SIOI
UNA Italy
OSSERVATORIO
sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana

Il contributo delle Nazioni Unite allo sviluppo dell'*International Cybersecurity Law*

Gian Maria Farnelli
Ricercatore di Diritto internazionale, Università di Bologna

Lo «spazio cibernetico» ha acquisito una crescente rilevanza sin dalla progettazione del «world wide web» ad opera di Berners-Lee nel 1989. La capacità della rete di collegare le persone e di veicolare contenuti e informazioni è divenuta una parte irrinunciabile della attualità, come il periodo di *lockdown* imposto dall'emergenza sanitaria da COVID-19 ha dimostrato.

In virtù di tale importanza tanto dello spazio cibernetico quanto di internet come sua infrastruttura portante, gli Stati hanno analizzato con crescente interesse le applicazioni strategico-militari della «tecnologia di informazione e comunicazione» (*Information & Communication Tecnology*, ICT). Bastino in questo senso gli esempi quali il *malware* STUXNET, tramite cui l'Amministrazione statunitense avrebbe ritardato il progetto iraniano di arricchimento dell'uranio; o i tre *ransomware* WannaCry, Petya e NotPetya, tramite i quali sono stati portati attacchi incapacitati a infrastrutture essenziali, quali il servizio sanitario britannico o la rete elettrica ucraina, da *hackers* che si ritiene siano vicini alla Federazione russa.

In questo modo, lo spazio cibernetico si è accreditato sempre di più come un nuovo teatro di conflitti, come giustamente rilevato durante il vertice NATO di Varsavia del luglio 2016. Lo spazio cibernetico si è quindi affiancato allo spazio cinetico come luogo di esercizio della forza, da parte tanto degli Stati che di attori non statali. Ciò perché nello spazio cibernetico la tradizionale asimmetria tra Stati e attori non statali nell'accesso agli strumenti bellici viene meno. Anche per questo motivo si è palesata in epoca recente la necessità di adeguare l'attuale sistema giuridico internazionale alle nuove sfide rappresentate dallo spazio cibernetico e più in generale dalla ICT, onde evitare che esso si caratterizzi come una "terra di nessuno" in cui la fondamentale norma sul divieto dell'uso della forza venga meno.

L'esigenza di tale adeguamento è stata indicata per la prima volta in seno alle Nazioni Unite più di vent'anni fa. Nel 1998, l'Assemblea generale adottò la risoluzione 53/70 su proposta della Federazione russa, in cui si esprimeva la preoccupazione che la ICT potesse essere impiegata per scopi «inconsistent with the objectives of maintaining international stability and security». Nella stessa risoluzione si invitavano gli Stati a esprimere le proprie considerazioni circa «[a]dvisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality» e si incaricava il Segretario generale di predisporre un rapporto annuale sul tema della rilevanza della ICT per la sicurezza internazionale. Inoltre, si inseriva ufficialmente nell'agenda dell'Assemblea il tema «Developments in the field of information and telecommunications in the context of international security».

Dal 2004, a seguito della risoluzione 58/32 dell'Assemblea generale, il Segretario generale è stato affiancato da un Gruppo esperti governativi (*Group of Governmental Expert*, GGE) incaricati di assisterlo nello studio della tematica. Il GGE, costituito inizialmente da 15 membri, divenuti 20 nel 2014 e 25 nel 2016, è stato fino al 2017 l'unico organismo in seno alle Nazioni Unite incaricato di analizzare i riflessi dello sviluppo della ICT sulla pace e sicurezza internazionale, in considerazione del «increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes» indicato già nel primo rapporto del 2010.

Nonostante alcune proposte dottrinali nel senso dell'opportunità di elaborare un quadro regolamentare *ad hoc*, il GGE si è espresso nel senso di considerare il diritto internazionale esistente applicabile allo spazio cibernetico e alle sfide poste dalla ICT. Basti ricordare in questo senso il par. 19 del secondo rapporto del GGE del 2013, dove si legge che «[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT (…) environment». Nel rapporto del 2013 si indica inoltre che nello spazio cibernetico trovino applicazione anche «international norms and principles that flow from sovereignty» (par. 20), nonché le regole sulla responsabilità internazionale (par. 23). La posizione del GGE è stata approvata e sostenuta dall'Assemblea generale, che con la risoluzione 68/243 ha invitato gli Stati a prendere in considerazione il rapporto del 2013.

L'Assemblea ha reiterato e rafforzato tale posizione con la risoluzione 70/237, in cui si raccomanda agli Stati di seguire le "linee guida" stabilite nel terzo rapporto del GGE del 2015. In tale ultimo studio, il GGE, oltre a reiterare la centralità della Carta ONU anche per le relazioni internazionali nello spazio cibernetico, ha invitato gli Stati ad applicare alcuni principi fondamentali della Carta anche ai loro rapporti con riguardo alla ICT e richiamato la loro responsabilità relativamente a tali infrastrutture in base alla considerazione secondo cui «States have jurisdiction over the ICT infrastrucutre located within their territory» (par. 28). Tra i principi della Carta esplicitamente richiamati dal GGE vale la pena menzionare il rispetto dei diritti umani, il principio dell'uguaglianza sovrana degli Stati e il regolamento pacifico delle controversie, il divieto di utilizzo della minaccia o dell'uso della forza e il principio di non ingerenza negli affari interni degli Stati codificati all'art. 2 della Carta ONU.

Le risoluzioni appena citate sono state adottate per *consensus*, a dimostrazione dell'ampia condivisione dei principi in esse delineate da parte della Comunità internazionale. Questo fatto risulta di particolare interesse ai fini della qualificazione di queste risoluzioni quali elementi di prassi successiva utili a interpretare la Carta ONU, seguendo il ragionamento fatto proprio dalla Commissione di diritto internazionale nell'ambito dei lavori su accordi e prassi successiva nell'interpretazione dei trattati (conclusione 12). Si potrebbe sostenere, quindi, che nell'ambito di applicazione "spaziale" della Carta ONU ricada, oggi, lo spazio cibernetico, oltre a quello cinetico.

Purtroppo, tale posizione non è sufficiente a risolvere i dubbi circa la precisa portata dell'applicazione della Carta allo spazio cibernetico. In particolare, appare chiaro come il richiamo alla sovranità dello Stato relativamente alle infrastrutture telematiche presenti

sul suo territorio non risolva totalmente i problemi collegati alla sua responsabilità con riguardo ad eventuali attacchi mediante ICT, in considerazione delle difficoltà tecniche di individuazione dell'autore e, quindi, di attribuzione della condotta. Non è altrettanto chiaro se sullo Stato incomba un obbligo di vigilanza nel senso di impedire che ICT entro la sua sovranità siano utilizzate, direttamente o indirettamente, per arrecare danni ad altri Stati.

Queste problematiche, che avrebbero dovuto essere oggetto di ulteriori lavori del GGE, risultano ancora non approfondite. Ciò anche a causa della brusca interruzione del confronto diplomatico e normativo condotto in sede ONU dalle Grandi potenze. Nel 2017, le forti tensioni geopolitiche tra un gruppo di Stati guidato dagli Stati Uniti e uno guidato dalla Federazione russa hanno indotto il GGE ad adottare due distinti rapporti, che hanno dato origine a due proposte di risoluzione all'Assemblea generale: una promossa dai Paesi occidentali, l'altra promossa da un gruppo di Stati guidati dalla Federazione russa e dalla Repubblica popolare cinese.

Le due proposte sono state successivamente adottate dall'Assemblea generale rispettivamente come risoluzione 73/266 e risoluzione 73/27, cristallizzando così la impossibilità di comporre le divergenze tra i due blocchi. Tale contrapposizione, fondata sulla competizione tra i due gruppi per affermare la propria *leadership* nello spazio cibernetico, riguarda apparentemente l'esatta applicazione della Carta ONU ad attività mediante ICT che possa arrecare danni ad uno Stato, con particolare riguardo al diritto alla legittima difesa individuale e collettiva che potrebbe derivare da tali operazioni.

Tale divergenza si può desumere analizzando comparativamente le dichiarazioni di Michele G. Markoff, *Deputy Coordinator for Cyber Issues* statunitense, e di Andrey Krutskikh, Rappresentante speciale russo per la Cooperazione internazionale su *Information Security.* Risulta tanto di interesse quanto paradossale notare come i rappresentanti dei due Stati siano concordi nell'individuare un disaccordo, pur invocando entrambi la medesima posizione di merito, ossia l'applicazione del diritto internazionale classico anche allo spazio cibernetico e alla ICT.

Il delegato statunitense, infatti, ha sostenuto che il fallimento delle trattative diplomatiche in seno al GGE sarebbe derivato dalla scarsa chiarezza del linguaggio del Rapporto finale presentato dal GGE nel biennio 2016-2017, il quale, contrariamente alla volontà degli Stati Uniti, non faceva emergere con chiarezza una posizione a favore dell'applicazione del diritto internazionale umanitario, del diritto naturale di legittima difesa e delle norme sulla responsabilità degli Stati, con particolare riguardo alla liceità delle contromisure, in quanto alcuni Stati avrebbero ritenuto che il riferimento allo *jus ad bellum* «would be incompatibile with the message the Group should be sending regarding the peaceful settlement of disputes and conflict prevention». Il Rappresentante speciale russo ha, a sua volta, individuato la ragione del fallimento dei lavori del GGE del 2017 nel «fundamental political disagreement among the participants concerning their visions of the future of the global information space and the principles by which it will be regulated». Questa divergenza politica sostanziale sarebbe stata generata principalmente dalla posizione dei Paesi occidentali, interessati a imporre un quadro normativo che legittimasse l'uso della forza nello spazio cibernetico, forti della loro supremazia

tecnologica.

A causa di questa spaccatura, la prosecuzione dei lavori sullo studio del rapporto tra spazio cibernetico, ICT e diritto internazionale sarà portata avanti in due fori di discussione paralleli per il periodo 2019-2021. Da un lato, continuerà ad operare il GGE, dall'altro, la già citata risoluzione 73/27 ha istituito un «open-ended working group» (OEWG) al fine di rendere la negoziazione sulla ICT in seno alle Nazioni Unite «more democratic, inclusive and transparent» (par. 5). I due organismi svolgeranno funzioni simili. Entrambi sono chiamati a valutare come il diritto internazionale esistente si applichi allo spazio cibernetico e valutare eventuali misure di *confidence building* da suggerire agli Stati. Stando ai primi documenti pubblicati dall'OEWG, in particolare alla seconda bozza del Rapporto del 2020, questo nuovo organismo non pare volersi discostare dalla posizione già espressa dal GGE secondo cui il diritto internazionale esistente sia applicabile allo spazio cibernetico e alle attività mediante ICT (paragrafi 26-37). Il Segretario generale ha comunque invitato gli Stati a far pervenire loro osservazioni scritte su tale posizione – adempimento cui alcuni governi, quale quello francese, hanno già dato seguito.

Ciò che differenzia i due organismi è la loro composizione. Il GGE, presieduto dal Brasile per il biennio 2019-2021, è tuttora composto solo da 25 Stati membri delle Nazioni Unite e porterà avanti un'interlocuzione solo con le principali organizzazioni regionali. L'OEWG, cui partecipano invece tutti gli Stati dell'ONU e che sarà presieduto dalla Svizzera per il biennio 2019-2020, coinvolgerà nei suoi lavori tutti i soggetti interessati, comprese le organizzazioni internazionali non interpellate dal GGE e gli attori non statali. Proprio l'interlocuzione con questi soggetti pare di interesse. La posizione secondo cui la Carta ONU si applicherebbe alle relazioni tra gli Stati nello spazio cibernetico e alle attività mediante ICT è già stata fatta propria da altre organizzazioni internazionali, tra cui spiccano il G7 con la "Dichiarazione sul comportamento responsabile degli Stati nel ciberspazio" del 2016, e la NATO con la seconda edizione del "Manuale di Tallin", adottata dal *Cyber Defence Centre of Excellence* nel 2017.

Non è poi da sottovalutare l'importanza che gli attori non statali hanno in questo ambito. Si fa in particolare riferimento alla *business community*, la quale detiene la maggior parte dei *know how* su come svolgere attività mediante ICT. Si può fare riferimento in questo senso alla proattività di Microsoft, che ha lanciato varie iniziative tra cui giova citare quella delle "International Cibersecurity Norms" contenute in apposito *policy paper* del 2015, la proposta di una "Digital Geneva Convention" del 2017 e la campagna di sensibilizzazione globale lanciata nel 2018 dall'eloquente titolo "Digital Peace Now". Come è chiaro, le tre iniziative mirano a spingere gli Stati a ridurre le proprie attività ostili nello spazio cibernetico e attraverso ICT.

In conclusione, si può rilevare come l'applicazione del diritto internazionale allo spazio cibernetico sia argomento di grande attualità. Nonostante le difficoltà diplomatiche sopra indicate, l'ONU continua a svolgere un ruolo guida anche in questo settore, cojnvolgendo gli Stati, nonché altri soggetti interessati appartenenti alla società civile.