Center for Cyber Security and International Relations Studies

LA VISIONE FRANCESE SUL DIRITTO INTERNAZIONALE NEL CYBERSPACE

Edoardo Sarti
Center for Cyber Security and International Relations

Il 9 settembre, giorno in cui sono iniziati a New York i lavori dell'OEWG delle Nazioni Unite sugli sviluppi nel campo dell'informazione e delle telecomunicazioni, il Ministero della Difesa francese ha pubblicato un documento in cui espone la propria posizione in merito all'applicabilità del diritto internazionale nel cyberspazio. Il documento, intitolato "*Droit International appliqué aux opérations dans le cyberspace*"[1], è composto da due parti: la prima si concentra sulle operazioni cibernetiche condotte in tempo di pace contro la Francia, mentre la seconda sull'applicabilità del diritto internazionale alle operazioni condotte nel cyberspazio in tempo di guerra. La Francia, con questo documento vuole riaffermare l'idea, condivisa con gli altri paesi europei e con gli Stati Uniti[2], secondo cui il cyberspazio deve essere regolato dal diritto internazionale. Facendo ciò mostra inoltre il proprio desiderio di ricoprire un ruolo di primo piano nelle future negoziazioni su questo tema.

LE OPERAZIONI CIBERNETICHE CONDOTTE IN TEMPO DI PACE CONTRO LA FRANCIA

La prima parte del documento si apre citando i lavori del GGE sugli sviluppi nel campo dell'informazione e delle telecomunicazioni, il cui risultato più importante è stato quello di aver affermato che gli Stati devono rispettare anche nel cyberspazio il diritto internazionale e la Carta delle Nazioni Unite, in particolare, i princìpi di uguaglianza sovrana tra gli Stati, di risoluzione pacifica delle controversie e l'astensione dal ricorrere alla minaccia o all'uso della forza contro l'integrità o l'indipendenza politica di qualsiasi Stato. Questi princìpi, uniti alla dichiarazione dell'esercizio della propria sovranità sui sistemi d'informazione situati sul suo territorio, permette alla Francia di affermare che "*qualsiasi attacco informatico contro i sistemi digitali francesi o qualsiasi produzione di effetti sul territorio francese tramite mezzi digitali da parte di un organo statale, una persona o un'entità che esercita prerogative di poteri pubblici o da una persona o da persone che agiscono su istruzioni o direttive o sotto il controllo di uno Stato costituisce una violazione di sovranità*" e che tali violazioni della sovranità nazionale possono comportare una risposta francese.

Come si evince da questo primo passaggio, la Francia fonda la legittimità della propria risposta

[1] Ministère des Armés, *Droit International appliqué aux opérations dans le cyberspace*, 9 settembre 2019.

[2] U.S. Department of State, *Joint Statement on Advancing Responsible State Behaviour in Cyberspace*, 23 settembre 2019

sull'applicazione nel cyberspazio di un principio fondamentale del diritto internazionale: la sovranità. Questa asserzione rappresenta da un lato un elemento di continuità rispetto al *Manuale di Tallinn* e dall'altro uno scostamento dalle posizioni di UK[3] e USA, molto più "freddi" in merito all'applicazione di tale principio nel cyberspazio.

In base all'art. 51 della Carta delle Nazioni Unite che regola l'esercizio della legittima difesa, la Francia si riserva la possibilità di rispondere agli attacchi informatici in violazione dei princìpi già citati. La decisione di un'eventuale risposta, e i mezzi con cui essa avviene (informatici o classici), dipendono dal tipo di attacco subìto: infatti, solo gli attacchi, i cui effetti e la cui ampiezza "*raggiungano una certa gravità*" e che "*siano paragonabili a quelli di un impiego della forza fisica*", possono essere qualificati come aggressione armata. Indubbiamente sono ascrivibili a tale categoria quegli attacchi cibernetici che causano la perdita di vite umane o danni fisici sostanziali. Tuttavia nel documento si legge che anche un attacco che non causa effetti fisici può essere qualificato come ricorso alla forza: "*In assenza di danni fisici, una cyber-operazione può essere considerata un ricorso alla forza secondo diversi criteri, in particolare le circostanze che prevalgono al momento dell'operazione, quali l'origine dell'operazione e la natura dell'istigatore (il suo carattere militare o meno), il grado di intrusione, gli effetti provocati o ricercati dall'operazione o ancora la natura del bersaglio*". Inoltre qualora i cyber-attacchi non raggiungano isolatamente la suddetta soglia, essi possono essere definiti come atti di aggressione se l'accumulo dei loro effetti raggiunga una soglia di gravità sufficiente o se contribuiscono ad operazioni condotte nel campo di azione fisica che costituiscono un'aggressione. Infine per essere definito come aggressione armata, un attacco cibernetico deve essere perpetrato, direttamente o indirettamente, da uno Stato. In tutti questi casi, la Francia è legittimata a rispondere, "*con mezzi informatici o classici, nel rispetto dei princìpi di necessità e di proporzionalità*". Il documento prevede la possibilità della legittima difesa preventiva rispetto a un cyber-attacco "*non ancora scatenato, ma sul punto di esserlo, in modo imminente e certo, purché l'impatto potenziale di tale aggressione sia sufficientemente grave*".

Tuttavia, è proprio sul concetto di legittima difesa che il documento introduce due importanti novità. La prima novità risiede nell'affermare che le contromisure collettive, in risposta a un cyber-attacco, non sono autorizzate, e che dunque, la Francia non le attuerà in risposta ad una violazione dei diritti di uno Stato terzo. Questa affermazione si pone in netto contrasto con le recenti dichiarazioni del Segretario Generale[4] della NATO, per cui un attacco cibernetico contro uno Stato

[3] https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[4] Stoltenberg J., *NATO will defend itself*, Prospect Magazine, 27 agosto 2019.

alleato innescherebbe una risposta collettiva sulla base dell'art. 5. La seconda novità è rappresentata dalla decisione di discostarsi dalla posizione del *Manuale di Tallinn* che autorizza uno Stato vittima di un cyber-attacco dal territorio di uno Stato terzo da parte di attori non statali a fare uso della legittima difesa contro tale Stato. Nella visione francese, invece, la violazione da parte di uno Stato del principio di dovuta diligenza comporterà l'attivazione di meccanismi a livello politico-diplomatico fino all'attuazione di contromisure o al deferimento al Consiglio di Sicurezza delle Nazioni Unite.

La possibilità di rispondere a un cyber-attacco e di porre in essere le contromisure ritenute più adeguate, dipende dalla capacità del paese che subisce l'attacco di individuare il responsabile. Le caratteristiche proprie del cyberspazio rendono infatti problematica l'attribuzione di intrusioni o attacchi informatici. Tuttavia il documento afferma che, dopo l'individuazione di un attacco, la Francia attua tutte le operazioni necessarie, di carattere principalmente tecnico[5], per la determinazione dell'autore dell'attacco. Inoltre, nel documento si legge che spetta alla Francia la decisione di attribuire pubblicamente l'attacco e di rendere noti gli elementi di prova su cui si fonda la legittimità dell'attribuzione. Dal momento che il diritto internazionale non obbliga gli Stati a rendere pubblici tali dettagli, "*la mancata attribuzione pubblica non costituisce un ostacolo definitivo all'applicazione del diritto internazionale, in particolare all'attuazione del diritto di replica offerto agli Stati*".

IL DIRITTO INTERNAZIONALE APPLICABILE ALLE CYBER-OPERAZIONI CONDOTTE IN UN CONFLITTO ARMATO

La seconda parte del documento si apre affermando in modo chiaro che, essendo il cyberspazio uno spazio di confronto come gli spazi terrestri, marittimi, aerei o lo spazio extra-atmosferico, le azioni offensive condotte in tale dominio devono essere subordinate al rispetto del Diritto Internazionale Umanitario (DIU). Perciò qualsiasi condotta offensiva cibernetica deve essere realizzata nel rispetto dei princìpi che disciplinano la condotta dei conflitti, siano essi conflitti armati internazionali (ostilità tra due Stati) o non internazionali (conflitto prolungato tra forza governative e gruppi armati). Il DIU deve essere applicato non solo nei conflitti in cui gli attacchi cibernetici siano usati come mezzo di supporto ma anche in caso di conflitto armato condotto esclusivamente nel cyberspazio, a condizione che tali operazioni raggiungano la soglia di violenza richiesta. Dunque "*ogni cyber-operazione condotta nel contesto di un conflitto armato in*

[5] "L'attribuzione si basa principalmente, ma non esclusivamente, su elementi tecnici raccolti durante le indagini condotte sull'attacco informatico, in particolare la determinazione dell'infrastruttura di attacco e di transito dell'operazione cibernetica, e la loro localizzazione, l'identificazione dei metodi operativi avversari, la cronologia generale delle attività dell'autore, l'ampiezza e la gravità dell'incidente e del perimetro compromesso, o ancora gli effetti ricercati dall'aggressore".

relazione ad esso e costitutiva di un atto di violenza, offensivo o difensivo, contro un'altra parte del conflitto è un attacco ai sensi dell'art. 49 del PA I alle Convenzioni di Ginevra". La Francia, a differenza di quanto sostenuto dal gruppo di esperti che hanno realizzato il *Manuale di Tallinn*, non ritiene necessaria l'esistenza di effetti materiali per qualificare un'operazione informatica come un attacco; è sufficiente infatti che tale operazione impedisca il normale funzionamento dei sistemi o strumenti colpiti. Ad esempio il documento cita la distruzione delle capacità informatiche offensive o convenzionali militari avversarie attraverso operazioni cibernetiche; nella visione francese si è in presenza di un attacco ai sensi del DIU.

Dal momento che il DIU si applica alle operazioni cibernetiche condotte in un conflitto armato, coloro che conducono tali operazioni devono rispettare i princìpi di distinzione, proporzionalità e precauzione che disciplinano la condotta delle ostilità. La posizione francese non si limita tuttavia ad affermare l'obbligo da parte degli Stati di rispettare questi princìpi ma prevede anche la possibilità che la "*violazione di questi principi in seguito a un'operazione cibernetica possa costituire un crimine di guerra ai sensi dello Statuto di Roma*". Lo Stato, o gli attori non statali, che prendono parte ad un conflitto e conducono operazioni offensive nel cyberspazio devono astenersi dal colpire obiettivi civili o dal condurre cyber-attacchi nel caso non siano in grado di limitare gli effetti (principio di distinzione)[6]. Inoltre, sulla base degli altri due princìpi, "*se la neutralizzazione o la distruzione di un obiettivo militare attraverso attacchi cibernetici rischia comunque di provocare danni civili, questi non devono superare il beneficio militare diretto e concreto atteso*". Per questo motivo l'uso di malware che si riproducono volontariamente e si diffondono senza controllo, e quindi in grado di causare danni significativi a sistemi o infrastrutture civili critici, è contrario al DIH.

PERCHÉ IL DOCUMENTO FRANCESE SULL'APPLICAZIONE DEL DIRITTO INTERNAZIONALE NEL CYBERSPAZIO È IMPORTANTE?

Il documento francese "*Droit International appliqué aux opérations dans le cyberspace*" ricopre senza dubbio una notevole importanza nelle attuali discussioni sugli sviluppi nel campo dell'informazione e delle telecomunicazioni nell'ambito della sicurezza internazionale. Se infatti i vari GGE hanno permesso di statuire l'applicabilità del diritto internazionale nel cyberspazio, le discussioni su come esso avvenga si sono arenate. Il 2019 si annuncia un anno

[6] Il documento francese definisce anche le caratteristiche che permettono di identificare un obiettivo come militare: esso contribuisce all'azione militare per natura (posti informatici delle forze armate, reti di comando militare, di localizzazione, di sorveglianza etc.), ubicazione (luoghi da cui vengono effettuati gli attacchi informatici), destinazione (uso prevedibile delle reti informatiche a fini militari), o uso (uso di una parte della rete a fini militari), e se la sua distruzione totale o parziale, la cattura o neutralizzazione conferiscono un preciso vantaggio militare.

importante, visto l'inizio dell'OEWG delle Nazioni Unite e del sesto GGE, che hanno il compito di regolare il comportamento degli Stati nel cyberspazio. Il documento francese, attraverso una precisa analisi di come il diritto internazionale debba essere applicato alle operazioni condotte nel cyberspazio in tempo di pace e di guerra e senza il timore di discostarsi dalle posizioni di alcuni alleati (come UK e USA sul tema della sovranità o sull'attivazione dell'art 5 NATO) o da quelle degli esperti che hanno realizzato il *Manuale di Tallinn*, si propone come modello per plasmare le visioni degli altri paesi su questo tema e offre una solida e coerente base per le future discussioni nei forum internazionali.

Tuttavia l'importanza di questa dichiarazione non risiede solo in questo ma anche nel voler, da un lato, evidenziare le capacità tecniche di cui la Francia dispone (come quelle utili per l'attribuzione) e, dall'altro, comunicare con decisione le linee guida della propria azione in questo dominio, affermando che gli attacchi di natura cibernetica alle proprie infrastrutture comporteranno una risposta, con operazioni cibernetiche o tradizionali, anche qualora i danni causati da tali operazioni non dovessero comportare danni fisici o perdita di vite umane.

Che si tratti di rispondere a operazioni nemiche contro le proprie infrastrutture nel cyberspazio o di negoziare a livello internazionale sulla regolamentazione della condotta degli Stati nel cyberspazio, la Francia, con questo documento, si dichiara pronta a divenire un attore sempre più centrale nel cyberspazio.