Così la governance del cyberspazio divide Occidente e asse Cina-Russia

Edoardo Sarti

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

Settembre 2019

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

Così la governance del cyberspazio divide Occidente e asse Cina-Russia

Edoardo Sarti

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Settembre 2019

Riguardo all'autore

Edoardo Sarti collabora col Center for Cyber Security and International Studies dal giugno 2019. Ha conseguito la Laurea Magistrale in "Relazioni Internazionali e Studi Europei" presso la Scuola di Scienze Politiche "Cesare Alfieri" dell'Università degli Studi di Firenze con la tesi dal titolo "Il ruolo delle organizzazioni internazionali per la cooperazione nel cyberspazio un approccio costruttivista". Nel 2019 ha conseguito il corso di perfezionamento in "Intelligence e sicurezza nazionale" presso l'Università di Firenze. La sua attività di ricerca per il CCSIRS include le Relazioni Internazionali nel cyberspazio, la cyber-diplomacy e l'analisi delle politiche nazionali ed internazionali relative al cyberspazio e alle tecnologie emergenti.

Così la governance del cyberspazio divide Occidente e asse Cina – Russia[1]

Il 9 settembre sono iniziati a New York i lavori dell'*Open-Ended Working Group* (OEWG) sugli sviluppi nel campo dell'informazione e delle telecomunicazioni per la sicurezza internazionale. Durante la prima giornata di lavori, l'ambasciatore russo Krutskikh ha affermato che, considerato il crescente numero di scontri e minacce nel cyberspazio, senza uno sforzo collettivo si arriverà inevitabilmente alla cyberwar e che dunque l'OEWG deve pervenire ad una definizione di regole e norme riguardo al comportamento degli Stati nella dimensione cyber. Questa dichiarazione appare tuttavia discordante con le operazioni condotte dalla Russia in questo dominio, dal momento che ad essa sono state attribuite numerose azioni offensive, come l'intrusione nelle elezioni americane del 2016 o gli attacchi cyber contro Estonia e Ucraina. Qual è dunque l'obiettivo della *cyber-diplomacy* russa?

La Russia e i forum internazionali

Fin dalla fine del secolo scorso la Russia si è fatta promotrice nei forum internazionali di un codice di condotta per regolare l'utilizzo dell'ICT da parte degli Stati, proponendo di istituire un *Group of Governmental Experts* (GGE), che esaminasse gli sviluppi nel settore dell'information security e contribuisse a rendere il cyberspazio un luogo sicuro e pacifico. Il desiderio di proteggere l'information environment e di limitare la proliferazione di information weapons derivava principalmente dalle preoccupazioni riguardo al dominio

[1] La seguente analisi è apparsa su Formiche.net il giorno 14 settembre 2019 ed è reperibile al seguente link: https://formiche.net/2019/09/governance-cyber-spazio-occidente-cina-russia/.

occidentale del settore dell'IT e alla superiorità militare americana in questo settore, che si è palesata a partire dalla Guerra del Golfo del 1991. Nonostante i 15 Stati presenti a questo GGE non riuscirono a produrre alcun risultato, esso rappresentò un passo importante perché fu seguito da altri tre GGE, svoltisi tra il 2009 e il 2015, che, mediando le posizioni distanti tra i vari paesi, riuscirono a raggiungere il consenso su una serie di questioni importanti, tra cui l'applicabilità del diritto internazionale nel cyberspazio, il riconoscimento della sovranità degli Stati, l'obbligo per essi di astenersi dal compiere atti illegittimi e l'inclusione di alcune norme non vincolanti.

Nel momento in cui però gli Stati (passati da 15 a 25) si sono ritrovati a dover definire in che modo il diritto internazionale si applicasse al cyberspazio, come richiesto dal mandato che ha istituito il quinto GGE (2016-2017), le posizioni di Stati Uniti e alleati da un lato e Russia e Cina dall'altro, si sono rivelate inconciliabili, decretando così il fallimento dell'ultimo GGE.

Le divergenze con l'Occidente

Il motivo del fallimento dell'ultimo GGE risiede nelle diverse vedute tra i paesi del Patto Atlantico e l'asse Cina-Russia in merito all'applicabilità al cyberspazio del diritto internazionale, nella sua totalità, e in particolare in riferimento all'articolo 51 della Carta delle Nazioni Unite che prevede "the inherent right of self-defence". Gli Stati Uniti e gli alleati si sono dichiarati favorevoli, in quanto questa norma rappresenterebbe un efficacie strumento di deterrenza nei confronti di attacchi cyber da parte di altri Stati. Russi e cinesi invece si sono fermamente opposti sostenendo, attraverso il discorso di un fidato alleato quale Cuba, che ciò porterebbe a "unilateral punitive force actions" invece che a risoluzioni pacifiche delle controversie tra Stati. La strategia russo-cinese in questo caso è chiara: favorire

un’ambiguità legale che garantisca una certa flessibilità e la possibilità di operare nel cyberspazio senza rischiare una rappresaglia collettiva per aver violato il diritto internazionale.

La strategia russo-cinese

E allora perché la Russia, insieme ad altri paesi come la Cina ha fatto approvare una risoluzione dell’Assemblea Generale per convocare l’OEWG “per sviluppare ulteriormente le regole, le norme e i princìpi del comportamento responsabile degli Stati nel cyberspazio”? Il primo obiettivo è quello di spostare il luogo di dibattito su questo tema da un forum ristretto di esperti, il GGE, all’OEWG perché in esso Russia e Cina possono contare su un numero più ampio (e crescente) di alleati. Questo nuovo folto gruppo che si è creato nell’ONU è rappresentato da tutti quei paesi che, guidati da Cina e Russia, si oppongono alla visione “occidentale” sul futuro dell’ICT. Potendo contare su un maggior numero di paesi alleati la Russia spera quindi di raggiungere l’obiettivo di far approvare un codice di condotta basato su nuove norme, diverse da quelle volute da USA e alleati, così da potersi permettere una certa flessibilità nelle proprie cyberoperations e, allo stesso tempo, affermare il principio, caro a Mosca si dal 2011 (ovvero da quando si è accorta del ruolo svolto dalla rete nelle “primavere arabe”) che condanna l’utilizzo dell’ICT per interferire negli affari economici e politici allo scopo di minare la stabilità degli altri Stati.

Appare dunque chiaro come le parole Krutskikh di un’apertura alla collaborazione per un codice di condotta non rappresentino una svolta nella cyberdiplomacy russa. Inoltre appare anche evidente che questa strategia collida con la visione di USA e alleati e che dunque un accordo che definisca entro limiti chiari l’azione degli Stati nel cyberspazio è ancora lontano.

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