Ecco come il cyber spazio sta cambiando le relazioni internazionali

Maya Santamaria

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

Dicembre 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

Ecco come il cyber spazio sta cambiando le relazioni internazionali

Maya Santamaria

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Dicembre 2018

Riguardo all’autore

Maya Santamaria è un'analista specializzata in cyber security e geopolitica. Dopo la laurea in Scienze Politiche e Relazioni Internazionali all'università La Sapienza di Roma, ha conseguito un master in Sicurezza, Geopolitica e Intelligence presso la Società Italiana per l'Organizzazione Internazionale (SIOI). Attualmente lavora come Cyber Security Analyst nell'azienda TS-WAY. Nel corso della sua carriera, ha collaborato con diversi enti di ricerca nazionali e stranieri, tra i quali l'Istituto di Alti Studi in Geopolitica e Scienze Ausiliarie (IsAG) ed il Centro di Geopolitica e Sicurezza in Studi sul Realismo (CGSRS) di Londra.

Ecco come il cyber spazio sta cambiando le relazioni internazionali[1]

Nell'ultimo decennio, la componente virtuale che caratterizza la sfera cyber e quella fisica e più materiale della dimensione politica hanno moltiplicato le loro interazioni al punto da arrivare a sovrapporsi sotto molteplici aspetti.

L'informatizzazione dei sistemi, infatti, ha reso inevitabile lo slittamento dei contrasti sul versante cibernetico, piano che riveste un ruolo cruciale in quanto è su di esso che si reggono gli equilibri di potere che caratterizzano il XXI secolo. Dopo terra, mare, aria e spazio, non solo la dimensione cyber rappresenta il quinto dominio delle attività militari e della dimensione bellica, ma ha assunto una posizione fondamentale che permette, in uno scenario sempre più liquido e in movimento, l'utilizzo di minacce trasversali ed asimmetriche che hanno profondamente mutato l'equilibrio tradizionale delle relazioni internazionali.

In realtà, la storia dei cyber conflitti ha radici meno vicine di quanto si pensi e che affondano nell'antico quadro dello spionaggio militare e dell'intelligence. Sebbene parole come *Information Warfare*, *Cyber Conflict* e *Cyber War* possano considerarsi parte di una terminologia lessicale moderna, esse non rappresentano altro che un'evoluzione – dettata dalla contingenza della democratizzazione dell'informazione – del tradizionale concetto di guerra, traslitterato dal piano fisico e psicologico a quello virtuale proprio grazie alla militarizzazione della rete e dello spazio cibernetico. I prodromi dei conflitti cibernetici si

[1] La seguente analisi è apparsa su il giorno https://formiche.net 18 luglio 2018 ed è reperibile al seguente link https://formiche.net/2018/12/cyber-spazio-relazioni-internazionali/.

fanno risalire alla seconda metà degli anni Ottanta, precisamente al 1986 con il primo caso di spionaggio dell'era informatica, passato alla storia col nome di Cuckoo's Egg, quando attaccanti della Germania dell'Ovest al soldo dei sovietici riuscirono ad esfiltrare un'ingente quantità di dati sensibili dai sistemi statunitensi, per poi cedere il materiale al Kgb.

Tuttavia, sebbene i paradigmi della geopolitica e delle relazioni internazionali siano rimasti gli stessi, lo scenario su cui si innestano è profondamente mutato, proprio in virtù della flessibilità che caratterizza il dominio cyber. Prendendo ad esame "L'Arte della Guerra", il trattato di strategia militare del generale Sun Tzu, infatti, non si può non notare che, sebbene le finalità siano pressoché immutate, strumenti a disposizione degli attaccanti e vulnerabilità degli attaccati hanno assunto un volto del tutto nuovo, fattore che ha causato lo spostamento dell'asse del conflitto su piani ben diversi da quelli delineati nel trattato del generale cinese. Prima di tutto, il continuo perfezionamento di tattiche e tools, con aggiornamenti e riconfigurazioni sempre nuove; in secondo luogo l'intangibilità della natura stessa del cyberspace che rende la misurazione dei successi e dei danni completamente aleatoria; infine, il livello di anonimità che può caratterizzare azioni perseguite da attori statali nelle prime fasi di un attacco, complicando la *detection* e la messa in atto di opportune pratiche di operational security, nonché prolungando i meccanismi di reazione.

La complessità che caratterizza la dimensione cibernetica si specchia a livello macroscopico sui rapporti tra Stati Nazione, il cui concetto di sovranità va oltre la tradizionale nozione westfaliana: si viene a delimitare un modello trans-statale, che si avvale di categorie inedite per riuscire a comporre compiutamente i nuovi confini, virtuali e non

più lineari, e le nuove caratteristiche portate in auge dalla rivoluzione digitale. I tradizionali modelli si svuotano e si riempiono di paradigmi più sfumati in cui i concetti non si applicano più alle logiche convenzionali dei conflitti tra Stati. E allora i vecchi archetipi che costituiscono gli approcci comuni su cui si fondano le teorie delle relazioni internazionali hanno bisogno di essere riconsiderati, alla luce delle nuove interazioni tra attori in gioco all'interno del contesto internazionale. Cambia anche l'approccio stato-centrico che ha caratterizzato gli equilibri del diciannovesimo e del ventesimo secolo poiché il modello delle relazioni internazionali è ora rappresentato da un interconnesso e anarchico sistema di interazioni in continuo cambiamento e aggiornamento. Concetti quali "potenza" e "supremazia" assumono un significato nuovo che si inserisce nel reticolato framework delle logiche dello spazio cibernetico; lo stesso sviluppo della capacità offensive in campo cyber non segue lo stesso percorso degli arsenali bellici convenzionali.

Lo scacchiere geopolitico digitale: focus sul Medio Oriente

Il mutamento di cui abbiamo parlato è accompagnato dal processo, ancora in divenire, di creazione di nuove forme di diritto che si devono adeguare alla complessità dei moderni panorami. È il caso del "The Tallinn Manual on the International Law Applicable to Cyber Warfare" – ora nella versione 2.0 –, nato dal progetto del Ccdcoe (Cooperative Cyber Defence Centre of Excellence) della Nato. Ragionando sui concetti di ius e bellum, il Manuale si pone l'obiettivo di far luce sugli ambiti di applicazione delle norme internazionali ai conflitti del cyberspace, riflettendo sulle nozioni di sovranità e giurisdizione.
L'ineluttabilità di affrontare e regolamentare tali temi si è manifestata con rinnovato vigore in seguito agli attacchi che colpirono – nella seconda metà degli anni duemila – l'Estonia prima e la Georgia poi,

mostrando come il mondo virtuale e quello “reale” fossero ormai intimamente connessi e interdipendenti.
Le motivazioni alla base degli attacchi di tipo DDoS sferrati dalla Russia furono, infatti, motivate dall’agenda politica di quegli anni e parte del disegno di Mosca di proseguire le tensioni geopolitiche sul piano dell’Information Warfare.

Ciò che tuttavia ha definitivamente alterato i modelli tradizionali delle relazioni internazionali e gli assiomi della geopolitica è stato il caso Stuxnet, il violento, complesso e distruttivo attacco di matrice israelo-statunitense che ha colpito i sistemi di controllo industriale della centrale nucleare iraniana di Natanz nel 2010. Parte dell’operazione dell’intelligence di Washington denominata “Olympic Games” volta a mappare gli impianti iraniani e ostacolarne i progressi nell’ambito del nucleare, Stuxnet ha rappresentato l’inizio di una nuova epoca, imponendo un ripensamento a livello globale dell’impatto della dimensione cibernetica – e della sua struttura reticolare – su quella prettamente fisica.

Come detto, la diffusione di Stuxnet ha indubbiamente segnato un punto di non ritorno nelle relazioni internazionali e, nello specifico, negli equilibri di potere in Medio Oriente e nel Golfo Persico. In seguito ai fatti di Natanz, l’Iran ha moltiplicato i suoi sforzi per sviluppare un proprio efficace arsenale digitale: nell’ultimo quinquennio i gruppi di cyber-spionaggio collegati al governo di Teheran si sono moltiplicati e hanno implementato tecniche sempre più sofisticate, dando avvio ad un processo di evoluzione informatica in senso nazionale. Ne sono esempi il malware Shamoon e l’Operation Saffron Rose (2013- 2014) perpetrata dal gruppo state-sponsored iraniano Ajax Security Team che ha condotto una pluralità

di operazioni di spionaggio contro obiettivi della difesa statunitensi e dissidenti dello stesso governo di Teheran.

Il processo di evoluzione e metamorfosi dei gruppi iraniani ha rispecchiato, a livello cibernetico, il mutevole e liquido scenario che caratterizza l'equilibrio mediorientale. Sul piano geopolitico, infatti, l'Iran è attivo su molteplici fronti. Uno su tutti la Siria, dove si riflettono a livello macroscopico i contrasti con Gerusalemme, quest'ultima interessata a scongiurare l'ipotesi di un rafforzamento di Teheran sulle posizioni perse dallo Stato Islamico.

Inoltre, proprio l'Iran è stato protagonista della crisi che ha scosso il Qatar nel giugno 2017 e che ha mostrato la potenza dell'impatto della sfera digitale sulle relazioni tra Stati. Le false dichiarazioni attribuite ad al-Thani e apparse sul sito della Qatar News Agency hanno infatti innescato la serie di eventi culminata con l'isolamento di Doha da parte degli Stati del Golfo, guidati da Riad. Le motivazioni dietro al blocco sono dipese proprio dalle relazioni del Qatar con l'Iran, come mostrato dalle 13 richieste imposte ad al-Thani per porre fino all'isolamento. Tra di esse, infatti, figurava l'interruzione dei rapporti commerciali, economici, politici e diplomatici con l'Iran e l'espulsione dei membri della Guardia Rivoluzionaria. Tuttavia, al contrario di quanto auspicato dai progetti sauditi, il rifiuto di Doha di piegarsi alle condizioni ha rafforzato l'influenza iraniana sul territorio, allargandone il bacino di influenza. Ciò che è interessante, è che un'azione altrimenti diplomaticamente e politicamente impossibile è stata messa in pratica proprio grazie ad una compromissione informatica. In effetti è stata proprio la violazione dell'agenzia di news del Qatar che ha permesso alla coalizione saudita di ottenere un alibi per "giustificare" le proprie mosse.

Gli scenari

L'analisi del panorama del Medio Oriente mostra come la proliferazione di cyber weapons sia ormai un fenomeno crescente e in grado di scuotere e modificare i delicati equilibri regionali. Cyber-spionaggio, strumenti di sorveglianza, disinformazione e attacchi alle infrastrutture critiche sono ormai gli strumenti utilizzati dalla nuova forma di guerra asimmetrica che ha modificato non solo il piano di battaglia ma anche il volto delle strategie militari, aggiungendone un nuovo livello di complessità.

Lo slittamento dei contrasti sul versante cibernetico, infatti, ha rappresentato un passaggio obbligato e quasi naturale: ad ogni attività rilevante nel "mondo reale" è ormai associata una parallela mossa nel reame digitale. Ecco perché ha senso riferirsi agli equilibri mutati e ai nuovi modelli con il termine Geopolitica 2.0. Tali cambiamenti saranno assimilati con ancora più forza negli scenari futuri:

– Le organizzazioni terroristiche fanno ormai ampio uso dei sistemi informatici al punto che è stato coniato il termine cyber-terrorism inteso come il punto di intersezione tra le attività terroristiche e la realtà cibernetica.

– I Governi, il Cremlino su tutti, moltiplicano i loro sforzi per generare caos e diffondere disinformazione attraverso fake news e propaganda. È ciò che Basarab and Serdiuk chiamano *hybression*, crasi di *hybrid and aggression*, in riferimento alla strategia militare di Mosca, messa in atto per polarizzare la società e paralizzare gli ordinamenti.

– Le attività sponsorizzata dagli Stati, e relativi gruppi Apt, sono cresciute esponenzialmente. Gli attacchi alla supply chain sono diventati sempre più sofisticati e difficili da mitigare. Ne sono un esempio quelli di Shamoon del novembre 2016 ma anche la diffusione di WannaCry e NotPetya.

Inoltre si fa un uso sempre più massiccio di exploit 0-day e di tool che consentono attacchi di tipo fileless. Allo stesso modo, si sono moltiplicati i malware per dispositivi mobili usati per intercettazioni e attività di spionaggio, spesso al fine di colpire dissidenti interni, giornalisti, attivisti dei diritti umani e minoranze etniche.

La potenza della minaccia asimmetrica spinge a confrontarsi con una nuova e inedita dimensione duale, mentre l'arena globale e le relazioni internazionali hanno inglobato le caratteristiche di anarchia e incertezza che contraddistinguono la dimensione cyber, fattore che ha reso possibile la concretizzazione di nuove dinamiche basate su processi sempre più mutevoli. Il panorama mediorientale è esemplificativo a riguardo, così come lo è il casus belli che ha portato all'isolamento del Qatar.

Parimenti, è paradigmatica la situazione della Corea del Nord. Il potenziale cyber di Pyongyang è cresciuto in sofisticatezza e qualità, come hanno mostrato gli attacchi del gruppo *state-sponsored* Lazarus contro la Sony Entertainment (novembre 2014), la diffusione del ransomware WannaCry e i colpi rivolti alle istituzioni finanziarie. Alla luce del complesso quadro che caratterizza l'equilibrio geopolitico della Corea del Nord, infatti, il duplice obiettivo di Pyongyang risponde alla necessità di colpire infrastrutture critiche di

target specifici, estorcendo al tempo stesso ingenti quantità di denaro (e tentando di sopperire così alle sanzioni).

Questa è un'altra dimostrazione di come i classici paradigmi che da sempre hanno caratterizzato le relazioni internazionali rispondano ora a logiche totalmente nuove e di come la faccia virtuale della geopolitica abbia fatto propri i meccanismi dell'ultima fase della *digital revolution*. L'assenza di barriere che caratterizza le attuali coordinate del cyberspazio permette agli attori in gioco di muoversi su uno scacchiere fluido in cui gli equilibri mutano con la stessa velocità che contraddistingue i cambiamenti in atto nel volatile e incerto ambiente virtuale. Sarà proprio su questi nuovi equilibri e complessità che si continueranno a plasmare, in maniera sempre più preponderante, le dinamiche di politica interna ed esterna in ambito bilaterale e multilaterale dei prossimi anni.

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