CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 06 – Giugno 2016

EXECUTIVE SUMMARY

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*.

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.

In conseguenza di questo importantissimo e ormai atteso riconoscimento, che impatta su tutti gli Stati appartenenti all'Alleanza atlantica, occorrerà al più presto avviare una riflessione molto seria e approfondita sugli elementi che devono necessariamente sorreggere una simile dichiarazione.

Ciò, soprattutto alla luce dell'estensione anche al cyber-spazio della clausola di difesa collettiva, che, com'è noto, dal settembre del 2014 prevede che gli Stati appartenenti alla NATO si forniscano reciproca assistenza anche in caso di aggressione attraverso attacchi cibernetici.

Infatti, seppure in quest'ambito il principale obiettivo della NATO è sempre stato e resterà ancora quello di difendere i propri sistemi informatici e di aiutare gli Stati membri a sviluppare le più idonee capacità di *cyber-defence*, il riconoscimento del cyber-spazio come dominio per le operazioni militari comporterà – già nel breve periodo – una necessaria evoluzione di questa postura, al fine di integrare al più presto lo spazio cibernetico nel campo della difesa collettiva.

In quest'ottica, allora, al pari di ciò che già oggi avviene con le armi convenzionali, occorrerà che ogni singolo Stato dell'Alleanza atlantica e la stessa NATO – magari attraverso la creazione di uno specifico *Cyber Command* – si dotino quanto prima anche di capacità offensive per il cyber-spazio da utilizzare, ovviamente, come mera reazione ad eventuali attacchi (cibernetici e non) portati nei confronti della NATO o di uno dei Paesi alleati.

Durante il mese di giugno, inoltre, sia il governo italiano, che quello israeliano hanno annunciato pubblicamente l'intenzione di creare un *Cyber Command*.

Quello italiano, il *Comando Interforze per le Operazioni Cibernetiche* (CIOC), che potrebbe rendere attivo il suo primo nucleo operativo già entro un anno, sarà impegnato su un duplice fronte. Da un lato, garantire il proprio contributo alla sicurezza nazionale italiana, potenziando le capacità di difesa da attacchi cibernetici, dall'altro sviluppare le capacità di pianificazione e

conduzione di *Computer Network Operations* (CNO) a supporto delle operazioni militari sia in Italia, che al di fuori dei confini nazionali.

Quello israeliano, invece, costituito all'interno della *Israel Defense Forces* ed operativo entro due anni, avrà il compito di svolgere operazioni militari offensive e difensive nel e attraverso il cyber-spazio, centralizzando le competenze, rispettivamente, dell'*Unità 8200* del *Military Intelligence Directorate* e del *C4I Telecommunications Directorate*.

In merito al costituendo *Cyber Command*, sarà interessante verificare nel tempo la sua precisa collocazione all'interno della complessa organizzazione governativa israeliana per la *cyber-security* e le sinergie che saranno instaurate con le altre strutture già presenti al suo interno. Infatti, apparati come il *National Cyber Bureau*, deputato a svolgere funzioni consultive e di *policy* per il Primo Ministro, e la *National Cyber Security Authority*, responsabile della protezione delle infrastrutture critiche e del CERT nazionale, così come le agenzie di *intelligence* come lo *Shin Bet* e il *Mossad*, sono molto attive e strutturate anche in questo settore.

Infine, anche il governo ucraino ha mosso degli importanti passi in avanti nel settore della sicurezza cibernetica. Agli inizi di giugno, infatti, il Presidente Petro Porošenko ha firmato il decreto per la costituzione del primo *National Cybersecurity Coordination Centre* ucraino.

Questa decisione fa il pari con la recente pubblicazione della prima *cyber-strategy* dell'Ucraina, che, dal marzo del 2016, ha assegnato al *National Security and Defense Council* il compito di coordinare tutte le attività relative al settore della sicurezza cibernetica tra le varie agenzie governative.

Il *National Cybersecurity Coordination Centre* ucraino avrà come scopi, tra gli altri, quello di coordinare le attività in ambito sicurezza nazionale e Difesa dei soggetti istituzionali deputati all'attuazione della *cyber-strategy*, di accrescere il livello di efficienza della pubblica amministrazione nella formulazione ed attuazione delle politiche nazionali nel campo della sicurezza informatica, di contribuire all'implementazione delle normative tese alla salvaguardia delle risorse informative statali, delle informazioni classificate e della sicurezza delle infrastrutture critiche nazionali dalle minacce cibernetiche.

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*.

ISRAELE

Alla fine di giugno, l'*Israel Defense Forces* (IDF) ha annunciato pubblicamente l'intenzione di rendere operativo entro due anni il proprio *Cyber Command*.

La struttura, la cui sede al momento è segreta, avrà il compito di svolgere operazioni militari offensive e difensive nel e attraverso il cyber-spazio, andando quindi a centralizzare le competenze, rispettivamente, dell'*Unità 8200* del *Military Intelligence Directorate* e del *C4I Telecommunications Directorate*.

Occorre evidenziare fin da subito come la decisione del governo israeliano si allinei perfettamente con quella delle principali potenze a livello internazionale (si veda, all'interno del presente documento, anche quanto stabilito di recente dal governo italiano).

Già da tempo, infatti, si assiste ad un accentramento delle capacità e delle competenze – sia difensive, che offensive – in ambito di *cyber-intelligence* e *cyber-warfare* sotto una linea di comando unica e più breve possibile. Ciò, appare evidente, al fine non solo di razionalizzare al meglio gli investimenti economici, che risultano in costante crescita, ma soprattutto di incrementare l'efficienza e l'efficacia d'azione delle strutture operanti nel e attraverso il cyber-spazio, rendendole più snelle e reattive (per approfondire quanto fatto da Stati Uniti e Cina, si veda in particolare il "*Cyber Strategy & Policy Brief*" di gennaio 2016).

Infatti, gli attacchi cibernetici vengono percepiti sempre di più come parte integrante non solo dei piani volti alla salvaguardia della sicurezza nazione, ma anche di quelli tesi al raggiungimento degli obiettivi e degli interessi statali.

In merito al costituendo *Cyber Command*, peraltro, sarà interessante verificare nel tempo la sua precisa collocazione all'interno della complessa organizzazione governativa israeliana per la *cyber-security* e le sinergie che saranno instaurate con le altre strutture già presenti al suo interno.
Infatti, apparati come il *National Cyber Bureau*, deputato a svolgere funzioni consultive e di *policy* per il Primo Ministro, e la *National Cyber Security Authority*, responsabile della protezione delle infrastrutture critiche e del CERT nazionale, così come le agenzie di *intelligence* come lo *Shin Bet* e il *Mossad*, sono molto attive e strutturate anche in questo settore.

Riuscire a massimizzare la cooperazione e soprattutto l'*info-sharing* dovrebbe essere, allora, uno dei primi pilastri strategici per il futuro *Cyber Command*.

Un elemento fondamentale – questo, come molti altri – che si spera possa trovare presto una collocazione coerente e organizzata all'interno di una specifica *cyber-strategy*, che, almeno al momento, risulta ancora mancare al governo israeliano.

ITALIA

Il "*Libro Bianco per la Sicurezza Internazionale e la Difesa*", redatto dal Ministero della Difesa italiano e approvato nell'aprile del 2015, fa della *cyber-defence* e dell'estensione delle operazioni militari nel dominio cibernetico una delle sue priorità strategiche ed uno dei più importanti programmi di investimento per il triennio 2016/2018.

In quest'ottica, la Difesa italiana ha pianificato, tra le altre cose, la creazione del *Comando Interforze per le Operazioni Cibernetiche* (CIOC).

Il *Comando* sarà impegnato su un duplice fronte. Da un lato, garantire il proprio contributo alla sicurezza nazionale italiana, potenziando le capacità di difesa da attacchi cibernetici, dall'altro sviluppare le capacità di pianificazione e conduzione di *Computer Network Operations* (CNO) a supporto delle operazioni militari sia in Italia, che al di fuori dei confini nazionali.

Seppure siano molto poche le informazioni disponibili, alcuni recenti interventi pubblici da parte di ufficiali delle Forze Armate italiane hanno evidenziato che, nonostante si sia ancora in una fase di progettazione, il *Comando Interforze per le Operazioni Cibernetiche* potrebbe rendere attivo il suo primo nucleo operativo già entro un anno. Tuttavia, almeno per il momento, l'attenzione sarebbe concentrata soprattutto sull'organizzazione del *Comando*, sulle tecnologie necessarie per la sua funzionalità, nonché sul personale e sul suo addestramento.

Sul piano organizzativo, invece, il *Comando Interforze per le Operazioni Cibernetiche* italiano opererà, verosimilmente, alle dipendenze del Capo di Stato Maggiore della Difesa (CaSMD), come organo tecnico-militare di vertice dell'amministrazione Difesa italiana, e soprattutto del suo Vice Comandante per le Operazioni (VCOM-OPS), quale responsabile della pianificazione operativa e dell'impiego delle forze militari in operazioni, ivi comprese quelle cibernetiche.

Inoltre, considerata già la presenza all'interno della struttura della Difesa italiana del *Comando C4 Difesa*, da tempo preposto alle attività gestionali interforze volte a garantire l'efficienza delle funzioni di comando, controllo, telecomunicazioni e informatica, appare plausibile che il futuro *Comando Interforze per le Operazioni Cibernetiche* trovi posto proprio all'interno della struttura del *Comando C4 Difesa*, assorbendo completamente la componente informatica e quindi anche il *CERT Difesa Technical Center* italiano.

Infine, sebbene i finanziamenti dedicati al settore della difesa cibernetica in Italia non siano al momento definiti in maniera puntuale nel documento di programmazione economica pluriennale del Ministero della Difesa, essi risultano ricompresi e spalmati all'interno del finanziamento – più ampio – dedicato ai "*Sistemi C4I a valenza interforze*".
Ciò nonostante, tenuto conto che il potenziamento delle capacità di *cyber-defence* viene definito in questo documento come uno dei programmi di finanziamento di maggior rilievo per la Difesa italiana, è presumibile che proprio questo settore sia deputato ad assorbire la più alta percentuale del *budget* di circa 22,4 milioni di euro previsti per i "*Sistemi C4I a valenza interforze*" nel triennio 2016/2018.

Da quanto accennato, appare evidente come l'Italia si stia allineando al contesto internazionale anche sotto il punto di vista della creazione di uno specifico *Cyber Command*.
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.

L'Italia, attraverso le attività del *Comando C4 Difesa*, già da tempo ha guardato al cyber-spazio come un dominio da cui difendersi e difendere la sicurezza nazionale.
L'evoluzione verso il futuro *Comando Interforze per le Operazioni Cibernetiche*, quindi, non può che essere guardata con estrema positività, soprattutto considerato l'enorme incremento nello sviluppo di capacità offensive nel e attraverso il cyber-spazio operato negli ultimi mesi dai principali attori internazionali (per approfondire, si vedano in particolare il "*Cyber Strategy & Policy Brief*" di gennaio, marzo, aprile e maggio 2016).

NATO – FOCUS SU CYBER-SPAZIO COME DOMINIO DI WARFARE

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.

In conseguenza di questo importantissimo e ormai atteso riconoscimento, che impatta su tutti gli Stati appartenenti all'Alleanza atlantica, occorrerà al più presto avviare una riflessione molto seria e approfondita sugli elementi che devono necessariamente sorreggere una simile dichiarazione.
Ciò, soprattutto alla luce dell'estensione anche al cyber-spazio della clausola di difesa collettiva, che, com'è noto, dal settembre del 2014 prevede che gli Stati appartenenti alla NATO si forniscano reciproca assistenza anche in caso di aggressione attraverso attacchi cibernetici.

Tuttavia, seppure in quest'ambito il principale obiettivo della NATO è sempre stato e resterà ancora quello di difendere i propri sistemi informatici e di aiutare gli Stati membri a sviluppare le più idonee capacità di *cyber-defence*, il riconoscimento del cyber-spazio come dominio per le operazioni militari comporterà – già nel breve periodo – una necessaria evoluzione di questa postura, al fine di integrare al più presto lo spazio cibernetico nel campo della difesa collettiva.

In quest'ottica, allora, al pari di ciò che già oggi avviene con le armi convenzionali, occorrerà che ogni singolo Stato dell'Alleanza atlantica e la stessa NATO – magari attraverso la creazione di uno specifico *Cyber Command* – si dotino quanto prima anche di capacità offensive per il cyber-spazio da utilizzare, ovviamente, come mera reazione ad eventuali attacchi (cibernetici e non) portati nei confronti della NATO o di uno dei Paesi alleati.

La NATO, perciò, dovrà essere quanto più diretta ed efficace possibile nell'esplicitare in maniera chiara come queste capacità militari offensive per il cyber-spazio possano inserirsi nella sua strategia di difesa e di deterrenza degli attacchi.

La strada che appare al momento migliore è quella che punta sullo sviluppo di una dottrina e delle procedure utili a consentire che gli attacchi informatici possano pienamente divenire capacità militari operative e che la NATO abbia il più ampio spettro possibile di opzioni utili a scoraggiare gli attacchi cibernetici degli avversari.

Nel far ciò, molti saranno gli elementi di criticità da dover superare. Il primo sarà senz'altro quello di distinguere nettamente ciò che l'Alleanza può svolgere sul piano della difesa cibernetica in tempo di pace e ciò che, invece, può essere attuato sul piano degli attacchi cibernetici in caso di vere e proprie operazioni militari o in caso di applicazione della clausola di difesa collettiva.

Inoltre, un ulteriore elemento di criticità sarà senz'altro quello di dover stabilire non solo la soglia oltre la quale un attacco informatico può essere considerato equivalente ad un attacco convenzionale, ma anche il livello di proporzionalità della reazione sul piano informatico rispetto al danno sofferto in conseguenza dell'attacco subìto.

Tuttavia, nonostante queste evidenti criticità, come già evidenziato all'interno del "*Cyber Strategy & Policy Brief*" di maggio 2016, 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 dev'essere oggigiorno uno dei principali obiettivi per tutti i governi e le organizzazioni internazionali. Ciò, al fine di evitare che la cosiddetta "militarizzazione del cyber-spazio" assuma ben presto contorni particolarmente foschi in conseguenza dell'assenza di precise regole di comportamento.

UCRAINA

Agli inizi di giugno, il Presidente Petro Porošenko ha firmato il decreto per la costituzione del primo *National Cybersecurity Coordination Centre* ucraino.

Questa decisione fa il pari con la recente pubblicazione della prima *cyber-strategy* dell'Ucraina, che, dal marzo del 2016, ha assegnato al *National Security and Defense Council* il compito di coordinare tutte le attività relative al settore della sicurezza cibernetica tra le varie agenzie governative.

Non è un caso, infatti, che il *National Cybersecurity Coordination Centre* sarà collocato proprio all'interno del *National Security and Defense Council* e sarà guidato dal suo segretario, Oleksandr Turchynov. Ne faranno parte, inoltre, gli alti rappresentanti del Ministero della Difesa, il Capo di Stato Maggiore della Difesa, i vertici dei servizi segreti ucraini (il *Sluzhba Bezpeky Ukrayiny* e il *Sluzhba Zovnishnoi Rozvidky Ukrainy*), della polizia nazionale, della Banca Nazionale ucraina e gli altri membri istituzionali che ricoprono incarichi nel settore della *cyber-security*.

Il *National Cybersecurity Coordination Centre* avrà come scopi, tra gli altri, quello di coordinare le attività in ambito sicurezza nazionale e Difesa dei soggetti istituzionali deputati all'attuazione della *cyber-strategy*, di accrescere il livello di efficienza della pubblica amministrazione nella formulazione ed attuazione delle politiche nazionali nel campo della sicurezza informatica, di contribuire all'implementazione delle normative tese alla salvaguardia delle risorse informative statali, delle informazioni classificate e della sicurezza delle infrastrutture critiche nazionali dalle minacce cibernetiche.

La *cyber-strategy*, prima, e la creazione del *National Cybersecurity Coordination Centre* adesso, rappresentano senz'altro degli importanti passi in avanti del governo di Porošenko nel settore della sicurezza cibernetica. Proprio l'Ucraina, infatti, è stata di recente vittima del primo attacco informatico ad una centrale elettrica – pubblicamente conosciuto – che abbia prodotto conseguenze tangibili sulla popolazione.

Il 23 dicembre 2015, infatti, le compagnie energetiche *PrykarpattiaOblEnergo* e *KyivOblEnergo*, deputate ad erogare energia elettrica nella regione occidentale dell'Ucraina, hanno affermato di aver subìto un attacco informatico ai sistemi di gestione di numerose sottostazioni elettriche, causando un *blackout* esteso e prolungato in gran parte della regione che ha tenuto al buio oltre 225.000 persone (per approfondire, si veda il "*Cyber Strategy & Policy Brief*" di gennaio 2016).

In conseguenza di questi recenti avvenimenti e anche in ragione dell'evoluzione dell'approccio strategico verso questo settore da parte degli altri Paesi, non stupisce che anche l'Ucraina abbia pianificato nella sua *cyber-strategy* la creazione di un'unità militare completamente deputata a svolgere attività di "*Active Cyber Defence*". Infatti, seppure tutta l'impostazione della strategia risulti orientata verso una postura marcatamente difensiva, non si può sottacere come il governo Porošenko delinei, invece, sul piano militare un approccio maggiormente reattivo nei confronti dei futuri attacchi cibernetici. Un approccio che, tuttavia, come più volte approfondito nei precedenti "*Cyber Strategy & Policy Brief*" (si vedano, in particolare, quelli di gennaio, marzo, aprile e maggio 2016), in realtà insegue quello delle principali potenze a livello internazionale, che sempre più velocemente sono impegnate nello sviluppo di capacità offensive per svolgere operazioni militari nel e attraverso il cyber-spazio.

Infine, nell'attesa di poter analizzare nel corso del tempo il livello di attuazione della *cyber-strategy* ucraina attraverso le attività del *National Cybersecurity Coordination Centre*, occorre sottolineare fin da subito la mancanza di un elemento cardine, che pare essere fortemente sottovalutato nell'impostazione strategica del governo Porošenko, ovvero la cooperazione tra pubblico e privati.

Seppure l'*Action Plan* per l'attuazione della strategia, approvato dal Consiglio dei Ministri ucraino alla fine di giugno, introduca questo elemento, occorre comunque evidenziare la sua centralità ed importanza nel contesto della sicurezza cibernetica.

E' utile osservare, infatti, come le caratteristiche tipiche del cyber-spazio facciano sì che la cooperazione ad ampio spettro sia qui, più che in altri settori, un elemento assolutamente necessario ed imprescindibile. Ciò soprattutto a causa dell'impossibilità per ciascun attore coinvolto all'interno di questo 'dominio' di disporre – da solo – del quadro complessivo della minaccia cibernetica e di tutte le informazioni necessarie per fronteggiarla.

Il governo, quindi, deve necessariamente allacciare relazioni strette con i privati, peraltro non di rado possessori della maggior parte delle infrastrutture critiche, in quanto è spesso incapace di ricavare autonomamente le cosiddette 'informazioni di soglia' sulle tecniche operative, sugli strumenti e sulle tecnologie utilizzate, nonché – a volte – persino sulle strategie adottate dagli attori che operano nel e attraverso il cyber-spazio.

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.*

Cyber Strategy & Policy Brief (Volume 5 – 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.*