CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 07/08 – Luglio/Agosto 2016

EXECUTIVE SUMMARY

Parole chiave: *Cyber Warfare, FBI, DHS, ODNI, Regole di ingaggio per il cyber-spazio, Stati Uniti*.

Il numero di attacchi informatici cresce in maniera costante non solo sotto il punto di vista quantitativo, quanto soprattutto sotto quello qualitativo, sia che si guardi ai bersagli colpiti, che alla complessità o ai reali obiettivi degli attacchi.

Se si guarda ai recenti avvenimenti, ad esempio, anche volendo tralasciare per una volta le minacce legate allo spionaggio elettronico e alle attività di *cyber-warfare*, appare chiaro come la propaganda, la disinformazione e la guerra psicologica abbiano da tempo trovato nuove "strade" – peraltro anche molto efficaci – proprio grazie al cyber-spazio, che appare essere ormai uno dei principali protagonisti anche di tentativi di influenzare la campagna elettorale americana.

La scarsa capacità di generare deterrenza (si veda sul tema il "*Cyber Strategy & Policy Brief*" di marzo 2016), unita all'incapacità di coordinare ruoli, competenze e risposte alle minacce cibernetiche, contribuisce quindi a creare uno scenario evidentemente preoccupante.

In quest'ottica, sulla scia di quanto predisposto nel mese di febbraio attraverso il "*Cybersecurity National Action Plan*" (si veda sul tema il "*Cyber Strategy & Policy Brief*" di febbraio 2016), è da guardare con estremo interesse la recente *Presidential Policy Directive* del Presidente Obama, denominata "PPD-41 -- *United States Cyber Incident Coordination*", che tende appunto a riorganizzare in maniera chiara e coerente la macchina di gestione degli incidenti informatici sul piano governativo federale.

L'obiettivo di questa riforma è quello di creare un piano di coordinamento dei ruoli e di concentrazione degli sforzi, che attraverso l'azione di un *Cyber Unified Coordination Group* possa fronteggiare le minacce cibernetiche di alto profilo che per dimensione, natura o intensità siano tali da incidere sulla sicurezza nazionale americana e su quella dei suoi cittadini.

Un obiettivo tanto ambizioso, quanto ormai utile ed imprescindibile, soprattutto in strutture molto complesse come lo è quella americana, che adesso però si attende al vaglio dell'attuazione e della sua implementazione.

Il focus di questo mese, invece, è sulle regole di ingaggio per il cyber-spazio.

Sebbene le operazioni militari nel e attraverso il cyber-spazio abbiano ormai assunto un ruolo fondamentale soprattutto nel facilitare attacchi convenzionali da parte delle Forze Armate, le regole di ingaggio restano nella maggior parte dei casi segrete e rappresentano uno degli argomenti meno dibattuti nel settore della 'sicurezza cibernetica' (e non solo).

Ciò principalmente perché, in linea generale, le regole di ingaggio hanno come scopo quello di delineare e specificare le circostanze ed i limiti entro cui le Forze Armate possono iniziare e/o continuare il combattimento contro le forze contrapposte, codificando i comportamenti autorizzati e non autorizzati da assumere o non assumere in presenza di determinate attività o azioni ostili.

Questo comporta, come detto, una notevole esigenza di segretezza sui contenuti. Le regole di ingaggio per il cyber-spazio non fanno ovviamente eccezione.

La predisposizione di regole di ingaggio per il cyber-spazio appare allo stato attuale un'attività particolarmente complessa, frutto di competenze militari, legali e tecniche/tecnologiche di non facile comprensione ed attuazione.

Tuttavia, il sempre maggiore utilizzo del cyber-spazio come supporto alle operazioni militari e l'incremento costante del numero e della qualità degli attacchi informatici – sempre più orientati a colpire le infrastrutture critiche di una nazione – rende quest'esigenza attuale ed quanto mai improcrastinabile.

Di seguito e in ordine alfabetico vengono brevemente analizzate le principali notizie e i più importanti avvenimenti in materia di *cyber-security* che hanno caratterizzato quest'ultimo mese sul piano strategico e di *policy*.

FOCUS SULLE REGOLE DI INGAGGIO PER IL CYBER-SPAZIO

Il 14 giugno scorso, i Ministri della Difesa dei Paesi appartenenti al blocco NATO hanno approvato il riconoscimento del cyber-spazio come quinto dominio della conflittualità, dopo terra, mare, aria e spazio. Riconoscimento, poi, ufficializzato durante il 27esimo incontro dei capi di Stato e di governo della NATO tenutosi agli inizi di luglio a Varsavia (per approfondire, si veda anche il *"Cyber Strategy & Policy Brief"* di giugno 2016).

Tuttavia, la quasi totalità dei principali attori statuali si è già da tempo dotata di apposite strutture per far fronte alla cosiddetta 'minaccia cibernetica', sia sul piano governativo centrale, che sul quello delle attività di intelligence e delle operazioni militari.

Nonostante sia ancora oggi molto complesso comprendere quanti e quali Stati abbiano dato vita ad uno specifico comando per le operazioni militari nel e attraverso il cyber-spazio, all'incirca 60 nazioni hanno già sviluppato unità per la *cyber-defence*. Un numero che sale a 100 Paesi se si guarda, invece, anche a chi è in procinto di svilupparle.

In quest'ottica, sebbene le operazioni militari nel e attraverso il cyber-spazio abbiano ormai assunto un ruolo fondamentale soprattutto nel facilitare attacchi convenzionali da parte delle Forze Armate, le regole di ingaggio restano nella maggior parte dei casi segrete e rappresentano uno degli argomenti meno dibattuti nel settore della 'sicurezza cibernetica' (e non solo).

Ciò principalmente perché, in linea generale, le regole di ingaggio hanno come scopo quello di delineare e specificare le circostanze ed i limiti entro cui le Forze Armate possono iniziare e/o continuare il combattimento contro le forze contrapposte, codificando i comportamenti autorizzati e non autorizzati da assumere o non assumere in presenza di determinate attività o azioni ostili.

Questo comporta, come detto, una notevole esigenza di segretezza sui contenuti. Le regole di ingaggio per il cyber-spazio non fanno ovviamente eccezione.
Tuttavia, le regole di ingaggio rappresentano anche un documento spesso tanto breve, quanto complesso.

Nel settore delle operazioni militari nel e attraverso il cyber-spazio, sono il frutto della sintesi di principi legali, strategici, operativi e tattici, che hanno alla base una precisa e approfondita conoscenza ed analisi:

- degli aspetti strategici ed operativi dello specifico dominio della conflittualità, in questo caso il cyber-spazio;

- della specifica situazione geopolitica al momento della loro redazione;
- degli obiettivi politico-strategici che si intende raggiungere con l'attacco informatico;
- delle reali capacità di reazione dei soggetti attaccati, ivi comprese ovviamente quelle di *cyber-warfare*;
- degli eventuali ulteriori Stati e/o soggetti terzi che potrebbero decidere di intervenire e/o di appoggiare le operazioni nemiche, ivi comprese quelle nel e attraverso il cyber-spazio;
- delle possibili reazioni internazionali ad un'eventuale rappresaglia all'attacco informatico subìto;
- delle proprie capacità di difesa e soprattutto di attacco nel e attraverso il cyber-spazio.

Sotto il piano puramente attuativo, invece, un ruolo fondamentale è riservato all'unità tecnico-informatica di uno Stato, che, sia in caso di applicazione di regole d'ingaggio per la mera difesa, sia in caso di una reazione necessaria ad un attacco informatico, deve poter indicare in tempi ragionevolmente brevi la sorgente e l'autore dell'attacco.

Qui nasce il primo problema. Nel cyber-spazio, infatti, è molto facile riuscirsi a garantire un ottimo livello di anonimato ed è quindi altrettanto semplice rendere molto complesso il lavoro di attribuzione della responsabilità dell'attacco informatico al suo autore materiale o al reale mandate.

Ulteriori elementi di criticità sorgono, poi, anche sul piano legale. L'eventuale reazione ad un attacco informatico da parte di uno Stato deve obbligatoriamente sottostare a tutti i principi di diritto internazionale già noti per i conflitti combattuti nei domini "tradizionali", ovvero terra, mare, aria e spazio.

I principi di necessità, proporzionalità e distinzione sono solo alcuni dei vincoli legali internazionali già esistenti ed applicabili ovviamente anche all'utilizzo da parte degli Stati di strumenti informatici per scopi militari. Nei fatti, però, tener conto ed adempire a questi principi non è quasi mai di così facile attuazione.

Un ultimo elemento critico, infine, è dato dalla velocità dell'attacco informatico nelle sue fasi finali, ovvero quella dell'invio contro il bersaglio e della produzione degli effetti. La sua immediatezza, infatti, rende al momento impossibile la realizzazione del cosiddetto ciclo OODA (Osservare, Orientare, Decidere, Agire), lasciando necessariamente alle macchine e, appunto, a delle regole di ingaggio già predisposte e "tarate" per ogni tipologia diversa di situazione la decisione sul da farsi, sia in fase difensiva, che eventualmente reattiva.

Com'è facile immaginare, anche in ragione dei due elementi di criticità visti in precedenza, la predisposizione di regole di ingaggio per il cyber-spazio appare allo stato attuale un'attività

particolarmente complessa, frutto di competenze militari, legali e tecniche/tecnologiche di non facile comprensione ed attuazione.

Tuttavia, il sempre maggiore utilizzo del cyber-spazio come supporto alle operazioni militari e l'incremento costante del numero e della qualità degli attacchi informatici – sempre più orientati a colpire le infrastrutture critiche di una nazione – rende quest'esigenza attuale ed quanto mai improcrastinabile.

STATI UNITI

Il numero di attacchi informatici cresce in maniera costante non solo sotto il punto di vista quantitativo, quanto soprattutto sotto quello qualitativo, sia che si guardi ai bersagli colpiti, che alla complessità o ai reali obiettivi degli attacchi.

Se si guarda ai recenti avvenimenti, ad esempio, anche volendo tralasciare per una volta le minacce legate allo spionaggio elettronico e alle attività di *cyber-warfare*, appare chiaro come la propaganda, la disinformazione e la guerra psicologica abbiano da tempo trovato nuove "strade" – peraltro anche molto efficaci – proprio grazie al cyber-spazio, che appare essere ormai uno dei principali protagonisti anche di tentativi di influenzare la campagna elettorale americana.

La scarsa capacità di generare deterrenza (si veda sul tema il "*Cyber Strategy & Policy Brief*" di marzo 2016), unita all'incapacità di coordinare ruoli, competenze e risposte alle minacce cibernetiche, contribuisce quindi a creare uno scenario evidentemente preoccupante.

In quest'ottica, sulla scia di quanto predisposto nel mese di febbraio attraverso il "*Cybersecurity National Action Plan*" (si veda sul tema il "*Cyber Strategy & Policy Brief*" di febbraio 2016), è da guardare con estremo interesse la recente *Presidential Policy Directive* del Presidente Obama, denominata "PPD-41 -- *United States Cyber Incident Coordination*", che tende appunto a riorganizzare in maniera chiara e coerente la macchina di gestione degli incidenti informatici sul piano governativo federale.

Alla luce di quanto si legge nella *Direttiva*, un ruolo fondamentale è assegnato al Dipartimento di Giustizia americano, che, attraverso l'FBI e la sua *National Cyber Investigative Joint Task Force*, avrà il compito di soprintendere alle attività di risposta alle minacce cibernetiche che dovessero attentare agli interessi nazionali o economici degli Stati Uniti, alle sue relazioni internazionali, oppure alla salute, alla sicurezza o alle libertà civili del popolo americano.

Attività di risposta che – occorre specificarlo fin da subito – in questo campo si sostanziano non solo in azioni tese a mitigare la minaccia e ad agevolare lo scambio di informazioni tra gli enti coinvolti, ma soprattutto a svolgere vere e proprie operazioni di investigazione e raccolta di prove e di informazioni di intelligence volte ad attribuire la responsabilità dell'attacco e a collegare i vari incidenti informatici occorsi.

Fornire assistenza tecnica ai soggetti pubblici o privati colpiti da un attacco cibernetico è compito, invece, del *Department of Homeland Security* (DHS) e soprattutto del suo *National Cybersecurity and Communications Integration Center* (NCCIC). A questa struttura, costituita nel 2009 e che vanta di avere al suo interno anche lo US-CERT e l'ICS-CERT, è affidato quindi il compito di ridurre le vulnerabilità e mitigarne gli effetti, sia attraverso attività strettamente tecniche, che di *information sharing* e di *alert* verso ulteriori bersagli potenzialmente esposti.

Infine, il terzo pilastro delineato dalla "*United States Cyber Incident Coordination*" è ovviamente quello dell'intelligence. Compito affidato all'*Office of the Director of National Intelligence* e al suo *Cyber Threat Intelligence Integration Center*.

Appare chiaro, allora, come l'obiettivo di questa riforma sia quello di creare un piano di coordinamento dei ruoli e di concentrazione degli sforzi, che attraverso l'azione di un *Cyber Unified Coordination Group* possa fronteggiare le minacce cibernetiche di alto profilo che per dimensione, natura o intensità siano tali da incidere sulla sicurezza nazionale americana e su quella dei suoi cittadini.

Un obiettivo tanto ambizioso, quanto ormai utile ed imprescindibile, soprattutto in strutture molto complesse come lo è quella americana, che adesso però si attende al vaglio dell'attuazione e della sua implementazione.

Sul piano militare, invece, il mese di luglio è stato caratterizzato dalla richiesta al Congresso americano del *budget* per il 2017 per il settore della 'sicurezza cibernetica'. La domanda del Segretario della Difesa si è attestata su 6.7 miliardi di dollari, ovvero 900 milioni in più (il 15,5%) rispetto alle richieste dell'anno precedente.

Lo stanziamento di questo importo proietta il *budget* quinquennale 2017-2021 delle Forze Armate americane per la *cyber-security* alla considerevole cifra di 34.6 miliardi di dollari.
La maggior parte di questi fondi saranno spesi nella protezione dei sistemi informatici del Dipartimento della Difesa americano e nello sviluppo delle capacità per le operazioni militari nel e attraverso il cyber-spazio.

Per approfondire gli sviluppi progettuali delle Forze Armate americane per il cyber-spazio, si vedano il "*Cyber Strategy & Policy Brief*" di gennaio e marzo 2016.

NOTE SULL'AUTORE

Stefano Mele è avvocato specializzato in *Diritto delle Tecnologie, Privacy, Sicurezza delle Informazioni e Intelligence* e lavora a Milano come *'of Counsel'* di Carnelutti Studio Legale Associato. Dottore di ricerca presso l'Università degli Studi di Foggia, collabora presso le cattedre di Informatica Giuridica e Informatica Giuridica Avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano. E' socio fondatore e *Partner* del Moire Consulting Group ed è Presidente del "*Gruppo di lavoro sulla cyber-security*" della Camera di Commercio americana in Italia (AMCHAM). È Coordinatore dell'Osservatorio *InfoWarfare e Tecnologie emergenti* dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli' e membro del International Institute for Strategic Studies (IISS). È inoltre docente presso istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO, nonché autore di numerose pubblicazioni scientifiche e articoli sui temi della *cyber-security*, *cyber-intelligence*, *cyber-terrorism* e *cyber-warfare*.
Nel 2014, la NATO lo ha inserito nella lista dei suoi *Key Opinion Leaders for Cyberspace Security*.
Nel 2014, la rivista *Forbes* lo ha inserito tra i 20 migliori *Cyber Policy Experts* al mondo da seguire in Rete.

Per maggiori informazioni sull'autore: www.stefanomele.it

CONSULTA ANCHE I VOLUMI PRECEDENTI

Cyber Strategy & Policy Brief (Volume 01 – Gennaio 2016)

Parole chiave: *Active Cyber-Defence, Cina, Cyber Warfare, Deterrenza, GCHQ, Israele, NSA, People's Liberation Army, Regno Unito, Russia, Stati Uniti, Strategia, U.S. Cyber Command, Ucraina.*

Cyber Strategy & Policy Brief (Volume 02 – Febbraio 2016)

Parole chiave: *Arabia Saudita, Casa Bianca, Corea del Nord, Cyber Intelligence, Cyber Warfare, Iran, Italia, Stati Uniti, Stato Islamico, Strategia, Terrorismo*.

Cyber Strategy & Policy Brief (Volume 03 – Marzo 2016)

Parole chiave: *Cyber Command, Cyber Intelligence, Cyber Warfare, Danimarca, Deterrenza, GCHQ, Iran, Marine Corps, Regno Unito, Stati Uniti, Strategia, Syrian Electronic Army*.

Cyber Strategy & Policy Brief (Volume 04 – Aprile 2016)

Parole chiave: *Australia, Cina, Cyber Intelligence, Cyber Warfare, Germania, Information Dominance, Russia, Stati Uniti, Strategia, U.S. Air Force.*

Cyber Strategy & Policy Brief (Volume 05 – Maggio 2016)

Parole chiave: *Active Cyber Defence, Cyber Intelligence, Cyber Warfare, G7, Giappone, Iran, Nazioni Unite, Stati Uniti, Strategia, Supreme Council for Cyberspace, U.S. Naval Academy.*

Cyber Strategy & Policy Brief (Volume 06 – Giugno 2016)

Parole chiave: *Comando C4 Difesa, Comando Interforze per le Operazioni Cibernetiche, Cyber Command, Cyber Intelligence, Cyber Warfare, Israele, Israel Defense Forces, Italia, NATO, Strategia, Ucraina, Ukraine National Cybersecurity Coordination Centre.*