CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 05 – Maggio 2016

EXECUTIVE SUMMARY

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

A fine maggio, i leader dei Paesi del G7 si sono incontrati ad Ise-Shima, in Giappone, per discutere delle principali sfide politiche ed economiche globali. Tra i numerosi temi affrontati, anche la *cyber-security* ha assunto un ruolo di primo piano e la pubblicazione del documento dal titolo "*G7 Principles and Actions on Cyber*" appare di sicuro rilievo per gli analisi di questo settore.

Ad una giustissima e sempre auspicabile riaffermazione dei principi tesi a salvaguardare i diritti umani, la privacy e la protezione dei dati personali, nonché la cooperazione e la condivisione delle informazioni per il contrasto al terrorismo e al *cyber-crime*, ciò che appare molto interessante è l'esplicito riconoscimento da parte dei leader del G7 della possibilità che, in alcune circostanze, gli attacchi informatici possano essere qualificati come uso della forza o come attacco armato sul piano della Carta delle Nazioni Uniti e del diritto internazionale consuetudinario. Da ciò, quindi, discende per gli Stati il diritto alla legittima difesa sia individuale, che collettiva, come previsto dall'art. 51 della Carta delle Nazioni Unite.

Nonostante i passi avanti svolti finora, occorre comprendere con urgenza che proprio quello della creazione di un *framework* internazionale di norme globalmente condivise per l'utilizzo delle capacità offensive nel e attraverso il cyber-spazio sia oggi giorno uno dei principali obiettivi per tutti i governi. Ciò, al fine di evitare che la cosiddetta "militarizzazione del cyber-spazio" assuma ben presto contorni particolarmente foschi in assenza di precise regole di comportamento da parte degli Stati.

Sotto il punto di vista dei singoli Stati, invece, il governo giapponese ha pubblicamente annunciato la creazione di un'agenzia per la protezione delle infrastrutture critiche dagli 'attacchi cibernetici'.

La *Industrial Cybersecurity Promotion Agency*, questo il probabile nome dell'agenzia, sarà un ente basato sullo schema della cooperazione pubblico-privati, che vedrà la luce nel 2017 grazie ad un cospicuo finanziamento da parte di alcune società del mondo privato.

L'agenzia si configurerà come organo extra-governativo incorporato all'interno del Ministero dell'Economia, del Commercio e dell'Industria ed avrà due compiti fondamentali: il primo, quello di incrementare lo specifico *know-how* tecnico e tecnologico nel settore della *cyber-security*, il secondo quello di coordinare e realizzare ricerche per lo sviluppo di contromisure dagli 'attacchi cibernetici' contro le infrastrutture critiche nazionali giapponesi.

Anche il governo di Teheran ha fatto parlare di sé durante il mese di maggio. Attraverso la voce del suo *Supreme Council of Cyberspace*, infatti, ha ufficialmente richiesto agli operatori stranieri che offrono servizi di *social media* e di messaggistica istantanea di trasferire entro un anno all'interno dei confini iraniani i *data center* che gestiscono e archiviano i dati dei propri cittadini.

Il governo iraniano continua a dimostrare di temere che, attraverso le tecnologie e la rete Internet, possano penetrare a livello sociale concetti, ideali e stili di vita occidentali in contrasto con gli interessi dell'attuale *leadership* politica o che ne minino la stabilità.

Quanto delineato evidenzia in maniera chiara, quindi, come il governo di Teheran stia operando dal punto di vista difensivo per il raggiungimento di due obiettivi fondamentali. Il primo, come approfondito anche nel *Cyber Strategy & Policy Brief* di febbraio 2016, è quello di proteggere le proprie infrastrutture critiche dagli 'attacchi cibernetici' provenienti principalmente dall'Arabia Saudita e dai Paesi del Golfo filo-Ryad, così come dagli Stati Uniti e da Israele. Il secondo, invece, è quello di proteggere la leadership governativa frenando le attività di propaganda e di informazione nel cyber-spazio operate dai partiti interni di opposizione e dai gruppi di dissenso politico e sociale.

Infine, il mese di maggio ha visto la U.S. Naval Academy laureare i suoi primi 27 guardiamarina in "*Cyber Operations*".

E' la prima volta in assoluto per una scuola di formazione militare americana che dei giovani ufficiali vengono addestrati attraverso un percorso formativo completamente dedicato alle operazioni militari nel e attraverso il cyber-spazio.

Formare e addestrare a questo tipo di operazioni militari i futuri ufficiali delle forze armate e farlo fin da subito con specifici percorsi formativi, appare ormai un'esigenza quanto mai reale e tangibile. Lo scenario attuale, infatti, ci proietta – già nel brevissimo periodo – ad un ruolo sempre più rilevante delle tecnologie e della rete Internet nelle attività militari, soprattutto in un'ottica di facilitazione di attacchi cinetici.

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 SU DOCUMENTO "*G7 PRINCIPLES AND ACTIONS ON CYBER*"

A fine maggio, i leader dei Paesi del G7 si sono incontrati ad Ise-Shima, in Giappone, per discutere delle principali sfide politiche ed economiche globali. Tra i numerosi temi affrontati, anche la *cyber-security* ha assunto un ruolo di primo piano e la pubblicazione del documento dal titolo "*G7 Principles and Actions on Cyber*" appare di sicuro rilievo per gli analisi di questo settore.

Occorre evidenziare, peraltro, come questa sia la prima volta in assoluto che i rappresentanti del G7 abbiano deciso di predisporre uno specifico documento completamente dedicato ai principi e alle azioni da intraprendere nel settore della cosiddetta 'sicurezza cibernetica'.

Per trovare un analogo interessamento condiviso su questi temi ad un così alto livello istituzionale, infatti, occorre tornare indietro di ben cinque anni, quando, nel 2011, prima del 37° incontro dei leader dei Paesi del G8, il Presidente Sarkozy organizzò l'"e-G8 Forum".

Tuttavia, non appare un caso che un simile documento sia stato predisposto e pubblicato durante la presidenza del G7 da parte del Giappone, dato che da tempo questo stato ha fatto della *cyber-security* una priorità della propria agenda politica e strategica.

In merito al contenuto, il documento del G7 si concentra su temi perfettamente in linea con l'approccio strategico seguito sul piano internazionale dalle principali potenze occidentali, nonché con quanto delineato nella *cyber-strategy* europea.

Tuttavia, ad una giustissima e sempre auspicabile riaffermazione dei principi tesi a salvaguardare i diritti umani, la privacy e la protezione dei dati personali, nonché la cooperazione e la condivisione delle informazioni per il contrasto al terrorismo e al *cyber-crime*, ciò che appare molto interessante è l'esplicito riconoscimento da parte dei leader del G7 della possibilità che, in alcune circostanze, gli attacchi informatici possano essere qualificati come uso della forza o come attacco armato sul piano della Carta delle Nazioni Uniti e del diritto internazionale consuetudinario.

Da ciò, quindi, discende per gli Stati il diritto alla legittima difesa sia individuale, che collettiva, come previsto dall'art. 51 della Carta delle Nazioni Unite.

Questa tendenza, evidenzia – come più volte già sottolineato (si vedano il "*Cyber Strategy & Policy Brief*" di gennaio, di marzo e di aprile 2016) – quanto l'approccio strategico delle principali potenze stia velocemente mutando da una mera difesa attiva (*Active Cyber-Defence*) ad un vero e proprio sviluppo di capacità offensive per il cyber-spazio. Tutto ciò, però, senza che in seno agli organismi internazionali si siano consolidate delle chiare strategie su questo tema e senza soprattutto un *framework* internazionale di norme globalmente condivise ed accettate per l'utilizzo delle capacità offensive nel e attraverso il cyber-spazio.

In questo senso, però, occorre puntualizzare come già nel 2013, all'esito della riunione del *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* delle Nazioni Unite, sia stato convenuto che il diritto internazionale vigente si applichi anche all'interno del 'dominio cibernetico', così come i concetti tradizionali di sovranità statale.

A quest'affermazione ha fatto seguito, nel 2015, una più completa specificazione di questi principi. Nell'ultimo report del *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* delle Nazioni Unite, infatti, tra le altre cose, è stato esplicitamente affermato che:

a. Gli Stati esercitano la loro giurisdizione sulle infrastrutture informatiche situate sul loro territorio.
b. Nell'utilizzo degli strumenti informatici, gli Stati devono rispettare, oltre agli altri principi del diritto internazionale, quello dell'inviolabilità della sovranità territoriale altrui, della parità tra le diverse sovranità territoriali, il principio di risoluzione delle controversie mediante mezzi pacifici e la non ingerenza nelle questioni interne di altri Stati. I vincoli legali internazionali già esistenti sono applicabili anche all'utilizzo da parte degli Stati di strumenti informatici. Gli Stati devono comunque adempiere alle obbligazioni loro derivanti dagli accordi internazionali riguardo la protezione dei diritti umani e delle libertà fondamentali.
c. […]
d. Il Gruppo ha osservato il consolidarsi di questi principi internazionali, incluso, dove possibile, quelli di umanità, necessità, proporzionalità e distinzione.
e. Gli Stati non possono commettere atti internazionalmente illeciti mediante strumenti informatici neanche attraverso deleghe a parti terze che operino su indicazione dello Stato in questione e devono assicurarsi del fatto che il loro territorio non sia utilizzato da attori non statali al fine di commettere tali atti.
f. Gli Stati devono adempiere i loro doveri riguardo agli atti internazionalmente illeciti a loro riconducibili secondo il diritto internazionale. Comunque sia, indizi sul fatto che un attacco informatico sia stato lanciato o abbia origine dal territorio di uno Stato o da un'infrastruttura informatica appartenente a questo non sono sufficienti ad attribuire la suddetta attività allo Stato in questione. Il Gruppo ha osservato che l'accusa di organizzare o condurre atti illeciti contro un altro Stato deve essere comprovata.

Nonostante i passi avanti svolti finora, occorre comprendere con urgenza che proprio quello della creazione di un *framework* internazionale di norme globalmente condivise per l'utilizzo delle capacità offensive nel e attraverso il cyber-spazio sia oggi giorno uno dei principali obiettivi per tutti i governi.
Ciò, al fine di evitare che la cosiddetta "militarizzazione del cyber-spazio" assuma ben presto contorni particolarmente foschi in assenza di precise regole di comportamento da parte degli Stati.

GIAPPONE

Durante il mese di maggio, il governo giapponese ha pubblicamente annunciato la creazione di un'agenzia per la protezione delle infrastrutture critiche dagli 'attacchi cibernetici'.

La *Industrial Cybersecurity Promotion Agency*, questo il probabile nome dell'agenzia, sarà un ente basato sullo schema della cooperazione pubblico-privati, che vedrà la luce nel 2017 grazie ad un cospicuo finanziamento da parte di alcune società del mondo privato.

L'agenzia si configurerà come organo extra-governativo incorporato all'interno del Ministero dell'Economia, del Commercio e dell'Industria ed avrà due compiti fondamentali: il primo, quello di incrementare lo specifico *know-how* tecnico e tecnologico nel settore della *cyber-security*, il secondo quello di coordinare e realizzare ricerche per lo sviluppo di contromisure dagli 'attacchi cibernetici' contro le infrastrutture critiche nazionali giapponesi.

Tuttavia, l'impegno del Giappone nei confronti della sicurezza delle infrastrutture critiche non deve sorprendere. Sin dal 2005, infatti, attraverso il primo "*Action Plan on Information Security Measures for Critical Infrastructures*" e fino ai nostri giorni con la terza revisione della "*Basic Policy of Critical Information Infrastructure Protection*", questa problematica è sempre stata tra le massime priorità dell'agenda politica dei governi che si sono susseguiti nel tempo.

Appare naturale, quindi, che proprio la protezione delle infrastrutture critiche dagli 'attacchi cibernetici' sia uno dei principali pilastri strategici alla base della *cyber-strategy* del Giappone.

Peraltro il documento strategico, aggiornato nel settembre del 2015, dopo aver individuato quest'esigenza e rimarcato quali settori debbano essere considerati come critici, delinea anche tre azioni operative tese a rendere quanto più efficace ed effettivo possibile questo pilastro.

Dal condurre una costante revisione dei metodi e degli strumenti utilizzati per proteggere le infrastrutture critiche, applicandoli – ove possibile – anche alle altre realtà societarie private, passando per l'indispensabile condivisione delle informazioni sulle minacce, fino alla predisposizione di un vero e proprio supporto governativo per rendere più solida la sicurezza dei sistemi informatici di queste strutture, l'intenzione del governo del Primo Ministro Shinzo Abe pare essere proprio quella di concentrarsi sulla protezione dei cittadini e dei sistemi che garantiscono loro i servizi essenziali e le principali attività economiche.

Viceversa, ciò che pare essere al momento una piccola zona d'ombra è la ragione per cui il governo giapponese abbia deciso di incardinare la *Industrial Cybersecurity Promotion Agency* all'interno del Ministero dell'Economia, del Commercio e dell'Industria.

Tenuto conto che la protezione delle infrastrutture critiche rappresenta forse il principale elemento per la sicurezza nazionale, per la sicurezza dei cittadini e per il benessere economico

di ogni Stato, una simile struttura avrebbe trovato la sua naturale e migliore collazione nel *National Information Security Center* giapponese.

Infatti, seppure la *Industrial Cybersecurity Promotion Agency* avrà come scopo quello di incrementare lo specifico *know-how* tecnico e tecnologico nel settore della *cyber-security*, nonché di coordinare e realizzare ricerche per lo sviluppo di contromisure dagli 'attacchi cibernetici' contro le infrastrutture critiche nazionali giapponesi, è il *National Information Security Center* l'organo governativo deputato, tra le altre cose, all'analisi e al contrasto degli attacchi informatici nei confronti delle reti governative del Giappone.

Includere la *Industrial Cybersecurity Promotion Agency* all'interno del *National Information Security Center* permetterebbe, quindi, di creare quella giusta sinergia tra esigenze operative e linee di sviluppo e di ricerca che rappresenta oggi giorno il principale volano di crescita del settore.

Infine, un simile assetto andrebbe a ricalcare la tendenza dei governi delle principali potenze economiche, che da un po' di tempo a questa parte continuano ad accentrare strutture e competenze in materia di *cyber-security* sotto linee di gestione uniche e quanto più brevi possibili (per approfondire, si vedano il "*Cyber Strategy & Policy Brief*" di gennaio, di marzo e di aprile 2016).

IRAN

Alla fine di maggio, il governo di Teheran, attraverso la voce del suo *Supreme Council of Cyberspace*, ha ufficialmente richiesto agli operatori stranieri che offrono servizi di *social media* e di messaggistica istantanea di trasferire all'interno dei confini iraniani i *data center* che gestiscono e archiviano i dati dei propri cittadini. Abolhassan Firouzabadi, segretario del *Supreme Council*, ha affermato, inoltre, che ciò dovrà avvenire entro un anno, pena l'esclusione di questi servizi dal territorio.

Se circa metà della popolazione iraniana (39 milioni di persone) possiede oggi giorno uno *smartphone*, quello dei *social media* e dei servizi di messaggistica istantanea è un mercato che in Iran raggiunge quasi 14 milioni di utenti e dove, secondo un sondaggio ufficiale del 2013 svolto dal Ministero della Gioventù e dello Sport, il 69,3% della fascia più giovane della popolazione regolarmente aggira i filtri governativi per utilizzare questi servizi.

Infatti, seppure applicazioni come Telegram (che gode di un bacino di circa 20 milioni di utenti) e Instagram rappresentano i servizi occidentali più utilizzati sul territorio iraniano, *social network* come Facebook e Twitter risultano, invece, bloccati dai filtri governativi.

L'atteggiamento del governo del Presidente Rouhani non risulta di certo nuovo. Forme di controllo e repressione di questo genere di servizi – peraltro anche maggiormente capillari e indiscriminate – possono farsi risalire già al 2009, durante la presidenza di Ahmadinejad.

Inoltre, occorre evidenziare come il *Supreme Council of Cyberspace* abbia da tempo instaurato uno specifico comitato per il controllo dei contenuti pubblicati sui *social media*, al cui interno siede almeno un rappresentante dell'Intelligence, del Ministro dell'Interno, del Ministero della Cultura, nonché delle Forze di Polizia iraniane deputate alla repressione dei crimini informatici.

Quanto delineato evidenzia in maniera chiara come il governo di Teheran stia operando dal punto di vista difensivo per il raggiungimento di due obiettivi fondamentali. Il primo, come approfondito anche nel *Cyber Strategy & Policy Brief* di febbraio 2016, è quello di proteggere le proprie infrastrutture critiche dagli 'attacchi cibernetici' provenienti principalmente dall'Arabia Saudita e dai Paesi del Golfo filo-Ryad, così come dagli Stati Uniti e da Israele. Il secondo, invece, è quello di proteggere la l*eadership* governativa frenando le attività di propaganda e di informazione nel cyber-spazio operate dai partiti interni di opposizione e dai gruppi di dissenso politico e sociale.

Infine, attraverso queste ultime decisioni, il governo iraniano continua a dimostrare di temere che, attraverso le tecnologie e la rete Internet, possano penetrare a livello sociale concetti, ideali e stili di vita occidentali in contrasto con gli interessi dell'attuale *leadership* politica o che ne minino la stabilità.

STATI UNITI

Alla fine di maggio la *U.S. Naval Academy* ha laureato i suoi primi 27 guardiamarina in "*Cyber Operations*".

E' la prima volta in assoluto per una scuola di formazione militare americana che dei giovani ufficiali vengano addestrati attraverso un percorso formativo completamente dedicato alle operazioni militari nel e attraverso il cyber-spazio.

Nella primavera del 2013, infatti, la *U.S. Naval Academy* fu la prima a delineare un percorso di istruzione di ben tre anni totalmente focalizzato su questo settore, decidendo di affiancarlo ai percorsi di laurea tecnico informatici tradizionali.

Tuttavia, la laurea in "*Cyber Operations*" non si limita ad una formazione puramente tecnica e tecnologica sui temi della sicurezza informatica, della crittografia, della programmazione e della *computer forensics*, ma si concentra anche nel fornire gli strumenti e le capacità in materia di *policy*, di normativa legale e persino di *social engineering* alla futura *leadership* della Marina Militare americana.

L'approccio seguito dalla *U.S. Naval Academy* – del tutto innovativo nel mondo occidentale – non può che rappresentare un esempio da seguire per qualsiasi governo, soprattutto nel settore militare.

Formare e addestrare alle operazioni militari nel e attraverso il cyber-spazio i futuri ufficiali delle forze armate e farlo fin da subito con specifici percorsi formativi, appare ormai un'esigenza quanto mai reale e tangibile. Lo scenario attuale, infatti, ci proietta – già nel brevissimo periodo – ad un ruolo sempre più rilevante delle tecnologie e della rete Internet nelle attività militari, soprattutto in un'ottica di facilitazione di attacchi cinetici.

Ciò, a maggior ragione, sul piano internazionale, sia alla luce del contenuto del documento "*G7 Principles and Actions on Cyber*", di cui si è detto in precedenza, che in ragione della imminente e fondamentale decisione dei Ministri della Difesa dei Paesi membri della NATO di dichiarare ufficialmente il cyber-spazio come un dominio operativo al pari di terra, aria, mare e spazio (argomento di cui si dirà nel prossimo volume del "*Cyber Strategy & Policy Brief*").

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 1 – 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 2 – 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 3 – 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 4 – Aprile 2016)

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