CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 11 / 12 – Novembre / Dicembre 2016

EXECUTIVE SUMMARY

Parole chiave: *Arabia Saudita, Attacchi Cibernetici, Cina, Cyber Command, Cyber Strategy, Governance, India, Infrastrutture Critiche, Iran, Legge, OPEC, Sicurezza Cibernetica.*

Nonostante stia facendo enormi passi in avanti per modernizzare e digitalizzare le proprie infrastrutture nazionali e i relativi processi, l'**Arabia Saudita** appare essere ancora indietro nella capacità di garantire alti standard di sicurezza cibernetica per i suoi principali *asset* strategici, risultando tuttora il Paese del Medio Oriente maggiormente colpito da attacchi informatici.

Ne è una riprova, ad esempio, la recente ondata di attacchi cibernetici subìti a metà novembre da numerose agenzie governative saudite, tra cui la Banca Centrale, il Ministero dei Trasporti e anche l'Autorità Generale dell'Aviazione Civile, costretti a bloccare per alcuni giorni le attività a seguito della cancellazione massiva dei dati indispensabili al funzionamento dei sistemi informatici.

Dall'analisi delle informazioni finora disponibili, si può evincere come sia davvero poco probabile la tesi cavalcata attualmente dai *media* e dalla maggior parte degli esperti che punta il dito in maniera diretta contro **l'Iran**. Molto più probabile appare, invece, l'eventualità di un attacco da parte di gruppi sponsorizzati dal governo iraniano o vicini ad altri Paesi ostili al governo di Riyad. Questi soggetti, infatti, potrebbero essere intenzionati a verificare le abilità e le capacità di soglia dell'Arabia Saudita e delle sue principali istituzioni pubbliche e private, al fine di creare moderati danni politici ed economici nel breve periodo e soprattutto di acquisire preziose informazioni per future ed ipotetiche attività di conflitto nel e attraverso il cyber-spazio.

Sul versante dell'Asia meridionale, invece, agli inizi di dicembre si sono rincorse voci sui *media* della imminente costituzione del primo ***Cyber Command* dell'India**, teso ad unificare e concentrare gli sforzi delle singole Forze Armate per contrastare e mitigare al meglio le sempre più pressanti minacce alla sicurezza nazionale provenienti dal cyber-spazio.

Nonostante questo progetto sia in cantiere sin dal 2010, i tempi non paiono essere ancora maturi e l'attuazione di questo importantissimo obiettivo, che allineerebbe l'India alle altre principali nazioni sia in ambito regionale che globale, pare inspiegabilmente diluirsi ancora una volta nel tempo.

La mancanza di un approccio olistico al problema della sicurezza cibernetica, che metta a fattor comune gli sforzi dei singoli attori istituzionali e del mondo privato disegnando un'architettura

istituzionale coerente e lineare con gli obiettivi, rappresenta senz'altro il principale terreno su cui il governo indiano è chiamato oggigiorno ad intervenire con urgenza e soprattutto con una visione prospettica.

Infine, il focus di questo volume è incentrato sul **nuovo approccio politico-strategico e normativo in materia di sicurezza cibernetica della Cina**.

Comprendere gli obiettivi e le capacità della Cina nel campo della sicurezza cibernetica rappresenta un problema urgente per cogliere appieno la stabilità del quadrante asiatico, nonché, in considerazione delle ambizioni di Pechino di ampliare la propria sfera di influenza in tutto il mondo, anche per capire la politica internazionale in generale.

Il focus, quindi, analizza in maniera approfondita sia la **prima legge del governo di Pechino completamente focalizzata sulla *cyber-security*, che il nuovo documento strategico nazionale per la sicurezza dello spazio cibernetico**.

ARABIA SAUDITA

Nonostante stia facendo enormi passi in avanti per modernizzare e digitalizzare le proprie infrastrutture nazionali e i relativi processi, l'Arabia Saudita appare essere ancora indietro nella capacità di garantire alti standard di sicurezza cibernetica per i suoi principali *asset* strategici, risultando tuttora il Paese del Medio Oriente maggiormente colpito da attacchi informatici.

Se da un lato, infatti, il recente "*National Transformation Program 2030*", attraverso un investimento nei primi 5 anni del progetto di 268 miliardi di Riyal (oltre 66,5 miliardi di euro), punta in maniera ambiziosa a creare nel lungo periodo un vero e proprio ecosistema digitale e all'avanguardia in tutti i 24 enti governativi rilevanti per lo sviluppo economico saudita, dall'altro il governo di Riyad appare ancora in forte ritardo nel settore della sicurezza cibernetica, tanto sul piano strettamente tecnico, quanto soprattutto su quello strategico, di *policy* e legale.

E' una riprova di quanto affermato, ad esempio, la recente ondata di attacchi cibernetici subìti a metà novembre da numerose agenzie governative saudite, tra cui la Banca Centrale, il Ministero dei Trasporti e anche l'Autorità Generale dell'Aviazione Civile, costretti a bloccare per alcuni giorni le attività a seguito della cancellazione massiva dei dati indispensabili al funzionamento dei sistemi informatici.

Seppure le informazioni disponibili siano ancora molto scarne, le società che hanno avuto modo di analizzare il *malware* utilizzato (*Disttrack Wiper* – W32.Disttrack.B) hanno messo in evidenza la sua evidente similitudine con *Shamoon*, ovvero con il *malware* probabilmente adoperato dall'Iran per colpire nel 2012 alcune società saudite operanti nel settore energetico – come, ad esempio, Saudi Aramco – cancellando anche in quel caso i dati critici per il funzionamento dei sistemi informatici.

Questa similitudine di obiettivi e mezzi, unita alle costanti tensioni diplomatiche tra l'Arabia Saudita e l'Iran, hanno portato la maggior parte degli analisti a puntare il dito ancora una volta proprio contro il governo di Teheran.

Del resto, come ampiamente analizzato all'interno del *Cyber Strategy & Policy Brief* di febbraio 2016, Arabia Saudita e Iran sono da tempo impegnati in una strategia di ritorsione equivalente (meglio nota con il termine "*Tit-for-Tat*"), utilizzando anche il cyber-spazio come strumento di provocazione o di reazione.

All'interno del volume di febbraio, infatti, dopo l'ennesima interruzione dei rapporti diplomatici tra i due Stati, si era già anticipato come fosse plausibile che il governo iraniano, onde evitare

un'eccessiva *escalation*, si sarebbe potuto avvalere proprio del cyber-spazio come principale territorio di scontro nei confronti dei sauditi.

Tuttavia, considerate le scarse informazioni al momento disponibili, in questa fase preliminare di analisi risulta opportuno non escludere a priori anche altre ipotesi.

Infatti, potrebbe sembrare altrettanto plausibile che soggetti terzi – quasi certamente statuali o sponsorizzati da uno Stato – possano aver simulato un attacco informatico proveniente dall'Iran per provare ad incrinare i rapporti fra i due Stati alla vigilia dell'accordo sul taglio alla produzione giornaliera di greggio. Accordo, poi, effettivamente raggiunto tra Arabia Saudita e Iran durante il 171esimo meeting dell'Organizzazione dei Paesi Esportatori di Petrolio (OPEC).

Su questa tesi, però, occorre fare due importanti riflessioni.
La prima è senz'altro che un simile attacco informatico – peraltro portato contro uno solo degli attori in gioco – difficilmente avrebbe potuto far precipitare i rapporti diplomatici tra Arabia Saudita e Iran al punto tale da far saltare un accordo su una materia così rilevante. Ne è una riprova il fatto che, nonostante quanto accaduto, l'accordo sia stato comunque siglato.

La seconda riflessione, invece, deriva dalla difficoltà di identificare uno Stato terzo non solo preparato per condurre attacchi cibernetici coordinati su più bersagli sauditi di medio-alto profilo, quanto soprattutto capace di trarre beneficio dall'auspicato naufragio dell'accordo tra i due governi. Analizzando lo scenario, però, Stati Uniti, Russia e gli altri principali attori che posseggono entrambe queste caratteristiche trarranno tutti un vantaggio economico da questo accordo. Ciò, quindi, fa venir meno un loro possibile movente e vacillare ancor di più la tesi esposta dalla maggior parte dei *media* internazionali.

Sul piano delle ulteriori ipotesi, allora, molto più probabile appare l'eventualità di un attacco da parte di gruppi sponsorizzati dal governo iraniano o vicini ad altri Paesi ostili al governo di Riyad. Questi soggetti, infatti, potrebbero essere intenzionati a verificare le abilità e le capacità di soglia dell'Arabia Saudita e delle sue principali istituzioni pubbliche e private, al fine di creare moderati danni politici ed economici nel breve periodo e soprattutto di acquisire preziose informazioni per future ed ipotetiche attività di conflitto nel e attraverso il cyber-spazio.

In conclusione, al di là di chi sia il reale mandante di quest'ultima ondata di attacchi cibernetici, dall'analisi complessiva delle attività politico-strategiche svolte finora dal governo di Riyad, risulta evidente come i numerosi e copiosi investimenti economici messi in campo dall'Arabia Saudita pecchino, in realtà, di un raccordo strategico e normativo capace di svolgere quel ruolo fondamentale di stimolo per il settore pubblico e privato, così come di collante per la loro reciproca collaborazione.

Nonostante il governo saudita abbia chiaramente evidenziato nella sua *National Information Security Strategy* del 2013 la necessità di far fronte e superare simili mancanze, al momento questa raccomandazione pare ancora ben lontana dall'essere attuata.

Ciò ha fatto sì che i principali attori pubblici e privati sauditi abbiano sviluppato nel tempo sistemi di protezione e iniziative nel campo della sicurezza cibernetica solo dopo essere stati bersaglio di un attacco informatico e soprattutto in maniera individuale e non coordinata.

L'auspicio, allora, è che il governo di Riyad concentri quanto prima i suoi sforzi tanto sul piano strettamente tecnico della sicurezza cibernetica, quanto soprattutto su quello strategico, di *policy* e legale, al fine di affiancare al rilevante impegno economico anche una visione strategica chiara e pragmatica che sia di aiuto a tutto il settore.

CINA – FOCUS SU NUOVO APPROCCIO POLITICO-STRATEGICO E NORMATIVO IN MATERIA DI SICUREZZA CIBERNETICA

Comprendere gli obiettivi e le capacità della Cina nel campo della sicurezza cibernetica rappresenta un problema urgente per cogliere appieno la stabilità del quadrante asiatico, nonché, in considerazione delle ambizioni di Pechino di ampliare la propria sfera di influenza in tutto il mondo, anche per capire la politica internazionale in generale. Nonostante riuscire a svolgere una reale valutazione di queste capacità sia un lavoro particolarmente complesso e spesso persino controverso anche fra gli esperti, due recenti documenti mettono bene in evidenza gli obiettivi e gli interessi della Cina nel settore della sicurezza cibernetica.

Il 07 novembre 2016, infatti, il governo di Pechino ha adottato la sua prima legge completamente focalizzata sulla *cyber-security*, mentre, poco prima della fine dell'anno, ha reso pubblico il nuovo documento strategico nazionale per la sicurezza dello spazio cibernetico.

La prima "*Legge della Repubblica Popolare Cinese sulla Sicurezza Cibernetica*"

Per quanto attiene la "*Legge della Repubblica Popolare Cinese sulla Sicurezza Cibernetica*", che entrerà in vigore agli inizi del prossimo giugno, l'intento dichiarato nell'articolo 1 è quello di garantire la sicurezza delle reti per salvaguardare la sovranità sul cyber-spazio, la sicurezza nazionale e gli interessi sociali, ma anche per proteggere i diritti legittimi e gli interessi dei cittadini, delle persone giuridiche e delle altre organizzazioni, nonché per promuovere lo sviluppo economico e sociale attraverso le tecnologie.

Tuttavia, ad una lettura complessiva del testo di legge, si può evidenziare come l'intero tessuto normativo delineato dal legislatore cinese miri, in realtà, a rafforzare attraverso le norme la possibilità e le capacità di controllo del governo di Pechino nei confronti dei cittadini e degli attori pubblici e privati che operano sul territorio della Repubblica Popolare Cinese.

La normativa, peraltro, non fa altro che cristallizzare al suo interno obblighi e divieti per cittadini e operatori che forniscono prodotti e servizi informatici già da tempo vigenti in via informale.

In tale ottica, ad esempio, l'articolo 12 – tra le altre cose – proibisce esplicitamente ad ogni persona e organizzazione di utilizzare le reti per ledere l'onore o gli interessi nazionali cinesi, così come vieta di incitare alla sovversione della sovranità nazionale o al rovesciamento del sistema socialista, oppure di diffondere informazioni false tese a turbare l'ordine economico e sociale.

Sul piano degli attori pubblici e privati, inoltre, seppure appare comunque pregevole lo sforzo fatto dal legislatore cinese di dettare già all'interno della legge alcune misure "minime" di sicurezza per gli operatori di rete (art. 21) e per le società classificabili come infrastrutture critiche informatiche (art. 34), a cui dovranno essere affiancati – a seconda dei settori – uno o più dei sette "*Standard Nazionali in materia di Sicurezza Cibernetica e Protezione dei Dati*" attualmente in fase di consultazione pubblica, alcune perplessità sorgono, invece, dall'analisi di altri articoli del testo normativo.

È questo il caso, ad esempio, dell'articolo 23, che impedisce la vendita o la fornitura di apparecchiature di rete e di prodotti per la loro sicurezza qualora non siano ispezionati e certificati da un istituto governativo che ne attesti l'adesione ai principi dettati dalla normativa cinese e agli *standard* di sicurezza previsti a livello nazionale.

Così come è il caso dell'articolo 37 – uno dei più controversi – che richiede alle società classificabili come infrastrutture critiche informatiche di conservare all'interno del territorio continentale della Repubblica Popolare Cinese tutti i dati personali e ogni altra informazione rilevante acquisita o generata in Cina durante lo svolgimento delle loro attività. Peraltro, qualora per comprovate esigenze di *business* sia necessario inviarle all'estero, queste stesse società dovranno sottoporsi ad una valutazione dei livelli di sicurezza da parte di specifiche strutture statali.

Com'è facilmente evidenziabile, ci si trova dinanzi ad un approccio particolarmente rigido da parte del governo di Pechino, che sostanzialmente ricalca quello da tempo tenuto da altri Stati come la Russia o l'Iran, di cui si è scritto nel *Cyber Strategy & Policy Brief* di maggio 2016.

Ulteriori perplessità derivano, inoltre, dal dettato dell'articolo 58, che riserva al Consiglio di Stato in via diretta o ai governi delle province, delle regioni autonome o dei comuni cinesi su

approvazione preventiva del Consiglio di Stato, la possibilità di limitare temporaneamente le comunicazioni informatiche in caso ci sia necessità di proteggere la sicurezza nazionale, l'ordine pubblico o di rispondere a gravi incidenti di sicurezza che impattino sui cittadini.

L'articolo 75, infine, precisa che nel caso in cui istituzioni straniere, organizzazioni o individui svolgano attacchi, intrusioni, interferenze, danni o altre attività che mettano in pericolo le infrastrutture critiche informatiche della Repubblica Popolare Cinese, causando gravi conseguenze, oltre a risponderne legalmente, il Ministero della Pubblica Sicurezza e le altre strutture statali competenti potrebbero decidere di reagire congelando i beni o adottando ulteriori misure punitive non meglio specificate.

Ad una lettura complessiva di questa prima "*Legge della Repubblica Popolare Cinese sulla Sicurezza Cibernetica*", seppure si evinca in maniera chiara il rilevante e anche pregevole sforzo effettuato dal legislatore cinese per organizzare e armonizzare l'intera materia della sicurezza cibernetica all'interno di un unico testo di legge, non si possono sottacere alcune preoccupazioni su quelle previsioni normative orientate in maniera evidente a garantire al governo di Pechino un forte controllo domestico su tutte le attività svolte nel e attraverso il cyber-spazio da parte dei cittadini, degli operatori pubblici e di quelli privati sia nazionali che internazionali.

Il nuovo documento strategico nazionale in materia di sicurezza cibernetica

Pubblicata il 27 dicembre 2016, la nuova *cyber-strategy* cinese è incentrata principalmente su due obiettivi strategici intimamente connessi con la "*Legge della Repubblica Popolare Cinese sulla Sicurezza Cibernetica*" finora analizzata, ovvero la tutela della sovranità nazionale sul cyber-spazio e la protezione delle proprie infrastrutture critiche informatiche.

Infatti, proprio la difesa della sovranità nazionale sul cyber-spazio è posta all'interno del documento come primo e più importante pilastro strategico per il governo di Pechino, tanto da affermare esplicitamente la volontà di volerla tutelare opponendosi in maniera risoluta ad ogni tentativo di utilizzare la rete Internet per sovvertire il regime nazionale cinese o per sabotare la sua sovranità sul territorio. Per garantirsi questo obiettivo, la Cina afferma, peraltro, di essere pronta ad utilizzare qualsiasi mezzo ritenuto necessario, sia esso scientifico, tecnologico, legale, diplomatico o anche militare.

Unitamente a questo pilastro strategico va letto anche il successivo inerente la tutela della sicurezza nazionale. L'obiettivo in questo caso è quello di prevenire, reprimere e punire secondo la legge una serie di comportamenti ben delineati all'interno della strategia, ovvero:

1. Qualsiasi tentativo di utilizzare la rete Internet per attività di tradimento, separatismo, incitamento alla ribellione o all'eversione o al rovesciamento del regime di dittatura democratica del popolo.

2. Qualsiasi tentativo di utilizzare la rete Internet per sottrarre o far trapelare segreti di Stato o per svolgere altre simili azioni tese a danneggiare la sicurezza nazionale.
3. Qualsiasi tentativo da parte di potenze straniere di utilizzare la rete Internet per attività di infiltrazione, distruzione, sovversione e separatismo.

Il secondo obiettivo strategico predominante all'interno di questa nuova *cyber-strategy* è quello di proteggere le infrastrutture critiche informatiche della Cina.

Sia la legge analizzata in precedenza, che la nuova strategia danno, però, una definizione molto ampia e soprattutto troppo generica di infrastruttura critica informatica, ricomprendendo al suo interno qualsiasi infrastruttura rilevante per la sicurezza nazionale, per l'economia del Paese, nonché per il sostentamento dei suoi cittadini.

La strategia, inoltre, sviscera numerose attività preventive di sicurezza cibernetica tese esclusivamente alla difesa di queste infrastrutture, focalizzando l'attenzione su due elementi:

1. la loro protezione attraverso il rafforzamento delle procedure tese all'identificazione degli utenti, alla prevenzione degli attacchi, al loro monitoraggio e all'*early warning*; e
2. la creazione di deterrenza negli attaccanti grazie alla sicurezza delle infrastrutture critiche informatiche.

Inoltre, in linea con quanto previsto dall'articolo 23 della legge poc'anzi analizzata, il governo di Pechino ribadisce l'intenzione di impedire l'utilizzo in ambito governativo di prodotti e servizi tecnologici che non siano preventivamente ispezionati e certificati da un istituto governativo che ne attesti l'adesione ai principi dettati dalla normativa cinese e agli *standard* di sicurezza previsti a livello nazionale.

La strategia, infine, prevede anche ulteriori obiettivi di sicuro rilievo, come, ad esempio, il rafforzamento delle capacità per il contrasto al terrorismo *on-line*, al controspionaggio e al furto di informazioni, che però vengono soltanto nominati senza alcun approfondimento specifico, oppure la concentrazione degli sforzi per il perfezionamento della *governance* dei sistemi e delle reti nazionali soprattutto attraverso la promulgazione di leggi (come quella qui commentata), o ancora il consolidamento della cooperazione internazionale attraverso l'azione delle Nazioni Unite e la ratifica di accordi bilaterali e multilaterali.

In conclusione, l'analisi congiunta della nuova strategia e della prima legge sulla sicurezza cibernetica evidenziano un approccio da parte di Pechino evidentemente teso a proteggere anzitutto la leadership politica, monitorando e nel caso frenando le attività di informazione e di propaganda operate attraverso il cyber-spazio principalmente dai partiti interni di opposizione e dai gruppi portatori di dissenso politico e sociale.

Contestualmente, l'attenzione governativa risulta rivolta in maniera evidente anche all'affermazione e alla strenua salvaguardia della propria sovranità nazionale sui temi della sicurezza cibernetica, così come al rafforzamento dei livelli di protezione e di difesa delle sue infrastrutture critiche informatiche.

È possibile identificare, quindi, delle priorità strategiche del tutto simili a quelle già delineate nelle precedenti *cyber-strategy* della Cina. Tuttavia, non può non evidenziarsi una maggiore maturità e apertura del governo di Pechino a guardare alla cooperazione internazionale come ad un elemento fondamentale per la sicurezza dello spazio cibernetico e per lo sviluppo dei propri interessi economici e delle sue ambizioni geopolitiche.

INDIA

Agli inizi di dicembre, come ormai da tempo ciclicamente accade, si sono rincorse voci sui *media* indiani della imminente costituzione del primo *Cyber Command*, teso ad unificare e concentrare gli sforzi delle singole Forze Armate per contrastare e mitigare al meglio le sempre più pressanti minacce alla sicurezza nazionale provenienti dal cyber-spazio.

Nonostante questo progetto sia in cantiere sin dal 2010, i tempi non paiono essere ancora maturi e l'attuazione di questo importantissimo obiettivo, che allineerebbe l'India alle altre principali nazioni sia in ambito regionale che globale, pare inspiegabilmente diluirsi ancora una volta nel tempo.

Ciò, peraltro, nonostante il recente nuovo inasprirsi delle tensioni tra India e Pakistan sia sfociato più volte anche in ondate di attacchi informatici mirati ai sistemi governativi indiani.

Del resto, con oltre 460 milioni di utenti su Internet nel 2016, ovvero il 34,8% della popolazione, ed una crescita di circa 100 milioni di nuovi utenti all'anno, l'India non può e non ha mai potuto ignorare il problema della sicurezza cibernetica.

Nonostante ciò, questo Stato appare essere al momento ancora particolarmente indietro rispetto agli altri Paesi nella pianificazione politico-strategica di questo settore e soprattutto nell'attuazione di quanto delineato nella sua *cyber-strategy* del 2013.

Infatti, seppure i ben 14 pilastri strategici della *National Cyber Security Policy* indiana, pubblicata nel 2013 e non ancora aggiornata, avessero posto le basi in maniera corretta e lungimirante per lo sviluppo del settore sia a livello di sicurezza nazionale, che di contrasto alle attività criminali, così come di incremento della conoscenza di queste problematiche da parte

dei cittadini, la sua successiva attuazione, dopo ben tre anni, risulta ancora lontana dalla maggior parte di questi obiettivi.

Inoltre, anche la creazione nel dicembre del 2014 della figura del *Coordinatore Nazionale per la Sicurezza Cibernetica* non è riuscita ad incidere sul piano politico come ci si sarebbe aspettati. Infatti, nonostante i pregevoli sforzi messi in campo finora per il contrasto al crimine informatico, è mancata quella giusta accelerazione del processo di riforma e raccordo istituzionale auspicato dalla *cyber-strategy* indiana e indispensabile per far fronte alle minacce cibernetiche in maniera efficiente ed efficace.

In conclusione, la mancanza di un approccio olistico al problema della sicurezza cibernetica, che metta a fattor comune gli sforzi dei singoli attori istituzionali e del mondo privato disegnando un'architettura istituzionale coerente e lineare con gli obiettivi, rappresenta senz'altro il principale terreno su cui il governo indiano è chiamato oggigiorno ad intervenire con urgenza e soprattutto con una visione prospettica.

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 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.*

Cyber Strategy & Policy Brief (Volume 07 e 08 – Luglio/Agosto 2016)

Parole chiave: *Cyber Warfare, FBI, DHS, ODNI, Regole di Ingaggio per il Cyber-Spazio, Stati Uniti.*

Cyber Strategy & Policy Brief (Volume 09 – Settembre 2016)

Parole chiave: *Cyber Warfare, Department of Homeland Security (DHS), Diritto Internazionale, Elezioni, Influenza Informativa, Information Warfare, Nazioni Unite, Offensive Cyberspace Operations, Office of the Director of National Intelligence (ODNI), Propaganda, Russia, Sistemi di voto elettronico, Spionaggio, Stati Uniti.*

Cyber Strategy & Policy Brief (Volume 10 – Ottobre 2016)

Parole chiave: *Analisi del Rischio, Associazione delle Nazioni del Sud-Est Asiatico (ASEAN), Crimini Informatici, G7, Infrastrutture Critiche, Settore Finanziario, Sicurezza Nazionale, Singapore, Strategia, Turchia, Stati Uniti.*