commentary

ISPI

Commentary, 25 settembre 2015

CYBER SECURITY: UN FRONTE SEMPRE PIÙ CALDO

STEFANO MELE E FRANCESCO N. MORO

È nel mondo virtuale (il cosiddetto "cyber-spazio") che la competizione fra Stati Uniti e Cina sembra aver assunto contorni reali e tangibili. Ne è esempio recente l'attacco allo U.S. Office of Personnel Management – attribuito alla Cina – che avrebbe portato alla sottrazione delle schede personali di 4,2 milioni tra dipendenti ed ex dipendenti dell'amministrazione americana, ivi compresi quelli appartenenti alle agenzie di intelligence. L'attacco informatico ha inevitabilmente inasprito le relazioni fra i due Paesi ed è proprio per questo che la *cyber-security* sta avendo proprio in queste ore un ruolo di assoluto rilievo all'interno del nuovo vertice USA-Cina. Tuttavia, l'esperienza ha finora insegnato che non si è mai riusciti ad andare oltre ai meri proclami. Guardando avanti, difficilmente le cose sembrano poter cambiare. Nei giorni scorsi, ad esempio, diverse fonti – fra cui New York Times e Guardian – hanno riportato che i due Paesi sono in procinto di definire un accordo bilaterale, il primo nel suo genere, sulla limitazione dell'uso delle cosiddette cyber-armi per colpire infrastrutture critiche nazionali. Oltre la retorica, però, questo accordo bilaterale non sarà niente più che un "codice di condotta" redatto da un gruppo di esperti dei due Paesi in seno alle Nazioni Unite: un testo, quindi, molto lontano dall'essere realmente capace di imporre vere e proprie limitazioni ai due attori internazionali. Ammesso che sia poi tecnicamente possibile, in concreto, imporle e soprattutto verificarne la violazione.

In attesa dell'esito di questo incontro, tuttavia, una breve ricognizione sulle forze e le questioni in campo, soprattutto sul meno noto approccio cinese in ambito internazionale, può essere utile.

In prima battuta, occorre domandarsi quali siano le ragioni che spingono Pechino a puntare così tanto sul cyber-spazio, soprattutto nei confronti degli Stati Uniti e degli altri principali attori sullo scacchiere geopolitico. Da un lato, a livello militare, la Cina è consapevole che un eventuale conflitto con gli USA richiederebbe la capacità di limitare la superiorità americana in ambito di C^4ISTAR, al fine di provare ad "accecare", o meglio, ad "annebbiare la vista" ai superiori assetti militari americani, soprattutto sul piano tecnologico. Dall'altro – ma la questione è collegata – la Cina è in cerca di soluzioni che le permettano di avanzare dal punto di vista industriale più rapidamente di quanto le proprie risorse interne abbiano finora permesso. Ciò, soprattutto in quei settori ad alto contenuto tecnologico, dove la difesa la fa certamente da padrona. La sottrazione di informazioni riservate, di *know-how* e di proprietà intellettuale attraverso attacchi informatici, costituisce proprio uno dei migliori e più efficaci strumenti per raggiungere tale obiettivo.

Stefano Mele, Istituto Italiano di Studi Strategici "Niccolò Machiavelli" e Carnelutti Studio Legale Associato – Milano(www.stefanomele.it)
Francesco N. Moro, Università di Milano Bicocca e "Competere" (www.venusinarms.com e www.competere.eu)

In seconda battuta, per conseguire gli obiettivi strategici appena delineati, il governo cinese ha promosso sempre più lo sviluppo di una dottrina per il cyber-spazio che fosse coerente non solo con le finalità poste, ma anche con la propria struttura di governo. Infatti, mentre molti Stati hanno da tempo incluso le attività di *cyber-warfare* all'interno della più ampia dottrina di *information warfare*, l'approccio cinese è stato più articolato ed ha privilegiato nel tempo la fusione tra il *cyber-warfare* e l'*electronic warfare*. Ciò ha portato alla creazione di una dottrina di "*Integrated Network and Electronic Warfare*", che ha favorito l'evoluzione del concetto di *information warfare* verso quello di "*Information Confrontation*". Questo ha fatto sì che tutti gli elementi dell'*information warfare* – sia difensivi che offensivi, sia elettronici che non elettronici – siano stati integrati sotto una singola ed univoca linea di comando.

Un ultimo punto, strettamente legato al livello tattico e delle operazioni, evidenzia anche un notevole aumento del numero e della qualità dei cyber-attacchi. Seppure con il (giusto) *caveat*,non esiste certezza assoluta che tutte le operazioni di spionaggio elettronico pubblicamente imputate alla Cina siano realmente attribuibili al governo di Pechino o ad azioni di gruppi esterni da questo sponsorizzati, appare comunque certo che molti di questi attacchi vengano portati a segno proprio attraverso sistemi informatici presenti proprio sul territorio cinese. Nonostante Pechino abbia sempre negato responsabilità dirette per la quasi totalità degli attacchi informatici che gli sono attribuiti, per operazioni ad ampio spettro sia contro bersagli governativi che contro società private – come *Titan Rain* (2003), *GhostNet* (2009), *Operation Aurora* (2009), *Shady RAT* (2011), *Night Dragon* (2011) e *APT30* (2015) – il dito viene puntato con sempre maggior frequenza (e certezza) proprio verso il governo cinese, tanto che la fama dei gruppi governativi cinesi dediti a questo genere di attività è ormai indiscussa e in alcuni casi – come quello della *Unità 61398* del *Terzo Dipartimento* della *People's Liberation Army* (PLA) – anche pubblicamente nota. Peraltro, gli attacchi ai sistemi informatici di British Aerospace (2012) o Lockheed Martin (2009 e 2013) mostrano in maniera chiara come l'acquisizione di segreti industriali sia comunque uno degli obiettivi principali di Pechino. Non deve sorprendere, allora, come l'improvvisa diminuzione del numero degli attacchi informatici provenienti dalla Cina nelle settimane antecedenti il vertice in atto, volta senz'altro a favorire un clima più disteso con gli Stati Uniti, implicitamente riveli come il governo di Pechino – aldilà dei *caveat* – possa in realtà agevolmente controllare la situazione sul suo territorio e agire all'occorrenza per diminuire il numero e la portata degli attacchi informatici nei confronti dei Paesi terzi.

Pertanto, ciò che deve far più riflettere, è la mancanza di reali strumenti in mano agli Stati Uniti – e non solo – per provare a contrastare questo genere di comportamenti, sia sul piano della reazione che della dissuasione. In termini di risposte, oltre a quanto finora accennato, l'ordine esecutivo firmato dal Presidente Obama nell'aprile di quest'anno, teso a sanzionare finanziariamente gli individui identificati come responsabili di cyber-attacchi, è finora risultato inapplicato nella pratica. Altrettanto improduttiva è risultata ad oggi – e per ovvie ragioni – l'incriminazione della Corte della Pennsylvania per sottrazione di segreti industriali degli Stati Uniti sollevata nel 2014 nei confronti di 5 ufficiali dell'esercito cinese. Questo nonostante le capacità degli Stati Uniti di rintracciare gli autori degli attacchi informatici stiano progredendo velocemente e – non bisogna dimenticarlo – Internet e l'utilizzo delle tecnologie informatiche rappresentino prima di tutto un vantaggio strategico impareggiabile per gli stessi USA. Sembra sempre più evidente, in questo contesto, come un problema di Washington sia quello – classico – di chi si trova a mantenere una situazione di superiorità (industriale, tecnologica, convenzionale, ecc.) cercando di rintracciare il sottilissimo equilibrio fra il difendersi dagli attacchi e dissuaderli ed evitare che le proprie azioni di risposta portino ad una *escalation* del "conflitto".

Per concludere, il tema della *cyber-security* è sicuramente quanto mai centrale nelle relazioni bilaterali USA-Cina e

la sua importanza è destinata a crescere nel tempo. Pensare – e poi implementare – accordi che contengano misure di *confidence-building*, tese soprattutto ad evitare una corsa agli armamenti e a identificarne i limiti in termini di *target* e strumenti utilizzabili, è certamente un passo a cui guardare in maniera favorevole. Un passo, però, che almeno nella sua attuale conformazione appare troppo "timido" e soprattutto complicato nelle successive fasi di attuazione e di verifica. D'altro canto, un eventuale accordo tra le parti difficilmente potrà risolvere alla radice alcune questioni di fondo. Per il governo di Pechino, infatti, la ricerca di segreti industriali e di capacità di "*denial*" rimangono priorità strategiche essenziali e imprescindibili; così come per gli attori non governativi basati in Cina, la sottrazione di dati tramite attacchi a "privati" – dai singoli alle *corporations* – continua a costituire sempre più oggi un'opportunità molto comoda e redditizia.