CYBERWAR E CYBER TERRORISM: UNA MINACCIA CONCRETA

di Ilaria Stivala

In un mondo sempre più interconnesso, sia a livello economico che a livello politico, ma anche sempre più a rischio di minacce, coloro che si occupano di garantire la difesa nazionale devono estendere le loro valutazioni dei rischi prendendo in considerazione un'ampia serie di aspetti che vanno dalla protezione dei propri cittadini all'interno dei confini nazionali, alla protezione di infrastrutture materiali e immateriali che permettono di erogare i servizi essenziali alla società. Oggi grazie all'uso sempre più pervasivo delle tecnologie le autorità sono costrette a prendere atto della necessità di elaborare un nuovo concetto di sicurezza che prenda in considerazione anche il cyber spazio - ossia quell'insieme di reti e sistemi informativi con cui vengono erogati servizi indispensabili a cittadini- che a causa dell'elevata vulnerabilità può essere sfruttato da organizzazioni criminali o gruppi terroristici. A fronte di questo evolversi della tecnologia e delle capacità degli hacktivisti di infiltrarsi nei sistemi non stupisce che nel 2010 l'allora vice-segretario della Difesa americano William J. Lynn III abbia pubblicamente qualificato il cyber-spazio come il "quinto dominio della conflittualità" - dopo terra, mare, aria e spazio- e che la maggior parte degli Stati si siano immediatamente mossi per predisporre una strategia per far fronte alla criminalità cibernetica. [1]

L'Organizzazione per la Cooperazione di Shanghai, guidata da Russia e Cina, nel 2015 ha proposto all'Assemblea Generale delle Nazioni Unite una serie di linee guida che dovrebbero guidare gli Stati al fine di sviluppare un sistema di deterrenza in vista dei conflitti nel cyber spazio e creare apposite strutture politiche e decisionali per far fronte alla minaccia come identificare e rafforzare le infrastrutture critiche, stabilire leggi e regole di condotta nazionali ad hoc, rafforzare leggi e

[1] https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cybersecurity.html

partnership internazionali. Da ciò ben si comprende quanto l'approccio globale al problema sia fortemente incardinato sulle attività diplomatiche e di partnership su più livelli, nonché sulla parte prettamente tecnica/tecnologica della materia. Il contesto cibernetico sembra dunque essersi trasformato in un nuovo possibile campo di battaglia su cui portare in essere offensive ed operazioni tatticamente e strategicamente rilevanti, sia dal punto di vista degli effetti generati che della natura degli obbiettivi colpiti. Pensando alle possibili minacce attuali per il cyber spazio è impossibile non prendere in considerazione lo Stato Islamico, il quale fin dalle sue prime rivendicazioni si è ampiamente servito dello strumento mediatico: innanzitutto ne ha fatto uso in termini di "marketing", facendo propaganda al fine di diffondere il terrore in tutto il mondo e raccogliere proseliti, in secondo luogo se n'è servito al fine di finanziarsi, infine ultimo ma non meno importante è il suo utilizzo da parte di esperti per compiere attacchi informatici alle infrastrutture sensibili dei Paesi ostili a ISIS.[2] Eventi che confermano la pervasiva presenza dello Stato Islamico nel cyber spazio possono essere quello in Francia, quando tra il 10 e il 16 Gennaio migliaia di siti giornalistici sono stati sotto attacchi informatici, oppure il messaggio minaccioso «Siamo già qui, nei vostri Pc e nelle vostre case» che sedicenti affiliati al califfato di Abu Bakr al Baghdadi hanno pubblicato nel profilo Twitter del quotidiano americano "Albuquerque Journal", dopo essersi infiltrati nel relativo sistema informatico, e la scritta apparsa nella homepage della Malaysia Airways: «Errore 404 - aereo non trovato. Isis vincerà»[3]. Ma il raid più grave, almeno simbolicamente, è quello avvenuto contro gli account Twitter e Facebook del Comando Centrale delle truppe Usa a Tampa, in cui sono comparse frasi come: «Lo Stato Islamico vi insegue» e «guardatevi le spalle».[4] Sebbene un rapporto di Flashpoint, leader mondiale nell'analisi dei dati web a scopi di intelligence, sottolinei come lo Stato Islamico da una parte sia ancora troppo male organizzato e sotto finanziato per causare danni reali e dall'altra il fatto che i target dei suoi attacchi siano di tipo mediatico, siti di notizie e social network, la preoccupazione resta elevata. A diffondere un maggiore senso di insicurezza ha contribuito anche il recente annuncio riguardante l'aggregazione di quattro distinte squadre "cyber" pro- ISIS in un unico gruppo: gli Stati Cyber Califfato. La risposta statunitense è stata la predisposizione di un'operazione congiunta, tuttora in corso, tra NSA (National Security Agency) e DISA (Defence information System Agency) al fine di prevenire ed eliminare la struttura di propaganda su internet e sui social, i primi luoghi di reclutamento e di influenza ideologica usati dallo Stato Islamico, e le sue azioni cibernetiche.[5]

[2] http://www.difesaonline.it/geopolitica/analisi/cyber-warfare-scenari-critici-e-i-rischi-attuali

[3] http://espresso.repubblica.it/plus/articoli/2015/02/02/news/isis-al-qaeda-e-la-sfida-del-terrorismo-informatico-1.197769

[4] http://espresso.repubblica.it/plus/articoli/2015/02/02/news/isis-al-qaeda-e-la-sfida-del-terrorismo-informatico-1.197769

[5] http://urbanpost.it/terrorismo-usa-pronti-a-cyber-guerra-contro-lisis-prima-volta-nella-storia/

Tale obiettivo si presenta come molto difficile da raggiungere, non solo perché si tratterebbe della prima “cyber war”, ma anche perché nel frattempo il Califfato si è impegnato ad insegnare ai propri militanti misure per proteggere la loro identità online ed a criptare i messaggi in modo tale da renderli meno rintracciabili dalle autorità.