CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 02 – Febbraio 2016

PERCHÉ UN CYBER STRATEGY & POLICY BRIEF?

L'elevata pervasività delle tecnologie e della rete Internet in ogni strato dell'odierno tessuto sociale ha completamente trasformato – in un lasso di tempo peraltro esiguo – ogni aspetto della nostra società, dell'erogazione e gestione dei servizi, dell'accesso alle informazioni, della loro qualità e quantità, nonché dell'interazione tra questi elementi e il cittadino. Come se ciò non bastasse a sottolineare il loro ruolo cruciale nella cosiddetta 'società dell'informazione', le tecnologie e la rete Internet sono ormai alla base anche dei sistemi complessi che assicurano la corretta esecuzione dei settori strategici e sensibili di uno Stato, come quelli dell'energia, delle comunicazioni, dei trasporti, della finanza e così via. Esse rappresentano, quindi, uno dei principali cardini intorno a cui ruota il benessere economico e sociale di ogni Stato, nonché il piano di appoggio e il motore della sua crescita.

Peraltro, l'analisi dello scenario corrente e dei principali documenti strategici nazionali in ambito di *cyber-security* delineano contorni particolarmente evidenti delle direttrici di minaccia, causate principalmente dallo scarso livello di percezione e consapevolezza di queste problematiche, dal vuoto normativo e di regolamentazione sovrannazionale del settore, dal debole livello di collaborazione interna e internazionale, nonché dalla scarsa capacità di raggiungere un adeguato *standard* di sicurezza informatica e di resilienza dei sistemi critici nazionali.

Garantire un approccio strategico alla sicurezza di questo settore, pianificarne la crescita, valutare i rischi a breve, medio e lungo termine, nonché svolgere attività previsionali sulla sua evoluzione, rappresentano, quindi, un compito ormai imprescindibile, da porre come prioritario nell'agenda politica di ogni buon governo, soprattutto oggi che la protezione del cosiddetto 'spazio cibernetico' rappresenta per tutti una sfida ad elevato grado di priorità.

Il *Cyber Strategy & Policy Brief* si pone come scopo quello di sensibilizzare ogni mese i lettori su questi argomenti, analizzando i principali avvenimenti a livello internazionale, al fine di desumere i *trend* della 'minaccia cibernetica' e le lezioni apprese utili alla salvaguardia della nostra sicurezza nazionale.

EXECUTIVE SUMMARY

Il mese di febbraio ha visto come protagonisti alcuni attori "emergenti" nel panorama delle attività di *cyber-warfare*, come l'Iran e la Corea del Nord, tornare ad impiegare le loro competenze in questo settore per supportare scopi strategici di breve periodo. In particolare l'Iran, uno degli Stati con la più rilevante e rapida crescita in questo campo, a seguito dell'inasprirsi dei rapporti diplomatici, potrebbe decidere di utilizzare proprio il cyber-spazio come principale terreno di scontro nei confronti dell'Arabia Saudita e dei Paesi del Golfo filo-Ryad.

Su un altro piano, l'Italia, attraverso la "*Relazione sulla politica dell'informazione per la sicurezza*" del 2015, ha posto in evidenza i primi frutti del grande sforzo effettuato soprattutto dal Comparto Intelligence nel costruire e portare avanti quanto delineato dalla normativa nazionale in materia di 'sicurezza cibernetica' e dalla successiva strategia. Tuttavia, all'alba dei tre anni dalla loro pubblicazione, ciò che pare mancare al momento nel dibattito italiano è sia una riflessione strutturata – in ottica evolutiva – tesa alla nascita di una vera e propria politica di *cyber-security* nazionale, sia un'attenta valutazione sull'urgenza che il governo italiano muti l'approccio strategico nei confronti della 'sicurezza cibernetica' da meramente difensivo a proattivo.

Infine, il recente sforzo di pianificazione strategica fatto dal governo americano attraverso il "*Cybersecurity National Action Plan*" appare essere sicuramente molto interessante. Le direttrici su cui si muove il *Piano*, infatti, vanno da un'ampia riorganizzazione e un maggiore coordinamento centrale delle attività federali in materia di sicurezza informatica e privacy, fino ad una grande e giustissima attenzione verso l'incremento della consapevolezza dei cittadini americani nei confronti delle problematiche che scaturiscono da questo settore.
Rafforzare la sicurezza informatica a livello federale e responsabilizzare i cittadini, ma anche proteggere la loro privacy, migliorare la protezione e la resilienza delle infrastrutture critiche, così come ingegnerizzare e produrre gli strumenti tecnologici con un approccio di "*security by design*", sono gli assi portanti della strategia che la Casa Bianca ha delineato a febbraio per questo settore e su cui Obama ha deciso di puntare ben 19 miliardi di dollari.

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*.

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

COREA DEL NORD

Nel mese di febbraio, la Corea del Nord è tornata a far parlare di sé anche per le attività svolte nel e attraverso il cyber-spazio. In particolare, un'ondata di attacchi informatici di medio-bassa entità si è abbattuta, ancora una volta, nei confronti della Corea del Sud, che ha immediatamente alzato il livello di allerta per questo genere di minaccia.

In quest'ottica, occorre evidenziare come da tempo la Corea del Nord veda sempre più il cyber-spazio come uno strumento utile per i suoi scopi di controllo del territorio, propaganda, spionaggio e *cyber-warfare*. Ciò, complici anche alcune delle caratteristiche implicite di questo dominio, ovvero l'asimmetricità della minaccia, la possibilità di denegare agevolmente la propria responsabilità nel caso in cui un 'attacco cibernetico' sia scoperto e l'elevata efficacia di un attacco informatico in relazione agli investimenti relativamente bassi per la sua organizzazione ed attuazione.

A ciò, inoltre, si aggiunga anche che la Corea del Nord può vantare una impareggiabile "carta" per la difesa in caso di contrattacco da parte di uno Stato avversario, fornita, da un lato, dal basso livello di penetrazione delle tecnologie nel tessuto socio-economico e dallo scarso livello di digitalizzazione delle proprie infrastrutture sensibili nazionali, dall'altra, dalla possibilità di potersi disconnettere dalla rete Internet con poche difficoltà, interrompendo di fatto qualsiasi contrattacco informatico in atto.

Peraltro, occorre evidenziare che proprio le metodologie di guerra asimmetrica e non convenzionale sono da sempre quelle predilette dal governo nord coreano – sia in tempo di pace, che di guerra – per contrastare la forza militare dei suoi principali antagonisti: la Corea del Sud e gli Stati Uniti. Appare evidente, infatti, come la strategia del governo di Pyongyang sia quella di lanciare attacchi non convenzionali a bassa intensità con obiettivi meramente provocatori, guardandosi bene, però, dal far scivolare gli eventi verso una *escalation* non controllabile o verso una situazione di conflitto che li vedrebbe sicuramente sconfitti.

In questo quadro strategico la Corea del Nord, come anticipato, ha puntato sin dal 2009 sulle operazioni nel e attraverso il cyber-spazio come parte integrante della propria strategia nazionale, creando all'interno dei due più importanti dipartimenti governativi, il *Reconnaissance General Bureau* e il *General Staff Department* della *Korean People's Army*, delle specifiche unità per le attività – rispettivamente – di *intelligence* e di *cyber-warfare*.

Per quanto finora analizzato, seppure nel breve periodo la Corea del Nord non sembra volersi distaccare dalla propria strategia fondata esclusivamente su attacchi informatici a bassa intensità con mere finalità provocatorie, nel tempo la maggiore confidenza nell'utilizzo di questi strumenti, il successo delle operazioni di disturbo, nonché la mancanza di una vera risposta efficace e coordinata da parte dei governi, porteranno nel breve periodo ad un

innalzamento della frequenza di questo genere di attacchi informatici, mentre nel medio periodo, se non contrastati, indurranno la Corea del Nord ad aumentare queste azioni sia sul piano dell'intensità, che soprattutto della qualità.

IRAN

Per valutare appieno l'approccio dell'Iran alle tematiche relative alla *cyber-security* e al c*yber-warfare*, occorre anzitutto precisare quale sia il contesto strategico entro cui questo Stato opera, così come quali siano gli obiettivi strategici che si prefigge di raggiungere in un'ottica di medio-lungo periodo.

Va fin da subito evidenziato come il principale obiettivo strategico di Teheran sia quello di vedersi riconosciuta come una potenza regionale. Questo Stato, infatti, è principalmente impegnato nella storica ostilità nei confronti dell'Arabia Saudita (il suo principale competitore strategico) e dei Paesi del Golfo filo-Ryad, nonché contro gli Stati Uniti ed Israele.
Tuttavia, occorre anche precisare come il governo iraniano, in realtà, non consideri gli Stati Uniti come il suo principale nemico, ma anzi punti ad essere riconosciuta come potenza regionale innanzitutto dal governo di Washington.

In questo quadro generale, quindi, devono essere letti gli ultimi avvenimenti che hanno visto come protagonista il governo iraniano. Proprio di recente, infatti, l'Arabia Saudita e i Paesi del Golfo ad essa alleati hanno interrotto ancora una volta i rapporti diplomatici con il governo di Teheran a seguito dell'attacco alla missione diplomatica saudita in Iran. Attacco orchestrato – con molta probabilità – dal governo iraniano come reazione all'esecuzione della condanna a morte dello sceicco Nimr Baqir al-Nimr da parte del governo saudita.

Seppure allo stato attuale appare molto improbabile che – almeno nel breve periodo – queste tensioni possano sfociare in un vero e proprio conflitto tra Arabia Saudita e Iran, appare invece molto più plausibile che il governo iraniano in questa fase si possa avvalere proprio del cyber-spazio come principale territorio di scontro.
Del resto, l'Iran non è assolutamente nuovo a questo tipo di approccio e anzi già in passato ha sfruttato la "carta" degli attacchi informatici durante periodi di crisi diplomatica (si vedano, ad esempio, gli attacchi a Saudi Aramco e RasGas nel 2012). Per di più, nel corso dell'interno 2015, l'Iran ha più volte utilizzato lo spionaggio elettronico, la propaganda e in alcuni casi persino attacchi informatici per sostenere le proprie priorità strategiche e di sicurezza, nonché per influenzare gli eventi nel proprio quadrante di interesse geopolitico.

Per raggiungere questi obiettivi, sin dal 2009 l'Iran ha investito ingenti risorse nello sviluppo di capacità sia difensive, che offensive da sfruttare in caso di conflitti nel e attraverso il cyber-spazio, arrivando a stanziare – già nel 2011 – più di 1 miliardo di dollari per l'acquisizione degli

strumenti utili a compiere operazioni di spionaggio elettronico e di *cyber-warfare*, per consolidare e aggiornare il comparto della *cyber-defence*, nonché per formare le competenze umane necessarie al raggiungimento di queste finalità. In particolare sotto la presidenza di Hassan Rouhani, dal 2013 quindi, l'Iran ha incredibilmente accelerato in questo settore, arrivando oggi giorno a poter essere considerata una delle cinque "cyber-potenze" a livello globale.

D'altro canto, anche gli Stati Uniti – e non solo loro – hanno da tempo pianificato attacchi ai sistemi informatici dell'Iran come una possibile opzione in caso di conflitto. Al di là del ben noto *Stuxnet*, è notizia di questo mese che proprio il governo di Washington avrebbe da tempo studiato un attacco informatico su larga scala ai sistemi iraniani di controllo dello spazio aereo, a quelli delle comunicazioni e ai sistemi deputati all'erogazione dell'energia elettrica. '*Nitro Zeus*', questo il nome in codice del piano di attacco, sarebbe stato tuttavia momentaneamente accantonato a seguito dell'accordo raggiunto sul programma nucleare iraniano.

Alla luce di quanto finora analizzato, i continui ed ingenti investimenti in termini economici, organizzativi e di capitale umano destinati da Teheran al settore della *cyber-security* e allo sviluppo di capacità di *cyber-warfare*, fanno attualmente dell'Iran lo Stato "emergente" con la più rilevante e rapida crescita in questo settore.

Al riguardo, occorre puntualizzare che la *cyber-strategy* iraniana costituisce parte integrante della dottrina nazionale per la guerra asimmetrica – per Teheran uno dei concetti cardine della concezione di uso della forza – che giustifica, quindi, almeno sul piano teorico, la naturale propensione dell'Iran verso le attività offensive nel e attraverso il cyber-spazio. Peraltro, le attività offensive di *cyber-warfare*, così come le metodologie classiche di guerra asimmetrica (terrorismo, guerriglia, ecc.), sono viste dalla *leadership* iraniana come uno strumento assolutamente utile e particolarmente efficace per infliggere danni rilevanti ad un nemico militarmente e tecnologicamente superiore.

Se così è, proseguendo lungo questa direttrice di sviluppo, nel medio periodo l'Iran arriverà a recitare in questo settore un ruolo primario all'interno dello scacchiere geopolitico internazionale. Un ruolo in un primo tempo molto simile a quello attualmente interpretato dalla Cina, ma teso a trasformarsi rapidamente in uno molto più simile a quello attualmente interpretato dalla Russia.

ITALIA

Alla fine di febbraio, come ogni anno, è stata presentata al Parlamento italiano la "*Relazione sulla politica dell'informazione per la sicurezza*". Il documento esplicita i principali temi all'attenzione del Comparto Intelligence italiano: dal terrorismo di matrice *jihadista* (con le sue

proiezioni in direzione dell'Italia e dell'Europa), alla spinta migratoria verso lo spazio Schengen; dalle vulnerabilità di natura economico-finanziaria, alle aggressioni di matrice spionistica e criminale, sia a carattere "tradizionale", che operanti nel e attraverso il cyber-spazio.

La *Relazione*, infatti, specifica che proprio la 'minaccia cibernetica' costituisce, in prospettiva, la vera e propria "nuova frontiera" per l'intelligence e per le amministrazioni italiane che concorrono alla sicurezza nazionale, arrivando a qualificarla come una delle tre principali sfide per il Sistema Paese italiano insieme al terrorismo *jihadista* e alla minaccia economico-finanziaria.

Peraltro, nel corso del 2015, la matrice statuale degli attacchi informatici ha continuato a caratterizzare le più significative attività di spionaggio elettronico in danno ad obiettivi nazionali di rilevanza strategica. Il *trend* che si è potuto registrare, inoltre, evidenzia un continuo incremento qualitativo e quantitativo delle azioni contro alcune Istituzioni e contro l'industria italiana ad alto contenuto tecnologico ed innovativo, al fine di esfiltrare informazioni sensibili e *know how* pregiato, nonché di garantirsi un accesso ai medesimi sistemi informatici in vista di successive azioni di attacco.

Molteplici esempi di quanto affermato possono rinvenirsi, ad esempio, nel contesto della competizione economica tra Paesi, ove molte attività di spionaggio elettronico sono state poste in essere da numerosi attori ostili, al fine di accrescere la loro capacità conoscitiva nei confronti delle aziende italiane. La *Relazione* evidenzia come questa metodologia di ingerenza da parte di potenziali acquirenti stranieri mira a svolgere attività di *due diligence* occulte per conseguire un vantaggio informativo sleale, su cui far leva durante la fase di negoziazione per l'acquisizione del controllo di operatori economici italiani.

Inoltre, alla luce dell'analisi svolta dal Comparto Intelligence italiano, il *modus operandi* di questi soggetti ha continuato a tradursi in una minaccia persistente e avanzata (*Advanced Persistent Threat* o APT) caratterizzata soprattutto dall'impiego di *software* malevolo (c.d. *malware*). Inoltre, l'osservazione dei "gruppi" operanti nell'ambito delle campagne APT ha rivelato sempre più la loro propensione sul piano tecnico a:

- impiegare *malware* altamente modulare, con componenti deputati allo svolgimento di specifiche funzioni, utilizzate o meno a seconda del bersaglio;
- reingegnerizzare i *malware* già conosciuti, contribuendo, tra l'altro, alla proliferazione di questo genere di strumenti tecnologici, resi poi anche facilmente reperibili in Rete;
- fare ricorso – nella scrittura dei codici malevoli – a stringhe di caratteri in lingue diverse, ovvero riconducibili ad altri attori ostili, al fine di rendere maggiormente difficoltosa ed incerta l'attribuzione di un attacco informatico;
- sottrarre le credenziali amministrative di *host* della *intranet* del bersaglio, al fine di preservare il controllo del sistema informatico anche a fronte di attività di recupero della piena funzionalità dei sistemi attaccati;

- utilizzare dei *proxy* (individui o gruppi) nella conduzione degli attacchi informatici, al fine di garantire un ulteriore livello di anonimato, cosicché, anche in caso di un'eventuale scoperta dell'attacco da parte del bersaglio, resti garantita la possibilità di negare ogni coinvolgimento.

Infine, alla luce della ricognizione svolta all'interno della *Relazione*, il Comparto Intelligence evidenzia come nel settore della *cyber-security* siano obiettivi assolutamente prioritari per il governo italiano:

- il potenziamento del sistema di reazione ad eventi occorsi nel e attraverso il cyber-spazio;
- l'implementazione da parte di tutti gli attori pubblici e privati dei requisiti minimi di 'sicurezza cibernetica';
- l'adozione di iniziative interistituzionali coordinate nei settori del partenariato pubblico-privato, nell'attività di ricerca e sviluppo e nella cooperazione internazionale.

In linea generale, la "*Relazione sulla politica dell'informazione per la sicurezza*" del 2015 delinea e centra in maniera molto precisa il *trend* della 'minaccia cibernetica'. La *Relazione*, inoltre, pone in evidenza i primi frutti del grande sforzo effettuato soprattutto dal Comparto Intelligence nel costruire e portare avanti quanto delineato dalla normativa italiana in materia di 'sicurezza cibernetica' nel Decreto del Presidente del Consiglio dei Ministri del gennaio 2013 e nella successiva strategia.

Tuttavia, all'alba dei tre anni dalla sua entrata in vigore, ciò che pare mancare al momento nel dibattito italiano è, da un lato, una riflessione strutturata – in ottica evolutiva – tesa alla nascita di una vera e propria politica di *cyber-security* nazionale, alla quale peraltro mancano ancora oggi alcuni pilastri normativi imprescindibili (come, ad esempio, una definizione di sicurezza nazionale, nel cui alveo deve necessariamente essere ricompresa gran parte della tematica della 'sicurezza cibernetica').

Dall'altro lato, invece, emerge con forza la necessità che in questo settore il governo italiano muti l'approccio strategico nei confronti della 'sicurezza cibernetica' da meramente difensivo (ovvero di mera gestione di eventuali crisi, di prevenzione degli attacchi informatici e di riduzione dei loro danni) a proattivo, cercando quindi di prevedere e anticipare le tendenze e i mutamenti futuri di questo settore per pianificarne in tempo le opportune azioni e strategie.

Tutto questo, ovviamente, non può e non potrà esistere senza un coerente e convinto appoggio del piano politico a questo ormai imprescindibile settore, al fine di destinare quanto prima le opportune risorse finanziarie per arginare questa minaccia e intraprendere ogni azione richiesta dalla sua costante e repentina evoluzione.

STATI UNITI

Come anticipato nel precedente fascicolo, agli inizi di febbraio la Casa Bianca ha reso pubblico il suo "*Cybersecurity National Action Plan*": un documento strategico teso a potenziare le capacità e soprattutto la solidità in materia di sicurezza informatica del governo federale e di tutto il paese attraverso specifiche azioni di breve e di medio-lungo periodo. I punti più salienti del *Piano* delineano alcune direttrici di azione molto interessanti tese a:

- creare la "*Commission on Enhancing National Cybersecurity*". Composta da 12 esperti provenienti dal mondo privato della *cyber-security* e della privacy, la *Commissione* avrà come scopo principale quello di fornire raccomandazioni in merito alle migliori azioni da intraprendere per rafforzare la 'sicurezza cibernetica' sia del settore pubblico, che di quello privato, difendendo e salvaguardando la privacy dei soggetti coinvolti, al fine di garantire la sicurezza pubblica, economica e nazionale degli Stati Uniti. Inoltre, un ulteriore compito della *Commissione* sarà quello di incentivare la cooperazione tra governo federale, statale e degli enti locali con il settore privato per lo sviluppo, la promozione e l'utilizzo di tecnologie, *policy* e *best practice* per la sicurezza informatica;
- modernizzare attraverso un fondo da 3.1 miliardi di dollari ("*Information Technology Modernization Fund*") l'infrastruttura tecnologica governativa e come il governo americano gestisce le problematiche connesse al settore della sicurezza informatica. Ciò sarà possibile anche grazie all'introduzione all'interno del governo federale americano – per la prima volta – della figura del *Federal Chief Information Security Officer*, che avrà specifici compiti di pianificare, guidare e implementare una politica di sicurezza informatica tecnica a livello governativo federale;
- fornire ai cittadini americani gli strumenti per rafforzare il proprio livello di sicurezza informatica, andando oltre il semplice utilizzo della *password* e prevedendo livelli di protezione maggiori. In quest'ottica, la "*National Cyber Security Alliance*" lancerà una massiccia campagna di sensibilizzazione verso i cittadini in favore dei metodi di autenticazione multifattore. Questa nuova "*National Cybersecurity Awareness Campaign*" sarà svolta in collaborazione con i maggiori *player* del mercato tecnologico (come Google, Facebook, DropBox e Microsoft) per la parte relativa alla sicurezza informatica dei dati dei cittadini, unitamente ai maggiori *player* del settore finanziario (come MasterCard, Visa, PayPal e Venmo) per la sicurezza delle transazioni economiche;
- istituire il "*Federal Privacy Council*", composto dai rappresentanti di vertice di alcune agenzie federali, per coordinare e unificare le linee guida utili alla raccolta e conservazione dei dati personali da parte del governo americano.

Complessivamente, lo sforzo del governo americano appare essere sicuramente molto rilevante ed interessante. Le direttrici su cui si muove il "*Cybersecurity National Action Plan*",

infatti, vanno da un'ampia riorganizzazione e un maggiore coordinamento centrale delle attività federali in materia di sicurezza informatica e privacy, fino ad una grande e giustissima attenzione verso l'incremento della consapevolezza dei cittadini americani nei confronti delle problematiche che scaturiscono da questo settore.

Rafforzare la sicurezza informatica a livello federale e responsabilizzare i cittadini, ma anche proteggere la loro privacy, migliorare la protezione e la resilienza delle infrastrutture critiche, così come ingegnerizzare e produrre gli strumenti tecnologici con un approccio di "*security by design*", sono gli assi portanti della strategia che la Casa Bianca ha delineato a febbraio per questo settore e su cui Obama ha deciso di puntare ben 19 miliardi di dollari.

Un ulteriore segnale per tutti i governi che il problema della sicurezza dei dati e delle informazioni dev'essere immediatamente affrontato in maniera strategica e con interventi tanto nel breve, quanto nel medio-lungo periodo anche e soprattutto nel settore della pubblica amministrazione.

TERRORISMO: STATO ISLAMICO

Allo stato attuale, lo Stato Islamico rappresenta senza ombra di dubbio la principale minaccia terroristica per tutti i Paesi occidentali.

Il numero sempre più elevato di cittadini europei coinvolti in azioni terroristiche, ha portato già da tempo gli esperti del settore a riflettere in modo più attento e approfondito sui metodi e i mezzi utilizzati da questa organizzazione terroristica per radicalizzare e plasmare la mente dei futuri *shahid*. Ciò, nonostante la loro vicinanza per nascita e per cultura ai principi occidentali, nonché la loro distanza dai territori di radicalizzazione delle dottrine religiose.

In quest'ambito, uno degli strumenti maggiormente utilizzati ed efficaci è senza dubbio la rete Internet. Infatti, è proprio grazie ad un utilizzo strategico della comunicazione attraverso la Rete, che lo Stato Islamico ha sempre più ridotto le distanze geografiche con i propri adepti, alimentando il loro coinvolgimento emotivo e l'adesione ai principi della *jihad* e del martirio.
In effetti, lo Stato Islamico ha fatto delle tecnologie e della rete Internet il principale strumento di supporto al raggiungimento dei propri scopi terroristici, sfruttandole principalmente per propaganda, proselitismo, radicalizzazione, raccolta di fondi e per un primo livello di reclutamento e indottrinamento.

Tuttavia, a dispetto dei proclami giornalistici che considerano lo Stato Islamico come capace di compiere attacchi informatici di alto profilo, quali, ad esempio, quelli alle infrastrutture critiche nazionali, oppure di essere in grado di sviluppare autonomamente delle 'cyber-armi', nella

realtà dei fatti quest'organizzazione terroristica non è assolutamente riuscita a compiere questo "salto di qualità".

I quattro principali gruppi che supportano lo Stato Islamico e che sembrano ad esso legati – il '*Cyber Caliphate*', la '*Elite Islamic State Hackers*', la '*Islamic Cyber Army*' e la *'Islamic State Hacking Divison*' – hanno dimostrato, in realtà, scarse capacità sul piano degli attacchi informatici, arrivando a compiere meri *Denial of Service*, *defacement* di siti web e di *account* di *social network*, nonché a divulgare dati personali di alcuni soggetti governativi ottenuti grazie a tecniche elementari di ingegneria sociale.

Ciò su cui lo Stato Islamico è maggiormente concentrato, invece, è la ricerca di metodi e strumenti di comunicazione che siano quanto più sicuri possibile.
Infatti, facendo della propaganda su Internet uno degli assi portanti delle proprie attività di proselitismo, l'elevata esposizione ha portato in alcuni casi all'identificazione, alla geolocalizzazione e finanche all'uccisione di alcuni soggetti chiave della propaganda *jihadista*. E' questo il caso, ad esempio, di Junaid Hussain, anche noto come Abu Hussain al-Britani, nato a Birmingham e membro di spicco del '*Cyber Caliphate*', individuato e ucciso da un drone americano nell'agosto del 2015 a Raqqa, in Siria, anche grazie alle informazioni ottenute dalle tracce lasciate dalle sue attività *online*.

Ciò nonostante, ancora una volta, seppure la propaganda – ripresa poi dai *media* – ritragga lo Stato Islamico come capace di sviluppare *software* utile a rendere totalmente sicure le comunicazioni degli appartenenti al gruppo terroristico – come, ad esempio, il recente caso dell'applicazione per cellulari denominata '*Alrawi*' – in realtà di questi *software*, così come dell'applicazione '*Alrawi*', non c'è alcuna traccia. Anzi, proprio sul tema delle comunicazioni sicure, le informazioni in possesso fanno propendere anche nel caso dello Stato Islamico per l'utilizzo diffuso tra i suoi ranghi della ben nota applicazione per cellulari '*Telegram*'. Tutto il resto è mera propaganda.

Per quanto finora analizzato, nel breve-medio periodo non si ritiene che sul piano delle capacità dello Stato Islamico in materia di attacchi informatici per scopi terroristici la situazione possa evolvere in maniera significativa rispetto a quella fin qui delineata. Di conseguenza, almeno sul piano della 'sicurezza cibernetica', il livello di pericolosità di questa minaccia per i Paesi occidentali può considerarsi ancora molto basso.

Peraltro, seppure le informazioni disponibili facciano emergere una notevole e costante attenzione di questo gruppo terroristico verso il reclutamento di ingegneri informatici e di specialisti nel campo della sicurezza informatica (attingendo persino dal mondo degli attivisti di *Anonymous*), la principale preoccupazione per il mondo occidentale arriva esclusivamente da alcuni Stati vicini all'organizzazione terroristica, che potrebbero cominciare a supportare le attività dello Stato Islamico anche nel cyber-spazio.

Ciò potrebbe accadere, persino nel breve periodo, o attraverso finanziamenti, che però – occorre precisarlo – difficilmente verrebbero poi realmente impiegati dallo Stato Islamico per innalzare le proprie capacità offensive nel e attraverso il cyber-spazio, oppure – cosa più probabile – fornendo loro in maniera diretta *software* e *know-how* utile ad effettuare attacchi informatici verso obiettivi critici di uno Stato.

Tuttavia, se anche questo scenario dovesse realizzarsi, il livello di pericolosità di tale minaccia per i Paesi occidentali potrà considerarsi comunque medio-basso, in conseguenza della quasi certa mancanza di continuità e persistenza nel tempo degli attacchi. Attacchi che, peraltro, per lo Stato "finanziatore" sarebbero tesi esclusivamente a reiterare la ben nota prassi di un attacco informatico esperito attraverso lo sfruttamento di un attore non statale con mere funzioni di intermediario ("*proxy*").

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