CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 10 – Ottobre 2016

EXECUTIVE SUMMARY

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*.

A metà ottobre, i Ministri delle Finanze e i Governatori delle Banche Centrali dei Paesi del G7 hanno reso pubblico il documento dal titolo "*G7 Fundamental Elements of Cybersecurity for the Financial Sector*".

I principi generali tracciati all'interno di questa linea guida hanno l'obiettivo di fornire un quadro di riferimento comune per lo sviluppo di strategie in materia di sicurezza cibernetica per gli operatori del settore finanziario sia pubblici che privati.

Il documento amalgama in maniera semplice e lineare i principi fondamentali tipici di ogni processo di gestione del rischio aziendale, al di là se ci si focalizzi sul settore finanziario o meno. L'approccio, del resto, non potrebbe essere differente, soprattutto in considerazione del ventaglio particolarmente ampio di realtà finanziarie da coprire attraverso queste linee guida, non solo sotto il punto di vista prettamente operativo, quanto soprattutto anche sotto quello geografico.

Sul piano statale, invece, sia Singapore che la Turchia hanno reso pubblici gli aggiornamenti delle loro *cybersecurity strategy*.

Appare innegabile come siano molte le iniziative nel settore della sicurezza cibernetica che il governo di Singapore, dal 2013 ad oggi, continua a mettere in campo. La maggior parte di queste, però, appaiono essere ancora troppo concentrate verso l'interno della nazione o al massimo verso i Paesi dell'Associazione delle Nazioni del Sud-Est Asiatico (ASEAN).

In quest'ottica, allora, quanto mai opportuna potrebbe essere una maggiore apertura del governo di Singapore anche nei confronti degli altri attori internazionali, al fine di condividere esperienze, informazioni e *best practice* per il contrasto di questa minaccia.
Ciò a maggior ragione per un Paese come Singapore che – per sua stessa ammissione anche all'interno della nuova *cybersecurity strategy* – si candida ad essere "*un centro sicuro e affidabile*" a livello internazionale per il settore della sicurezza cibernetica.

La *National Cyber Security Strategy 2016-2019* della Turchia appare un documento sicuramente molto interessante, anche se una migliore esplicitazione, descrizione e

strutturazione degli obiettivi strategici potrebbe permettere una sua più immediata comprensione e soprattutto attuazione.

Al di là di ciò, occorre evidenziare come siano molto interessanti – anche se forse un po' tardive – alcune azioni che il governo turco intende intraprendere, come, ad esempio, l'obiettivo di creare un inventario delle infrastrutture critiche nazionali evidenziando i requisiti e le necessità di sicurezza cibernetica di ognuna di esse, oppure l'intenzione di dare un ampio supporto legislativo, economico e di personale teso al rafforzamento dei *Cyber Incidents Response Team* (CIRT), così come la volontà di creare un'autorità pubblica centrale alle dirette dipendenze del Primo Ministro per coordinare tutti gli sforzi governativi in questo settore.

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 SUL DOCUMENTO "G7 *FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR*"

A metà ottobre, i Ministri delle Finanze e i Governatori delle Banche Centrali dei Paesi del G7 hanno reso pubblico il documento dal titolo "*G7 Fundamental Elements of Cybersecurity for the Financial Sector*".

I principi generali tracciati all'interno di questa linea guida hanno l'obiettivo di fornire un quadro di riferimento comune per lo sviluppo di strategie in materia di sicurezza cibernetica per gli operatori del settore finanziario sia pubblici che privati.

L'odierna pubblicazione segue, peraltro, quanto già delineato alla fine di maggio di quest'anno dai leader di governo dei Paesi del G7 all'interno del documento dal titolo "*G7 Principles and Actions on Cyber*", per la cui analisi si rimanda a quanto approfondito all'interno del *Cyber Strategy & Policy Brief* di maggio 2016.

Il "G7 *Fundamental Elements of Cybersecurity for the Financial Sector*" delinea ben otto principi generali per gli operatori del settore finanziario, ovvero:

1. **Strategia e Framework per la Sicurezza Cibernetica.**

   L'obiettivo è quello di realizzare e mantenere nel tempo una strategia e un *framework* comune incentrati sui rischi cibernetici specifici per l'ambito finanziario, che siano ispirati a principi e norme nazionali, internazionali e di settore.

2. **Governance.**

   L'obiettivo è quello di creare strutture di *governance* in grado di operare in maniera efficace, aumentando le responsabilità attraverso incarichi e linee gerarchiche e di riporto chiare.

3. **Analisi del Rischio e Controllo.**

   L'obiettivo è quello di misurare il rischio cibernetico proveniente da individui, processi e tecnologie, evidenziando i dati a supporto di ogni funzione, attività, prodotto e servizio identificato.

4. **Monitoraggio.**

   L'obiettivo è quello di definire dei processi di monitoraggio che permettano di individuare agevolmente gli incidenti cibernetici e di verificare periodicamente l'efficacia dei controlli effettuati attraverso attività di monitoraggio, controllo e ispezione della rete, oltre che per mezzo di esercitazioni.

5. Risposta.

L'obiettivo è quello di riuscire tempestivamente ad (a) identificare la natura, la portata e gli effetti di un incidente cibernetico; (b) contenere l'incidente e limitare al minimo i suoi effetti; (c) informare gli attori interni ed esterni (Forze dell'Ordine, autorità di controllo e altri enti pubblici, ma anche azionisti, altri fornitori di servizi e i clienti, se dovuto); e (d) coordinare risposte collettive, se necessario.

6. Ripristino.

L'obiettivo è quello di riprendere l'operatività in maniera responsabile, consentendo però di continuare a ricercare soluzioni all'incidente attraverso i seguenti comportamenti: (a) eliminare ciò che è pericoloso; (b) ristabilire il regolare funzionamento dei sistemi e dei dati, confermandone la regolarità; (c) identificare e attenuare gli effetti dannosi di tutte le vulnerabilità sfruttate durante l'incidente; (d) porre rimedio alle vulnerabilità per evitare che simili incidenti si verifichino nuovamente; e (e) gestire in modo adeguato la comunicazione sia interna che esterna.

7. Condivisione delle Informazioni.

L'obiettivo è quello di impegnarsi a condividere in maniera tempestiva informazioni attendibili e utili sia con gli attori interni che esterni (ivi compresi gli enti e gli organismi pubblici operanti sia all'interno che al di fuori del settore finanziario) su minacce, vulnerabilità, incidenti e risposte, in modo da migliorare le capacità di difesa, limitare i danni, incrementare la consapevolezza della situazione e accrescere la conoscenza di questi temi.

8. Apprendimento Continuo.

L'obiettivo è quello di revisionare periodicamente la strategia e il *framework* per la sicurezza cibernetica e inoltre, se gli eventi dovessero richiederlo, di dedicarsi alle evoluzioni dei rischi cibernetici, stanziare fondi, identificare e cercare di colmare eventuali lacune e trarre insegnamento dalle lezioni apprese.

Com'è facilmente desumibile, il documento amalgama in maniera semplice e lineare i principi fondamentali tipici di ogni processo di gestione del rischio aziendale, al di là se ci si focalizzi sul settore finanziario o meno.

L'approccio, del resto, non potrebbe essere differente, soprattutto in considerazione del ventaglio particolarmente ampio di realtà finanziarie da coprire attraverso queste linee guida, non solo sotto il punto di vista prettamente operativo, quanto soprattutto anche sotto quello geografico.

Ciò che più rileva, allora, è sicuramente la volontà ferma dei Paesi del G7 di continuare a concentrare i loro sforzi anche sulle problematiche relative al mondo della sicurezza

cibernetica, come già avvenuto nel maggio di quest'anno e come ci si aspetta avverrà ancora in futuro durante la presidenza italiana del G7 del prossimo anno.

SINGAPORE

Agli inizi di ottobre, il governo di Singapore ha aggiornato la sua *cybersecurity strategy*, pubblicando un documento approfondito e ben strutturato, che ha l'obiettivo di tracciare le nuove linee strategiche di sviluppo di questo settore nel medio-lungo periodo.

In realtà, la sicurezza cibernetica è risultata sin dal 2005 uno degli elementi cardine della politica nazionale di questo Stato. Nel corso degli anni, infatti, sono state pubblicate ben altre tre strategie: le prime due denominate *Infocomm Security Masterplan,* aventi come finalità lo sviluppo delle capacità e competenze utili alla protezione dalle minacce cibernetiche dei sistemi informatici della pubblica amministrazione (2005) e delle infrastrutture critiche (2008). L'ultima, resa pubblica nel 2013 e denominata *National Cyber Security Masterplan 2018*, rivolta a proteggere, con un approccio più strutturato e olistico, l'intero ecosistema governativo e civile.

Proprio da quest'ultima strategia è scaturita anche la creazione – nel 2015 – di due strutture chiave nell'assetto organizzativo nazionale per il contrasto a queste minacce: la *Cyber Security Agency of Singapore* e il *Cybercrime Command*. La prima, incardinata all'interno dell'ufficio del Primo Ministro, con lo scopo di centralizzare e coordinare tutte le agenzie e le iniziative in materia di sicurezza cibernetica fino ad allora realizzate (come, ad esempio, la *Singapore Infocomm Technology Security Authority* e il *Singapore Computer Emergency Response Team*). La seconda, alle dipendenze del Ministero dell'Interno, con lo scopo di creare un'unità di *élite* della *Singapore Police Force*, deputata specificatamente alle investigazioni digitali sia sul piano nazionale che internazionale.

Il nuovo documento strategico nazionale per la sicurezza cibernetica, denominato *Singapore's Cybersecurity Strategy*, fonda la sua azione su quattro linee strategiche molto ampie, ma ben centrate sulle più importanti e condivise esigenze a livello internazionale, ovvero:

1. **Rendere le infrastrutture resilienti agli attacchi informatici.**

   L'obiettivo è quello di proteggere anzitutto le infrastrutture critiche nazionali e la loro capacità di erogare tutti i servizi essenziali per la collettività. Ciò deve avvenire non solo elevando il livello di sicurezza cibernetica di queste infrastrutture attraverso il ben noto principio della "*Security-by-Design*", ma anche sviluppando processi di gestione del rischio e piani di intervento e di recupero dell'operatività che siano ben strutturati e calibrati.

2. **Rendere il cyber-spazio più sicuro.**

L'obiettivo è quello di continuare a contrastare in maniera sempre più coordinata ed efficace i crimini informatici – tanto sul piano nazionale, che internazionale – proteggendo al contempo i dati personali dei cittadini. In quest'ottica, un ruolo sicuramente decisivo sarà svolto anche dall'attuazione o meno del *National Cybercrime Action Plan*, varato nel luglio del 2016 dal Ministero dell'Interno. Questo *Piano Nazionale*, infatti, poggia le sue basi su quattro pilasti strategici molto efficaci e concreti, ovvero la prevenzione dei crimini informatici, la costante analisi prospettica di lungo periodo dello scenario criminale e delle sue evoluzioni, l'irrobustimento e la semplificazione del sistema di giustizia penale, nonché il contrasto alla criminalità informatica come responsabilità condivisa sia sul piano nazionale che internazionale.

3. **Sviluppare un ecosistema vivace nel settore della sicurezza cibernetica.**

L'obiettivo è quello di stringere accordi di collaborazione con il settore privato e l'accademia per lo sviluppo di una cultura della sicurezza cibernetica, che porti alla nascita di un ecosistema nazionale di aziende, start-up, programmi di ricerca e sviluppo in questo settore, nonché alla creazione di forza lavoro specializzata.

4. **Rafforzare la collaborazione internazionale.**

L'obiettivo è quello di sviluppare ancora più intensi rapporti di cooperazione e collaborazione per il contrasto alle minacce cibernetiche e al crimine informatico sul piano internazionale e, in particolare, con i Paesi dell'Associazione delle Nazioni del Sud-Est Asiatico (ASEAN).

Come evidenziato in precedenza, l'analisi della *Singapore's Cybersecurity Strategy* mostra un approccio basato su pochi pilastri strategici e molto ampi. Nonostante ciò, il documento appare coerente e ben centrato sulle più importanti e condivise priorità strategiche per il settore della sicurezza cibernetica individuate dai principali attori internazionali.

Opportunamente ambiziosi per un arco temporale di lungo periodo appaiono, inoltre, gli obiettivi concernenti la protezione e la resilienza delle infrastrutture critiche nazionali e soprattutto il contrasto al crimine informatico, intimamente legato all'attuazione del *National Cybercrime Action Plan*.

Appare innegabile come siano molte le iniziative nel settore della sicurezza cibernetica che il governo di Singapore, dal 2013 ad oggi, continua a mettere in campo. La maggior parte di queste, però, appaiono essere ancora troppo concentrate verso l'interno della nazione o al massimo verso i Paesi dell'Associazione delle Nazioni del Sud-Est Asiatico (ASEAN).

In quest'ottica, allora, quanto mai opportuna potrebbe essere una maggiore apertura del governo di Singapore anche nei confronti degli altri attori internazionali, al fine di condividere esperienze, informazioni e *best practice* per il contrasto di questa minaccia.
Ciò a maggior ragione per un Paese come Singapore che – per sua stessa ammissione anche all'interno della nuova *cybersecurity strategy* – si candida ad essere "*un centro sicuro e affidabile*" a livello internazionale per il settore della sicurezza cibernetica.

STATI UNITI

La galassia di aziende che supportano il mondo governativo sono da sempre uno degli anelli più deboli per un'efficace strategia di difesa e contrasto nei confronti della minaccia cibernetica e soprattutto dello spionaggio elettronico.

Creare soluzioni efficaci in materia di sicurezza delle informazioni, sensibilizzando e soprattutto responsabilizzando questo genere di attori, è allora quanto di più auspicabile da parte di ogni governo che voglia davvero salvaguardare le proprie informazioni riservate dagli attacchi informatici portati nel e attraverso il cyber-spazio.

Proprio nel solco di quest'esigenza si inserisce la *Final Rule* del *Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities*, divenuta totalmente operativa già dal 03 novembre 2016.

Questa norma, infatti, impone a tutte le aziende e ai loro subappaltatori che svolgono qualsiasi tipologia di attività nei confronti del Dipartimento della Difesa americano di comunicare entro 72 ore qualsiasi tipologia di incidente informatico occorso ai loro sistemi.

La norma cristallizza due principi fondamentali, da un lato, quello di obbligare le società satellite che collaborano con il mondo della Difesa americana alla condivisione delle informazioni relative a qualsivoglia incidente informatico, dall'altro di costringerle a farlo in un arco temporale che sia quanto più breve possibile.

L'intento sotteso è molto evidente: non solo raccogliere le informazioni sugli incidenti informatici per proteggere i progetti o i programmi di sviluppo in atto, ma anche e soprattutto di mettere quelle informazioni a sistema affinché siano immediatamente utilizzate per scopi di contrasto alla criminalità informatica, così come per attività di contro-intelligence e di sicurezza nazionale.

In merito a questo punto, la *Final Rule* è molto precisa ed esplicitamente sottolinea questi obiettivi, classificando come informazioni privilegiate da condividere proprio quelle utili al Dipartimento della Difesa americano per le attività di analisi forense degli incidenti informatici.

Questo approccio, peraltro, trova ancor di più la sua logica nell'obbligo per le aziende collaboratrici di condividere anche le "semplici" violazioni alle procedure interne di sicurezza. Questa specificazione è palesemente atta a contenere i casi di esfiltrazione di informazioni riservate da parte di eventuali dipendenti infedeli: tema particolarmente critico per gli Stati Uniti, soprattutto dopo le vicende di Edward Snowden e, più di recente, di Harold Thomas Martin III.

Questa impostazione differenzia in maniera netta questo programma di condivisione delle informazioni con quello – ben più famoso – denominato *Cybersecurity Information Sharing Act* (CISA), ove le informazioni sono raccolte e messe a sistema per i soli scopi di sicurezza informatica.

L'entrata in vigore della *Final Rule* evidenzia ancora una volta il grande lavoro in atto nel settore della sicurezza cibernetica da parte del Dipartimento della Difesa americano, che sembra avere finora l'approccio più coerente e globale a questo settore.

TURCHIA

Presentata agli inizi di settembre, ma resa pubblica in inglese soltanto ad ottobre, la *National Cyber Security Strategy 2016-2019* della Turchia aggiorna il precedente documento dal titolo *National Cyber Security Strategy and 2013-2014 Action Plan*, dettando i nuovi indirizzi strategici per il settore della sicurezza cibernetica nel triennio 2016-2019.

La precedente strategia aveva indentificato 7 linee di azione di alto livello da porre in essere attraverso ben 29 indirizzi operativi, accuratamente individuati all'interno del suo *2013-2014 Action Plan* sia sotto il punto di vista dei contenuti, che delle tempistiche e dei soggetti responsabili della loro attuazione.

Appare interessante evidenziare come il governo turco, pur non avendo dato attuazione all'intero *2013-2014 Action Plan*, abbia comunque posto in essere nel tempo alcune iniziative di particolare rilievo.

E' questo il caso, ad esempio, dell'*Ulusal Siber Olaylara Müdahale Merkezi* (Centro Nazionale per la Risposta agli Incidenti Informatici) e dei suoi *Siber Olaylara Mildahale Ekipleri* (Team di Risposta agli Incidenti Informatici), che hanno il compito di fornire un'assistenza costante e

continuativa per individuare e contrastare le minacce cibernetiche che attentino alla sicurezza nazionale turca. Così come di sicuro rilievo sono le numerose azioni poste sotto la responsabilità del *Türkiye Bilimsel ve Teknolojik Araştırma Kurumu* (Consiglio Turco per la Ricerca Scientifica e Tecnologica) per la salvaguardia della sicurezza informatica delle infrastrutture critiche nazionali, oppure ancora la creazione, nel dicembre del 2012, del *TSK Siber Savunma Komutanlığı* (Comando Militare per la Sicurezza Cibernetica).

Attraverso l'odierna *National Cyber Security Strategy 2016-2019*, il governo di Ankara ha deciso di puntare su due obiettivi principali: il primo, teso a porre in essere ogni azione utile per far comprendere a tutti gli *stakeholder* che la sicurezza cibernetica è parte integrante della sicurezza nazionale turca; il secondo, volto a far acquisire le competenze tecnologiche e di *governance* necessarie affinché sia il settore pubblico che il settore privato raggiungano e mantengano elevati livelli di sicurezza cibernetica.

Per conseguire questi obiettivi, il governo turco ha identificato ben 5 pilatri strategici, ovvero:

1. **Rafforzare la difesa cibernetica e la protezione delle infrastrutture critiche nazionali.**

   L'obiettivo è quello di ridurre i rischi derivanti dagli attacchi cibernetici che possano nuocere all'economia turca, alle infrastrutture critiche e alla collettività.

2. **Contrastare il crimine informatico.**

   L'obiettivo è quello di ridurre i rischi causati dalle attività criminali nel e attraverso il cyber-spazio che possano affliggere le istituzioni e i cittadini.

3. **Migliorare la consapevolezza della minaccia e le competenze umane per contrastarla.**

   L'obiettivo è quello di porre in essere ogni azione necessaria affinché la cultura della sicurezza cibernetica raggiunga ogni strato e grado della società.

4. **Sviluppare un ecosistema nel settore della sicurezza cibernetica.**

   L'obiettivo è quello di realizzare, attraverso il contributo di tutti gli *stakeholder* sia del settore pubblico che di quello privato e non governativo, ogni azione utile ad identificare ed implementare tutti i requisiti di legge e le tecnologie necessarie allo sviluppo di un ecosistema nazionale nel settore della sicurezza cibernetica.

5. **Integrare la sicurezza cibernetica nella sicurezza nazionale.**

   L'obiettivo è quello di porre in essere ogni azione utile per far comprendere a tutti gli *stakeholder* che la sicurezza cibernetica è parte integrante della sicurezza nazionale turca.

La *National Cyber Security Strategy 2016-2019* appare, però, meno rigida rispetto alla precedente nell'individuazione dei tempi e dei ruoli. Infatti, seppure siano elencate ben 18

azioni operative per l'attuazione dei 5 principi strategici poc'anzi delineati, nessuna indicazione viene fornita – almeno nella sua versione pubblica – in merito alle tempistiche e alle singole responsabilità nella concretizzazione di ognuna di esse.

Al di là di ciò, occorre evidenziare come siano molto interessanti – anche se forse un po' tardive – alcune azioni che il governo turco intende intraprendere, come, ad esempio, l'obiettivo di creare un inventario delle infrastrutture critiche nazionali evidenziando i requisiti e le necessità di sicurezza cibernetica di ognuna di esse, oppure l'intenzione di dare un ampio supporto legislativo, economico e di personale teso al rafforzamento dei *Cyber Incidents Response Team* (CIRT), così come la volontà di creare un'autorità pubblica centrale alle dirette dipendenze del Primo Ministro per coordinare tutti gli sforzi governativi in questo settore.

In conclusione, la *National Cyber Security Strategy 2016-2019* appare un documento sicuramente molto interessante, anche se una migliore esplicitazione, descrizione e strutturazione degli obiettivi strategici potrebbe permettere una sua più immediata comprensione e soprattutto attuazione.

Nonostante ciò, il documento si concentra sulle più importanti e condivise priorità strategiche per il settore della sicurezza cibernetica individuate dai principali attori internazionali.

Occorre evidenziare, infine, come le maggiori critiche sull'operato del governo turco si siano finora incentrate sulle difficoltà di coordinare una risposta coerente ed efficace nei confronti degli attacchi cibernetici, nonostante il continuo impegno del *National Cyber Council*. In quest'ottica, appare evidente come il suo posizionamento all'interno del Ministero dei Trasporti, della Navigazione e delle Comunicazioni ne rallenti l'operato in caso di crisi cibernetiche e, soprattutto, diminuisca la sua capacità di incidere a livello politico e operativo.

Queste difficoltà, però, potrebbero presto trovare una soluzione proprio grazie alla nuova strategia. La volontà di creare un'autorità pubblica centrale – alle dirette dipendenze del Primo Ministro – con il compito di coordinare tutti gli sforzi governativi nel settore della sicurezza cibernetica dev'essere, infatti, una delle più rilevanti e urgenti priorità in fase di attuazione della *National Cyber Security Strategy 2016-2019*.

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 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.*

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.*