La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale

Edoardo Corsi

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

Ottobre 2018

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and International Relations Studies

La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale

Edoardo Corsi

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Ottobre 2018

Riguardo all'autore

Edoardo Corsi Ha conseguito una laurea specialistica in "European and International Studies" presso l'Università di Trento e la Scuola Sant'Anna di Pisa, con una tesi dal titolo" *Jus ad Bellum and the Challenge of Cyber Operations: Old Rules for New Weapons*?". Giornalista pubblicista, negli anni ha maturato alcune esperienze nel settore della comunicazione istituzionale: in particolare, nel 2016, ha ricoperto il ruolo di Communications Advisor presso l'Ufficio Stampa del Ministero degli Affari Esteri e della Cooperazione Internazionale. Per il Centro, si interessa principalmente di cyber security, diritto internazionale e delle relazioni, spesso complesse, tra questi due ambiti.

La Nato a difesa del cyber spazio? Il dilemma del diritto internazionale [1]

Nell'alleanza atlantica sembra emergere la convinzione che l'attacco cibernetico a un paese membro possa innescare il meccanismo di difesa collettiva. In realtà, nella zona grigia del cyber spazio, la cornice giuridica in cui collocare tale risposta risulta poco chiara. Vediamo cosa dice il diritto internazionale vigente

La Nato può intervenire a difesa di un Paese membro colpito da un attacco cyber da parte di un Paese straniero? La questione è avvolta nella nebbia, al momento.

Il problema è che stabilire con certezza il perimetro giuridico e l'applicabilità del meccanismo di difesa collettiva del cyber spazio nel contesto dell'attuale diritto internazionale è un esercizio legale complesso. E questo nonostante il riconoscimento del dominio cibernetico quale nuovo dominio operativo da difendere alla stregua di terra, mare, aria e spazio extra-atmosferico. Il tema trova di continuo riscontri nell'attualità, come dimostra la discussione in questi giorni all'interno del Consiglio UE, dove avanza la proposta di sanzionare i Paesi da cui proviene un attacco cyber.

La nascita di un "*Cyber Operations Center*" Nato

Sullo sfondo del dibattito sul ruolo degli Stati Uniti nell'Alleanza Atlantica, il Summit di Bruxelles dello scorso 11 luglio ha segnato un ulteriore, importante rafforzamento delle capacità cibernetiche dell'Organizzazione del Trattato dell'Atlantico del Nord (Nato). Il

[1] La seguente analisi è apparsa su Agenda Digitale il giorno 22 ottobre 2018 ed è reperibile al seguente link: https://www.agendadigitale.eu/sicurezza/la-nato-a-difesa-del-cyber-spazio-il-dilemma-nel-diritto-internazionale/ .

Summit ha infatti stabilito la nascita di un **"***Cyber Operations Center"* con l'obiettivo coordinare le operazioni degli alleati nel dominio cibernetico. Non solo, tra i Paesi membri sembra essersi consolidata la convinzione per cui, in determinate circostanze, un attacco cibernetico contro uno di essi potrebbe costituire un "attacco armato" ai sensi del diritto internazionale, innescando così il meccanismo di difesa collettiva previsto dall'articolo 5 del Trattato del 1949. Un atteggiamento che testimonia la crescente pericolosità della minaccia cyber e rischia di trasformare l'arena digitale in un terreno di confronto tra Stati.

Ad oggi, però, la cornice giuridica internazionale in cui collocare tale, eventuale conflitto risulta poco chiara. Le obiettive difficoltà nell'applicazione dell'esistente corpus normativo alle operazioni cibernetiche condotte dagli Stati, unite all'assenza di una convenzione *ad hoc,* rendono il cyber spazio una dimensione apparentemente senza regole. Un moderno "Wild West" in cui valutare le condizioni e modalità di applicazione del *casus foederis* della Nato presenta alcune problematiche.

Il cyber spazio e la quinta dimensione della conflittualità

Nelle società moderne, il funzionamento di numerose "infrastrutture critiche" – comprese quelle militari – si basa sull'utilizzo di sistemi informativi che agiscono su reti interconnesse. La protezione di queste infrastrutture nel cyber spazio pone quindi complesse – e per certi versi inedite – sfide alla sicurezza degli Stati e la minaccia cyber rappresenta oggi uno dei temi caldi dell'agenda internazionale. I cyber attacchi possono essere definiti come attacchi perpetrati da attori privati o statali per mezzo di armi cibernetiche e informatiche. Secondo

alcune stime, solo nel 2017 se ne sono registrati più di 160.000, con danni pari a circa 500 miliardi di dollari[2]. La facilità di accesso al dominio cibernetico e la sostanziale impunità garantita dal Web rendono infatti particolarmente complesso l'esercizio della sovranità statale in questo nuovo dominio. Non solo: il basso costo delle armi cibernetiche, soprattutto se comparato con quelle tradizionali, offre agli attori non statali la possibilità di esercitare un'influenza rilevante. Per questi motivi, la cyber security[3] ha attirato l'attenzione di numerose organizzazioni internazionali, compresa la Nato.

Nel 2016, nel corso del Summit di Varsavia, i membri dell'Alleanza hanno riconosciuto nel cyberspazio un nuovo dominio operativo da difendere alla stregua di terra, mare, aria e spazio extra-atmosferico[4]. Una "quinta dimensione" della conflittualità, dunque, in cui coordinare l'azione dei Paesi membri ed investire risorse. Al di là delle questioni terminologiche, tuttavia, il nuovo atteggiamento della Nato sembra rispondere ad una chiara tendenza: la crescente minaccia cibernetica proveniente dalla Russia. Dal "Distributed Denial of Service" (Ddos) lanciato contro l'Estonia nel 2007 [5]al più recente attacco diretto contro una centrale elettrica ucraina nel 2015, in numerose occasioni il Governo russo è stato accusato di aver orchestrato, o quanto meno favorito, attacchi cibernetici diretti contro alcuni Stati occidentali. Sebbene la responsabilità di Mosca non sia mai stata provata definitivamente, secondo alcuni osservatori il Cremlino utilizzerebbe questo nuovo tipo di arma per destabilizzare

[2] Tara Seals, *Cyberattacks Doubled in 2017, 160,000 cyberattacks*, https://www.infosecurity-magazine.com/news/cyberattacks-doubled-in-2017
[3] Agenda Digitale, *Tutto su Cyber Security, disponibile* al seguente link https://www.agendadigitale.eu/tag/cyber-security/
[4] NATO Summit Warsaw 2016, http://www.nato.int/cps/en/natohq/events_132023.html
[5] Micheal N. Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts', pag. 151 in *Proceedings of a Workshop on Deterring Cyberattacks: Information Strategies and Developing Options for U.S Policy,* 2010.

l'unità dell'Alleanza e perseguire obiettivi politici difficilmente raggiungibili con armi tradizionali. Proprio a seguito di uno di questi episodi, il Segretario Generale della Nato J. Stoltenberg ha recentemente dichiarato che un attacco cibernetico contro un Paese membro potrebbe configurarsi come un "attacco armato"[4]. Detto in altri termini: secondo Stoltenberg un cyber-attacco potrebbe innescare il meccanismo di difesa collettiva previsto dall'articolo 5 della Nato, consentendo così di intervenire – con mezzi cibernetici o tradizionali – a soccorso dello Stato vittima. Per testare la validità di questo approccio occorre dunque chiedersi se ed in quali circostanze un attacco cibernetico può essere considerato un attacco armato ai sensi del diritto internazionale vigente.

Le *cyber-operations* e il diritto internazionale vigente

Come ricordato, e nonostante alcuni importanti tentativi di codificazione[6], ad oggi non esiste una convenzione internazionale volta a regolamentare le operazioni cibernetiche condotte dagli Stati**.** Di conseguenza, sulla base dell'errato assunto per cui in ambito internazionale quanto non espressamente vietato sarebbe permesso, si potrebbe supporre la facoltà degli Stati di condurre queste operazioni senza alcuna restrizione. In realtà non è così: attraverso un'interpretazione dinamica ed evolutiva del presente corpus normativo internazionale, sia esso di natura consuetudinaria o pattizia, è infatti possibile estendere alle operazioni cibernetiche delle norme

[6] Tra questi, particolare importanza ricopre il "Tallinn Manual on the International Law Applicable to Cyber Warfare", pubblicato dal NATO COOPERATIVE CYBER DEFENCE OF EXCELLENCE (CCDCOE) nel 2013. Pur caratterizzato da una natura non vincolante, il Tallinn Manual, nelle sue due versioni, è oggi uno dei più importanti tentativi volti a testare l'applicabilità del diritto internazionale vigente alle cyber operations. Il manuale è disponibile sul sito del CCDCOE https://ccdcoe.org/tallinn-manual.html

che, per chiare ragioni storiche, non le prevedono espressamente. Tale approccio trova ampio riscontro nella prassi e nella dottrina degli Stati ed acquisisce una particolare rilevanza con riguardo a due norme contenute nello Statuto delle Nazioni Unite del 1945: il divieto dell'uso della forza nelle relazioni internazionali (Art. 2.4) e il diritto alla legittima difesa in risposta ad un attacco armato (Art. 51). In un importante parere del 1996 sulla *Liceità della minaccia o dell'uso di armi nucleari*[7], la Corte Internazionale di Giustizia ha infatti affermato la validità di questi due principi indipendentemente dall'arma utilizzata[8]. Del resto, la sfida tra codificazione normativa ed evoluzione delle tecniche e mezzi di combattimento non è una prerogativa dell'era cyber: nonostante un uso massiccio durante la Prima Guerra mondiale, ad esempio, il Protocollo di Ginevra per la proibizione delle armi batteriologiche è entrato in vigore solo nel 1928.

Con riferimento alla Nato, l'articolo 51 della Carta Onu prevede che uno Stato vittima di un attacco armato possa esercitare un *droit naturel* alla "autotutela individuale o collettiva"[9]. Tale disposizione è traslata nel Trattato del Patto Atlantico del 1949, che ne esalta e specifica la declinazione "collettiva": ai sensi dell'articolo 5, infatti, un attacco armato contro un Paese Membro della Alleanza costituisce un attacco verso tutti gli altri e chiama quindi ciascuno di essi ad assistere l'aggredito[10]. Ma se né la carta Onu né il Patto Atlantico forniscono una definizione chiara del termine "attacco armato", la dottrina è quasi unanime nel ritenere solo gli usi della forza più gravi – bombardamenti,

[7] Corte Internazionale di Giustizia, "Legality of the Threat or Use of Nuclear Weapons", Advisory Opinion, Rep., 1996, para. 86 e ss.
[8] Questo ragionamento trova supporto anche nella cosiddetta "clausola Martens", contenuta nel preambolo della IV convenzione dell'Aja e nelle maggiori convenzioni internazionale e di diritto umanitario.
[9] Articolo 51, Carta delle Nazioni Unite (in lingua inglese) http://www.un.org/en/sections/un-charter/chapter-vii/index.html
[10] Articolo 5, Nato in lingua inglese https://www.nato.int/cps/en/natolive/official_texts_17120.htm

occupazioni militari etc. – in grado di giustificare il diritto alla legittima difesa[11]. A titolo di esempio, l'articolo 5 della Nato è stato "attivato" per la prima – e finora unica – volta dopo l'attentato dell'11 settembre 2001 contro gli Stati Uniti.

Tradotto in "cyber termini", ciò significa che, in teoria, solo un attacco cibernetico che provoca danni fisici e perdita di vite umane potrebbe configurarsi come un attacco armato e giustificare una risposta individuale o collettiva, non necessariamente con mezzi cibernetici. Tale interpretazione (detta "*effect-based approach*") ha trovato il supporto di alcuni Membri dell'Alleanza[12]. Su posizioni diverse si collocano invece Cina e Russia, contrarie ad una possibile militarizzazione del cyber spazio.

I problemi di attribuzione nel cyber spazio

Se, in punta di diritto, l'accettazione generale di un'analogia tra armi cibernetiche e tradizionali potrebbe trovare il supporto della Comunità internazionale, due aspetti complicano l'applicazione pratica di questo paradigma.

In primo luogo, e con l'eccezione dell'episodio avvenuto durante il conflitto russo-georgiano del 2008[13], la maggior parte dei cyber attacchi registrati finora non ha prodotto danni fisici e materiali della gravità

[11] Questa affermazione è corroborata dalla giurisprudenza internazionale. Si veda, in particolare: Corte Internazionale di Giustizia, sentenza *Attività militari e paramilitari in e contro il Nicaragua (Nicaragua vs. United States),*1986, par. 191; Risoluzione Assemblea Generale Nazioni Unite GA/RES/3314 (1974)

[12] Secondo la posizione ufficiale dell'amministrazione statunitense, ad esempio, in alcune circostanze gli attacchi cibernetici possono costituire un uso della forza secondo la Carta Onu. In particolare, stando a quanto dichiarato dall'allora Consigliere Legale del Dipartimento di Stato Harold Koh nel 2012, nel valutare i singoli casi è necessario considerare i fattori che riguardano la perdita di vite umane, il contesto dell'evento, gli obiettivi, le condizioni spaziali, gli effetti e l'intento dell'attacco stesso.

[13]In questo caso, il presunto attacco cibernetico lanciato da Mosca avrebbe superato la soglia "fissata" dall'articolo 51 non a causa agli effetti provocati ma poiché parte di una più generale operazione militare condotta con mezzi tradizionali, che ha portato all'occupazione russa dell'Ossezia del Sud (2008).

"richiesta" dall'articolo 51. Dal già citato attacco contro Estonia del 2007 all'assalto hacker avvenuto durante la recente crisi del Golfo tra Qatar e Emirati Arabi Uniti (2017)[14], queste operazioni sono risultate principalmente nella perdita di dati sensibili ed in interruzioni temporanee della connessione, effetti difficilmente valutabili attraverso le lenti tradizionali. In altre parole, pur violando chiaramente altre norme di diritto internazionale, ad oggi gli effetti provocati dalle armi cibernetiche sembrano non presentare le caratteristiche necessarie per attivare il *casus foederis* del Patto Atlantico.

In secondo luogo, se l'assenza di barriere fisiche rende il cyber-spazio il terreno ideale in cui "scagliare la pietra", l'anonimato garantito dal Web ne fa anche il contesto perfetto in cui "nascondere la mano". Attraverso una serie di tecniche, come ad esempio l'*IP spoofing*, in rete un utente può facilmente celare la propria identità. Ma se individuare chi si nasconde dietro un attacco cibernetico è essenzialmente una questione tecnica, nota come "identificazione", per il diritto internazionale l'attribuzione è quel processo legale necessario a stabilire se e in che circostanze la condotta di un individuo può essere attribuita ad uno Stato. In altre parole, l'attribuzione è un esercizio giuridico essenziale per distinguere tra un mero atto criminale e un atto di guerra nel cyber spazio. Ciò detto, ad oggi non è stato possibile attribuire con certezza la responsabilità di un attacco cibernetico ad uno Stato**.** Questo è dovuto da un lato alla natura stessa del Web, che garantisce ai corsari della rete una sostanziale impunità, dall'altro alla tendenza degli Stati a non denunciare tali eventi, probabilmente al fine di celare eventuali falle nei propri sistemi informatici.

[14] Ali Younes, Al Jazeera Online, *"Qatar says cyberattack originated from the UAE".* Link articolo https://www.aljazeera.com/news/2017/07/qatar-sheds-light-cyberattack-official-media-170720151344996.html

In conclusione, nonostante le dichiarazioni dei vertici dell'Alleanza, stabilire con certezza il perimetro giuridico e l'applicabilità del meccanismo di difesa collettiva della Nato in questo contesto è un esercizio legale complesso. Ciò non dipende tanto dall'assenza di una cornice normativa applicabile, quanto alle difficoltà nel considerare tutte le specificità della nuova minaccia cibernetica. Caratteristiche che fanno del cyber spazio una "zona grigia" che se favorisce gli assalitori, rischia altresì di innescare pericolose escalation.

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html