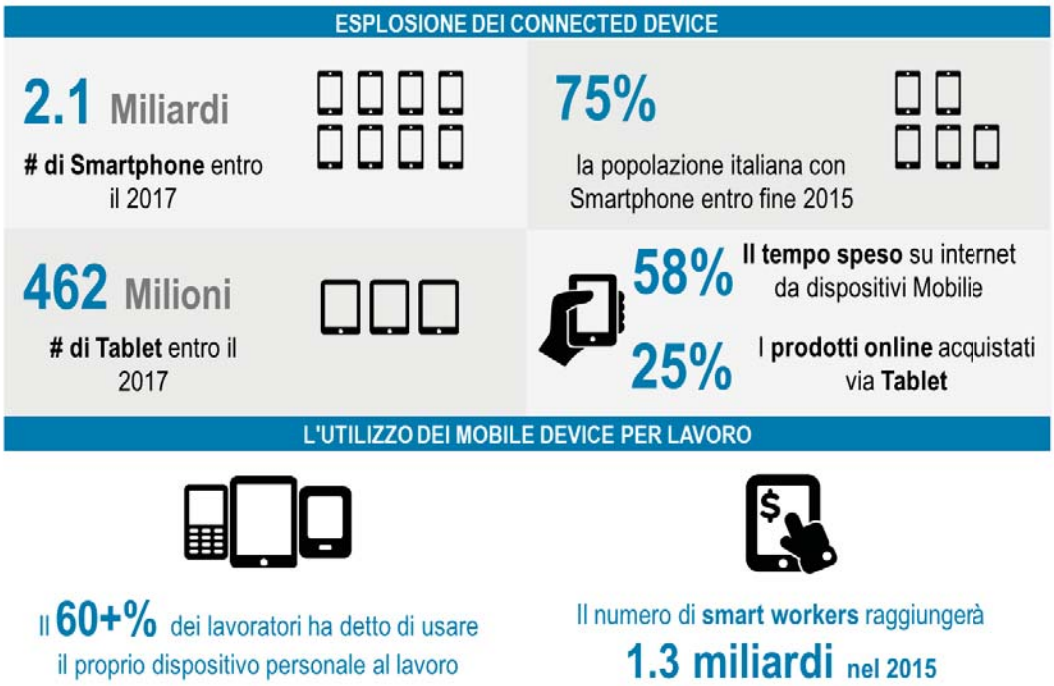
Cyber Defence Symposium di Chiavari

Gli atti

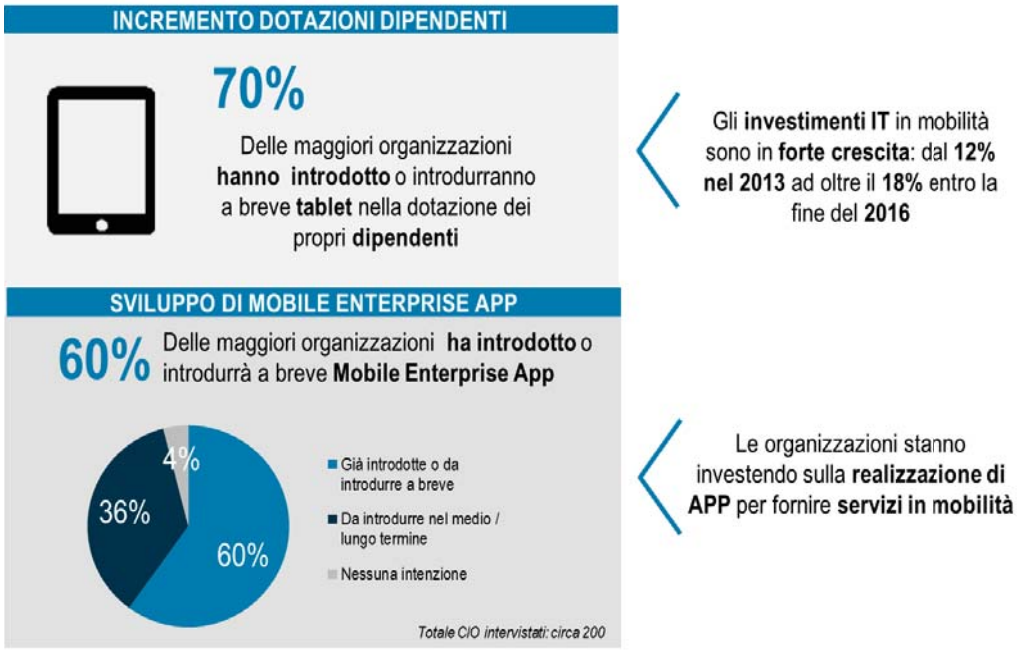
Il rischio Cyber nello scenario “Mobile”.

Un approccio per la sua efficace mitigazione.

Partiamo da un dato di fatto: i criminali operano dove si concentra il maggior numero di potenziali prede e dove esse sono meno protette e questo vale ovviamente anche per i *Cyber*-criminali.
Nel contesto “Cyber” la più alta aggregazione di utenti con maggiori vulnerabilità è nello scenario Mobility – ovvero i servizi acceduti mediante smartphone e tablet – ne risulta che proprio questo bacino di utenze rappresenti il cosiddetto anello debole della catena, su cui si stanno concentrando i più sofisticati schemi di attacco cyber-criminale.



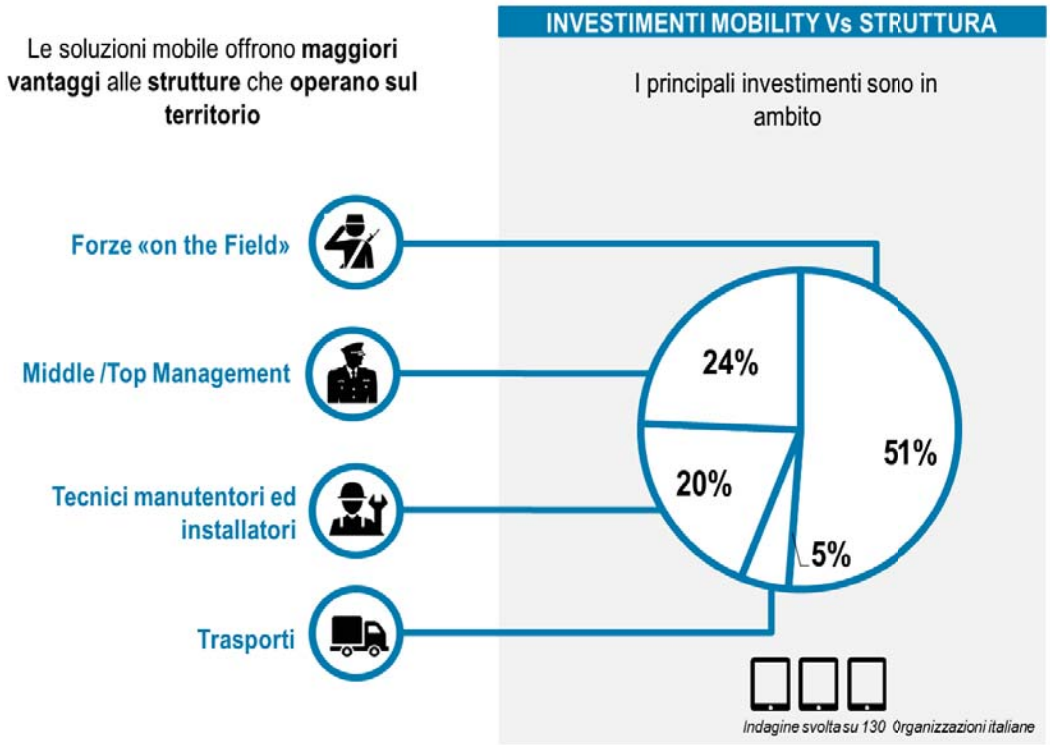
Comprenderne le ragioni è abbastanza intuitivo: l’utente, in possesso di smartphone o tablet, lo usa sempre più frequentemente in tutte le situazioni della sua vita, sia privata sia lavorativa spesso con commistione di informazioni.



Lo Smartphone: i rischi nell'interazione tra sfera privata e professionale

Lo smartphone è un oggetto che la maggior parte delle persone ha sempre con sè, addirittura nel raggio di un metro, per ventiquattr'ore su ventiquattro. Le sue modalità di utilizzo sono sempre più destrutturate e legate più a bisogni personali che non ad esigenze di business. Esse sono governate soprattutto dalla sfera emotiva piuttosto che dalla razionalità e dalla consapevolezza, e ciò genera una serie di nuove vulnerabilità proprie dell'ambito comportamentale della persona.
Con il suo smartphone, l'utente attraversa facilmente (in entrata ed in uscita) ogni tipo di perimetro (fisico e virtuale), diffonde, talvolta con leggerezza sui social-network molteplici informazioni, in real-time, su se stesso, sugli ambienti che frequenta, sulla sua vita privata e lavorativa. Porta dati anche riservati in qualunque posto in giro per il mondo; visualizza informazioni in luoghi pubblici senza curarsi di eventuali sguardi "indiscreti"; vive una commistione totale fra tutte le sue sfere d'interesse, proprio per questo tende a non accettare regole, anche se relative al suo ambito lavorativo, perchè impatterebbero necessariamente anche la sua sfera privata.

In tal modo l'utente - ed il suo smartphone - diventano il *"cavallo di troia"* ideale per bucare qualunque tipo di difesa perimetrale, che finisce per avere un'efficacia assimilabile ad una novella linea Maginot.
L'analisi delle più recenti dinamiche di attacco conferma difatti che l'azione cyber-criminale va concentrandosi sempre più sugli end-point Mobile degli utenti del Web. Ciò deriva, oltre che da una ragione banalmente numerica, da una motivazione tecnologica legata alla complessità necessaria alla protezione di uno smartphone che è direttamente correlata alla sua sofisticatezza e versatilità d'impiego.



Di fatto, gli smartphone hanno già realizzato molti aspetti della cosiddetta visione di *"ambiente intelligente"* che include, ad esempio, la disponibilità di applicazioni d'interazione con la realtà circostante e con l'ambiente fisico, realizzate con l'utilizzo di varie tipologie di sensori, pensiamo a quelle audio e video.
Molte vulnerabilità infatti si riscontrano proprio nei meccanismi di interazione degli smartphone con l'ambiente circostante.

La cultura della sicurezza ed i comportamenti dell'utente

Quasi tutti gli utenti, inoltre, presentano un livello di "cultura della sicurezza" sul contesto Mobile che è spesso insoddisfacente. Gran parte degli utilizzatori di PC, ad esempio, hanno istallato su di esso quanto meno un antivirus. Ma la percentuale di smartphone con un antivirus istallato è invece prossima a zero. Questo semplice dato evidenzia una mancanza di consapevolezza del rischio degli utenti Mobile che si esprime anche in vari altri atteggiamenti pericolosi. Le nuove tecnologie e l'ergonomia delle applicazioni incoraggiano infatti l'assunzione di numerosi comportamenti a rischio. Alcuni esempi:

- la visualità delle interfacce applicative, sempre più vicine alla gestualità naturale della persona, favorisce una visione superficiale dei contenuti, con conseguente perdita della capacità di analisi dei dettagli
- l'atteggiamento di impazienza, stimolato proprio dalla similitudine con la postura e le gestualità naturali che creano l'aspettativa di tempi di reattività equivalenti al comportamento umano, producono insofferenza nei confronti dei tempi di attesa, determinando l'acquisizione di profili comportamentali su cui si basano diverse tecniche di attacco
- La compulsività, intesa come l'acquisizione di automatismi compulsivi da "assuefazione all'uso", è sfruttata ad esempio per costruire interfacce artefatte finalizzate all'esecuzione inconsapevole di script malevoli o al reindirizzamento verso siti di diffusione malware

- Le relazioni anonime possibili nei social network invogliano l'utente alla de-responsabilizzazione ed all'abbassamento del limite etico, mentre inducono una maggiore schiettezza ed estroversione, con minor controllo delle informazioni trasmesse
- La sovraesposizione e la ricerca della visibilità - basti pensare alla moda dei Selfie – permette di ricostruire gran parte del profilo sociale, virtuale e reale, delle persone, che forniscono inconsapevolmente una mole di dati personali molto utili per fini malevoli.

I rischi dei "Social Networks" …

Soprattutto gli ultimi due punti derivano direttamente dalla diffusione dei social network ed alla loro frequentazione continua e pervasiva resa possibile dagli smartphone. Essi hanno ormai invaso il personale e professionale vissuto quotidiano di una larga fascia della popolazione. Il social networking continua a crescere, non solo come luogo di frequentazione virtuale dei singoli, ma anche come opportunità di business per le aziende.

Tuttavia, molti dei principali siti di social networking non garantiscono nè la sicurezza nè la privacy. Sorprendentemente, i problemi di privacy non hanno avuto alcun effetto negativo sulla velocità con cui gli utenti si iscrivono ai social network o sulla quantità di informazioni personali che sono disposti a fornire. Molto spesso infatti, le persone si uniscono ai social network per promuovere interazioni casuali con altri utenti sulla base delle informazioni presenti nei profili. Partendo da questa motivazione, è evidente che se un utente indica la sua religione o etnia, lo fa perché vuole che gli altri vengano a conoscenza di queste informazioni e sono disposti - anche implicitamente – ad accettare la possibilità che un (ipotetico) programma di classificazione abbia accesso ad esse. La propensione degli utenti a fornire informazioni con un livello di controllo più basso, ed in generale il più basso livello di guardia delle persone nella loro frequentazione dei social network, fanno sì che essi rappresentino ormai il target primario dei cyber-criminali. Stante la rete di relazioni attive nei social networks, è facile intuire come semplici attacchi alla rete di contatti di un utente possa immediatamente generare catene imponenti di propagazione di malware, sempre più spesso favoriti dall'inconsapevolezza nel compiere azioni pericolose.

… e delle "APP"

Del resto a tutt'oggi non esistono strumenti per la valutazione del livello di affidabilità delle controparti, né di stima dei rischi insiti nell'utilizzo dei servizi Mobile. Il criterio di valutazione della qualità di un'App adottato tipicamente da un utente medio, ad esempio, si concretizza nel valutare il numero di altri utenti che hanno già installato l'applicazione. Chiaramente, chiunque possa controllare una certa quantità di "drone account" può influenzare tale criterio. D'altro canto la varietà dei possibili scenari di rischio è tale che è praticamente impossibile per un utente, anche informato, fruire liberamente dei servizi Web e delle App mobile senza imbattersi in situazioni di rischio che vanno al di là della propria capacità di controllo. Proprio la grandissima disponibilità di applicazioni da Market store ufficiali e non, rappresenta un ulteriore elemento di vulnerabilità ampiamente sfruttato dai cyber-criminali. Gli utilizzatori tipici infatti sono o inconsapevoli o semplicemente sopraffatti dalla complessità e dalla frequenza delle azioni necessarie per mantenere sicuri le centinaia di programmi installati su un tipico end-point.

Anche gli utenti più sensibili alle problematiche di sicurezza rischiano di perderne rapidamente il controllo, determinando la compromissione dei propri devices nonostante il dispiegamento di misure di sicurezza anche complesse e diventando talvolta inconsapevolmente parte di sofisticati schemi di attacco perpetrati da sempre più numerosi ed agguerriti gruppi cyber-criminali. Questi ultimi, a loro volta, evolvono

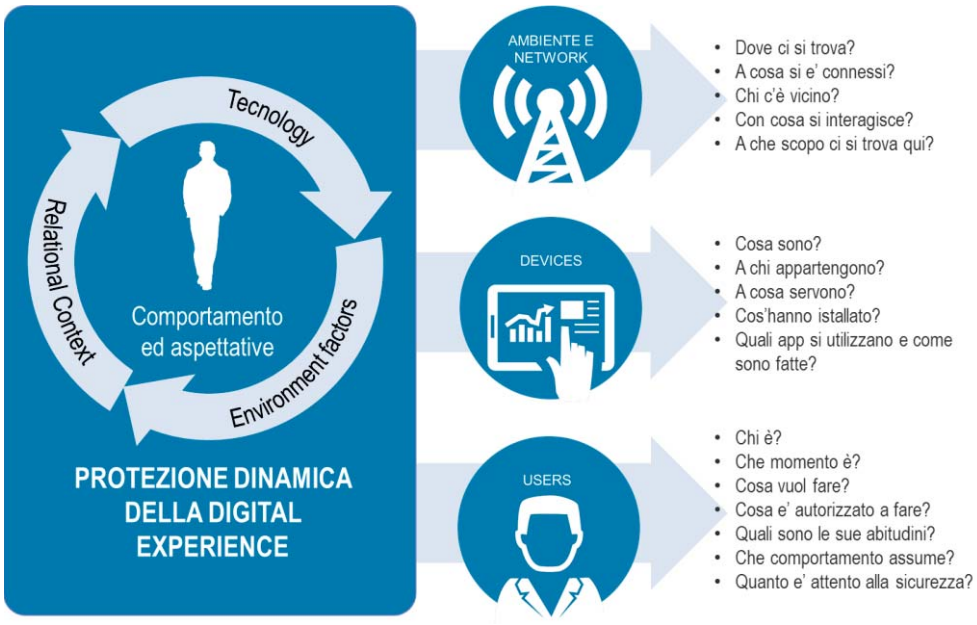
costantemente raffinando sempre più le loro tecniche; tendono ad operare per gruppi ben coordinati, condividendo risorse e strategie; possono "prendere in affitto" le dotazioni necessarie a realizzare azioni malevole o frodatorie ("Malware-as-a-service"); possono commissionare attacchi mirati a gruppi specializzati, e così via.

Anche nel cybercrimine esistono vere e proprie organizzazioni, spesso trasnazionali, che competono fra loro sulla base della capacità di controllare le risorse necessarie a condurre attacchi su vasta scala. Tali risorse sono sostanzialmente virtuali e "reclutate" nel Web attraverso la diffusione di malware, al fine di creare le cosiddette "botnet", che concorrono ad alimentare il circolo vizioso della diffusione di programmi malevoli.

Le iniziative di NTT DATA

Come si può vedere, il quadro d'insieme appare piuttosto critico e le strategie di risposta risultano ancora tutt'altro che definite e definitive. Di questo complesso scenario NTT Data si occupa da quasi un decennio. Notevoli sono stati gli investimenti in Ricerca e Sviluppo portati avanti in Giappone dalla capogruppo NTT (tra i primi 3 operatori TELCO al mondo e leader nel mondo come operatore Mobile con NTT Docomo) per costruire uno "resilient layer" per al protezione dei dispositivi mobile con la forte collaborazione del centro di Ricerca NTT I3 di Palo Alto in Sylicon Valley USA.

Questa importante capacità, know how e proprietà intellettuale, ha travato in Italia un ulteriore e significativo bacino di sviluppo, parte dell'iniziativa del "Distretto Tecnologico sulla Cybersecurity di Cosenza", una delle più importanti iniziative di ricerca in Europa cofinanziata per circa 30 Milioni di Euro, con il progetto di Ricerca "End-User Protection". L'obiettivo è finalizzare strategia e piattaforme tecnologiche a supporto che comprendano tutti i domini di vulnerabilità dell'ecosistema Mobile, con un approccio che possa effettivamente rappresentare una risposta ampia ed esaustiva a tutte le criticità sopra rappresentate.



La declinazione delle piattaforme sviluppate da NTT DATA è duplice ed è declinato, con diversi livelli di specializzazione, sia per utenze professionali di organizzazioni di tipo business che per gli utenti di **settori speciali quali la Difesa, e le forze di Polizia** che non possono assolutamente ritenersi neutrali rispetto ai

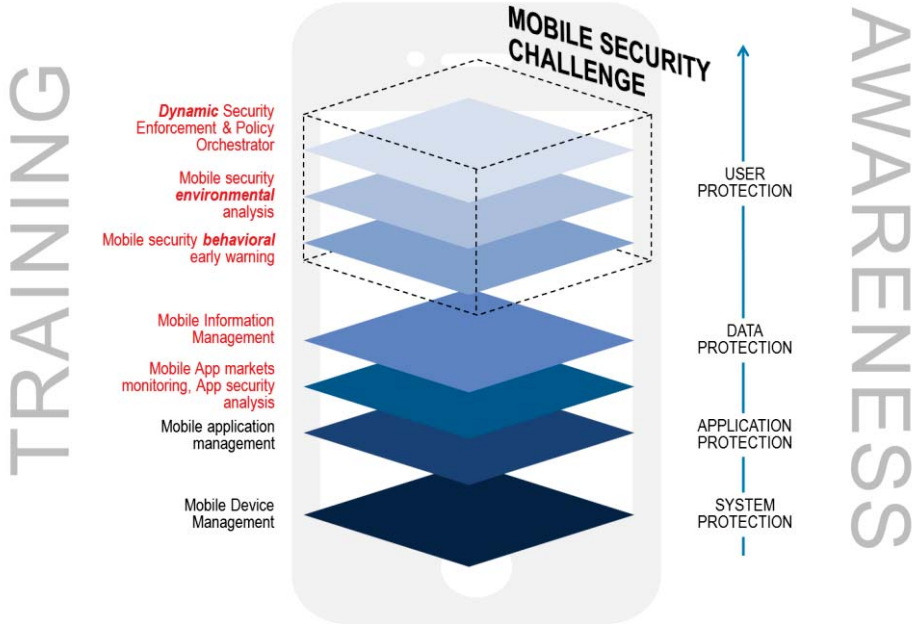
problemi sopra mossi della commistione delle informazioni tra sfera personale e quella professionale ed alle citate vulnerabilità che ne derivano. L'approccio tipico infatti basato su soluzioni di Mobile Device Management (MDM) e sull'adozione di politiche spinte di separazione delle reti e contesti non risolve il problema che spesso ha natura comportamentale ma è solo un primo e parziale approccio rispetto un tema ben più ampio ed articolato.

La sintesi dell'approccio NTT DATA

L'approccio NTT Data muove in definitiva dalla consapevolezza di un **nuovo perimetro da difendere: l'utente finale,** che in ultima analisi risulta essere **la *vera* e più preziosa *risorsa* dei cyber-criminali** come è testimoniato ampiamente dai numeri i quali rimandano al furto delle credenziali di accesso la quasi totalità degli attacchi informatici andati a buon fine.

Per tale ragione la strategia di NTT DATA si sviluppa proprio partendo dall'End-user e ponendosi nella sua ottica. End-user inteso come il soggetto finale dei servizi Mobile, gestiti individualmente ed utilizzati per fini conformi alle proprie personali necessità ed in accordo a proprie regole ed a quelle dettate dalla propria organizzazione quando previsto. Soprattutto questa utenza usa spesso il medesimo device per accedere ai sistemi informativi aziendali, in accordo a nuovi paradigmi quali il BYOD (Bring Your Own Device).

La possibilità di interagire con tali soggetti deriva dalla capacità di definire un scenario di sicurezza in grado di entrare in sintonia con essi, abituati a scegliere il proprio "portafoglio applicativo" in funzione della percezione di un bisogno immediato e fruendo di canali di approvvigionamento pensati appositamente per massimizzare le interazioni singole. La sfida di costruire un modello di sicurezza efficace in quest'area consiste nella capacità di indirizzare le necessità primarie di sicurezza dell'end-user proponendo un modello coerente con quelli affermati in tale dominio.

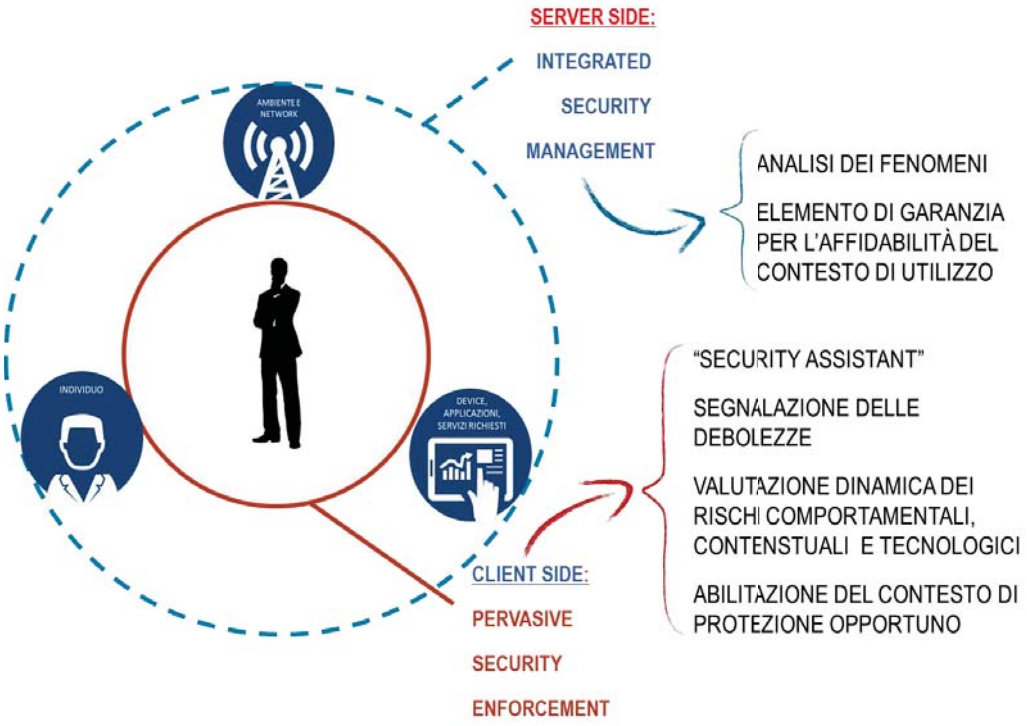


La sintesi di tale strategia NTT DATA è espressa dai molteplici risultati conseguiti in termini di tecnologie e di metodologie dalle attività di ricerca decennali sopra citate, tuttora in continua e dinamica evoluzione,vista l'evoluzione della minaccia stessa, e dal "**Programma ELISA** – **E**nd-user **Li**ght **S**ecurity **A**ssistant".

Pone quindi l'accento sulla protezione degli end-users indirizzando tutte le problematiche di rischio che, facendo leva sulle vulnerabilità proprie di ciascuna tipologia di device, determinano impatti diretti ed indiretti sull'utente finale, concorrendo nel contempo allo scenario di rischio dei sistemi ICT delle organizzazioni ed a quello globale del Web.

Il "Programma ELISA" realizza in definitiva l'approccio "client-oriented" di valutazione real-time del rischio connesso alla fruizione di servizi di Mobility, che possa identificare e rappresentare il profilo di rischio associato valutando, tra le altre molteplici capacità:

- il livello di protezione attivato sul device ed il profilo di sicurezza applicativo derivante dall'insieme di tutte le App installate, con il loro livello corrente di aggiornamento
- Il livello di "trusting" dei propri contatti, degli spazi cibernetici frequentati, delle transazioni finanziarie o commerciali in esecuzione sul device, verificando l'affidabilità e l'autenticità della controparte
- il rischio associato a profili comportamentali inappropriati, suggerendo all'utente il comportamento di sicurezza più adeguato (behaviour profiling / awareness) in funzione dell'effettivo contesto di utilizzo dello smartphone.



Questo ambizioso obiettivo di rimanere allo stato dell'arte con le tecnologie di difesa nel settore mobile sollecita molte tematiche che necessitano di continua ricerca ed innovazione, alcune specifiche pertinenti le peculiarità del contesto end-user, altre orientate a contribuire in senso generale allo sviluppo dei più avanzati sistemi di Cyber Security, che NTT Data intende perseguire con continuità nel tempo.

GIORGIO SCARPELLI **(Head of Application & Technology Service Center)**
PIERLUIGI LONERO **(Strategic Business Development Director)**

Analisi temporale di sorgenti informative eterogenee

Michele Colajanni, Mirco Marchetti, Andrea Balboni

Siti Web, agenzie di stampa, quotidiani, periodici, aziende e privati cittadini pubblicano quotidianamente elevate quantità di dati non strutturati, così come flussi continui di informazioni strutturate sono prodotte dai sistemi aziendali in rete. Questa enorme mole di informazioni apre nuove frontiere per l'intelligence, che, tuttavia, richiederà strumenti informatici innovativi a supporto degli analisti nei processi di sensemaking e decisionmaking.

Ad esempio, è possibile ricostruire reti di relazioni tra diverse entità, creando reti sociali che collegano persone, organizzazioni, aziende, luoghi ed eventi. È, inoltre, possibile analizzare come alcuni fenomeni di interesse evolvono nel tempo identificando chiaramente i momenti in cui si sono verificati eventi di particolare rilievo. Ai dati grezzi è possibile applicare molteplici algoritmi di advanced analytics al fine di identificare anomalie o effettuare analisi previsionali anche in tempo reale.

Caratteristiche delle sorgenti informative

La fattibilità di questi approcci non deve far ipotizzare che i risultati siano facili da ottenere. Sono necessari, infatti, strumenti informatici innovativi in grado di affrontare variabilità, dimensioni e eterogeneità dei dati in ingresso mai trattate in precedenza a simili scale temporali e dimensionali. Inoltre, i futuri sistemi dovranno sempre più essere in grado di gestire l'*imprevedibile* in fase di progetto. Quindi, non solo integrare sorgenti differenti, ma anche garantire la possibilità di integrare nuove fonti informative non previste nella fase iniziale di progetto. Occorre inoltre considerare che l'enorme mole di informazioni generate da sorgenti aperte sono tipicamente in linguaggio naturale, in diverse lingue, e privi di una specifica struttura. Tali documenti costituiscono un elemento importante per ogni operazione di OSINT (Open Source INTelligence, ovvero raccolte di informazioni da sorgenti aperte), ma la loro analisi mediante strumenti automatici richiede l'utilizzo di software complessi in grado di fornire qualche livello di interpretazione del testo e di estrarre entità rilevanti per gli analisti, quali persone, organizzazioni, luoghi, tempi e relative relazioni.

Requisiti dei sistemi di analisi

In uno scenario in cui il volume dei dati è destinato a crescere continuamente si impongono sfide molto interessanti anche a livello di prestazioni, efficacia e usabilità degli strumenti di analisi automatica. I sistemi dovrebbero consentire di effettuare interrogazioni sui dati in modo interattivo, permettendo quindi analisi esplorative da raffinare via via anche sulla base dei risultati intermedi ottenuti. Tale tipo di interattività comporta vincoli stringenti sui tempi di risposta che non devono crescere esponenzialmente all'aumentare della dimensione dei dati. Sebbene le architetture e i software adatti a scalare continuamente siano ancora oggetto di ricerca, si può facilmente ipotizzare che tutti gli approcci centralizzati, basati su una singola base di dati, siano inapplicabili indipendentemente dalle potenze hardware messe a disposizione, né è ipotizzabile che esista un'unica architettura adattabile a tutte le esigenze. Soluzioni efficaci saranno costituite da combinazioni di architetture, algoritmi e strategie di indicizzazione dei dati da integrare in modo adeguato alle necessità che di volta in volta emergeranno nella più classica interpretazione che "one size does not fit all".

Un secondo vincolo di usabilità è costituito dalla semplicità di interpretazione dei risultati. Anche in questo caso, non esiste una singola visualizzazione in grado di soddisfare tutte le possibili esigenze di analisi. Occorre quindi identificare la visualizzazione migliore per rappresentare graficamente i risultati di diverse tipologie di analisi. Ad esempio, un analista interessato nello studiare l'evoluzione di un fenomeno potrà richiedere la generazione di una serie temporale, mentre per l'analisi dei collegamenti che esistono tra persone e organizzazioni l'utilizzo di rappresentazioni a grafo potranno essere più adeguate.

Architettura per l'analisi temporale

Il Centro di Ricerca Interdipartimentale sulla Sicurezza dell'Università di Modena e Reggio Emilia (d'ora in poi, CRIS) ha sviluppato una architettura innovativa per l'analisi temporale di grandi quantità di sorgenti informative eterogenee, espressamente progettata per supportare gli analisti nei processi di OSINT, sensemaking e decisionmaking. L'architettura di alto livello è rappresentata in Figura 1.

L'architettura può essere alimentata con sorgenti dati eterogenee, sia strutturate sia in linguaggio naturale. Tutti i dati, prima di poter essere elaborati dall'architettura, attraversano una fase di pre-elaborazione. In questa fase, i dati non strutturati vengono analizzati da un motore di analisi semantica, mentre tutti i dati strutturati sono pre-elaborati da un componente software (Gateway) specifico per la struttura di ciascuna sorgente. Nuove sorgenti di informazione possono essere aggiunte semplicemente integrando un nuovo componente di pre-elaborazione, che andrà ad aggiungersi a quelli già esistenti in modo trasparente e senza la necessità di modificare altri componenti dell'architettura.

I dati pre-elaborati costituiscono l'input del motore di gestione dei dati, che svolge tre funzioni principali. La prima è associare a ogni documento un'etichetta temporale. Ad esempio, informazioni relative a un allarme di sicurezza rilevato all'interno di una rete sono associate al tempo corrispondente alla rilevazione dell'attacco informatico, mentre un articolo di giornale che descrive una notizia dell'ultima ora è associato alla data di pubblicazione. La seconda funzione consiste nel memorizzare in modo scalabile le entità e le relazioni estratte dai documenti pre-elaborati. La terza funzione consente di interrogare i dati memorizzati in modo estremamente efficiente, mantenendo i tempi di risposta costanti indipendentemente dalla quantità di dati memorizzati, nel rispetto dei requisiti descritti in precedenza.

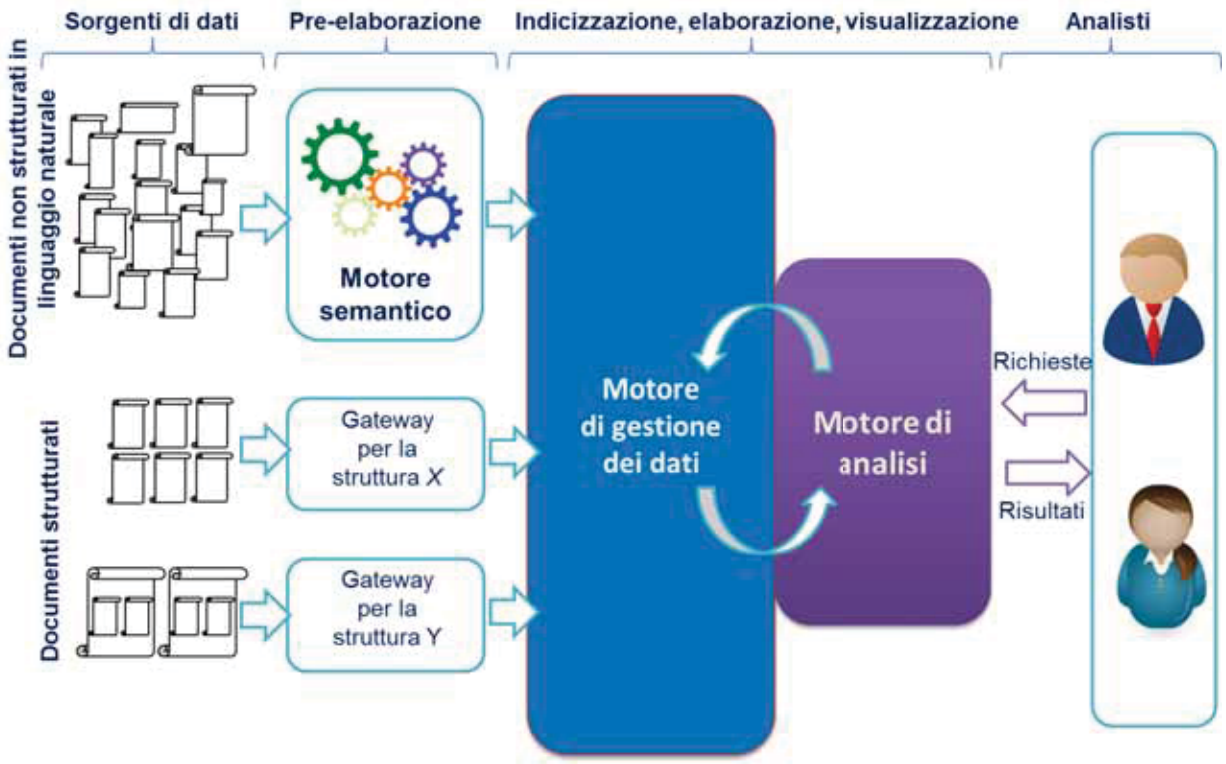


Figura 1. Architettura per l'analisi temporale di sorgenti informative eterogenee sviluppata dal Centro di Ricerca Interdipartimentale sulla Sicurezza e la prevenzione dei rischi (CRIS) dell'Università di Modena e Reggio Emilia.

Le funzioni di interrogazione e di visualizzazione sono svolte dal motore di analisi, la cui architettura è rappresentata in Figura 2. Gli analisti possono esprimere delle interrogazioni mediante interfacce grafiche, disponibili sia come software applicativo client sia come interfaccia Web. Il motore di analisi traduce le interrogazioni degli analisti in richieste che possono essere soddisfatte dal motore di gestione dati, il quale risponde con un sottoinsieme dei dati memorizzati. Le risposte del motore di gestione dei dati possono essere presentate graficamente agli analisti oppure possono essere sottoposte a ulteriori trasformazioni eseguite dal modulo di elaborazione. In particolare, è possibile sottoporre i risultati a numerose tecniche di analisi statistica e predittiva al fine di filtrare i dati eliminando il rumore, identificare anomalie e cambi di stato, calcolare previsioni. I risultati così ottenuti vengono trasformati nella rappresentazione grafica più opportuna e sottoposti agli analisti. Infine, è possibile esportare i dati in formati standard, permettendo quindi l'integrazione con strumenti di analisi diversi.

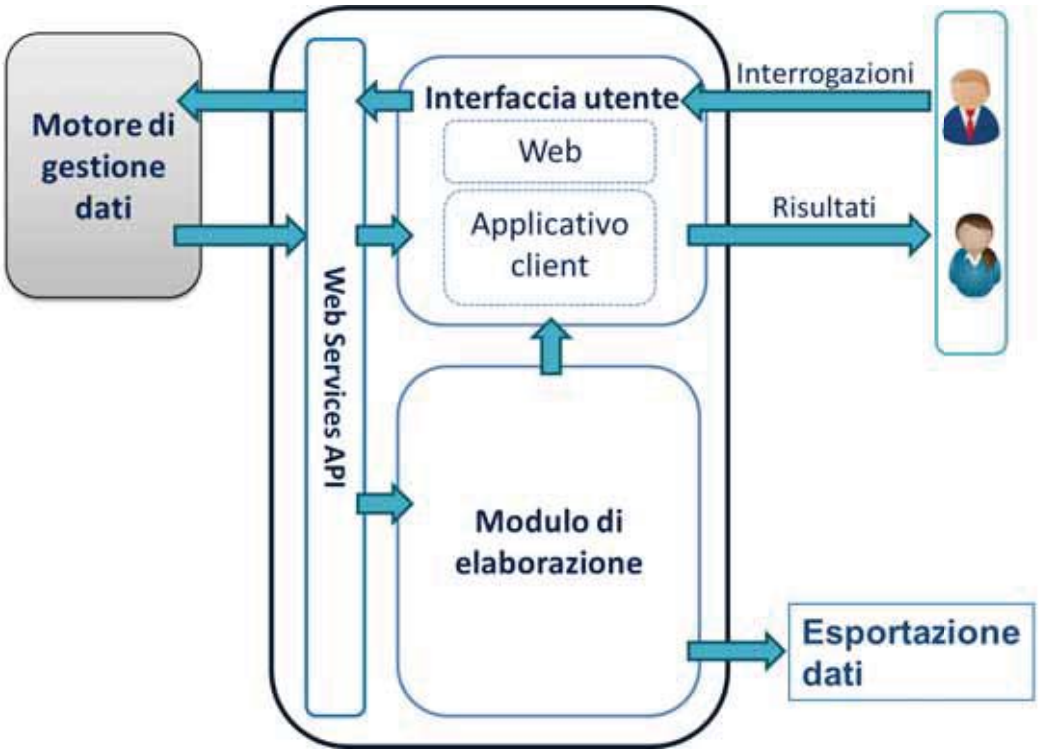


Figura 2. Architettura del motore di analisi.

Scenari di utilizzo

Il prototipo dell'architettura per l'analisi temporale di sorgenti informative eterogenee realizzato dal CRIS è alimentato sia con sorgenti strutturate sia con documenti in linguaggio naturale. In particolare, attualmente il motore di analisi dati contiene milioni di entità distinte estratte da allarmi di sicurezza e oltre un milione di entità distinte estratte dagli articoli pubblicati dalle principali agenzie di stampa e dai quotidiani nazionali e internazionali nell'arco di circa cinque anni. Grazie alle scelte progettuali effettuate, è in grado di rispondere a interrogazioni complesse in meno di tre minuti, tempo che non cresce all'aumentare dei dati.

Si riportano due esempi di utilizzo per dimostrare alcune delle capacità dell'architettura proposta. Come primo esempio, si considera un analista interessato allo studio della rete di relazioni di un particolare individuo in un dato intervallo temporale, quale la rete sociale di Abu Bakr Al-Baghdadi, autoproclamatosi "Califfo" del gruppo terroristico denominato "Stato Islamico" il 29 giugno 2014, nei mesi di novembre e

dicembre 2014. Per questo tipo di interrogazione, l'architettura di analisi produce come risultato un grafo, rappresentato in Figura 3. Ogni nodo del grafo corrisponde a una persona, mentre i segmenti che uniscono due nodi rappresentano le relazioni che collegano tra loro due persone. Dalla rappresentazione mediante grafo è possibile identificare immediatamente sia le relazioni dirette che collegano i contatti ad Abu Bakr Al-Baghdadi (al centro del grafo) sia la presenza di "cluster" di contatti con collegamenti diretti tra loro (rappresentati dai segmenti grigi in Figura 3). Si evidenzia, inoltre, che con una sola interrogazione è possibile produrre una sequenza di grafi sociali che rappresentano come le relazioni sociali di un individuo di interesse evolvono nel tempo.

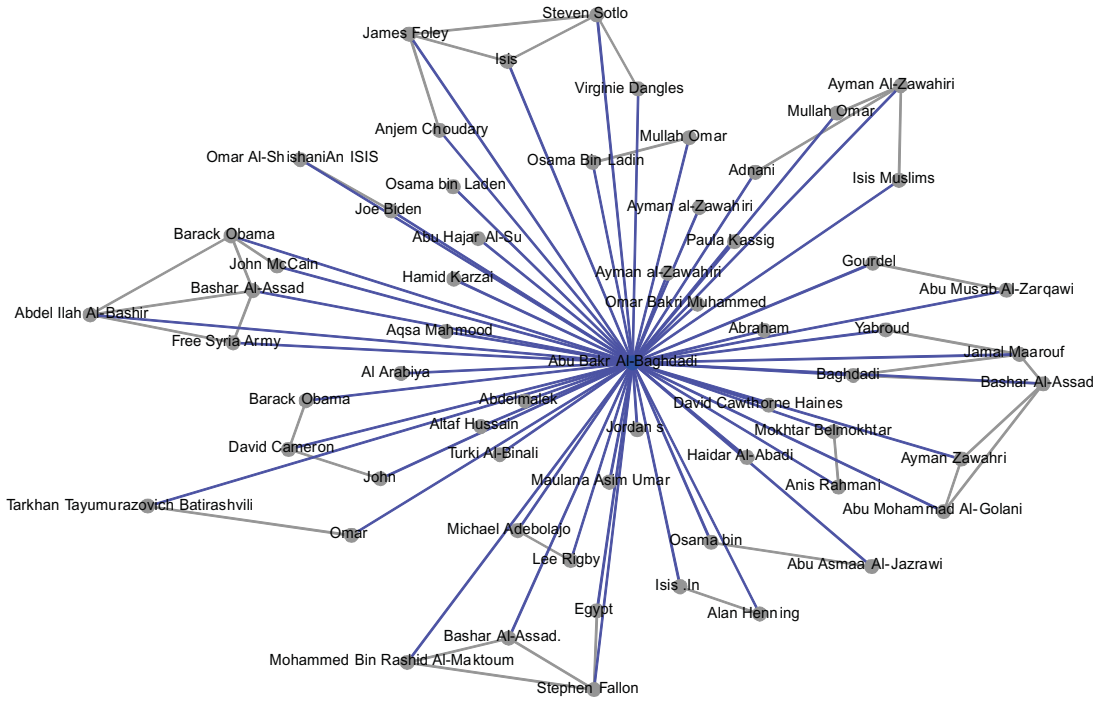


Figura 3. Rete sociale di Abu Bakr Al-Baghdadi nei mesi di novembre e dicembre 2014.

Un altro esempio di utilizzo consiste nella possibilità di indagare un particolare argomento al fine di verificare come i relativi eventi si sono evoluti nel tempo. Ad esempio, si consideri un analista intenzionato a verificare l'evoluzione temporale di tutti gli eventi relativi a atti di guerra tra Ucraina e Russia nel 2014 che vedono il coinvolgimento di Vladimir Putin. In questo caso, l'architettura produce come risultato una serie temporale rappresentata in Figura 4.

In questa serie temporale, l'asse delle ascisse rappresenta il tempo, mentre l'asse delle ordinate rappresenta il numero di notizie relative a fatti che corrispondono all'interrogazione eseguita dall'analista. I numeri posti in prossimità dei picchi e dei cambi di pendenza della serie temporale sono stati aggiunti per verificare l'efficacia di questa rappresentazione grafica nell'identificare i momenti maggiormente rilevanti per il fenomeno di interesse. Come validazione, è importante segnalare che i numeri corrispondono ai principali eventi nella crisi tra Russia e Ucraina pubblicati dalla BBC e rappresentati in Tabella 1. È possibile notare come un analista, osservando la Figura 4, possa identificare immediatamente i momenti in cui si sono verificati gli eventi più importanti relativi al fenomeno di interesse.

L'architettura per l'analisi temporale di sorgenti informative eterogenee è una soluzione promettente per effettuare analisi temporali su dati estratti da sorgenti informative eterogenee. In particolare, la possibilità di dare risposte a interrogazioni complesse e di evidenziare l'evoluzione temporale di fenomeni di interesse

è una base promettente per l'introduzione di metodologie di analisi innovative, applicabili in molteplici contesti e a diverse tipologie di analisi.

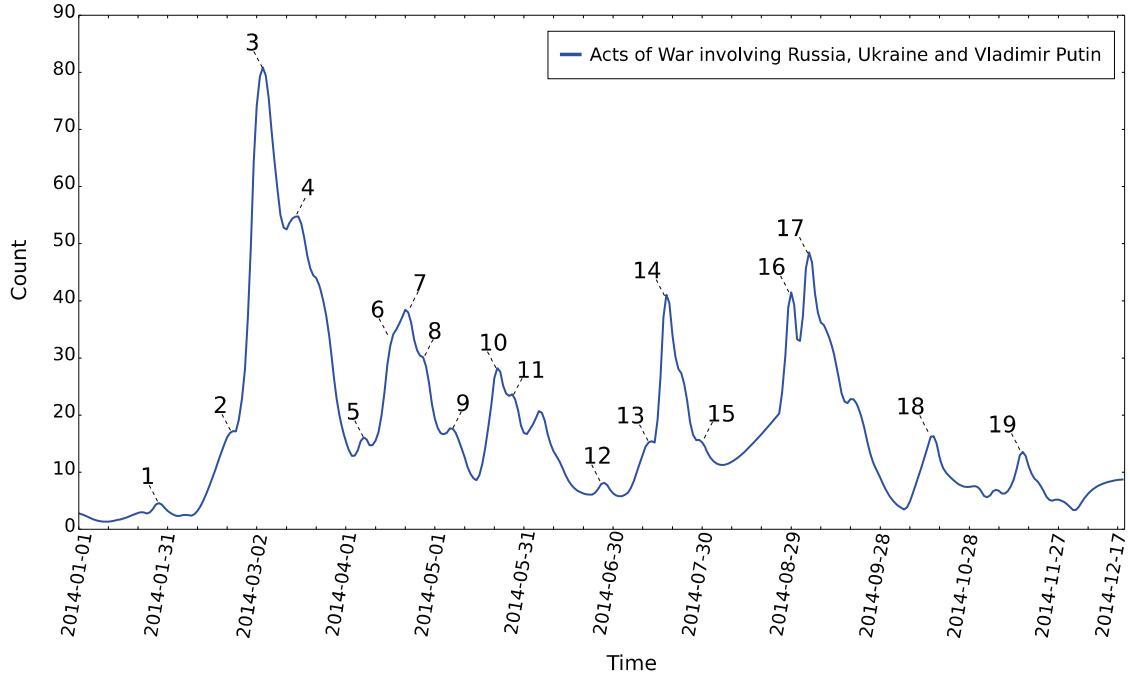


Figura 4: Atti di guerra relativi a Russia e Ucraina che coinvolgono Vladimir Putin.

Tabella 1: Eventi rilevanti della crisi tra Russia e Ucraina.

#	Fact
1	Prime Minister Mykola Azarov resigns and parliament annuls the anti-protest law. Parliament passes amnesty bill but opposition rejects conditions.
2	Kiev sees its worst day of violence for almost 70 years. At least 88 people are killed in 48 hours. Video shows uniformed snipers firing at protesters holding makeshift shields.
3	Russia's parliament approves President Vladimir Putin's request to use force in Ukraine to protect Russian interests.
4	President Putin signs a bill to absorb Crimea into the Russian Federation.
5	Protesters occupy government buildings in the east Ukrainian cities of Donetsk, Luhansk and Kharkiv, calling for a referendum on independence. Ukrainian authorities regain control of Kharkiv government buildings the next day.
6	Ukraine's acting President, Olexander Turchynov, announces the start of an "anti-terrorist operation" against pro-Russian separatists. It quickly stalls.
7	Russia, Ukraine, the US and the EU say they have agreed at talks in Geneva on steps to "de-escalate" the crisis in eastern Ukraine. Three people are killed when Ukrainian security forces fend off a raid on a base in Mariupol - the first violent deaths in the east.
8	Ukraine's acting president orders the relaunch of military operations against pro-Russian militants in the east.
9	Clashes in the Black Sea city of Odessa, leave 42 people dead, most of them pro-Russian activists. Most die when they are trapped in a burning building.
10	News coverage about upcoming elections in Ukraine
11	Ukraine elects Petro Poroshenko as president in an election not held in much of the east.
12	Russia's parliament cancels a parliamentary resolution authorising the use of Russian forces in Ukraine.
13	Rebels abandon their command centre at Sloviansk in the face of a government offensive.
14	Malaysia Airlines flight MH17 from Amsterdam is shot down near the village of Grabove in rebel-held territory, with the loss of 298 lives.
15	The EU and US announce new sanctions against Russia.
16	Rebel leader Alexander Zakharchenko says there are 3-4,000 Russian civilians in rebel ranks as the separatists open up a front on the Sea of Azov and capture Novoazovsk.

17	Ukraine and pro-Russian rebels sign a truce in Minsk.
18	President Putin orders thousands of troops stationed near the Ukrainian border to return to their bases.
19	Nato commander Gen Philip Breedlove says Russian military equipment and Russian combat troops have been seen entering Ukraine in columns over several days.

Cyber Defence e Analisi Forense: scenari e strumenti

Il profilo d'attacco delle nuove minacce informatiche è in continua evoluzione e impone un ripensamento complessivo delle dinamiche di difesa attiva. Un fattore determinante soprattutto considerando le specificità della Cyber Defence, settore in cui non è possibile gestire il rischio operativo cedendolo o accettandolo come sostenibile.

Si pensi alle caratteristiche di una delle più recenti minacce evolute, Rombertik, da poco trovato "in the wild" dal nostro centro di ricerca e sviluppo Talos: esso ha un comportamento insolito, inatteso, aggressivo e perfino autolesionista. Nell'analogia con il mondo cinetico sarebbe come trovarsi di fronte ad una spia che, libera nel nostro territorio, indossa una carica di esplosivo capace di ridurre in macerie un intero edificio. Una spia che esegue il suo compito, ma se intercettata, o nel caso in cui ritenga di essere stata scoperta, si tramuta in un kamikaze. Difficile gestire tali comportamenti estremi se non con nuove strategie di difesa.

Le Autorità Militari converranno sulla evidente necessità di gestire con un approccio strutturato tali nuovi scenari, con processi e tecnologie a supporto in grado di andare a segno verso i corretti bersagli, agendo a seguito di estensive analisi di ERM. Nell'ambito della tradizionale sicurezza fisica sono molte di più le differenze rispetto alle analogie che possiamo ravvedere nel confronto.

La "sicurezza" al 100% è un orizzonte complesso da traguardare nel cyber space mentre è criterio tassativo nel mondo cinetico della Difesa Nazionale. Nel cyber space la pura reazione è insufficiente se non accompagnata da una azione che nel mondo reale sarebbe definita "offensiva".

I nuovi modelli di analisi su big data hanno evidenziato che è possibile nel medio periodo costruire una efficace sicurezza predittiva. Ciò richiede anche la costruzione di nuove competenze interne (es. profili di data scientists).

L'analisi deve essere realizzata su decoy systems (falsi target) per permettere di operare a più livelli con un approccio empirico (costruzione della traccia virale in vitro e del relativo profilo di neutralizzazione), in grado di avere memoria di ciò che accade nel tempo (dinamica della propagazione dal Paziente Zero).

La sicurezza si definisce inoltre stabilendo una baseline in real-time (trusted scenario), verificando gli scostamenti significativi dal comportamento atteso del singolo utente e delle infrastrutture tecnologiche, tracciando costantemente ciò che accade nei tre tempi dell'attacco: "prima", "durante" e "dopo".

È necessario avere strumenti validi, utili e di immediato utilizzo per poter permettere un'analisi post mortem all'altezza dei migliori strumenti di indagine del mondo reale, poiché l'attività investigativa del cyber space porta il suo contributo fin nella situational room ed è identificata come strumento a supporto decisionale per mitigare la minaccia mentre essa si manifesta, anziché come strumento di ricostruzione dei fatti dopo che sono accaduti.

Infine, questo in diretta analogia con il mondo reale, è fondamentale identificare un partner tecnologico che abbia la capacità di fornire efficaci servizi informativi e servizi di threat intelligence di natura tecnologica. Un partner che possa cooperare con la Difesa Nazionale degli Stati e avere l'autorevolezza e le corrette referenze per garantire gli alti standard del settore della Difesa.

Cisco da anni opera nel settore, partecipando ai maggiori progetti OSINT nazionali e di intelligence su dati classificati, collaborando alla realizzazione delle maggiori infrastrutture di sicurezza in ambito NATO, e questo grazie al più grande laboratorio di ricerca tra tutti i produttori tecnologici, costituito da oltre 5000 tra ricercatori, analisti e sviluppatori dedicati al settore della cyber intelligence.

Se è vero che in media gli attacchi più raffinati restano occultati e invisibili alla vittima dell'attacco per oltre 200 giorni, le corrette tecnologie di cyber security possono portare visibilità e consapevolezza agli operatori e minimizzare l'impatto, permettendoci di sapere quando e come la minaccia si manifesterà di nuovo e lasciandoci modo di fare la prima mossa.

PR 23

Sinergia vincente fra big data e Machine Learning

Analizzare, Interpretare, Predire

Ing. Antonio Papa – EPS Datacom

Le esigenze alla base del progetto

L'impiego di analisti umani nella elaborazione dei dati provenienti dai molteplici sistemi di difesa in ambito informatico, fondamentale per le definizione di scenari complessi, incontra ostacoli ormai insuperabili a causa della dimensione raggiunta dai volumi dei dati da gestire.

EPS Datacom svolge con continuità attività di analisi sui sistemi informativi per alcune Infrastrutture Critiche Nazionali. Le analisi svolte sono prevalentemente di carattere comportamentale, relativi agli attacchi registrati dagli apparati di confine, e di scenario, per disegnare, con l'integrazione di attività OSINT, possibili scenari legati alla evoluzione della situazione geopolitica riguardante l'infrastruttura.

Tali esperienze, a fronte di risultati molto interessanti non ottenibili con i soli strumenti di sicurezza informatica, ha evidenziato la necessità di restringere i tempi di analisi – oggi nell'ordine dei mesi – e di allargare il campione di dati analizzati – oggi nell'ordine dei minuti.

Un caso recente riguarda una importante I.C. analizzata negli anni 2013 e 2014.

L'analisi relativa al 2013 (supportata da parallela attività OSINT) ha evidenziato un altissimo numero di attacchi, una forte concentrazione geografica e almeno due componenti di origine geopolitica: attacchi da movimenti di protesta italiani e attacchi mirati da un paese dell'Est Europa, per un probabile interesse in specifici contenuti di altre entità collegate alla I.C. sotto attacco.

Sorprendentemente l'analisi relativa al 2014 ha fornito scenari completamente mutati rispetto all'anno precedente: nonostante un incremento del 70% del traffico si è avuta la sorpresa di una drastica riduzione del numero degli attacchi, la polverizzazione delle origini degli attacchi rispetto alla concentrazione precedente, la scomparsa della attività dei movimenti di protesta italiani e l'emersione di attenzioni da parte dei paesi più tradizionalmente coinvolti in questo ambito.

L'analisi ha evidenziato i forti limiti legati al fattore umano: il campione è limitato e i tempi di elaborazione sono ormai incompatibili con requisiti di tempestività.

Al momento dell'analisi non erano però disponibili soluzioni tecnologiche per indagini che superassero le tradizionali valutazioni statistiche. Ed era altrettanto evidente l'impossibilità di gestire manualmente l'esplosione di dati da analizzare.

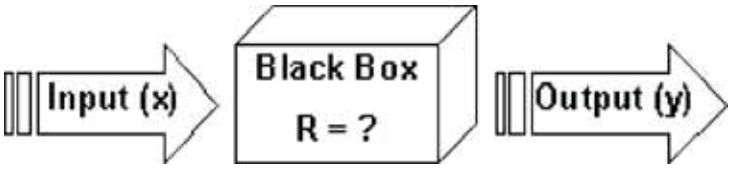
Le Reti Neurali Artificiali e l'Istituto Semeion

Da questa esigenza nasce la collaborazione con il centro di ricerche SEMEION, un Istituto Scientifico Speciale del MIUR specializzato nella ricerca nel campo dell'intelligenza artificiale focalizzato sulla scoperta di nuovi modelli matematici e algoritmi con particolare riferimento ai Sistemi Artificiali Adattivi. L'attività di ricerca è dimostrata da oltre 200 pubblicazioni su riviste internazionali e 11 brevetti internazionali.

L'idea alla base del PR23 è la valutazione dell'utilizzo delle Reti Neurali Artificiali a supporto del lavoro degli analisti. Tale idea è stata utilizzata per partecipare a un bando per stanziamenti per la ricerca applicata, bando poi vinta dal progetto.

Prima di procedere sulle caratteristiche del PR23 è necessaria una breve introduzione alle Reti Neurali Artificiali o ANN (Artificial Neural Network).

Per ANN si intendono algoritmi per ricostruire le regole (ovvero il contenuto della Black Box) che mettono in relazione un insieme di dati di Input per il problema considerato con l'insieme dei dati di Output, quando tale relazione è molto complessa. Le ANN auto-producono le regole sulla base di una esplorazione iterativa dell'evidenza empirica disponibile basata unicamente sull'insieme dei dati forniti. Una ANN addestrata (come tutte le intelligenze, hanno necessità di imparare) che abbia determinato le regole che meglio descrivono un certo fenomeno, può effettuare generalizzazioni e definire modelli



predittivi, quindi prevedere output anche su nuovi dati di input, purché rappresentativi del fenomeno in esame. Sono anche in grado, partendo da relazioni evidenti all'interno di un DB relazionale, di individuare dinamicamente le relazioni nascoste non visibili in altro modo. Le ANN sono particolarmente utili quando si analizza una rilevante massa di dati, senza avere una precisa idea dei processi che li hanno generati. Sono inoltre adattive: aggiungendo nuovi dati, le ANN aggiusteranno le loro regole di conseguenza, integrando i vecchi dati con i nuovi, senza bisogno di alcun intervento esterno.

Sintetizzando, le ANN sono in grado di individuare le relazioni nascoste e definire modelli predittivi basati su machine learning. I campi di applicazione delle ANN sono infiniti, dalla lettura di immagini digitali, di cui forniscono dettagli non altrimenti visibili, al riconoscimento di segnali radar, alla biologia fino a qualsiasi processo complesso basato su grandi moli di dati.

Un esempio di applicazione particolare è quella fatta per Scotland Yard, che ha analizzato il fenomeno del traffico di droga nell'area di Londra e che ha portato a numerosi arresti.

Il Programma 23

Dalla fusione delle esigenze di analisi avanzata, sia in termini quantitativi che qualitativi, e delle potenzialità delle ANN, nasce PR 23 che si propone di fornire capacità computazionale a processi di analisi fino ad oggi limitati dalla fisiologia umana.

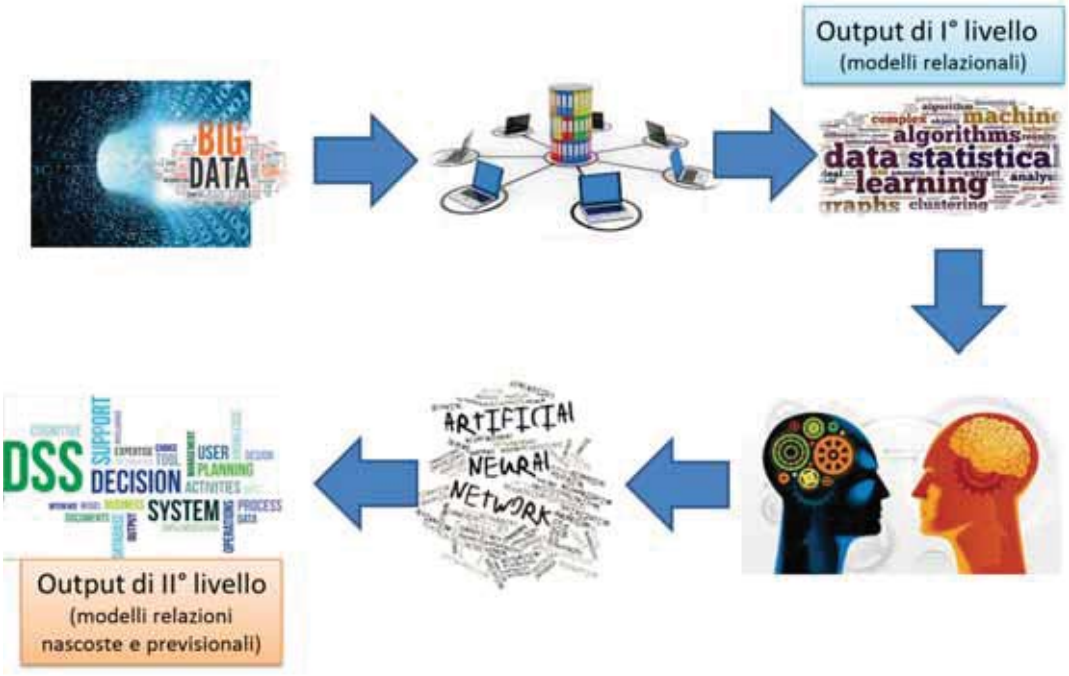
Il PROGRAMMA 23 lavora su due livelli di analisi:

1. Livello Statistico

I dati di Input del sistema, che nel caso specifico del prototipo PR23 sono costituiti da file di LOG provenienti da apparati di difesa perimetrale, a seguito di opportuna normalizzazione, alimentano un database relazionale appositamente disegnato e vengono analizzati a livello statistico, generando un output di I° livello in linea con molte soluzioni esistenti sul mercato.

2. Livello Previsionale

I dati di output di I° livello vengono poi acquisiti dalla componente ANN del sistema e vengono elaborati con i modelli adattivi artificiali: a partire da relazioni evidenti all'interno del DB relazionale, utilizzando sia tecniche semantiche, sia tecniche di Intelligent Data Mining, si passa all'individuazione di relazioni nascoste e a modelli



predittivi basati su machine learning. Gli output del processo di analisi costituiscono

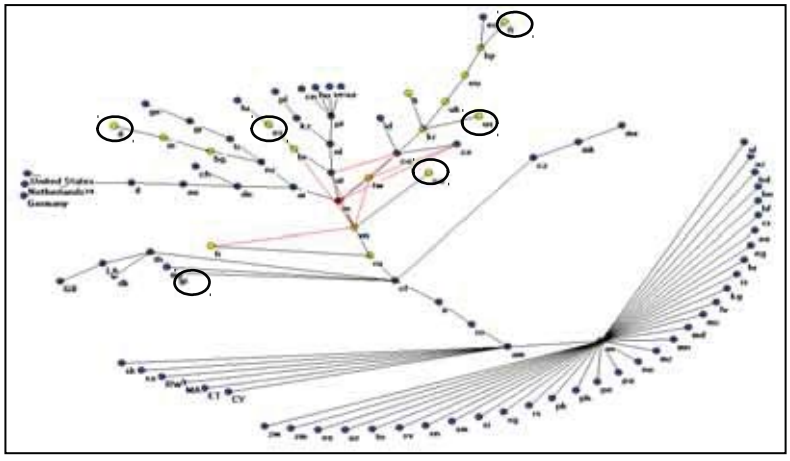
una serie di elementi utili per i decision support system utilizzati dagli analisti e dai decision maker. Il sistema fornisce inoltre la possibilità di effettuare simulazioni finalizzate alla previsione di scenari e di fornire informazioni utili al miglioramento della configurazione dei sistemi di difesa.

A livello tecnico, per l'analisi dei dataset sono stati utilizzati 6 tipi di Algoritmi (5 dei quali sotto copyright Semeion Vedi Bibliografia):

- Mappe AutoContrattive: per l'analisi multivariata non lineare di ogni data set di ogni giorno.
- MST, MRG e G_IN-OUT: per filtrare le informazioni chiave dalle matrici di tensori generati dalle Mappe AutoContrattive.
- Consensus Algorithm: per individuare in modo intelligente le concordanze, le discordanze e vari tipi di risonanza tra i grafi prodotti per ogni giornata e nelle varie Aree.
- Topological Weighted Centroid: per individuare la densità di probabilità geografica degli attacchi provenienti da quali aree e in quali giorni.

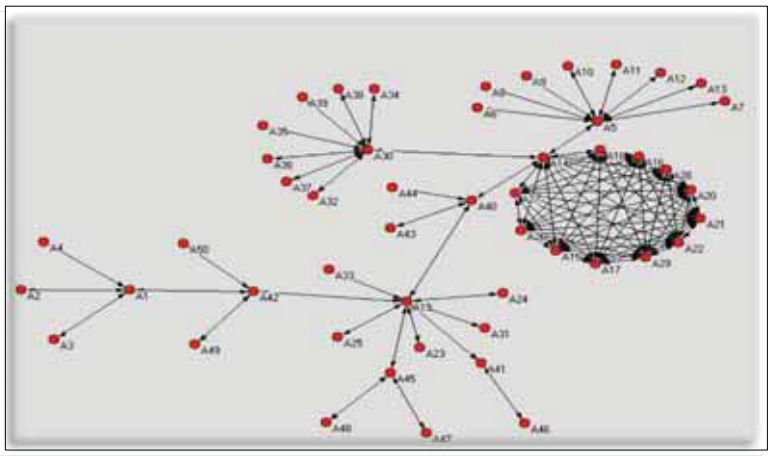
Fra i differenti output del programma, molto efficaci risultano essere i grafi, che ricordiamo essere non su base relazionale ma generati in base alle regole "nascoste" cui abbiamo accennato in precedenza. Due esempi di grafi, output del sistema, sono riportati in fondo all'articolo.

I primi risultati indicano operativi del PR 23 sono stati particolarmente incoraggianti. Il PR 23 ha consentito l'analisi di un campione molto più ampio e tempi in linea con l'evoluzione delle minacce; il tutto mantenendo l'efficacia dei risultati ottenuti manualmente e, tramite la componente predittiva, l'individuazione di possibili futuri scenari di minaccia.



Ricostruzione della rete logica degli attacchi per giorno ed aree di provenienza

Esempio Grafo MRG: in evidenza le aree che hanno subito attacchi "anomali".



Grafo dei tipi di attacchi avvenuti, con caratteristiche salienti:

- Attacchi tipici o episodici
- Attacchi organizzati o casuali

Esempio di grafo MRG in con un circuito a connessione totale in una parte periferica del grafo stesso. Attacco Tipico ed Organizzato

Il PR23 è uno strumento che si affianca agli attuali prodotti e soluzioni di sicurezza ICT con un approccio innovativo nel settore della cyber intelligence, non orientato alla ricerca delle specifiche minacce tecniche – cui sono delegati le molteplici architetture esistenti sul mercato – ma alla definizione di scenari predittivi riguardanti attori ostili alla infrastruttura e che tiene presente interessi interni ed esterni alla stessa.

La soluzione prevede la customizzazione dell'analisi che deve essere tarata sui sistemi ICT presenti e che deve tenere in considerazione l'ambiente in cui si opera e tutti gli stakeholders coinvolti.

[1] Capecchi V., Buscema B., Contucci P., D'Amore B. (Eds) Applications of Mathematics in Models, Artificial Neural Networks and Arts, DOI 10.1007/987-90-481-8581-8, Springer Scienze+Business Media,2010.

[2] Buscema M, Tastle W.J, (Eds), Intelligent Data Mining in Law Enforcement Analytics, DOI10.1007/978-94-007-4914-6, Springer Scienze+Business Media, 2013.

[3] Massimo Buscema, Enzo Grossi, Alvin Bronstein, Weldon Lodwick, Masoud Asadi-Zeydabadi, Roberto Benzi, Francis Newman, A New Algorithm for Identifying Possible Epidemic Sources with Application to the German Escherichia Coli Outbreak, in a Special Issue "Spatial Analysis and Data Mining", ISPRS International Journal of Geo-Information, 2013, 2(1):155-200.

[4] Bronstein, A. C., M. Buscema, A. Esfahani, W. A. Lodwick, and E. Grossi. "Locating the source of public health events using intelligent adaptive systems: 2011 United States listeriosis outbreak linked to whole cantaloupes." In CLINICAL TOXICOLOGY, vol. 51, no. 7, pp. 625-626. 52 VANDERBILT AVE, NEW YORK, NY 10017 USA: INFORMA HEALTHCARE, 2013.

[5] M. Buscema,P. L. Sacco, G. Ferilli, M. Breda, and E. Grossi, ,ANALYZING THE SEMANTICS OF POINT SPACES THROUGH THE TOPOLOGICAL WEIGHTED CENTROID AND OTHER MATHEMATICAL QUANTITIES: THE HIDDEN GEOMETRY OF THE GLOBAL ECONOMIC ORDER, Computational Intelligence, Volume 0, Number 0, 2014, doi: 10.1111/coin.12040.

IFI ADVISORY

INTELLIGENCE & FRAUD INVESTIGATION

Cyber Isis: la strategia mediatica del Califfato

Stefano Lupo

JUNIOR ANALYST

IFI Advisory

Gli obiettivi dell'azione mediatica dell'ISIS

Il gruppo che dapprima è stato conosciuto come "Al Qaeda in Iraq", poi come Stato Islamico in Iraq e Sham (Levante), e ora, dopo la proclamazione della rinascita del Califfato da parte del suo leader, Abu Bakr Al Baghdadi, il 29 giugno 2014, solo come "Stato Islamico", trae origine dal crollo del regime di Saddam Hussein nel 2003, a seguito delle operazione belliche degli Stati Uniti e dei suoi alleati.

L'ISIS (*Islamic State of Iraq and Sham*), come viene spesso citato sinteticamente, è stato creato su impulso del giordano Abu Musab Al Zarqawi, ucciso il 7 giugno 2006 da un raid americano. Al Zarqawi ha sempre avuto un rapporto particolarmente travagliato con l'establishment di Al Qaeda e con Osama Bin Laden *in primis*. Nato nel clima dell'insorgenza irachena, l'ISIS si è via via evoluto in un culto estremistico che differisce radicalmente da Al Qaeda stesso per due importanti ordine di ragioni: lo Stato Islamico punta a perseguire e colpire tutti i musulmani considerati eretici[1] partendo dal suo controllo territoriale tra Iraq e Siria e, proprio per questa ragione, aspira all'eliminazione del nemico vicino, mentre Al Qaeda vede ancora nel "lontano Occidente" il grande avversario da combattere.

Lo Stato Islamico, perennemente al centro delle cronache internazionali, ha fatto suoi alcuni elementi della "tradizione islamica", declinandoli tuttavia secondo immagini e strutture del pensiero moderno. L'ideologia che richiama la rinascita del "Califfato", le attività di estorsione e sequestri tipiche del crimine organizzato, le tattiche militari impiegate negli scontri armati e l'azione mediatica pianificata, rendono l'ISIS un fenomeno particolarmente complesso da affrontare e di non facile analisi. Secondo Michael Weiss e Hassan Hassan, i due autori de *Isis, Inside the Army of Terror,* lo Stato Islamico è un vero e proprio network della violenza strutturalmente basato su apparenti incongruenze: inclusivo, aspirante a raccogliere membri da ogni dove, anche dall'estero, ma settario dal punto di vista religioso, almeno secondo le dichiarazioni dei suoi membri, territoriale ma attento alla proiezione internazionale tramite i mezzi di comunicazione (in particolare i *social media* come Twitter, Facebook e altri)[2].

L'ISIS attribuisce primaria importanza all'uso evocativo che si può fare della violenza, sia per intimorire gli avversari, sia per attrarre nuove reclute o, in ogni caso, creare forme di affiliazione. Le azioni dimostrative violente, del resto, fanno parte del DNA del gruppo e risalgono a ben prima dell'emersione del fenomeno dei "social". Durante il periodo di ribellione al controllo americano e alleato dell'Iraq, ad esempio, sono state effettuate più di ottanta decapitazioni di musulmani ritenuti infedeli o di occidentali

1 Centrale per lo Stato Islamico, الدولة الإسلامية, *al-Dawla al-Islāmiyya*, è l'atto del *takfir,* ossia il poter dichiarare gravemente empio un individuo, colpevole di essere "infedele" (*kafir*) alla vera religione. Come si vedrà in corso di trattazione, l'elaborazione di un "nemico" è fondamentale per tutto l'impianto ideologico-politico-militare dell'ISIS.

2 **M.Weiss, H.Hassan**, *Isis: Inside the Army of Terror,* Regan Arts, New York, 2015.

catturati, tutte debitamente filmate e mostrate al pubblico. Molti uomini al centro dell'operato del gruppo, composto da radicali sunniti ed ex membri del partito iracheno Baath, al governo con Saddam Hussein, condividono la comune esperienza di aver soggiornato in centri di detenzione gestiti da truppe statunitensi, come il carcere di Abu Ghraib in Iraq o la prigione della base di Guantànamo, a Cuba[3].

Jessica Stern e J.M.Berger, nel loro *ISIS, the State of Terror*, esplorano in profondità la particolare propensione del gruppo terroristico nel dedicare molta attenzione all'aspetto comunicativo della propria azione. L'utilizzo dei social media, in particolare, rappresenta il miglior strumento al momento a disposizione dell'ISIS per traumatizzare "cuori e menti" degli avversari (o dei possibili sostenitori), normalizzare, attraverso la ripetizione cronologica delle torture e degli omicidi mostrati al mondo, la propria azione di rottura psicologica degli schemi concettuali e presentarsi come reale catalizzatore globale dei principali orientamenti radicali a sfondo islamico[4]. Decapitazioni, lapidazioni, fucilazioni devono essere assimilate come "procedure standard" da coloro che ricevono il messaggio.

L'aspetto mediatico della battaglia dello Stato Islamico, la sua proiezione di forza, ciò che un tempo si otteneva con una minaccia o dimostrazione di potenza (la cosiddetta "diplomazia delle cannoniere" ne è un rilevante esempio storico) si integra perfettamente nel suo piano politico-militare. L'uso intensivo e altamente competente dei social media e di tutto l'impianto informatico risponde alla logica di allargare il proprio raggio d'azione ben aldilà del settore mediorientale (laddove l'ISIS effettivamente opera) creando un ulteriore fronte di combattimento. L'hackeraggio di account Twitter o di siti internet, la comunicazione tramite social media che operano non solo gli agenti effettivi dell'ISIS ma anche simpatizzanti e curiosi che si avvicinano al "messaggio di rottura", non indica altro che la prosecuzione dello scontro. Mutuando Carl Von Clausewitz e il suo miliare "Della Guerra", si può forse arrivare ad affermare che l'attività cyber dello Stato Islamico rappresenta una vera e propria "continuazione della guerra"[5] con altri mezzi. Una guerra

3 Molti esponenti dello Stato Islamico sono entrati nel gruppo dopo la cosiddetta campagna "Breaking the Walls", condotta per più di un anno dal luglio 2012 al luglio 2013 ad opera di membri della prima ora del movimento per ingrossare i ranghi dell'ISIS, dopo le alterne vicende del 2008, in cui aveva subito violenti sconfitte, sia da parte del governo iracheno sia da parte delle principali tribù sunnite a cavallo del confine tra Iraq e Siria. L'ISIS ha portato a termine varie operazioni per far evadere numerosi detenuti. Quest'ultimi, una volta nelle fila dello Stato islamico, hanno ulteriormente innalzato il livello di violenza delle azioni dimostrative del gruppo, con particolare predilezione per le torture psicologiche. Interessante è in merito il punto di vista di Graeme Wood che, nell'articolo uscito su "The Atlantic" nel marzo 2015, *What Isis Really Wants,* rileva come l'osservanza religiosa estrema sia importante per lo Stato Islamico nella misura in cui diviene utile *identity maker* per evidenziare chi è all'interno del gruppo e chi ne è al di fuori. http://www.theatlantic.com/features/archive/2015/02/what-isis-really-wants/384980/

4 **J.Stern, J.M.Berger**, *ISIS, the State of Terror,* Harper Collins Publishers, New York, 2015.

5 **Carl Von Clausewitz**, *Della Guerra,* Einaudi, 2007. L'autore tedesco aveva individuato nella politica la "continuazione della guerra con altri mezzi".

psicologica solo in parte, visto il primario obiettivo dello Stato Islamico di reclutare nuovi ranghi per i teatri operativi di Siria e Iraq.

L'*image management* attuato dall'ISIS è efficace perché unisce la duplice componente della brutalità delle sue azioni al pragmatismo di un'attenta pianificazione flessibile, ossia sia territoriale sia mediatica. Più ancora della padronanza della tecnologia, in realtà di apprendimento non proibitivo, stupisce, dello Stato Islamico, la perfetta comprensione dell'evoluzione degli eventi e dei nuovi trend legati al terrorismo. Laddove Al Qaeda comunicava tramite videocassette o, al più, per mezzo di forum criptati, l'ISIS ha capito la fondamentale rilevanza di muovere dagli antichi network di comunicazione a innovativi punti nodali, caotici e nascosti, composti da attori che si influenzano vicendevolmente. Il tutto viene facilitato dal fatto che gran parte dell'attività di antiterrorismo è ancora troppo prossima ai vecchi canoni di comunicazione ed è quindi aumentato considerevolmente il *trade-off* tra la facilità di compiere attacchi o incursioni cyber (compreso i social media) e la difficoltà, per chi li subisce, di rimediare ai danni patiti. L'attività di hackeraggio, come del resto l'azione social del gruppo, punta a far sì che i propri sostenitori si rafforzino nella convinzione, fino a creare nuove cellule autonome e di successo (i punti nodali di cui sopra). L'azione di unità cyber dell'ISIS quali il *Cyber Caliphate* o la *Islamic State Hacking Division,* è proprio quella di coordinare gruppi operativi "distanti" dal normale teatro bellico.

Il Summary *"Isis Global Intelligence"*, dell'Institute for the Study of War, mostra i tre macro teatri operativi dello Stato Islamico, l'anello interno, rappresentato dalla Siria e dall'Iraq, ma anche da Giordania, Israele, Palestina e Libano, l'anello prossimo, in arancione, corrispondente grossomodo all'antica area geografica del Califfato, e l'anello esterno, quello più interessante ai fini del presente studio, comprendente l'Europa, gli Stati Uniti, l'Asia meridionale fino all'Australia e, soprattutto, il *cyber domain*[6]. La trasposizione di sé e del proprio messaggio è intimamente legata alle azioni "operative" del gruppo sia nell'anello interno sia nell'anello prossimo e, grazie all'azione di simpatizzanti, nell'anello esterno. La combinazione di attacchi di gruppi o di quelli che vengono definiti *lone wolves*, lupi solitari (combattenti isolati e, soprattutto, autonomi), e le determinate crisi nazionali o internazionali da essi provocate, come avvenuto a Parigi tra il 7 e l'8 gennaio 2015 o a Copenaghen, tra il 14 e il 15 febbraio, vengono seguite da quelle sono state abilmente definite "le code cyber degli eventi geopolitici"[7]. Esse non sono altro che un aumento più che esponenziale degli "attacchi cyber" a seguito di determinate azioni terroristiche (nei giorni immediatamente dopo gli attacchi di Parigi, peraltro rivendicati a favore non dello Stato Islamico, bensì di Al Qaeda nella Penisola Arabica, AQAP, nella sola Francia si sono

6 Institute for the Study of War. Isis Global Intelligence Summary 07/01/2015-18/02/2015 http://www.understandingwar.org/backgrounder/isis-global-intelligence-summary

7 The BatBlue Special Report, *Terror Goes Cyber: the Cyber Strategies and Capabilities of Al Qaeda, ISIS, AL Shabab and Boko Haram,* april 2015, http://www.batblue.com/bat-blue-special-report-terror-goes-cyber/

registrati circa 19.000 attacchi a siti web da parte di simpatizzanti del jihadismo, per la maggior parte sostenitori dello "Stato Islamico", da cui si nota la trasversalità di consensi).

Il fatto che attacchi compiuti "in favore" di AQAP vengano ripresi da sostenitori dello Stato Islamico non deve sorprendere. La dimensione operativa dell'ISIS, soprattutto grazie alla sua appendice cyber mediatica, gli consente di poter sfruttare al meglio qualsiasi attacco di matrice terroristica a sfondo islamico compiuto nel mondo (con una formula *win-win*, vale a dire che non importa che l'operazione abbia avuto successo, basta solo che abbia avuto luogo). Come si evidenzierà meglio nella terza parte, lo Stato Islamico tende a proporre, a livello di comunicazione mediatica, un messaggio ideologico molto più sfumato rispetto a quello, rigoroso, imposto nei territori che controlla fisicamente tra Iraq e Siria. Questo aspetto, volutamente pianificato, serve a rendere il proprio messaggio di opposizione all'occidente e a "tutti gli infedeli" più esportabile e più adattabile alle singole realtà in cui esso viene recepito. Così facendo l'ISIS massimizza il controllo della propria comunicazione in realtà abdicando alla sua gestione e "delegandolo". Tutto questo è possibile perché oramai lo Stato Islamico è un'organizzazione terroristica rivoluzionaria ibrida, nel senso che a tratti tende quasi ad assomigliare a un gruppo d'influenza a livello mondiale. Basti pensare che nei giorni immediatamente precedenti alla proclamazione del Califfato, il 29 giugno 2014, l'ISIS ha condotto via social media un'intensa campagna di *brand management* per valutare, tra i suoi sostenitori, la bontà e l'opportunità della proclamazione stessa[8]. L'eliminazione dei riferimenti "in Iraq e in Sham", inoltre, lo pone in contrasto con Al Qaeda per il predominio nel mondo jihadista e ne determina la contestualizzazione realmente globale (ecco spiegata la rilevanza dei tre teatri operativi).

L'iterazione dell'operato dell'ISIS, dalle attività belliche territoriali alle campagne mediatiche online, è continua e si auto alimenta. Essa inoltre risponde all'esigenza dell'ISIS di dover governare effettivamente il territorio sotto il suo controllo e, nel contempo, richiamare il maggior numero di sostenitori sia come *foreign fighters* in Medio Oriente sia come "cassa di risonanza" dello Stato Islamico a livello internazionale. Dice bene Aymen Al Tamimi, quando afferma che *baqiyya wa tatamaddad*, "rimanere ed espandersi" è, oltre a uno degli slogan più popolari, anche uno dei punti cardine del pensiero dell'ISIS[9]. L'espansione avviene spesso tramite reazioni sproporzionate nel mondo a causa delle cosiddette "code cyber" descritte in precedenza. La propaganda provoca la reazione di combattenti e/o aspiranti tali e allorquando l'azione di disturbo

8 È interessante notare, tuttavia, che nonostante la maggior parte delle risposte, arrivate soprattutto via Twitter, ritenesse prematuro la proclamazione del Califfato, e quindi fosse negativa, Al Baghdadi e il suo entourage abbiano deciso comunque di andare avanti nel loro progetto.

9 Tale pensiero è contenuto nel capitolo "The Islamic State Regional Strategy" all'interno de *The Islamic State Trough the Regional Lens,* a cura di Julien Barnes-Dacey, Ellie Geranmayeh e Daniel Levy, edito per lo *European Council on Foreign Relations,* www.ecfr.eu p. 19

mediatico, o l'attacco fisico, vengono compiuti, essi vengono prontamente rivendicati dall'ISIS, anche in assenza di reale connessione[10].

In estrema sintesi si possono evidenziare gli aspetti cardine che legano lo Stato Islamico al fenomeno della comunicazione, propaganda e attacco via internet:

a- L'ISIS ha rivoluzionato il modo in cui il terrorismo utilizza i social media per attività di propaganda e reclutamento, grazie a un network disperso di supporters che "massimizzano" la sua voce.
b- Le tattiche impiegate non sono sofisticate ma risultano estremamente efficienti e facilmente apprendibili.
c- Viene effettuato un "coordinamento a maglie larghe" con altri gruppi jihadisti e "lupi solitari" che rende ulteriormente difficile il controllo governativo.
d- Mantiene, ad ogni modo, un canale mediatico ufficiale tramite una serie articolata di pubblicazioni, pur continuando a privilegiare la dimensione social della propria comunicazione.

Perché la comunicazione dello Stato Islamico è efficace

Nel paragrafo precedente si è evidenziata l'azione mediatica condotta da gruppi risalenti allo Stato Islamico e alla sua propagazione social. Resta tuttavia da comprendere come tale messaggio risulti efficace, come cioè divenga condivisibile anche in aree del mondo molto eterogenee e perché lo Stato Islamico sia in grado di riuscire in tale impresa[11].

La comprensione da parte dei "vertici comunicativi" dell'ISIS (in particolare di Abu Amr al Shami, tra i principali coordinatori del lato mediatico dello Stato Islamico[12]) che la maggior parte dei sostenitori più attivi dello Stato Islamico generalmente non sia realmente dotta della religione Islamica (più frequente, come fenomeno, in coloro che risiedono nel "terzo anello d'azione") risulta prioritaria per il successo del messaggio evocativo. La motivazione individuale per unirsi allo Stato Islamico spesso ha più a che fare con le dinamiche d'adesione a un social network (direzione, identità, scopo, senso

10 Rileva il fenomeno *win-win* trattato sopra, che trova una delle più chiare esemplificazioni in quanto avvenuto il 3 maggio 2015 in Texas, negli USA. Due uomini sono stati uccisi dalla polizia la sera del 3 maggio 2015 a Garland, nei pressi di Dallas, fuori da una scuola dove era in corso un evento che prevedeva una mostra di vignette raffiguranti il profeta Maometto, con relativo dibattito. I due individui avevano prima aperto il fuoco ferendo un agente. Uno dei due assalitori, Elton Simpson, era stato indagato nel 2006 dall'FBI per aver cercato di unirsi a formazioni jihadiste in Somalia ed era stato incarcerato nel 2010. Lo Stato Islamico ha rivendicato l'accaduto. Si noti che il suo compagno, Nadir Hamid Soofi, era un semplice emarginato sociale, a differenza di Simpson stesso.

11 *Follow ISIS on Twitter: A Special Report on the Use of Social Media.* http://news.siteintelgroup.com/blog

12 http://treasury.gov/ofac/downloads/prgrmest.txt per maggiori dettagli.

d'appartenenza, rafforzamento) che con la reale comprensione delle norme religiose che accompagnano l'azione dell'ISIS. L'adattabilità del messaggio, spesso sfumato, ne diviene quindi uno degli aspetti di maggiore pericolosità, perché rende la propaganda dello Stato Islamico non solo fluida ma anche accattivante[13].

Aldilà della competenza tecnica degli artefici primi della comunicazione mediatica dell'ISIS[14], il grimaldello che fa penetrare il contenuto dello Stato Islamico è primariamente la violenza, come già evidenziato in precedenza, in tutte le sue forme, anche quelle più bestiali che ritraggono esecuzioni di massa. E' questo l'elemento per entrare "nei cuori e nelle menti", in una società globale oramai ampiamente abituata alle scene di intrinseca e pura violenza, sia reale, sia virtuale tramite videogiochi[15]. I sostenitori indipendenti giocano un ruolo chiave nelle campagne dell'ISIS. Secondo un report ICSR (*International Centre for the Study of Radicalization*), la maggior parte dei combattenti stranieri, riceve update da una rete di "disseminatori-simpatizzanti" che in realtà non ha contatti diretti con l'organizzazione e che è localizzata soprattutto in paesi occidentali[16]. Con il medesimo messaggio d'azione e di "morte partecipata", lo Stato Islamico riesce sia ad "ispirare" sia a "terrorizzare", vecchie tattiche con nuovi mezzi, una ricca platea di sostenitori dell'ISIS, che segue le sue vicende[17] ma che al contempo deve essere continuamente stimolate. L'iterazione continua della violenza, per quanto la normalizzi agli occhi di coloro che ricevono il messaggio, rischia anche di abituare troppo, rendendo necessaria una continua escalation per "mantenere vivo l'interesse". Il coinvolgimento basato più sull'emozione e sull'ideologia dell'aggressività che sull'appartenenza a un gruppo fisico diviene l'àncora di

13 Per citare alla lettera le parole del Professore Claudio Lo Jacono, Direttore della rivista Oriente Moderno ed esperto di Storia del Vicino Oriente islamico, "stiamo assistendo all'erosione delle basi culturali dell'Islam sunnita e alla crescita abnorme di un Islam 'altro'". In *Huffington Post,* "Il Jihadismo, una Nuova Fede", 08/04/2015, http://www.huffingtonpost.it/claudio-lo-jacono/il-jihadismo-nuova-fede_b_7024322.html

14 Interessante è l'approccio dell'applicazione Twitter "The Dawn of Glad Tidings" che raggruppa dati di simpatizzanti utenti twitter e ripropone i contenuti senza attivare la funzione spam del social media. Si vedano in particolare *The Guardian,* "Who Is Behind Isis's Terrfying Online Propaganda Operation?" http://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq , e *The Atlantic,* "How Isis Games Twitter". http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

15 Rileva qui un altro elemento che contraddistingue l'ISIS. Conoscere "i gusti" dei propri destinatari e il potere stimolante che la violenza, normalizzata, cioè resa ovvia dalla sua continua iterazione, ha nelle persone. Da qui tentativi propagandistici realmente di rottura, come l'imitazione grafica di un immagine che evoca il famoso videogioco bellico "Call of Duty". Nell'immagine modificata dall'ISIS segue la scritta: "Ciò che tu fai per finta, noi facciamo per davvero".

16 **J.A. Carter, S. Maher, P. R. Neumann**, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, ICSR, 06/2014, http://icsr.info/2014/06/8939/

salvezza di quanti operano al di fuori della cerchia fisica dell'ISIS ma che in fin dei conti agiscono per suo conto o a suo vantaggio: si assiste alla graduale preminenza di ideologia e messaggio emozionale nei confronti della pianificazione e del coordinamento[18]. Chi gestisce le basi concettuali della campagna mediatica dello Stato Islamico ben comprende che la maggior parte dei sostenitori occidentali non si impegnerà realmente in azioni di "movimento", come i terroristi "distaccati" o quelli impegnati nel "Califfato". Il ruolo chiave diviene quello di "propagatori" dell'influenza dell'ISIS, anche solo "retwittando" i suoi messaggi, contribuendo a veicolare la sua proiezione. È questo un compito comodo che si può portare a termine nell'ombra, senza superare "la soglia della moralità" di azioni violente, rendendo tanto più difficile il controllo da parte dei governi e delle Agenzie di Sicurezza. L'interessante spunto di Jarret Brachman rileva come l'emersione dell'Internet 2.0 abbia permesso la radicalizzazione di molti elementi senza una reale influenza diretta da parte di movimenti jihadisti, quasi come una sorta di indottrinamento fai-da-tè[19].

I bersagli preferiti della propaganda ISIS nel "terzo anello d'azione" sono elementi che provengo dalle aree più emarginate dei paesi bersaglio: gli ambienti legati alla logica dell'anticonsumismo, i figli di immigrati, specialmente se provenienti da aree a maggioranza islamica, elementi delle fasce sociali più deboli dal punto di vista socio-economico. Non è certo un caso che l'ISIS abbia speso particolare attenzione nei confronti delle manifestazioni di protesta e dei violenti scontri ad opera della comunità afroamericana negli Stati Uniti, a causa di alcune uccisioni indiscriminate da parte della polizia[20]. Ma, come afferma Stathis Kalyvas, politologo dell'Università di Yale, è questa una linea d'azione che accomuna l'ISIS più ai gruppi di militanti rivoluzionari che ai gruppi fondamentalisti islamici: l'esercizio in particolare della leva razzista fu, fin dall'epoca della

17 **J.M Berger, J. Morgan**, *The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter*, Brookings Institute, 20/03/2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf . Secondo i dati forniti, i sostenitori dell'ISIS seguono le "gesta" dello Stato islamico scegliendo per ¾ come lingua di comunicazione l'arabo, mentre un rilevante 1/5 adotta la lingua inglese. Si nota inoltre che i gruppi d'interesse e azione che si riferiscono all'ISIS sono di piccole dimensione (500-2000 account), ma solo da settembre a Dicembre 2014 ne sono stati sospesi da Twitter circa 1000.

18 Ecco perché nei quasi 14 anni di scontro con il jihadismo internazionale, se si prende come ideale data di partenza l'attacco alle Torri Gemelle di New York dell'11 settembre 2001, si sono colti risultati inferiori alle aspettative: i governi hanno sì combattuto per disgregare vari gruppi terroristici ma non sono riusciti a frantumare l'ideologia di base, che si è via via propagata, perdendo il reale nocciolo di impostazione salafita, per divenire quasi unicamente un inno all'azione di scontro.

19 **J. Brachman**, *Global Jihadism: Theory and Practice (Political Violence*, Routledge, NewYork&London 2009. Brachman, ex Direttore per le Ricerche dell'U.S. Military Academy's Combating Terrorism Center, individua la figura dei "jihobbysts", jihadisti per passione, o per "hobby", che si limitano ad effettuare compiti marginali o parziali, pur avendo, sommando tutte le azioni, un contributo importante.

guerra fredda, una linea guida di propaganda applicata nel terzo mondo da satelliti o agenti diretti dell'Unione Sovietica[21]. L'attività terroristica di questi anni si è sempre più uniformata a livello internazionale perché, in particolare per l'ISIS, l'atto di uccidere, o comunque di compiere azioni violente, è divenuto sempre meno il mezzo per ottenere il fine ultimo dettato dall'ideologia e sempre più il fine stesso: come dimostra la ripresa video della tragica esecuzione del giornalista americano James Foley il 19 agosto 2014, il killer del reporter, di chiara provenienza britannica, secondo l'accento del suo inglese, non ha mai fatto alcun accenno al benché minimo riferimento dottrinale musulmano per motivare l'uccisione di Foley stesso, accontentandosi di una lunga filippica nei confronti dell'Occidente. Le istanze dei gruppi terroristici sono sempre più disgiunte dai loro atti di violenza[22].

Leggendo le pagine di *The War of The Flea*, libro del 1965 dello storico Robert Taber, si trovano conferme delle basi concettuali del pensiero espresso da Kalyvas: l'azione dell'ISIS ha molto meno a che fare con le dottrine legate al Corano e molto più con le strategie rivoluzionarie di Mao Zedong e Che Guevara, una sorta di guerriglia del XX secolo adattata alla "Guerra Informativa"[23]. Sarebbe comunque riduttivo interpretare la propaganda mediatica del jihadismo e, nel nostro caso, dell'ISIS, come un mero lavaggio del cervello, una manipolazione per menti deboli. Essa certamente attinge da situazioni di grande disagio ma è importante considerare come spesso i giovani, principali bersagli dell'azione mediatica, non vengono "manipolati" contro la propria volontà. In molti casi le persone che subiscono processi di radicalizzazione adempiono per loro libera scelta[24].

---

20 Rilevano in particolare l'attenzione spesa nei confronti dei fatti di Ferguson in Missouri nel novembre 2014 e a Baltimora, in Maryland nell'aprile 2015. Frequenti i messaggi Twitter da parte dell'ISIS che esortavano "I fratelli neri" alla lotta contro l'oppressore americano. *ISIS supports Ferguson protesters: Islamic militants pledge to send over 'soldiers that don't sleep, whose drink is blood, and their play is carnage',* The Daily Mail, http://www.dailymail.co.uk/news/article-2850442/We-hear-help-ISIS-tweets-support-Ferguson-protesters-reject-corrupt-man-laws-like-democracy.html#ixzz3ZosDZqeG***;*** *Isis Using Baltimore Riots to Recruit African-Americans for 'Waging Jihad': Report,* International Business Times, http://www.ibtimes.co.in/isis-using-baltimore-unrest-recruit-african-americans-waging-jihad-report-630751

21
S. Kalyvas, *The logic of violence in the Islamic State's war,* The Washington Post, 07/07/2014, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/07/07/the-logic-of-violence-in-islamic-states-war/

22
D. Arkin, *James Wright Foley, Kidnapped Journalist, Apparently Executed by ISIS,* Nbc News, http://www.nbcnews.com/storyline/james-foley/james-wright-foley-kidnapped-journalist-apparently-executed-isis-n184376

23
R.Taber, *The War of the Flea: the Classic Study of Guerrilla Warfare,* Lybe Stuart Inc., New York, 1965.

Come riportato da Lord Carlile in *Digital Jihad: How Online Networks are Changing Extremists,* l'emergenza del cosiddetto "Dark Web", angoli oscuri della rete dove un buon numero di individui diventa propagatore, consapevole o inconsapevole, di messaggi di radicalizzazione, evidenzia la rilevanza della cosiddetta *online-offline syndrome*, ossia l'esistenza di persone che nella vita reale si comportano in una maniera, ma che davanti a un computer si trasformano in tutt'altro[25]. Tuttavia, è bene ricordare come, internet o non internet, seppure amplificate dalle interazioni "social", sono ancora le relazioni sociali nel mondo reale a dettare il passo, anche nel mondo della radicalizzazione sociale, che sia di matrice jihadista o meno. Persone che fanno parte di gruppi di amici, che si conoscono nel mondo reale, che hanno interessi simili, tendono a radicalizzarsi insieme e interagiscono con i combattenti "reali" tramite social media. Ecco perché si assiste alla creazione di gruppi radicali provenienti dai posti fra i più disomogenei (villaggi norvegesi, città australiane, paesi della campagna inglese). Si crea un iter continuo di radicalizzazione-propagazione: chi va a combattere in Medio Oriente perché convintosi, una volta tornato in patria, riporta la propria esperienza, divenendo "messaggio vivente", tra i più stimolanti veicoli di idee.

L'ISIS approfitta di un panorama comunicativo del tutto nuovo e affonda in situazioni di conflittualità che possono tornare utile al proprio disegno. La comunicazione mediatica, oltre che "terzo anello di scontro", diviene in realtà vero e proprio primo fronte di combattimento, per reclutare, indottrinare e terrorizzare. La comunicazione di atti di violenza tramite network amplifica gli incidenti locali, fino a trasformarli in crisi internazionali (la già citata "coda cyber") e si propaga dal globale al locale, dal pubblico al privato, da reale a virtuale, e viceversa[26].

Tale ultimo elemento si ricollega alla principale difficoltà patita dai governi nell'attività di repressione dei fenomeni di radicalizzazione, specie se di matrice terroristica e jihadista. La frammentazione dei gruppi, ma non dell'ideologia, ha portato, negli ultimi dieci anni, da una guerra globale al terrorismo, nell'idea all'epoca esposta dall'allora presidente americano G.W. Bush, a una serie di battaglie individuali da parte dei vari stati nei confronti del terrorismo, quest'ultimo ormai globale. In verità, come dimostrano negli

---

24
Interessante lo spunto del sociologo Frank Furedi, in F.Furedi, *ISIS's very modern war on the past,* http://www.frankfuredi.com/site/article/770 , occorre cautela nel sovrapporre la teoria della radicalizzazione e quella della manipolazione psicologica. In altri termini, l'ISIS riesce nell'impresa di influenzare il suo pubblico non tanto grazie alla sua maestria comunicativa, quanto già al dissenso già presente in alcuni strati delle società. Furedi cita l'anticonsumismo come una delle retoriche che più di altre divengono terreno fertile per sfoghi e processi di radicalizzazione.

25
Chatham House, *Digital Jihad: How online networks are changing extremists*, 02/03/2015.

26
J.D.Derian, *From War 2.0 to Quantum War: the Superpositionality of Global Violence*, Australian Journal of International Affairs, 67:5, 570-581, DOI, 2013

ultimi anni gli attacchi a Parigi e prima a Sidney, Boston, Ottawa e, ora, a Garland in Texas, ci si confronta oramai con una sorta di terrorismo glocale, globale e locale al medesimo tempo, globale nell'azione scaturita dalla propaganda mediatica e locale perché radicato nel territorio sotto il proprio controllo, vero motore delle direttrici di radicalizzazione[27].

Conclusione

I governi e gli enti militari che si occupano di contenere il fenomeno della radicalizzazione ideologica sono ormai quasi unanimi nel ritenere dannosa la mera sospensione degli account e dei dati internet ricollegabili al terrorismo jihadista e in particolare all'ISIS. Tale azione rappresenterebbe un grave danno per i governi, che perderebbero una complessa fonte di informazioni e di intelligence. Combattere l'estremismo violento, in particolare nella situazione socio-politica internazionale analizzata in precedenza, richiede l'attivazione e l'impegno, a fianco dei governi, non solo degli enti privati, in grado di sostenere gli alti costi della strumentazione tecnologica di controllo, ma anche della comunità internazionale stessa, che deve diventare la prima linea di contenimento nei confronti della radicalizzazione trasversale e imprevedibile. Il risultato di tale azione tripartita potrebbe e dovrebbe portare all'elaborazione di una vera e propria contro-narrativa (*counternarrative*) in grado di opporsi alla logica del terrore. E' necessario comunque essere obiettivi: la "coda cyber degli eventi geopolitici" continuerà ad avere importanza nel corso dei prossimi mesi, anche a causa del determinante ruolo dei giornali e delle pressioni nei giochi politici nazionali, importanti casse di risonanza. Rileva l'analisi di David Fidier, del *Council on Foreign Affairs*, che nota la necessità di una nuova strategia di CVE (*Countering Violent Extremism*): Fidier individua il felice paragone tra la lotta alla propaganda mediatica dell'ISIS e la classica campagna COIN (anti-terrorismo, *Counterinsurgency*). In particolare, Fidier trova analogie tra i tre step dell'attività di COIN (*clear-hold-build*, ripulire, mantenere, costruire) e una possibile azione di opposizione nei confronti dell'attività mediatica dello Stato Islamico. L'azione di "ripulire" è paragonabile al contenimento della proliferazione di utenze internet pro-ISIS, l'attività di "mantenere" può

27
Questo vale sia per l'ISIS tra Iraq e Siria, sia per Boko Haram nel Nord Nigeria, sia per Al Shabab tra Somalia e Kenya. L'ISIS rimane ad ogni modo ai vertici del fenomeno "glocale".

essere accostata all'azione di risposta da parte dell'opinione pubblica e della società civile che si oppone alla logica del messaggio di violenza transnazionale. L'atto di "costruire", infine, si ricollega alla minimizzazione degli aspetti cyber che facilitano l'operato dei terroristi, andando soprattutto alla fonte socio-culturale del problema della radicalizzazione diffusa[28].

Proprio tale ultimo aspetto, come d'altronde rileva per la vera e propria attività COIN, è l'elemento più difficile da affrontare. È bene ricordare, come accennato precedentemente, che il messaggio radicale di violenza è globale, ma le reazioni nella comunità internazionale spesso affondano in questioni locali e lì rimangono. Per tale ragione fa bene James P. Farwell a sottolineare la necessità di variare e adattare le tattiche e i metodi di lotta alla radicalizzazione da paese a paese e, a volte, anche all'interno del paese stesso. Affrontare gli aspetti locali o regionali di conflittualità dovrebbe divenire la prima azione dei governi in opposizione alla violenza transazionale, che trova nella comunicazione mediatica dell'ISIS[29] il più letale veicolo al momento in circolazione.

28
D.Fidier, *Is it the Time for a Counterinsurgency Approach to the Cyber War Against ISIS?*, 12/03/2015, Defense One, http://www.defenseone.com/threats/2015/03/it-time-counterinsurgency-approach-cyber-war-against-isis/107457/

29
J.P.Farwell, The Media Strategy of ISIS, Survival: Global Politics and Strategy, vol. 55, n.6, p49-55 12/2014/01/2015, 25 November 2014.

One-Way Traffic Keeps Secrets Secret

DataDiode makes outgoing network traffic impossible

There is widespread belief that the only foolproof and guaranteed way to prevent classified information leaks via a network is by making sure there is no physical connection. This is a misconception. Moreover, it would be unwise to isolate a network entirely from the outside digital world: after all, it needs to be able to receive incoming traffic. The solution that meets both requirements—no leaks, while allowing incoming traffic—is a so-called data diode: a physical device without IP address, software, firmware, or FPGAs (programmable chips) that allows network traffic to flow in one direction, but impossible to let traffic flow in the other way. This article is based on the presentation *Protecting Secrets from Cyber Crime,* held by Peter C. Geytenbeek, International Sales Director at Fox-IT, at the Defence Symposium in Chiavari, Italy in May 2015.

National governments have always been interested in learning each other's defense secrets and of ways to undermine each other's infrastructures. They deploy a wide array of resources—including digital weapons—for this purpose. The online threats currently facing defense organizations are already well-known. Less well-known, however, is that the instigation of digital resources has been around a lot longer than many people think. One of the oldest examples dates from the pre-Internet era.

Sabotage

In 1982, a Russian pipeline exploded in the Siberian city of Urengoy. It was the largest-ever non-nuclear explosion that was visible from space.

The cause was—allegedly—sabotage by the CIA. Not by agents on the spot, but by a Trojan horse planted by the CIA in the pipeline's operating software, which had been developed by a Canadian company.

Since then, malware—supposedly developed by "state actors" –

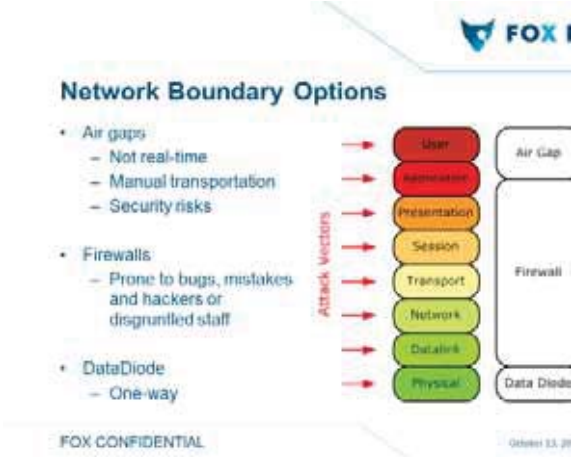
has surfaced on a regular basis, with Stuxnet being the most famous. Terrorists and hacktivists are also increasing their targeting of secrets and infrastructures of "unsympathetic countries."

Vulnerable

These trends are mounting pressure put on the defense networks that house secrets. Network design (architecture), security policy (e.g. enforcing passwords that meet specific requirements), network software and communication protocols are particularly vulnerable. A single blindspot in one of these areas can expose the network to infiltration.

Measures

One well-known way to rigorously isolate a network is to create an "air gap." The network would then stand alone and information would only be able to enter or leave via a USB stick, CD-ROM, or another medium. It is a tedious process and, most importantly, that it is unsafe because malware can still enter the network



through the media, and sensitive information can, in effect, leave by the same route.
Another option is to shield the network with a firewall, preferably a 'next generation'. However these are IP solutions that can be hacked, cannot guarantee faultless operation (bugs, backdoors), and are sensitive to configuration and administration errors, intentional or otherwise.
And finally, there is the **DataDiode**, which can make all outgoing—or incoming—network traffic impossible, but in a different way from the "air gap."

Hardware-only

Like its electronic namesake, a DataDiode is a device that enables one-way traffic. Current (data) can flow in one direction, but not in the other. The Fox-IT DataDiode is based on this principle. It is a hardware-only device with no software, programmable components, or IP address. This ensures that the DataDiode cannot be hacked from the outside, and thus makes it absolutely impervious to online attacks.

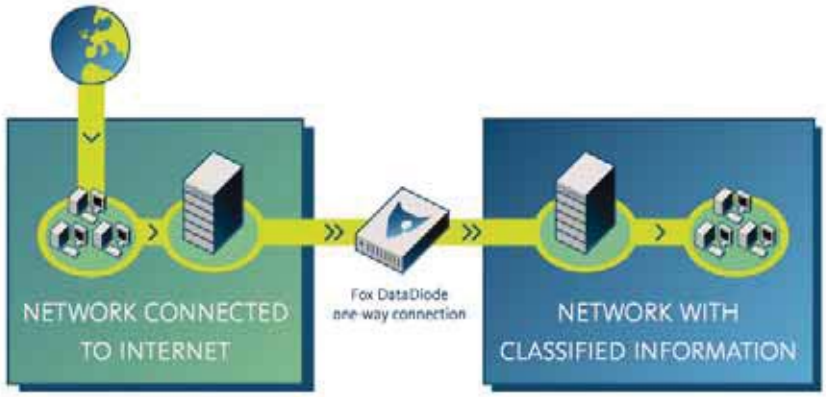
However, the electronic disabling of (data)traffic in one direction is not sufficient. A solid solution requires more. Most protocols are designed for and require two-way traffic and will be broken if traffic is blocked in one direction. If IP traffic in one direction is impossible, then there is no flow control either. For this too a solution is needed.

In principle

A DataDiode can ensure that outbound traffic is impossible. It can prevent leakages of confidential and classified information, but it does not stop incoming traffic which potentially can undermine a protected network. In practice, incoming traffic is first guided through a network with all the necessary security measures, ranging from antivirus to IPS and SIEM. Also, additional techniques are used, such as file format conversion (for example, Word to pdf), to neutralize potentially harmful content. The odds of this happening are minimal, but it is still theoretically possible that, despite all the measures, malware finds its way into a protected network. That

said, it is of primary importance to prevent any information from leaving the network.

Proxy Servers for Flow Control



Two proxy servers are used for flow control: one between the incoming traffic and the DataDiode and one between the DataDiode and the shielded network. This allows the data traffic flow to be controlled up to the diode and from the diode to the network. Bridging via the diode goes through a dedicated protocol with the ability to transfer data reliably without receiving feedback. Extensive testing and actual experience have shown this very short route to be error-free.

Certification

Because the complete DataDiode solution renders outbound traffic impossible, it guarantees against network leaks of confidential and classified information. The Fox DataDiode has the highest certification possible: it is the only CC EAL 7+ certified device in the world and it has received defense certifications from The Netherlands, Germany, the United States, Russia, and India.

Blocking Incoming Traffic

A DataDiode can of course also be set up to work in the other direction: meaning outbound traffic is allowed and incoming traffic blocked. This configuration is common in companies and organizations in the energy, oil & gas, and nuclear sectors, whom demand absolute guarantees that nothing can be disrupted by external traffic. Outbound traffic is used, for example, to send oil rig production

data and the like to corporate headquarters. This configuration can also prove useful for defense organizations. Take, for example, cases in which it is necessary to prevent external influences via a network (impacting launchers, for instance), but which harbor no secret information and require outbound traffic.

No Management, Low Cost

As the DataDiode itself is made up entirely of hardware, without software and programmable chips, there is no need for regular updates or device management. This has a very positive impact on the reliability of the device. The savings in maintenance and administration costs alone make the DataDiode a very attractive solution for guaranteed physical shielding of a network.

Fox-IT is an international security company offering products and services that cover the entire security spectrum, ranging from prevention and detection to intelligence gathering and rapid response to security incidents.

Currently, defense organizations and businesses in critical sectors, such as energy, in more than 40 countries deploy the Fox DataDiode to protect classified information on the one hand and physically shield production networks from malicious external network traffic on the other.

Il Traffico One-Way Tiene i Segreti "*SEGRETI*"

Il DataDiode rende impossibile il traffico in uscita dalla rete.

Esiste è la diffusa convinzione che l'unico modo, infallibile e garantito, per evitare fughe di informazioni classificate tramite reti dati sia quello di fare in modo che non vi sia alcun collegamento fisico tra di esse. Si tratta di un equivoco. Inoltre, non sarebbe saggio isolare completamente una rete dal mondo digitale esterno: dopo tutto ha bisogno di essere in grado di ricevere il traffico in ingresso. La soluzione che soddisfa entrambi i requisiti, nessuna perdita di dati consentendo il traffico in entrata, è il cosiddetto "DataDiode": un dispositivo fisico, senza indirizzo IP, senza software, senza firmware o FPGA (chip programmabili) che consente al traffico di rete di fluire in una sola direzione, impedendo che il flusso possa fluire in senso inverso. Questo articolo è un estratto della presentazione *Protecting Secrets from Cyber Crime,* tenuta da *Peter C. Geytenbeek*, International Sales Director at Fox-IT, al Cyber Defence Symposium tenutosi a Chiavari (Ge) nel maggio 2015.

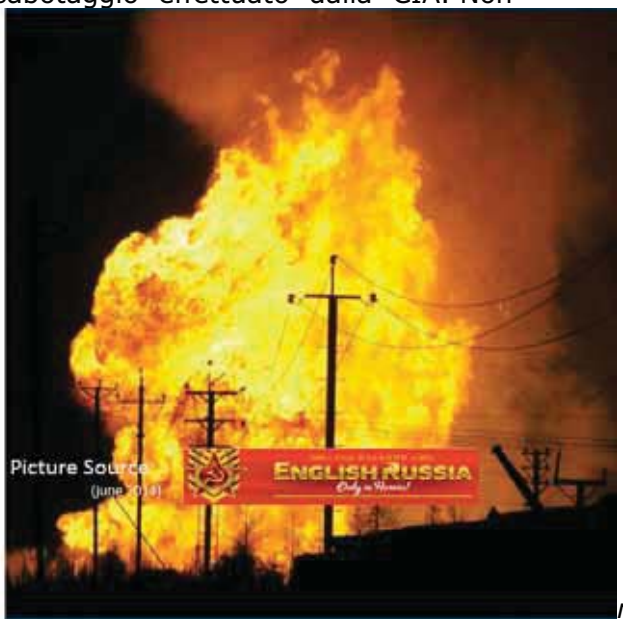
I governi nazionali da sempre sono interessati a conoscere i rispettivi segreti militari con l'obiettivo di minarne le rispettive infrastrutture. A questo scopo, negli anni hanno implementato una vasta gamma di armi tra le quali, negli ultimi tempi, spiccano decisamente quelle digitali. Le minacce online sono ormai ben note alle organizzazioni governative che devono provvedere alla sicurezza dei vari paesi. E' tuttavia poco noto che il tentativo di attacco alle risorse digitali sia più datato di quanto si possa credere. Alcuni esempi risalgono all'era "pre-internet".

Sabotaggi

Nel 1982, una conduttura di gas Russa esplose nella città siberiana di Urengoy. Si trattò della più grande esplosione "non nucleare" mai avvenuta, visibile anche dallo spazio.

Si trattò presumibilmente di un sabotaggio effettuato dalla CIA. Non da agenti presenti in loco, ma da un "Trojan Horse" impiantato dalla CIA nel sistema operativo che gestiva la conduttura, sistema sviluppato da una società canadese.

Da allora sono emersi con regolarità



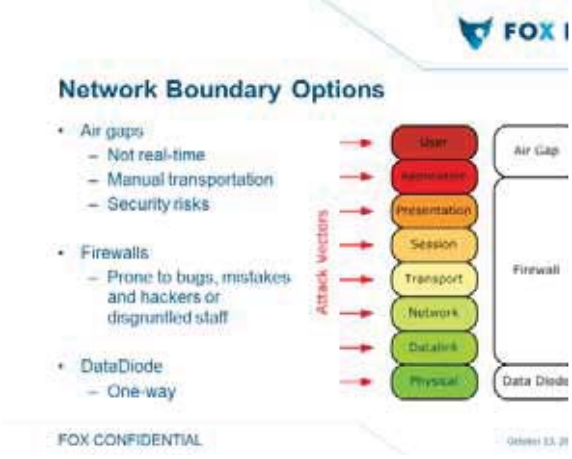
malware sviluppati da "attori di stato", dei quali il più famoso è sicuramente quello conosciuto con il nome di *Stuxnet*. Terroristi ed attivisti hanno incrementato notevolmente il numero di "nazioni nemiche" alle quali minare segreti ed infrastrutture.

Vulnerabilità

Questa nuova tendenza ha generato una grande pressione sulle reti delle diverse Difese nazionali per la protezione dei "segreti" memorizzati in esse. Il disegno delle reti (architettura), le policy di sicurezza (es. la definizione di passwords che rispettino determinate regole), i software di rete ed i protocolli di comunicazione possono risultare particolarmente vulnerabili. Un singolo "punto cieco" in una di queste aree può esporre la rete a possibili infiltrazioni.

Misure

Un modo ben conosciuto per isolare rigorosamente una rete è quello di creare un "air gap". La rete rimarrà isolate e le informazioni potranno entrare o uscire dalla rete stessa solamente tramite l'utilizzo di una chiavetta USB, di un CD-ROM o di un qualsiasi altro "media". Si tratta di un



processo noioso e, molto importante, non sicuro in quanto il malware può comunque entrare nella rete tramite il media e le informazioni possono essere prelevate nello stesso modo.
Un'altra opzione è quella di proteggere la rete tramite firewalls, preferibilmente quelli definiti come "*NGF*", *Next Generation Firewalls*.
Si tratta comunque di "soluzioni IP" che possono essere attaccate, che non possono garantire una operatività sicura (bugs, backdoors) e che sono sensibili ad errori di configurazione, errori amministrativi, intenzionali o di altro tipo.
Ed infine esiste il **DataDiode**, in grado di rendere impossibile fisicamente il traffic in entrato o uscita, ma in modo completamente differente rispetto ad un "air gap."

Solo Hardware

Come il suo elettronico omonimo, un DataDiode è un device che permette il traffico in una sola direzione. I dati possono fluire in una direzione, non nell'altra. Il Fox-IT DataDiode è basato su questo principio. E' un device "solo hardware" senza software, senza componenti programmabili e senza indirizzo IP. Questo fa sì che il DataDiode non possa essere attaccato dall'esterno, rendendolo quindi impermeabile ad attacchi online.

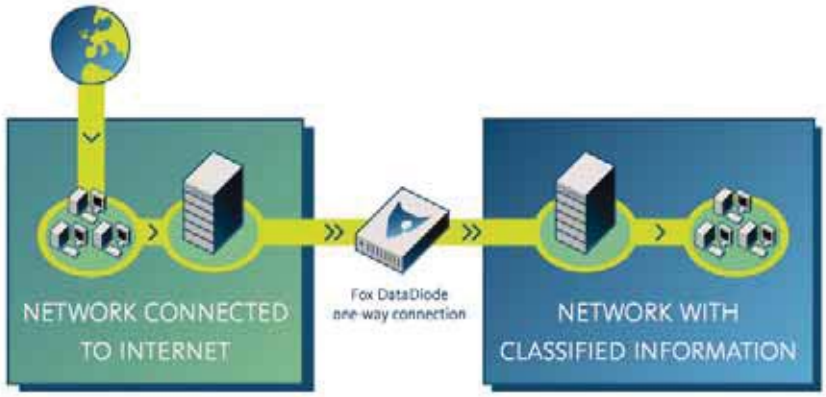
Comunque, il blocco elettronico del flusso dati in una direzione non è sufficiente. Una soluzione solida richiede di più. Molti protocolli sono disegnati per lavorare con un traffico "bi-direzionale" e sarebbero quindi bloccati in una direzione. Se il traffico IP è impossibile in una direzione, non viene gestito il "flow control".

In linea di principio

Un DataDiode può assicurare che il traffico in uscita sia impossibile. Può prevenire perdita di informazioni confidenziali e classificate, ma non ferma il traffico in entrata, che potenzialmente può minare la sicurezza di una rete protetta. Praticamente, il traffico in entrata deve essere prima guidato attraverso una rete dotata di tutte le necessarie misure di sicurezza, dall'antivirus all' IPS ed al SIEM. Quindi, in aggiunta, sono richieste tecniche addizionali come ad esempio la conversion del format (ad es. da Word a PDF), per neutralizzare contenuti potenzialmente dannosi. Le probabilità che ciò accada sono minime, ma è ancora

teoricamente possibile che, nonostante tutte le misure, il malware possa trovare la sua strada in una rete protetta. Detto questo, è di primaria importanza però per evitare che qualsiasi informazione possa lasciare la rete.

Proxy Servers per il Flow Control



I due proxy servers sono usati per il flow control (controllo di flusso): uno posizionato tra il traffico in entrata ed il DataDiode, l'altro tra il DataDiode e la rete protetta. Questo permette che il flusso di dati sia controllato sino al diodo e dal diodo verso la rete. Il passaggio dei dati dal Diodo utilizza un protocollo dedicato, in grado di trasferire dati in modo affidabile senza dover ricevere alcun feedback.
Una lunga serie di test e le esperienze "sul campo" hanno evidenziato la mancanza assoluta di errori in questo tipo di connessione.

Certificazione

Poichè la soluzione completa DataDiode rende impossibile il traffico in uscita, è la miglior garanzia possibile per evitare la perdita di informazioni confidenziali e classificate. Il *Fox DataDiode* ha la più alta certificazione possibile: e' l'unico device al mondo certificato "*CC EAL7+*" ed ha ricevuto certificazioni militari dalle difese olandesi, tedesche, americane, russe ed indiane

Blocco del traffico in entrata

Un DataDiode può essere impostato anche per lavorare nella direzione opposta; in questo caso sarebbe permesso il traffico in uscita e bloccato quello in entrata. Si tratta di una configurazione particolarmente adatta per società ed organizzazioni nei settori dell' *energia*, dell' *oil & gas* e del *nucleare*, settori che richiedono

un’assoluta garanzia che nulla possa essere messo in pericolo da attacchi esterni. Un esempio di traffico in uscita potrebbe essere quello relativo all’invio dei dati di produzione dalle piattaforme petrolifere al quartier generale della società. Ovviamente questa configurazione può essere utilizzata anche in ambiente militare. Prendiamo ad esempio il caso in cui sia necessario impedire influenze esterne dalla rete (impatto su lanci) garantendo però l’invio di dati non segreti verso l’esterno.

Nessuna Gestione, Bassi Costi

Poichè il DataDiode è un device puramente hardware, senza software e chips programmabili, non c’è alcuna necessità per aggiornamenti regolari o di gestione dello stesso. Questo ha un impatto assolutamente positivo sulla sua affidabilità. La riduzione dei costi per la manutenzione e la gestione rende il DataDiode una soluzione particolarmente interessante per garantire la protezione fisica di una rete.

Fox-IT è una Società operante nel settore della Sicurezza Informatica con un’offerta di prodotti e servizi che copre l'intero spettro di sicurezza, prodotti e servizi che vanno dalla prevenzione all’ individuazione ed alla raccolta di informazioni, garantendo tempi di risposta rapidi. Attualmente, in circa 40 paesi del mondo, organizzazioni della difesa e società operanti nei settori delle Infrastrutture Critiche hanno introdotto nei loro sistemi informatici la soluzione DataDiode di FoxIT per garantire la sicurezza delle proprie informazioni classificate da una parte e per proteggere le proprie reti di produzione dall’altra.

Sicurezza Digitale Integrata nel comparto della Difesa

Box : Chi e' Selex ES nella Cyber Security

Selex ES, organizzazione del gruppo Finmeccanica per le tecnologie elettroniche, di telecomunicazione, informatiche, è attiva dal 1947 (Marconi - UK) nell'ambito della sicurezza informativa e crittografia sia per il mondo della Difesa che per il mondo civile.

A Selex ES fa capo il maggiore progetto di cybersecurity mai aggiudicato fuori dai confini degli Stati Uniti: la rete di protezione cyber della NATO, che vede coinvolti 28 paesi. Attraverso i propri Security Operations Centre (SOC) localizzati in Italia e Regno Unito, Selex ES offre ai propri clienti la possibilità di un outsourcing end-to-end per la gestione della sicurezza. I SOC aziendali, attivi 24 ore su 24 365 giorni l'anno, utilizzano una expertise consolidata per offrire il monitoraggio continuo delle infrastrutture, l'immediata individuazione di attacchi e/o minacce ed in generale tutti i servizi necessari a garantire gli obiettivi di sicurezza del Cliente. I SOC erogano i propri servizi in modalità commerciale o secondo lo standard GPG-13(solo nel Regno Unito).

Selex ES, inoltre, ha la responsabilità della progettazione ed esecuzione di attività di protezione dell'amministrazione statale e di aziende private oltre che la realizzazione di servizi di intelligence e di analisi di informazioni da fonti aperte mediante una delle più potenti infrastrutture di supercalcolo dedicate a questo tema in Europa e nel mondo.

La vastissima esperienza di Selex ES nell'affrontare problematiche diverse, dall' Enterprise ICT all'ottimizzazione dei processi, mobilità e gestione dell'energia, sino allo sviluppo completo di sistemi militari e al controllo dei processi della Difesa , consente all'organizzazione di padroneggiare le complesse problematiche legate all'evoluzione tecnologica e quindi di prevenire, individuare e contrastare le minacce cyber più sofisticate e persistenti.

Selex ES ha una consolidata esperienza nell'affrontare le problematiche di sicurezza di ambiti di mercato peculiari quali Difesa, Industria, Air Traffic Management, Telco, Infrastrutture Critiche (CNI) . Selex ES propone servizi personalizzati che includono , tra gli altri, cyber risk management, progettazione , implementazione e certificazione di sistemi sicuri, oltre che consulenze specializzate nell'analisi e prevenzione di attacchi cibernetici sofisticati (Advanced Persistent Threat e nello sviluppo di strategie di mitigazione e disaster recovery.

UN NUOVO CONTESTO

Cosa succede oggi ? Il mondo cambia grazie all'enorme spinta all'evoluzione digitale imposta dalle condizioni economiche, sociali e politiche, dall'aumentata velocità di un mondo sempre più globalizzato e competitivo, dalla massa di nuovi servizi ed incremento della qualità della vita che verranno abilitati.

I nuovi paradigmi tecnologici (Mobile, Cloud, Social Media, Big Data, IoT) hanno avuto un forte impatto sia sui processi interni sia nella gestione delle relazioni con gli stakeholder esterni , aprendo la strada a nuovi modi di lavorare e di interagire delle aziende. Queste condizioni hanno portato a definire un modello di «open organization» molto diverso dai modelli precedenti

- I social media sono, ad esempio, sempre più utilizzati come canali per comunicare e interagire con i clienti (sia in ottica di marketing sia in ottica di user care), ma anche all'interno delle aziende come strumenti di collaboration e social enterprise, per incrementare e migliorare la produttività.
- La crescente diffusione dei dispositivi mobili offre agli utenti interni la possibilità di accedere a dati e applicazioni creando alle organizzazioni l'esigenza di adottare nuove politiche di gestione degli applicativi e delle informazioni

- **L'Internet of Things** è un trend in consolidamento nel comparto **Aerospazio & Difesa (A&D)**

- Molte aziende nell'area A&D stanno facendo evolvere il loro business progettando prodotti e servizi innovativi che sposano il nuovo paradigma IoT.

- L'aggiornamento tecnologico recepisce fenomeni emergenti quali **Big Data, Mobile, Cloud, Analytics**.

- Con l'introduzione dei cosidetti **smart devices**, l'IoT e la comunicazione **machine-to-machine (MtoM)** si stanno estendendo in molte aree in ambito A&D per efficientare i processi produttivi e sviluppare nuovi modelli di business.

- In particolare, la comunicazione machine-to-machine sta imponendo una forte accelerazione alla filiera applicativa dei **Big Data Analytics** in particolare **all'analisi predittiva** basata su tecniche di in-memory computing**.**

DOVE CI TROVIAMO PER LA SECURITY ?

Vediamo da un punto di vista strategico cosa ci dice la relazione dei Servizi per la Sicurezza della Repubblica, che da anni dedica un'attenzione particolare al tema della cyber security.

Dove si è focalizzata l'intelligence ?

- sulle minacce strutturate, persistenti e pervasive gravanti, potenzialmente o di fatto, sulla **sicurezza delle infrastrutture critiche nazionali**;

- sulle attività di spionaggio in ambiente digitale a danno di soggetti, sia pubblici che privati, operanti in settori di rilevanza strategica per la sicurezza nazionale, specie se titolari di **informazioni sensibili ovvero di conoscenze specialistiche** nei settori tecnologico e del *know-how* pregiato;
- sulle campagne e sui singoli attacchi riconducibili al fenomeno **dell'attivismo digitale, condotti contro *target* istituzionali;**
- sull'impiego della Rete per **comunicazione con finalità di propaganda**, disinformazione e controinformazione, proselitismo e **pianificazione** di **azioni terroristiche o criminali**

In particolare i servizi identificano un incremento qualitativo della minaccia, la comparsa dei governi nell'esecuzione di azioni nel cyber spazio e alla luce del delineato trend, è verosimile, per il 2015, il profilarsi di un ulteriore incremento della minaccia, sia per la progressiva sofisticazione delle tecniche di attacco e di penetrazione informatica, sia per lo sfruttamento di un ancora inadeguato livello di sicurezza tecnico-organizzativa e di percezione del rischio, sia, infine, per la continua espansione della "superficie di attacco", anche in ragione della crescente diffusione di applicativi per la telefonia mobile.

Si valuta che gli attori ostili tenderanno a fare sempre più ricorso a tecniche di spear phishing e di ingegneria sociale, come il monitoraggio delle relazioni e delle abitudini di un soggetto sui social media, al fine di comprometterne apparati o servizi di posta elettronica per successive penetrazioni a cascata verso l'organizzazione target cui appartiene o cui risulti, in qualche modo, collegato.

Tale scenario è destinato a risentire anche di livelli talora non adeguati di investimenti nel settore della sicurezza ICT che, impedendo un congruo standard di sicurezza dei processi e dei servizi, fanno venir meno di fatto la prima, necessaria ed auspicabile misura per il contenimento della minaccia.

In questo senso, le attività volte a ridurre la "superficie d'attacco" attraverso un ridimensionamento numerico dei data center pubblici – previsto dalla Strategia italiana per la crescita digitale (2014-2020) elaborata dalla Presidenza del Consiglio dei Ministri – risultano certamente funzionali allo scopo.

Allo stesso tempo, similmente a quanto avviato da altri partner europei, le piccole e medie imprese nazionali potrebbero giovarsi di un ambiente cloud comune e sicuro, quale driver di crescita e protezione del proprio know-how. Da menzionare, infine, i rischi legati alla gestione della supply chain di operatori pubblici e privati, laddove una non adeguata cornice di sicurezza potrebbe esporre i prodotti e la componentistica IT a potenziali manipolazioni nei passaggi dal fornitore all'utente finale.

DOVE CI TROVIAMO PER LA Difesa ?

Il nuovo contesto ha un grande impatto anche sui modelli di sicurezza che le organizzazioni devono implementare, il perimetro si allarga, nuovi canali si aprono, l'ottica diviene quella dello scambio continuo: le organizzazioni devono passare da un modello di protezione del business ad un modello di abilitazione del business, attraverso l'implementazione di strategie innovative di sicurezza.

Il tradizionale approccio alla sicurezza IT, associato prevalentemente al concetto di protezione delle attività, risulta insoddisfacente soprattutto per le organizzazioni e gli enti che hanno sempre più la necessità di operare in maniera aperta e sui canali digitali.

Ne deriva la necessità di rivedere i modelli attuali, in modo tale che questi non rappresentino un elemento di rigidità o un ostacolo nello sviluppo di business innovativi basati su una maggiore apertura dell'organizzazione verso l'esterno. Il concetto di sicurezza si deve ampliare per divenire un fattore "abilitatore" della crescita dell'ente.

Un nuovo approccio – associato ai giusti strumenti di gestione – permette infatti di avere degli impatti positivi su tutte le attività dell'organizzazione: ottimizzazione dei processi interni, aumento delle registrazioni ai propri servizi on line, migliore profilazione dei propri clienti, possibilità di implementare migliori processi di user retention e user loyalty associati ad una migliore user experience.

E' in quest'ottica ad esempio che L'Agenzia NCI ha definito un ambizioso **programma per modernizzare** nei prossimi cinque anni l'infrastruttura IT della NATO.

Il tender è originato dall'esigenza dei Comandi NATO di disporre di **soluzioni ICT resilienti** in tutte le sedi distribuite in grado di soddisfare le esigenze di business e nel contempo garantire la continuità del servizio per mezzo di un'**infrastruttura IT più efficace, più sicura e meno costosa** di quella esistente.

Costituisce di fatto il primo passo della NATO nel percorso evolutivo verso la tecnologia "**Cloud Computing**", attraverso la fornitura di una piattaforma di **private cloud** "on premise" per l'erogazione di servizi infrastrutturali (IaaS)

Sempre in quest'ottica va letto uno dei tre pilastri del più vasto **programma Forza NEC (Network Enabled Capability),** che si inserisce nel quadro della **Network Centric Warfare (NCW**): La **digitalizzazione dello spazio di manovra** e **la superiorità nella raccolta, gestione e disseminazione delle informazioni** diventa un vantaggio tattico-strategico.

- Questo risultato viene ottenuto combinando in maniera innovativa gli ultimi ritrovati tecnologici negli ambiti ISR, C4I e del munizionamento di precisione.
- Questo permette di "mettere in rete" piattaforme ed operatori, in modo che ogni singolo elemento sul campo di battaglia, sia esso uomo o macchina, agisca contemporaneamente da collettore, disseminatore ed utilizzatore finale di informazioni tatticamente e strategicamente rilevanti, su posizione e capacità sia delle forze nemiche che di quelle amiche.

CHE SI PUO FARE ?

La domanda sorge spontanea. Quali sono le operazioni da svolgere per migliorare e rendere più efficienti i nostri sistemi di Difesa dalla dimensione cyber?

Negli ultimi due anni in Italia il Presidente del Consiglio dei Ministri ha autorizzato la pubblicazione dei documenti strategici nazionali in materia di cyber-security.

Il primo è il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", ovvero la strategia vera e propria.

Il Quadro è la parte di più alto livello e ha come scopo, pertanto, quello di delineare le linee strategiche nazionali nel medio-lungo periodo. E' deputato, infatti, a contenere l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, e di quelli nazionali operanti al di fuori del territorio del Paese, nonché l'individuazione degli strumenti e delle procedure con cui perseguire l'accrescimento della capacità del Paese di prevenzione e risposta rispetto ad eventi nello spazio cibernetico, anche in un'ottica di diffusione della cultura della sicurezza.

Sei sono i pilastri strategici sui quali il governo italiano ha impostato la strategia.

Inoltre, per il raggiungimento di questi sei indirizzi strategici, sono stati coerentemente identificati undici indirizzi operativi all´interno del Quadro. Questi - come ci si aspetterebbe - spaziano da specifiche focalizzazioni su aspetti meramente tecnici e tecnologici, passando per l´incremento delle capacità di early warning e di incident response, fino alla imprescindibile cooperazione interna ed internazionale.

La seconda parte della strategia italiana per il cyber-spazio invece è relativa al "Piano nazionale per la protezione cibernetica e la sicurezza informatica", che rappresenta il documento operativo di breve periodo (2014-2015) volto ad individuare gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare quanto contenuto nel Quadro strategico nazionale.

Undici sono i punti operativi messi in piedi dal Piano:

1. Potenziamento delle capacità di intelligence, di Polizia e di Difesa civile e militare.

2. Potenziamento dell´organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati.

3. Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento.

4. Cooperazione internazionale ed esercitazioni.

5. Operatività del CERT nazionale, del CERT-Difesa e dei CERT dicasteri.

6. Interventi legislativi e compliance con obblighi internazionali.

7. Compliance a standard e protocolli di sicurezza.

8. Supporto allo sviluppo industriale e tecnologico.

9. Comunicazione strategica.

10. Risorse.

11. Implementazione di un sistema di information risk management nazionale.

La valutazione dei documenti strategici appena pubblicati è certamente positiva. La strategia italiana, infatti, si innesta perfettamente nel quadro delineato a livello internazionale dagli altri Stati sovrani, abbracciando in toto quei principi strategici comuni imprescindibili per un corretto approccio alla minaccia (per il cui approfondimento si rimanda a "I principi strategici delle politiche di cyber-security").

Bisogna seguirli ed implementarli nella pratica.

E' fondamentale che le iniziative e le progettualità digitali della Difesa "nascano sicure", ovvero che la cybersecurity e la resilienza dei sistemi siano previste sin dalla fase di progettazione e siano parte integrante del processo di realizzazione ed implementazione. E' altrettanto fondamentale, poi, che le strutture organizzative i processi ed i servizi di supporto alla sicurezza siano studiati e realizzati contestualmente, per mettere a disposizione dei cittadini e delle organizzazioni della Difesa piattaforme sicure e controllate, che possano veramente assolvere al ruolo di strumenti di sviluppo del paese, innovativi ed allineati a quelle che sono le tendenze di sviluppo tecnologiche che sempre più fanno parte delle nostra vita di ogni giorno. Questo si riflette, a livello Paese, in molteplici progettualità dalle iniziative Agid, allo SPID, a SPC sino all'ingresso di paradigmi come il Cloud nel mondo Difesa.

Il tema della digital security diviene quindi centrale: in questo mondo i servizi della Difesa sono digitalizzati per garantire efficienza ed efficacia all'azione amministrativa oltre che inclusione sociale ed una migliore relazione tra i cittadini, le imprese e le istituzioni. In questo mondo l'efficienza del sistema sociale, istituzionale ed economico diviene a tutti gli effetti una parte integrante del perimetro strategico del paese.

L'industria cosa può fare? Molto:

- Può realizzare servizi digitali di qualità, in termini di correttezza, rapidità ed usabilità
- Può collaborare con la Difesa per evidenziare le opportunità in termini di standard, di interoperabilità, di evoluzione
- Può realizzare le reti necessarie ai nuovi servizi
- Può aiutare la Difesa a creare servizi semplici ed usabili anche in condizioni di bassa abitudine o di limitate competenze
- Può curare la sicurezza di quanto realizza
- Può collaborare con la Difesa per sviluppare e diffondere best practice e cultura
- Può dare tramite i servizi di cybersecurity erogati alla Difesa la garanzia di protezione ed integrità delle applicazioni e delle informazioni

CONCLUSIONI

Selex ES vede quindi un'evoluzione rapida dello scenario strategico della digital security per la Difesa ed ha preparato una strategia basata su risposte su molteplici livelli:

- Governance : Una continua partecipazione alla definizione degli obiettivi e dei framework di digitalizzazione e sicurezza. Lo sviluppo di capacità e metodologie a supporto del moderno modello di cyber security che include mobilità cloud e impianti industriali
- Awareness : una rinnovata attenzione al tema dello scambio delle informazioni ed alla costruzione di servizi e capacità condivise sia in termini di Cyber Security che di ICT . La capacità di supportare i propri clienti attraverso training a cyber ranges
- Technology : Un'evoluzione dell'offerta di sicurezza cyber dalla protezione di perimetro a più sofisticati meccanismi basati sull'intelligenza artificiale, i big data, l'analisi comportamentale ed i metodi probabilistici
- Trust : Un'aumentata responsabilità delle aziende strategiche a supporto dei programmi di modernizzazione della Difesa , con un sempre maggiore ruolo da protagonista nelle iniziative più critiche come SPC
- Innovation : un incremento delle capacità e dei servizi offerti in termini di Supporto alle indagini, Big Data, Open Source Intelligence, Content Analysis a supporto delle rinnovate esigenze di proattività del comparto. Investimenti in prodotti e sviluppi tailorizzati sui bisogni del cliente.

Serve quindi una sensibilità particolare ed un cambio di paradigma per supportare al meglio questa delicata fase evolutiva. Un approccio metodologico che tenga conto di quanto ripoprtato, un investimento consistente in tecnologie e processi di cambiamento. Servono partner come Selex ES, che siano in grado di assicurare contemporaneamente l'innovazione e la sicurezza necessaria ad abilitarla e preservarla. In questo senso il ruolo delle aziende high-tech, e particolarmente di quelle del settore della Difesa e Sicurezza, riveste un ruolo fondamentale a supporto della capacità nazionale di definire un approccio, individuare strumenti ed implementare soluzioni e servizi per gestire i rischi.

La sindrome di Troia ed il modello di CERT 2.0
Il rischio dell'eccessiva confidenza nelle soluzioni standard e nuovi modelli per la cyber-defense.

Al giorno d'oggi la sicurezza informatica pone una serie di sfide a tutte le organizzazioni che devono necessariamente tutelare le proprie infrastrutture digitali.
Il rischio concreto è che, specialmente le realtà più avanzate, possano adagiarsi su una falsa sensazione di inviolabilità che deriva dall'implementazione di procedure standard e strumenti convenzionali per la difesa del perimetro.

Nella quasi totalità dei casi, questi accorgimenti risultano tuttavia inadatti e non sufficienti a garantire una protezione completa, specialmente di fronte a minacce mirate ed innovative che rompono gli schemi sino a quel momento conosciuti. Volendo trovare un'analogia storica con questo falso mito di sicurezza, basta tornare alla leggendaria caduta di Troia.

La città considerata inespugnabile e già capace di resistere ad anni di assedio da parte degli eserciti greci, fu infatti costretta a capitolare in seguito ad un'intuizione di Ulisse. L'utilizzo del celebre cavallo di legno rappresentò per i troiani un'incognita davanti alla quale abbassarono la guardia e crearono loro malgrado i presupposti per la disfatta. Come spesso accade nel panorama digitale, la minaccia è stata infatti portata all'interno del perimetro dagli stessi difensori, ignari del fatto che nascondesse una grave insidia. Non a caso una delle principali categorie di software malevoli prende il nome di Trojan Horse, uno strumento utilizzato dai cyber-criminali per far breccia all'interno dei sistemi target, presentato alle vittime come un file legittimo, necessario ed inoffensivo. In questo senso il trojan agisce proprio come il celebre cavallo di Ulisse, facendo forza, da una parte sulla fiducia e l'inconsapevolezza della vittima, dall'altra sulla conoscenza delle difese standard e convenzionali adottate.

Le compromissioni digitali frutto di attività mirate, condotte nell'ambito di specifiche operazioni criminali, comportano per le organizzazioni colpite una serie di ripercussioni più o meno debilitanti che possono esporle a danni economici, d'immagine, disservizi, sottrazione e/o pubblicazione di informazioni sensibili e confidenziali e, in alcuni casi, persino alla cessazione delle attività.

Per portare un esempio, nei mesi scorsi ha destato senz'altro scalpore il caso Sony, poi ribattezzato Sony Hack. In particolare un collettivo di pirati informatici conosciuto come "Guardians Of Peace" (GOP) è riuscito ad intrudere la rete della divisione Pictures Entertainment del colosso giapponese, mettendo progressivamente le mani sull'intero network aziendale. Inizialmente e con troppa fretta attribuito ad individui nordcoreani vicini al Governo di Pyongyang, presumibilmente offesi dal film "The Interview" prodotto dalla stessa Sony, l'episodio è stato poi collegato ad un team di criminali russi, quasi certamente mossi da fini economici. Nel caso specifico, l'operazione è stata possibile grazie

ad una minuziosa e capillare attività di compromissione di singoli dipendenti in India, Russia ed altri paesi asiatici, adescati con la tecnica dello spear-phishing con l'obiettivo di fargli installare inconsapevolmente dei RAT (Remote Administration Tool) nelle macchine della società. Anche in questo caso quindi il pericolo è stato portato all'interno del perimetro dalle stesse vittime, sicuramente colpevoli di eccessiva leggerezza ma anche poco aiutate dagli strumenti di rilevazione standard adottate nell'organizzazione.

L'aspetto sul quale è doveroso porre l'attenzione è senza dubbio quello della prevenzione e della consapevolezza circa l'evoluzione del panorama cyber-criminale e delle minacce emergenti. Gli stessi Computer Emergency Response Team (CERT), per come li conosciamo oggi, basano il proprio fondamento sulla risposta immediata a minacce digitali che vengono scovate all'interno delle infrastrutture dell'organizzazione o su sistemi perimetrali della stessa. Un'impostazione di questo tipo presenta inevitabilmente delle criticità che finiscono con l'impattare sulle realtà colpite. I dati dimostrano come l'approccio descritto sia quasi sufficiente per identificare ed in seguito bloccare attacchi digitali conosciuti e considerati "standard" ma al contrario del tutto inadeguato alla detection di offensive mirate alle organizzazioni o al proprio personale.

L'obiettivo da perseguire è quello di un'integrazione all'attuale schema operativo dei CERT, ancora fermo ai tre step di Detection, Analysis e Response.

Il modello ideale è quello di un Computer Emergency Response Team 2.0, più efficace, che estenda le proprie funzioni con attività di Cyber Defense intelligenti. L'approccio deve basarsi sulla convinzione che per identificare e bloccare in tempi opportuni una minaccia sia necessario applicare strumenti e soluzioni capaci di fornire forecast delle possibili insidie e dettagli circa gli autori delle azioni, i loro cyber armamenti e le strategie di attacco.

A questo scopo diventa indispensabile uno schema incentrato sul concetto di "prevenzione" che integri il discovery ed il tracciamento delle minacce digitali e metta in condizione gli analisti e le organizzazioni di avere, in anticipo rispetto agli eventi, un quadro informativo completo per essere preparati alle possibili conseguenze delle minacce emergenti. Ai tre step sopra citati dovranno quindi aggiungersi quelli di Threat Discovery, Preventive Defense Activity e Monitor Activity.

Tali attività dovranno essere in grado di approfondire ed informare i possibili target a 360 gradi anche per quanto concerne i diversi ambiti di business o di interesse in cui operano e le altre realtà attive negli stessi settori. Avere questo tipo di informazioni risulterà decisivo sia in termini di prevenzione che per una tempestiva reaction volta a limitare considerevolmente le ripercussioni degli attacchi.