber war costituiscono nuove tipologie di minacce portate alla società, balzate agli onori delle cronache negli ultimi due decenni, cogliendo impreparati, a livello mondiale, organi legislativi e magistrature a inquadrare tali forme criminose e di belligeranza nelle fattispecie previste dalla vigente normativa.
Le posizioni assunte dai vari Stati sono spesso differenti tra di loro a causa della diversa sensibilità con cui viene affrontato il contesto cibernetico, e delle dissimili motivazioni di carattere politico, sociale e culturale.
In tale quadro generale, ai giorni d'oggi si evidenziano sostanzialmente due antitetiche tendenze:

– ridurre e controllare l'utilizzo di internet da parte dei cittadini, in modo da garantire sia la sicurezza della rete che la stabilità dei regimi (come avviene, ad esempio, in Russia, Cina e Iran);
– assicurare la massima libertà di espressione in rete, pur adottando le necessarie strategie e procedure per salvaguardare la sicurezza informatica (un fermo atteggiamento in tal senso è stato recentemente assunto dall'Unione europea).

La mancanza di uno specifico codice di diritto internazionale pone seri interrogativi nell'affrontare le complesse tematiche delle cyber war e della reazione legittima di uno Stato a un attacco informatico, aspetti sui quali si ritiene opportuno soffermarci.
In assenza di una definizione unanimemente accettata di cyber war, è difficile inquadrare gli atti ostili perpetrati da attori statuali nel ciberspazio nelle tradizionali categorie di ius ad bellum, ius in bello, ius post bellum, tipiche dei conflitti armati; ovvero 'l'uso della forza' che costituisce il presupposto per l'esercizio del 'diritto naturale di autotutela individuale e collettiva' nel rispetto del principio di proporzionalità della difesa prevista dal diritto internazionale umanitario. Sotto tale aspetto, tuttavia, presso i Paesi tecnologicamente più avanzati si sta assistendo a un sostanziale cambiamento nell'approccio strategico alla problematica, consistente nel passaggio dai concetti di mera difesa allo sviluppo di capacità offensive di reazione. Peraltro, sulla base delle situazioni fino a oggi verificatesi, è spesso prevalso il ricorso a un confronto asimmetrico tra attaccante e attaccato, che si sostanzia nella conduzione di attacchi informatici da parte di singoli individui, organizzazioni terroristiche o mercenarie, rimasti per lo più anonimi, contro obiettivi istituzionali di uno Stato sovrano che, quindi, viene a trovarsi nella condizione di non poter reagire nei confronti dell'aggressore. Anche nei casi in cui si è avuto il fondato sospetto di una regia statuale dietro rilevanti attacchi cibernetici tesi a carpire segreti industriali o a interrompere la funzionalità delle istituzioni, ovvero a provocare danneggiamenti in complessi industriali, non è stato possibile dimostrarlo con atti inconfutabili.
Tale concreta difficoltà di identificare con assoluta certezza gli autori degli attacchi cyber porterebbe a vanificare la 'dottrina' della deterrenza fino a oggi adottata da alcune potenze militari per prevenire attacchi con armi convenzionali o nucleari, ovvero scoraggiare i potenziali nemici a attaccare, incutendo in loro il timore di devastanti ritorsioni.

Negli ultimi tempi, l'adozione di strategie deterrenti sta prendendo piede anche nel cyberspace. Si citano, a tal proposito: le comunicazioni del governo iraniano con le quali si autodefinisce come terza potenza cyber al mondo; la diffusione di notizie, da parte del governo Usa, circa il rafforzamento dell'Us Cyber Command che passerà, nel giro di pochi anni, da 900 a 4.000 cyber warrior, con spiccate capacità di attacco; gli attacchi informatici della Corea del Nord contro quella del Sud, definibili atti dimostrativi delle proprie capacità di cyber attack.
Alle difficoltà di identificazione degli autori degli attacchi informatici si aggiunge l'inadeguatezza della potestà degli Stati circoscritta ai confini territoriali, mentre la minaccia informatica supera tali limiti in quanto transnazionale. A titolo di esempio, si citano società private o gruppi di individui che, pur risiedendo in Stati insospettabili, sono disponibili a essere 'arruolati' per la realizzazione di operazioni mercenarie per conto di soggetti terzi; singoli hactivist residenti nelle nazioni più disparate che son pronti a coalizzarsi per sferrare attacchi alle istituzioni di un determinato Stato, per motivi ideologici, politici o religiosi.
Sussiste, inoltre, la difficoltà di individuare, sempre sul piano normativo, una valida corrispondenza tra un attacco armato e un cyber attack, che potrebbe essere determinata solo sulla base di una ponderata valutazione delle discendenti conseguenze, dato che non necessariamente un attacco cibernetico può comportare il verificarsi di evidenti danni fisici.
Gli attacchi cyber lanciati fino a oggi possono apparire poco distruttivi rispetto al grado di lesività e distruzione dei mezzi e dei metodi di combattimento tradizionali impiegati nei conflitti armati. Allo stato attuale, si può ritenere che l'utilizzo del cyberspace per finalità belliche sia limitato a un ruolo di facilitatore per attacchi cinetici convenzionali. Ciò nondimeno si prevedono, per un avvenire ormai prossimo, dati allarmanti e i potenziali attacchi informatici potrebbero causare conseguenze devastanti non inferiori ai danni realizzati dalle armi convenzionali. Difatti, quanto maggiore sarà l'ormai inarrestabile integrazione in rete delle infrastrutture critiche di uno Stato, tanto si aggraverà la potenziale vulnerabilità del sistema Paese.
A livello di diritto internazionale, perché possa realizzarsi l'auspicata armonizzazione delle norme e delle dottrine strategiche, occorrerà dare dapprima una risposta convincente alle principali questioni legali connesse ai limiti di operatività nello spazio cibernetico. In particolare:

– l'individuazione della normativa applicabile, travalicando la rete internet i confini nazionali;
– la disciplina del diritto 'all'uso della forza' attraverso cyber weapon e delle prerogative della difesa nei confronti di combattenti e non combattenti (popolazione civile);
– la riconducibilità di un cyber-attacco a un attacco armato;
– le modalità di reazione a un attacco cyber facendo uso di armi convenzionali;
– la determinazione del livello di proporzionalità della reazione rispetto all'attacco subito;
– il modus operandi per l'attribuzione giuridica certa della responsabilità di un attacco.

Per quanto noto, al momento gli Usa appaiono essere l'unico Paese ad aver strutturato una concreta strategia per far fronte a una cyber war, arrivando a teorizzare la possibilità di rispondere in maniera convenzionale, cioè con armi cinetiche, a un attacco informatico. La dottrina Usa sulle Cyber Space Operations prevede attività militari offensive verso obiettivi militari non solo al fine di degradare, danneggiare o distruggere l'accesso, il funzionamento o la disponibilità delle capacità di quest'ultimo ma anche per controllare o modificare le informazioni, i sistemi informatici o le reti dell'avversario.
In Cina, il 31 dicembre 2015, la Central Military Commission ha annunciato di aver completato una riforma sostanziale della People's Liberation Army, istituendo nuovi organismi tra i quali la Strategic Support Force, deputata, stando a alcune fonti, alle operazioni militari e di intelligence nel cyberspace, sia difensive che offensive, oltre che alle operazioni militari condotte nello spazio e all'Electronic Warfare.
Nello stesso periodo, anche la Gran Bretagna, il 23 novembre 2015, ha pubblicato la sua nuova Strategic Defense and Security Review nella quale si prevede, tra l'altro, che le proprie Forze armate conseguano capacità offensive avanzate nel dominio cyber.
In mancanza di norme specifiche sul piano del diritto internazionale in materia di cyber war, non si esclude la possibilità che possano identificarsi norme consuetudinarie potenzialmente applicabili, come previsto dalle convenzioni dell'Aia e di Ginevra (clausola Martens)[2], volte a colmare lacune nella codificazione del diritto internazionale.
Stante l'attuale vuoto normativo, presso il Nato Cooperative Cyber Defence Centre of Excellence, istituito nel 2008 a Tallinn (Estonia), è stato pubblicato nel marzo 2013, un manuale, frutto di uno sforzo teso a verificare se e come le vigenti normative internazionali, afferenti alla belligeranza, possano essere estese a questa nuova forma di guerra. Nel documento *Tallinn Manual on The International Law Applicable to Cyber Warfare* – più semplicemente noto come *The Tallinn Manual* – sono esaminate leggi, trattati, statuti, convenzioni, protocolli, regolamenti, dichiarazioni, decisioni, sentenze, testi, articoli e studi internazionali e ne viene valutata l'applicabilità alla governance del cyber warfare. In termini generali, il documento abbraccia sia lo jus ad bellum, ovvero le norme internazionali che governano il ricorso alla forza da parte delle nazioni come strumento delle loro politiche nazionali, sia lo jus in bello, ovvero le norme internazionali che regolano la condotta nei conflitti armati. Le altre attività svolte nel ciberspazio, come quelle relative al cyber crime, non vengono affrontate. Particolare enfasi è posta sulle operazioni cyber-to-cyber, in senso assolutamente restrittivo, mentre non prende in esame gli ancor più complessi aspetti legali connessi a operazioni kinetic-to-cyber, quali attacchi aerei contro centri di controllo cibernetici oppure operazioni Electronic Warfare-to-cyber.

2. Si deve al diplomatico e giurista estone Fyodor Fyodorovich Martens (1845-1909) la clausola secondo la quale, nell'attesa di una completa codificazione del diritto in materia di conflitti armati, nei casi non compresi nelle disposizioni adottate, le popolazioni e i combattenti sono protetti dai diritti in uso presso i Paesi civili, dai principi umanitari e da quelli dettati dalla coscienza pubblica.

Il manuale è articolato in n. 95 regole (R*ule*) che abbracciano i seguenti aspetti:
- Stati e ciberspazio (sovranità, giurisdizione e controllo, responsabilità);
- uso della forza (proibizione dell'uso della forza, autodifesa, azioni delle organizzazioni internazionali);
- leggi dei conflitti armati (applicabilità delle leggi, limitazioni geografiche, responsabilità criminali di comandanti e superiori ecc.);
- condotta delle ostilità (conflitti armati, cyber-attacchi, mezzi e metodi di attacco, condotta degli attacchi, uso improprio, spionaggio, assedi, zone territoriali ecc.);
- persone, oggetti e attività particolari (personale, infrastrutture e mezzi dell'Onu, prigionieri, bambini, giornalisti, installazioni particolari – quali dighe e centrali;
- nucleari, sopravvivenza della popolazione civile, proprietà culturali, ambiente naturale, comunicazioni e archivi, punizioni collettive, assistenza umanitaria);
- occupazione del territorio (rispetto delle persone, ordine pubblico e sicurezza, confisca di beni);
- neutralità (protezione delle cyber-infrastrutture neutrali, cyber operation nei territori neutrali ecc.).

Le regole sono corredate da commenti, sia per orientare la valutazione della loro applicabilità su base legale sia per spiegarne il contenuto informativo e indirizzarle alle loro pratiche implicazioni nel contesto cyber, esponendo differenti punti di vista e interpretazioni. Nel M*anuale* vengono sistematicamente ripresi i concetti che regolano il diritto internazionale umanitario, focalizzando l'obbligo di evitare danni inutili con azioni di cyber warfare, che devono essere rivolte solo verso strutture e membri delle Forze armate o assimilabili, ponendo l'accento sulla netta separazione tra i combattenti e la popolazione civile, la quale non deve essere oggetto di attacchi.
È utile evidenziare che il documento non rappresenta il punto di vista ufficiale né della Nato né dello stesso centro di eccellenza di Tallinn, bensì solo quello degli esperti. In ogni modo, esso costituisce un validissimo punto di riferimento per quanto riguarda le considerazioni concernenti l'applicabilità alla cyber war del quadro normativo che regola i conflitti internazionali.
I pareri, al riguardo, non sono sempre concordi, spaziando da quelli assolutamente favorevoli all'estensione delle leggi che regolano i conflitti armati, secondo le linee dettate dai pronunciamenti della Corte di Giustizia Internazionale, che fanno riferimento a «tutti gli usi della forza senza riguardo dell'arma utilizzata», a pareri di discordanza basati sul principio che «ogni azione non espressamente vietata dalle leggi internazionali è implicitamente ammessa». A render ancor più complessa l'interpretazione in materia viene anche fatto rilevare come la mancanza presso gli Stati sovrani di specifiche leggi mirate alla gestione dei conflitti nel cyberspace non li esoneri dagli obblighi di rispettare le vigenti norme internazionali anche nel corso di operazioni condotte con strumenti informatici.

In tal senso, nel 2015, il Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security dell'Onu ha convenuto, tra l'altro, che gli Stati:

– esercitano la loro giurisdizione sulle infrastrutture informatiche situate sul loro territorio;
– nell'utilizzo degli strumenti informatici devono rispettare i vincoli legali internazionali esistenti, tra i quali quello dell'inviolabilità delle sovranità territoriali altrui;
– non possono commettere atti internazionalmente illeciti mediante strumenti informatici, neanche attraverso deleghe a terze parti, e devono assicurarsi che il loro territorio non venga utilizzato da attori non statali al fine di commettere tali atti;
– in sede di conflitto, le accuse relative all'organizzazione o al supporto di atti illeciti nel ciberspazio devono essere debitamente comprovate.

L'assoggettabilità delle operazioni informatiche alle norme contenute nella Carta delle Nazioni Unite[3] riguardanti lo ius ad bellum porta ad alcune considerazioni e valutazioni. In particolare, l'art. 2 (4): «Tutti gli Stati membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza... » può ritenersi applicabile e essenziale alle operazioni informatiche per garantire un ambiente digitale aperto, sicuro pacifico e accessibile. Tuttavia, dall'analisi del testo, si evince che per poterlo invocare, in caso di minacce e/o attacchi cyber, è necessario che ricorrano le seguenti condizioni:

– la condotta aggressiva deve essere imputabile a uno Stato (e non a individui o gruppi armati);
– l'attacco informatico deve poter essere classificato come un 'utilizzo della forza' (eventualmente basandosi sul criterio della gravità degli effetti che seguono un attacco, paragonandoli a quelli di un attacco armato);
– l'attività malevola deve avvenire nell'ambito delle relazioni internazionali (cioè rivolta da uno Stato verso un altro Stato membro).

Tra queste, quella che presenta le maggiori difficoltà interpretative è la prima, ovvero la possibilità di poter indiscutibilmente attribuire la responsabilità di una determinata condotta a uno specifico Stato. In tal senso, l'Assemblea Generale dell'Onu ha approvato una serie di criteri per giungere all'attestazione di tale responsabilità, molti dei quali possono ritenersi mutuabili anche nel cyberspace. In primo luogo viene stabilito che il comportamento di un organo statale – a prescindere dalla sua natura, funzione e posizione nella struttura organizzativa dello Stato cui appartiene – sarà considerato come atto dello Stato stesso, ai sensi del diritto internazionale.

3. Firmata da 51 Stati membri originari e adottata, per acclamazione, il 26 giugno 1945 a San Francisco

Ciò può avvenire anche nei casi in cui l'azione malevola non sia perpetrata da un organo di Stato, bensì da un soggetto (ad esempio parastatale, pubblico, privato ecc.) abilitato a esercitare prerogative di governo.

Infine, uno Stato, pur non rientrando nella casistica precedente, può ritenersi responsabile di un'azione qualora, ancorché non ne sia l'artefice, ne abbia avuto conoscenza e l'abbia adottata come propria o, comunque, non abbia adottato le necessarie misure preventive.

Per quanto concerne la possibilità di una legittima reazione nel cyberspace da parte di uno Stato le cui infrastrutture vitali siano state oggetto di attacco informatico (il cosiddetto H*acking back*), è possibile far riferimento all'art. 51 della citata Carta delle Nazioni Unite: «Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale... » che, pertanto, sancisce che la legittima difesa è un diritto innato dello Stato e, in tal caso, si configura come un'eccezione al divieto dell'uso della forza.

Nel merito, la Corte Internazionale di Giustizia ha stabilito che il suddetto articolo si applica a «qualsiasi uso della forza» indipendentemente dal mezzo utilizzato; conseguentemente, è leggittimo ritenere che la sua validità si estenda anche nell'ambito informatico ove, un 'attacco armato' potrebbe in realtà consistere in un cyber attack volto a colpire le vitali e fondamentali infrastrutture (governative, economiche, sociali, politiche) nazionali, anche in assenza di riscontrabili danni fisici. Ovviamente, l'adozione di contromisure cibernetiche o cinetiche, quale forma di legittima reazione, non può prescindere dai seguenti irrinunciabili presupposti: necessità dell'uso della forza, proporzionalità della risposta e immediatezza della reazione.