CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 09 – Settembre 2016

EXECUTIVE SUMMARY

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.*

Il volume di settembre del "*Cyber Strategy & Policy Brief*" è completamente dedicato alle tensioni tra Stati Uniti e Russia alla vigilia delle elezioni americane.

All'alba delle ormai imminenti elezioni presidenziali, infatti, il governo russo è sospettato di svolgere operazioni di influenza informativa tese a condizionare la campagna elettorale americana, in particolar modo attraverso la sottrazione illecita e la successiva pubblicazione su Internet di email private e di informazioni riservate del Comitato Nazionale Democratico.

A questo sospetto, inoltre, si aggiunge anche quello di svolgere regolarmente un lavoro di analisi da remoto dei sistemi informatici deputati alla gestione del voto elettronico di alcuni Stati americani, al fine di verificarne la solidità sul piano della sicurezza per provare a manometterne il funzionamento e quindi anche i risultati.

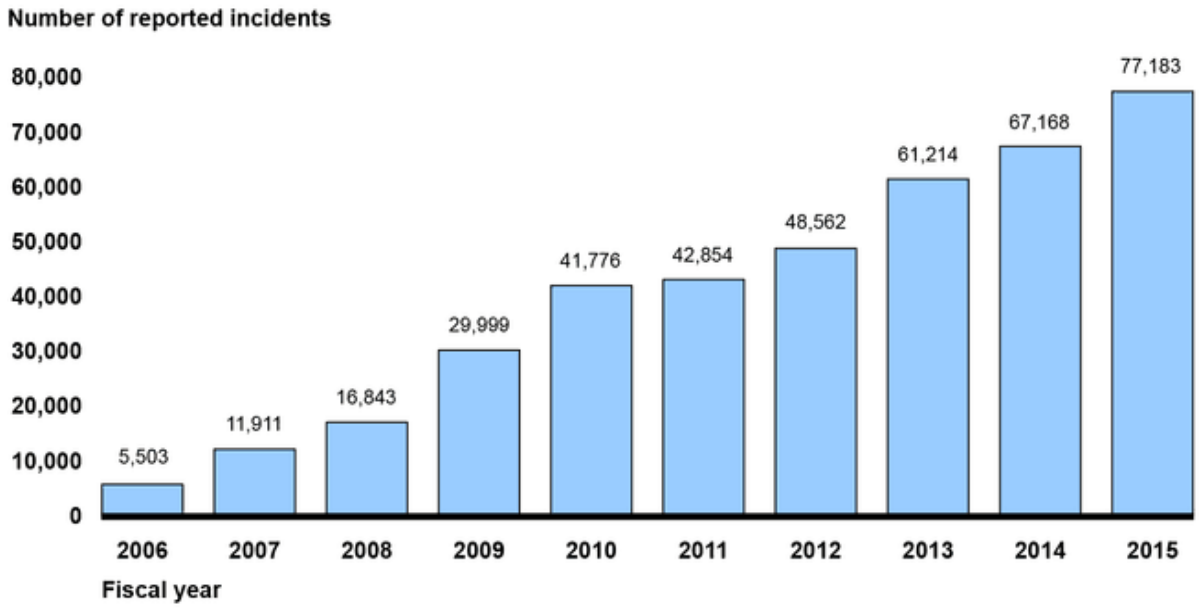
Il *paper*, pertanto, analizza:

- Le accuse formali degli Stati Uniti alla Russia.
- La strategia russa.
- La strategia americana.
- Le problematiche di una reazione americana.
- La strategia di protezione dei sistemi di voto elettronico.
- Le possibili risposte degli Stati Uniti alle attività russe.

FOCUS SU ELEZIONI AMERICANE E TENSIONI POLITICHE TRA STATI UNITI E RUSSIA

Gli Stati Uniti continuano ad essere uno dei principali bersagli degli attacchi informatici da parte dei più importanti attori a livello internazionale, siano essi statali o sponsorizzati da uno Stato, organizzazioni criminali, gruppi terroristici o semplici attivisti.

Secondo recenti stime ufficiali, il numero di incidenti informatici subiti dalle sole agenzie federali statunitensi è aumentato negli ultimi dieci anni del 1.300%. Nel 2015, infatti, sono stati registrati ben 77.183 incidenti contro i 5.503 del 2006.



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Se si guarda ai recenti avvenimenti, appare chiaro come minacce legate alla propaganda, alla disinformazione, alla manipolazione delle informazioni e allo spionaggio abbiano da tempo trovato nuove "strade" – peraltro anche molto efficaci – proprio grazie al cyber-spazio.

Come analizzato anche all'interno del *"Cyber Strategy & Policy Brief"* di marzo 2016, l'attuale incapacità di generare reale deterrenza, unita alle difficoltà nel coordinare ruoli, competenze e risposte alle minacce cibernetiche, contribuisce a creare sul piano internazionale una trama sempre più fitta e preoccupante.

Le accuse formali degli Stati Uniti alla Russia.

All'interno di questo scenario si inquadrano le recenti accuse formali nei confronti della Russia mosse dal *Department of Homeland Security* (DHS) e dall'*Office of the Director of National Intelligence* (ODNI) americano.

All'alba delle ormai imminenti elezioni presidenziali, infatti, il governo russo è sospettato di svolgere operazioni di influenza informativa tese a condizionare la campagna elettorale americana, in particolar modo attraverso la sottrazione illecita e la successiva pubblicazione su Internet di email private e di informazioni riservate del Comitato Nazionale Democratico.
A questo sospetto, inoltre, si aggiunge anche quello di svolgere regolarmente un lavoro di analisi da remoto dei sistemi informatici deputati alla gestione del voto elettronico di alcuni Stati americani, al fine di verificarne la solidità sul piano della sicurezza per provare a manometterne il funzionamento e quindi anche i risultati.

La strategia russa.

Il governo russo, però, non è assolutamente nuovo a questo genere di comportamenti. Ad esempio, stando alle accuse, i tentativi di influenzare la campagna elettorale presidenziale in Ucraina nel 2014 si sono basati proprio su intense attività di influenza informativa, di propaganda, così come su attacchi informatici tesi a violare la sicurezza dei sistemi di voto elettronico o a sottrarre informazioni riservate da riversare poi su Internet.

Tuttavia, queste tipologie di attività si devono inquadrare non solo nel preciso momento storico in cui avvengono, come da ultimo, ad esempio, il voto presidenziale americano, ma nel più ampio approccio strategico di Mosca, teso da sempre a destabilizzare e seminare incertezza nelle istituzioni dei Paesi considerati nemici attraverso operazioni di influenza, ingerenza, disinformazione e intossicazione informativa. La strategia russa, infatti, è principalmente una strategia di influenza e non di forza, che mira quindi a minare la coerenza interna dei governi e non a distruggerli completamente.

La strategia americana.

Simili accuse da parte di Washington – peraltro così dirette – evidenziano, allora, un obiettivo politico-strategico molto preciso.

Cominciando a perseguire in maniera diretta e formale gli autori materiali dei crimini informatici di natura statale o sponsorizzati da uno Stato, il governo americano prova anzitutto a dimostrare pubblicamente le proprie capacità di rintracciare gli autori di quegli attacchi.

Ciò significa inviare a livello internazionale il messaggio di essere in grado di risolvere il principale problema nel settore della sicurezza cibernetica, ovvero l'anonimato e l'incapacità di

attribuire con certezza e in tempi ragionevoli la responsabilità di un attacco informatico ai suoi autori materiali.
Peraltro – ed è questo un ulteriore elemento fondamentale – l'acquisizione di questa capacità concorre a colmare uno dei principali "vuoti" per il rafforzamento di una strategia di deterrenza per il cyber-spazio che sia realmente coerente ed efficace.

Invero, come si è avuto modo di approfondire anche nel *"Cyber Strategy & Policy Brief"* di marzo 2016, gli Stati Uniti da tempo hanno cominciato a portare avanti questo genere di strategia. Già nel maggio del 2014, infatti, il Dipartimento della Giustizia americano ha formalmente accusato di spionaggio elettronico cinque membri della *Unità 61938* della *People's Liberation Army* (PLA) cinese per aver violato i sistemi informatici di sei aziende americane alla ricerca di segreti industriali.

A questa prima denuncia ha fatto seguito un'altra, agli inizi del 2016, nei confronti di ben sette iraniani, impiegati in due aziende private operanti per il governo di Teheran e il suo *Islamic Revolutionary Guard Corps*, per aver condotto – tra il 2011 e il 2013 – una campagna coordinata di attacchi informatici contro il settore finanziario degli Stati Uniti. Inoltre, per uno di questi sette iraniani l'accusa è anche di aver abusivamente conseguito più volte l'accesso ai sistemi informatici di comando e controllo di una diga di New York.

Le problematiche di una reazione americana.

Ciononostante, se da un lato appaiono evidenti i benefici di questo approccio reattivo agli attacchi informatici subiti, dall'altro simili accuse pubbliche implicano per gli Stati Uniti alcune problematiche di non poco conto.

Sul piano legale, anzitutto, occorre evidenziare come proprio il governo americano sia stato tra i principali promotori e firmatari del rapporto alle Nazioni Unite del 2015 predisposto dal Gruppo di Esperti Governativi, in cui, proprio in merito agli attacchi informatici, si statuisce che l'accusa di organizzare o supportare atti illeciti contro un altro Stato dovrebbe essere sempre provata.

Tuttavia, dimostrare le responsabilità del governo russo significherebbe per gli Stati Uniti rendere pubbliche le proprie capacità di intelligence nei confronti di Mosca, peraltro quasi certamente non solo quelle nel settore cibernetico. Dal canto suo, il governo russo, acquisite queste informazioni, potrebbe agevolmente comprendere le proprie falle e i propri punti deboli, rimediando in tempi molto brevi e indebolendo così le capacità di intelligence americane.

E' di tutta evidenza, dunque, che anche in merito alla minacciata reazione agli attacchi informatici russi, Obama dovrà confrontarsi con decisioni molto complesse.

Sul piano della politica militare, però, le opzioni per il governo statunitense di certo non mancano.

Infatti, seppure gli Stati Uniti abbiano cominciato a ragionare ed organizzare le proprie forze per l'*information warfare* e la *cyber-warfare* all'indomani della prima guerra del Golfo del 1991, lo sfruttamento del cyber-spazio per scopi militari operativi è stato ufficializzato nel 2004, quando l'allora *National Military Strategy* esplicitamente statuì che "*le Forze Armate* [americane] *devono avere la capacità di operare attraverso i domini dell'aria, della terra, del mare, dello spazio e del cyberspazio"*. Concetto sfociato, poi, nella *Quadrennial Defense Review* del 2006, in cui si dichiarò per la prima volta che il Dipartimento della Difesa americano avrebbe considerato il cyber-spazio come un nuovo dominio per la conflittualità.

Per di più, la de-secretazione della dottrina militare *Joint Publication 3-12* del 2013 dedicata proprio alle "*Cyberspace Operations*" ha da tempo evidenziato come il Pentagono abbia dato formale riconoscimento e impieghi attività militari offensive volte a "*proiettare forza nel e attraverso il cyber-spazio*", al fine di "*degradare, danneggiare o distruggere l'accesso, il funzionamento o la disponibilità delle capacità di un bersaglio ad un livello e per un periodo di tempo determinato*", oppure per "*controllare o modificare le informazioni, i sistemi informatici o le reti dell'avversario*" (attività denominate "*Offensive Cyberspace Operations*" o OCO).

A queste statuizioni si deve aggiungere, infine, anche quella importantissima del 2011 contenuta nella *International Strategy for Cyberspace*, in cui gli Stati Uniti si sono riservati il diritto di rispondere ad un atto ostile occorso nel o attraverso il cyber-spazio con ogni mezzo necessario – diplomatico, informativo, militare ed economico. Ciò, quindi, lascia trasparire la possibilità di rispondere ad un attacco informatico subìto anche con un'operazione militare convenzionale.

Tuttavia, questo genere di previsioni e all'atto pratico anche di operazioni militari prestano ancora oggi il fianco a rilevanti questioni – soprattutto giuridiche – ancora ben lontane dal trovare una soluzione.

Infatti, è ormai pacifico che le vigenti norme di diritto internazionale siano applicabili anche all'utilizzo da parte degli Stati di strumenti informatici. Fra i tanti principi fondamentali enunciati, quelli di umanità, necessità, proporzionalità e distinzione devono essere sempre tenuti in debita considerazione, a maggior ragione nel caso di una reazione militare ad un attacco.

Conformarsi a questi principi di diritto e controllare l'*escalation* di un attacco informatico, quindi, non è allo stato attuale un'attività facile e immediata.

La strategia di protezione dei sistemi di voto elettronico.

Un ulteriore elemento di questa strategia riguarda la messa in sicurezza dei sistemi deputati alla gestione del voto elettronico, presi sempre più di mira da attacchi informatici con l'avvicinarsi della data delle votazioni presidenziali americane.

Infatti, negli Stati Uniti ben 5 Stati votano in maniera completamente elettronica – Delaware, Georgia, Louisiana, South Carolina, and New Jersey – mentre altri 10 hanno un sistema di voto misto.
Pertanto, considerato lo scarso livello di protezione di questi sistemi e spesso anche la mancanza delle opportune verifiche post-elettorali sulla coerenza dei dati di voto, il pericolo che i risultati delle votazioni possano essere falsati attraverso un attacco informatico appare concreto.

In quest'ottica, due proposte di legge – incardinate il 20 settembre 2016 alla Camera dei Rappresentanti degli Stati Uniti – mirano proprio a mitigare questo rischio.

La prima, in particolare, denominata "*Election Infrastructure and Security Promotion Act of 2016*", ha come obiettivo quello di richiedere al *Department of Homeland Security* (DHS) americano di classificare questo genere di sistemi informatici come infrastruttura critica nazionale, al pari di quelli elettrici ed energetici, di quelli idrici, delle varie reti di telecomunicazione e di trasporto pubblico, del circuito bancario e finanziario e così via.

La seconda proposta di legge, denominata "*Election Integrity Act* ", mira, tra le altre cose, a limitare l'acquisto di sistemi elettronici di voto sprovvisti di metodi cartacei di verifica post-elettorale.

Per quanto le due proposte di legge appaiano evidentemente tardive rispetto alle imminenti elezioni presidenziali americane, il loro obiettivo è certamente quello di sbloccare in futuro investimenti federali per rendere più sicuro tutto il meccanismo di voto elettronico.

Tuttavia, classificare i sistemi informatici deputati alla gestione del voto elettronico come un'infrastruttura critica nazionale degli Stati Uniti, significa anzitutto qualificare gli attacchi informatici che dovessero colpirla nell'alveo delle minacce cibernetiche di alto profilo, ovvero quelle "*suscettibili di provocare un danno dimostrabile agli interessi degli Stati Uniti in materia di sicurezza nazionale e relazioni internazionali, oppure un danno all'economia, alla fiducia dei cittadini, alle libertà civili, alla salute e alla sicurezza del popolo americano*", così come di recente definite all'interno della *Presidential Policy Directive* n. 41 "*United States Cyber Incident Coordination*" (per approfondimenti, si vedano il "*Cyber Strategy & Policy Brief*" di febbraio e di luglio/agosto 2016).

A questo genere di attacchi informatici, quindi, gli Stati Uniti potrebbero decidere di rispondere in maniera più dura e soprattutto coordinata su più fronti, non solo quello informatico, ma anche quello diplomatico, economico e addirittura – come in precedenza approfondito – anche con operazioni militari cinetiche.

Le possibili risposte degli Stati Uniti alle attività russe.

Quanto finora analizzato lascia presagire che, al di là di possibili operazioni clandestine nel e attraverso il cyber-spazio, un'ipotetica risposta pubblica del governo americano nei confronti della Russia potrebbe avvenire ancora una volta attraverso gli strumenti tipici di reazione diplomatica, economica e di supporto militare alle nazioni limitrofe ai confini russi.

Una prima opzione potrebbe essere, allora, quella di ricorrere alle sanzioni economiche previste all'interno del *Presidential Executive Order* "*Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*" del 01 aprile 2015.

Grazie a questo *Executive Order*, infatti, potrebbero essere congelate le proprietà e i conti bancari presenti negli Stati Uniti che siano riferibili a Putin e agli altri leader russi vicini al Presidente.

Questa possibilità, peraltro, non risulta totalmente nuova. Già nel 1999, infatti, la Casa Bianca approvò in via preliminare un piano molto simile per colpire e prosciugare i conti bancari esteri dell'allora leader serbo Milosevic e dei suoi fedelissimi. Così come, nel 2003, poco prima della seconda invasione dell'Iraq, un analogo progetto fu pianificato sempre dagli Stati Uniti per colpire il sistema finanziario di Saddam Hussein.

Una seconda opzione, invece, potrebbe essere quella di rivelare le conversazioni che provino il coinvolgimento del governo russo negli attacchi informatici contro i *server* del Comitato Nazionale Democratico e contro i sistemi di voto elettronico.

Ad esempio, rendere pubblici i nomi dei politici o degli ufficiali che hanno materialmente autorizzato questi attacchi informatici, non solo fornirebbe una prova rispetto alle accuse sollevate dalla Casa Bianca, ma metterebbe senz'altro Mosca in una difficile posizione sul piano internazionale.

Tuttavia, come si è detto in precedenza, ciò dovrebbe avvenire senza ovviamente esporre eccessivamente le capacità di intelligence degli Stati Uniti, al fine di evitare che la Russia comprenda le sue falle di sicurezza o le fonti utilizzate da Washington.

Un'ultima opzione, infine, potrebbe essere quella di esporre pubblicamente i metodi e i sistemi di controllo interno operati da Mosca sui contenuti pubblicati e sulle attività svolte su

Internet dai cittadini russi. Ciò, al fine di minare la stabilità interna del governo in carica e la leadership del Presidente Putin con attività peraltro molto simili a quelle subite dagli Stati Uniti.

Qualsiasi percorso dovesse essere effettivamente scelto, dovrà essere ponderato e pianificato nei minimi dettagli, onde evitare un'*escalation* poi difficilmente gestibile. Del resto, sembra pacifico poter affermare che l'elezione del nuovo Presidente degli Stati Uniti porterà già nel brevissimo periodo ad un affievolirsi di queste schermaglie, anche se non alla soluzione del problema.

Ciò che appare evidente, però, è come – al di là del caso concreto – la prolungata inazione e la lentezza dei governi sul piano internazionale, unita alla costante incapacità di trovare risposte comuni alle 'minacce cibernetiche', stia velocemente portando ad un incremento esponenziale e quasi ingestibile di attacchi informatici a supporto di operazioni di influenza informativa, di spionaggio e di *cyber-warfare*.

Pensare e poi implementare accordi che contengano misure di *confidence-building*, tese soprattutto ad evitare una corsa agli armamenti e a identificarne i limiti in termini di *target* e strumenti utilizzabili, è certamente un passo a cui guardare ormai in maniera urgente.

NOTE SULL'AUTORE

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

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

CONSULTA ANCHE I VOLUMI PRECEDENTI

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

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

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

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

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

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

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

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

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

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

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

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

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.*