In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

La Web-based Intelligence nei modelli adattativi di sicurezza e gli aspetti multidisciplinari di attivazione ed analisi

Giampiero Bonfiglio, Ludovica Coletta, Alessandra Teresa Coscarella, Martina Limonta, Panfilo Ventresca

Business Integration Partners s.p.a.
giampiero.bonfiglio@mail-bip.com; ludovica.coletta@mail-bip.com; alessandrateresa.coscarella@mail-bip.com; martina.limonta@mail-bip.com; panfilo.ventresca@mail-bip.com

Abstract

L'ascesa del cyberspazio come centro delle realtà sociali, politiche, economiche e culturali (SPEC) ha evidenziato una perdita di efficacia nell'approccio tradizionale di Sicurezza a favore di un nuovo modello di Adaptive Cyber Security capace di riconoscere e adattarsi all'evolversi delle minacce del cyberspazio.

La Web-based Intelligence rappresenta lo strumento abilitante per l'Adaptive Cyber Security, attraverso il monitoraggio e l'analisi del canale web in tutte le suedimensioni (open, deep web, dark web).

La stretta relazione tra la realtà SPEC e le azioni nel cyberspazio richiede quindi che la stessa Web-based Intelligence si muova secondo un approccio multidisciplinare che integri la componente tecnologica di rilevazione, l'analisi comportamentale degli attacchi e quella socio-politica del contesto di azione.

Tale approccio si caratterizza per una maggiore efficacia nella correlazione e interpretazione degli eventi, consentendo il riconoscimento di vere e proprie modalità di azione e la rilevazione dei motivi scatenanti l'esecuzione di attacchi, a favore di un modello di sicurezza che si adatta alla continua evoluzione del cyberspazio.

1 Introduzione

La "Digital Transformation" sta riscrivendo i modelli di business e di governo attraverso una digitalizzazione che rivoluziona la sfera pubblica e privata delle nostre vite, rendendo il cyberspazio il centro delle realtà sociali, politiche, economiche e culturali (SPEC).

Da un'accurata analisi di tale fenomeno emerge una dipendenza sempre maggiore dal cyberspazio da parte dei principali contesti produttivi e decisionali, dei sistemi aziendali e finanziari, delle infrastrutture critiche e persino dei sistemi elettorali e politici.

Negli ultimi anni l'equilibrio di tali sistemi è stato minato da un incremento senza precedenti degli attacchi informatici perpetrati nel cyberspazio e veicolati da motivazioni che spaziano da vantaggi economici e competitivi fino a ragioni di natura sociale, con ingenti impatti sulla solidità delle più grandi realtà istituzionali e industriali.

Tale evoluzione è strettamente connessa alla rivoluzione digitale che ha determinato un incremento nella disponibilità di strumenti sempre più complessi e potenti, ad uso del vasto pubblico, benevolo e non.

L'evoluzione delle minacce può essere analizzata secondo un andamento a fasi: dagli anni '70/80, con i primi attacchi di hacker individuali mossi da curiosità tecnica, agli anni '90 in cui gruppi organizzati hanno iniziato a veicolare virus e worm con l'intento di manomettere sistemi e alterare siti web (il cosiddetto *Defacement*). Nei primi anni del 2000, si è verificata una sempre crescente organizzazione dei gruppi criminali attivi nel cyberspazio, complici i maggiori ritorni economici a basso rischio derivanti, ad esempio, dalla possibilità di anonimato reso possibile dal web.

Sono nate e continuano a nascere realtà criminali fortemente organizzate, sia a livello nazionale sia internazionale, caratterizzate dal ricorso a sistemi di attacco complessi e strategici, quali gli "Advanced Persistent Threats" (APT) [1], per scopi governativi (es. attacchi DDoS[2] su obiettivi nazionali come la Georgia ed Estonia) o aziendali (campagna di attacchi "Aurora" diretti a Google).

Una nuova fase di attacchi è appena iniziata. Si tratta di azioni estremamente complesse e sovranazionali che mirano al furto di dati direttamente da realtà multinazionali, come ad esempio le azioni intraprese su Google[3], Ebay[4] e Yahoo[5] negli ultimi anni.

Il Cyber attacco su larga scala, inoltre, ha oramai assunto una connotazione di minaccia internazionale e a forte impatto sull'economia mondiale, nonché sugli equilibri socio-economici, al pari degli attacchi terroristici, delle crisi finanziarie o della disoccupazione.

Fronteggiare il Cybercrime rappresenta una sfida sempre più complessa a causa del numero di realtà coinvolte, di architetture decentralizzate e transnazionalità della rete. È dunque sempre più evidente come l'approccio "statico" della Information Security mostri i suoi limiti nell'assicurare un adeguato livello di protezione, a favore invece di un modello adattativo, l'Adaptive Cyber Security Model, in grado di adeguare il livello di protezione rispetto all'eterogeneità di eventi e alla variabilità/volubilità delle minacce.

La capacità di adattamento fonda la sua efficacia sull'attività di Intelligence, diretta al reperimento di informazioni su eventi, minacce e attacchi. Questo avviene su canali tradizionali e oramai in maniera massiva sul cyberspazio, dove è emerso il ruolo cruciale della Web-based Intelligence come centro del monitoraggio e identificazione delle informazioni rilevanti e dei potenziali eventi malevoli da cui proteggersi.

Operando nel cyberspazio, la Web-based Intelligence ne eredita caratteristiche e interconnessioni, analizzando gli eventi (IT e non) secondo un approccio multidisciplinare che integra l'ambito politico, economico e sociale per riuscire a interpretare e contestualizzare le informazioni in modo appropriato.

[1] Advanced Persistent Threat (APT), processo di attacco basato su tecniche di hacking utilizzate su base furtiva e continua mirato alla raccolta di informazioni in maniera indebita da una realtà target

[2] Distributed Denial of Service (DDoS), attacco in cui una moltitudine di sistemi compromessi vengono utilizzati per rendere indisponibile un singolo sistema target verso i suoi utenti

[3] Attacco Aurora, operazione di attacchi cyber del 2009 condotti attraverso tecniche APT da gruppi basati in Cina verso multi-nazionali americane come Google, Adobe, Juniper, Rackspace. U.S.-China Economic and Security Review Commission, *2010 Report to Congress*

[4] Furto di informazioni ai danni di Ebay nel 2014, compromesso database con i dati dei clienti, impattati 145 milioni di utenti http://blog.trendmicro.com/trendlabs-security-intelligence/ebay-latest-victim-of-massive-data-breach/

[5] Furto di informazioni ai danni di Yahoo nel 2014, evento segnalato nel 2016 con impatto su 500 milioni di utenti della piattaforma internet. https://help.yahoo.com/kb/account/SLN27925.html

2 Adaptive Cyber Security Model

L'Adaptive Cyber Security Model va oltre la tradizionale architettura di sicurezza basata sul principio di definizione di un perimetro di difesa statico, non più sufficiente a fronteggiare i continui stimoli e le sfide sempre nuove provenienti dal cyberspazio. La peculiarità del modello risiede nella sua capacità di adeguare il perimetro e le misure di sicurezza in maniera puntuale e continuativa rispetto al contesto attraverso una combinazione di tecnologie e processi che consentano di far fronte a tale dinamicità.

Questo nuovo paradigma di sicurezza si compone sia della parte più canonica di protezione degli asset, sia di quella più avanguardista di analisi di intelligence e contestuale per il monitoraggio real-time dei rischi.

Proprio gli standard di sicurezza ISO/IEC 27004, ISO/IEC 27032 e il NIST SP 800-55 e i framework di Cyber security sia di carattere nazionale (Framework Nazionale per la Cyber Security-CIS) che internazionale (Framework for Improving Critical Infrastructure Cyber Security-NIST), sottolineano la necessità per le organizzazioni di avere una piena comprensione del proprio ambiente operativo e dei possibili rischi di sicurezza da fronteggiare.

L'Adaptive Cyber Security Model, pertanto, fa propri questi concetti e va oltre un modello di sicurezza tipicamente reattivo nei confronti delle minacce che si presentano ed è, invece, orientato verso un'azione proattiva in cui il costante monitoraggio del contesto alimenta le attività di rilevazione e di prevenzione.

Il modello prevede dunque specifiche azioni dirette all'analisi delle informazioni e all'adozione delle contromisure di sicurezza appropriate, vedi CERT e SOC, i quali risultano evoluti secondo logiche proattive al fine di agire prima che un evento malevolo si verifichi. Funzioni distintive in tale nuova architettura di sicurezza sono, ad esempio, quelle di Intelligence tra cui: Early Warning and Security Intelligence, Feed and Reputation, Industry Threats Reporting, Countermeasures Efficacy evaluation, Threats Categorisation and Monitoring; altre legate alla Security Analysis come l'Ethical Hacking e la Source Code Review; e altre ancora più di natura tecnica come il Vulnerability Assessment (VA) e il Penetration Test (PT).

In considerazione proprio della moltitudine di funzioni e sorgenti, va ricordata l'importanza dell'Information Sharing per assicurare una base di informazioni quanto più consistente e uniforme.

Al fine di intervenire preventivamente a difesa degli asset aziendali e realizzare adeguate contromisure di sicurezza, il modello adattativo si basa sulla raccolta e analisi di dati e informazioni provenienti da diverse fonti. Oltre alle più tradizionali (es. bug reports dei vendor, nuove vulnerabilità tecniche, risultati dei VA), la Cyber Intelligence ha assunto recentemente particolare rilevanza. La consapevolezza della realtà mutevole e l'esigenza del costante adattamento alla stessa fa sì che il modello necessiti di un'attenzione particolare al Web, sia aperto che sommerso, in quanto fonte dal contenuto informativo più ricco. Il web è, infatti, oramai largamente utilizzato come canale principale di comunicazione e al tempo stesso come luogo di incontro e collaborazione per scopi leciti e non leciti.

3 La Web-based intelligence

L'intelligence è ben rappresentabile dall'unione tra "information" e "analysis"[6], per cui si configura come "actionable knowledge". È' un processo e un prodotto dell'analisi informativa che consente di dedurre dagli elementi, dai fatti e dagli aspetti del tempo presente, ciò che avverrà in quello futuro. In tal senso, la Web-based intelligence si configura come intelligence che utilizza il web come ambiente nel quale rinvenire le informazioni e come strumento sul quale effettuare il

[6] M.E. Bonfanti, A.P. Rabera, Internet-based Intelligence: Prediction or Foreknowledge? in E. Mordini, M. Green, Internet-based Intelligence in Public health emergencies; p.11;

processo di analisi, per mezzo di strumenti più o meno complessi dal punto di vista tecnologico[7]. Le molteplici definizioni disponibili in letteratura ne evidenziano, inoltre, il fattore caratterizzante della multidisciplinarietà. Proprio questo suo sviluppo su una moltitudine di piani tematici, può essere una delle ulteriori chiavi interpretative con cui è possibile definirla come nuova forma di intelligence che si sviluppa utilizzando il web come canale e strumento abilitante per le attività di analisi e investigazione[8].

La Web-based Intelligence si focalizza sul web, aperto e sommerso, per raccogliere informazioni attraverso metolodologie e tecniche a volte specifiche per l'OSINT, il Deep Web e il Dark Web.

Il suo obiettivo consiste nel facilitare il riconoscimento preventivo di eventuali attacchi cyber, individuando *ex-ante* comportamenti e/o azioni preparatorie all'attacco.

Rispetto alle altre tecniche esistenti dirette a una pura analisi del traffico e delle attività malevole, il modello di Web-based Intelligence è arricchito da tecnologie avanzate e paradigmi propri della ricerca investigativa, molecolare e multicanale, nonché fortemente guidata da logiche preventive e predittive.

Le tecniche di ricerca, analisi e contestualizzazione proprie della Web-based Intelligence, sono affinate con l'obiettivo di tenere in piena considerazione gli aspetti non esclusivamente tecnologici, ma anche economici, geopolitici, giuridici, socio-comportamentali e criminologici legati a un particolare evento. Questo nella piena consapevolezza che un attacco informatico a un'organizzazione potrebbe costituire un danno esteso all'intero sistema paese qualora colpisse, ad esempio, le sue infrastrutture critiche.

L'analisi secondo tali direttrici permette dunque di contestualizzare opportunamente eventi e azioni malevole, in modo da identificare mandanti, motivazioni e obiettivi.

3.1 Il patrimonio informativo del Web

Se la Web-based Intelligence può essere considerata come la fonte più ricca di contenuti per il modello proattivo di Cyber security precedentemente descritto, questa a sua volta in quanto prodotto di un'analisi, attinge a un vasto patrimonio informativo/umano presente sul Web. Questo è costituito da fonti indicizzate e fonti informative desumibili dal Deep Web e dal Dark Web.

Per ciò che concerne le fonti indicizzate (Open) rinvenibili sul web, queste sono caratterizzate da ampia accessibilità e disponibilità, ma non sempre da autenticità. Non è, infatti, universalmente possibile verificare la veridicità della notizia e della sua fonte. Di conseguenza per le fonti Open è necessario il procedimento di analisi che porta alla validazione dell'informazione stessa e all'elaborazione del prodotto finito. Le informazioni e i dati desumibili, invece dal Deep Web e dal Dark Web si differenziano da quelle Open in quanto non presentano immediata disponibilità. Il rinvenimento di tali informazioni, infatti, prevede un passaggio investigativo aggiuntivo, mediante l'inserimento e l'omologazione dell'utente in questi particolari contesti governati da regole culturali, in alcuni casi, linguistiche, proprie. Gli attori che agiscono nel Deep Web e nel Dark Web sono, infatti, soggetti a un riconoscimento reciproco che è anche il fattore inclusivo nell'ambiente stesso. La reperibilità delle informazioni dipende, pertanto, da questo accesso soggetto a limitazioni. Oltre a tale difficoltà di accesso, resta appropriato il ragionamento circa la veridicità delle informazioni desumbili da tali fonti. Il contesto socio-culturale che circonda gli ambienti del Deep e del Dark Web fa sì che le fonti non indicizzate si caratterizzino per una veridicità ancora meno certa delle fonti "open". Ciò è dato dal peculiare popolamento di tali ambienti da parte di attori con interessi leciti e non, i quali, di conseguenza, possono avere interessi propri nella diffusione di informazioni false e/o nella disinformazione.

[7] Ibidem;

[8] Ivi, cit. p. 13, "The Laplacian model gains additional support from the (relatively) recent ascent to prominence of "Internet-based Intelligence". For present purposes, we may characterize Internet-based Intelligence as what is produced when information (data and metadata)is sourced from the Internet and analyzed for actionable insight via manual - but more often and more powerfully (at least in terms of processing capacity) automated means."

Una componente essenziale sia delle sorgenti Open sia delle informazioni desumibili da Deep Web e dal Dark Web, consiste nell'intervento umano con cui verranno selezionati i filtri più appropriati per procedere con l'analisi e la validazione delle suddette informazioni. C'è da considerare anche la complessità degli strumenti a supporto della raccolta e dell'analisi delle tre principali aree del Web (Open, Deep, Dark), abilitati da tecnologie spesso eterogenee ma sempre caratterizzate da motori (statistici, semantici, ontologici e di tipo machine learning) che devono essere configurati anche con competenze di natura non solo tecnica, bensì multidisciplinare (es. conoscenza linguistica, ontologica etc).

3.2 Un processo multidisciplinare di analisi delle informazioni

Molte delle tecniche di Web-based Intelligence adottate finora si focalizzano su una pura analisi del traffico e delle attività malevole, attraverso raccolta di informazioni ad ampio spettro, indirizzata a un puro supporto per una successiva azione di sicurezza di tipo reattivo che tuttavia può risultare insufficiente nel reagire agli attacchi odierni spesso ad alto spettro e intensità (come, ad esempio, il DDoS).

L'esigenza attuale è che questo approccio venga arricchito, secondo un'ottica multidisciplinare, da un livello di interpretazione delle informazioni e di loro correlazione secondo una nuova dimensione socio-criminologica, politica, economica e culturale, per permettere l'identificazione e il riconoscimento di strategie di attacco complesse, nonché di vere e proprie operazioni di e-crime.

La dimensione socio-criminologica e psicologica è utile a tracciare il profilo dell'attaccante, il suo modus operandi e la sua fingerprint. Mediante questa attività di interpretazione, condotta con dinamiche proprie dell'analisi comportamentale, è possibile inquadrare varie tipologie di attaccanti e di attacchi per categorizzarli, semplificando di conseguenza la capacità di risposta alle tipologie individuate.

La contestualizzazione secondo la dimensione politico-economica di riferimento è utile per poter inquadrare quanto raccolto in precedenza e ottenere una sintesi del contesto e delle motivazioni per cui determinati attacchi informatici nascono e vengono perpetrati. Ad esempio, un cyber criminale potrebbe sferrare un attacco verso un'infrastruttura critica di un paese, in occasione di un importante negoziato su tematiche globali, al fine di destabilizzarlo e far prevalere propri interessi. La contestualizzazione delle informazioni tecniche e comportamentali su un attacco cyber con quelle relative a un particolare scenario di riferimento, è dunque fondamentale per poter associare degli elementi comuni e ricercare dei collegamenti.

Le informazioni raccolte sono di tipo strutturato e non strutturato in base al livello di organizzazione e pertanto seguono un iter di processamento basato su logiche differenti.

Nel primo caso, sono caratterizzate da un alto grado di organizzazione e derivano dalle sorgenti dati che forniscono flussi continui di informazioni e che è possibile utilizzare con un minimo effort di standardizzazione.

Nel caso di informazioni non strutturate, al contrario, non è possibile identificare modelli dati specifici, in quanto queste provengono invece dalla raccolta da sorgenti come articoli, report tecnici, forum, blog e social media. La raccolta e conseguente analisi di tali informazioni risulta un'attività ad alta complessità, in relazione all'eterogeneità dei contenuti (es. riconoscimento linguistico) e del contesto; per tale motivo vengono utilizzate tecniche specifiche per il contesto e perimetro analizzato, quali la social media analytics, text mining, sentiment analysis e geospatial analysis.

Le informazioni nella loro complessità vengono quindi parametrizzate e filtrate secondo logiche fuzzy per confluire in una base di conoscenza caratterizzata da strutture di dati comuni e interpretabili automaticamente che è possibile correlare per riconoscere, ad esempio, legami temporali, logici, e/o di causa/effetto.

Qui si inserisce l'utilizzo di tecniche di machine learning basate su logiche semantiche, statistiche e ontologiche con l'obiettivo di integrare e combinare le informazioni sugli eventi con quelle di contesto, derivanti dalla componente geo-politica, economica, sociale e culturale.

Il modello confluisce in un sistema di near-real time analytics, dedicato all'identificazione delle minacce di sicurezza che immagazzina i dati rilevanti di contesto, di eventi e attacchi, per compararli con serie storiche attraverso tecniche di big data analysis.

La Web-based Intelligence permette, quindi, di comprendere la motivazione e la natura degli attacchi, le evoluzioni e i fattori che influenzano la loro emersione, con l'obiettivo di sviluppare strategie di difesa efficienti rispetto ai vari tipi di minacce che affiorano. Per tali ragioni, la Web Based Intelligence costituisce la componente più ricca di informazioni per l'attuazione di un modello adattativo efficace.

La necessità di sfruttare al meglio le informazioni contenute in ciascun canale di analisi (tecnologico, comportamentale o geopolitico), richiama l'approccio multidisciplinare nella forma di una specifica conoscenza del singolo ambito, nonché degli strumenti e delle metodologie per analizzare, interpretare e contestualizzare.

Pertanto, è necessario dotarsi competenze specifiche di settore che siano in grado di aggiungere il fattore esperienziale al fine di coglierne gli aspetti rilevanti per l'organizzazione.

Il bagaglio di conoscenze e competenze per approcciare a ciascun ambito differiscono dunque necessariamente tra loro: ne deriva che per un'applicazione efficace del modello adattativo con componenti di Web-based Intelligence, è necessario dotarsi di competenze e skill eterogenei, multidisciplinari e non esclusivamente tecnici.

L'approccio multidisciplinare e multidimensionale permette quindi di ottenere un'informazione quanto più possibile completa, in grado di tenere conto delle variabili endogene ed esogene che ruotano attorno a un attacco informatico.

L'attuazione della Web-based Intelligence combinata con un modello adattativo all'interno di un'organizzazione consente di avere un quadro quanto più esteso di una possibile minaccia cyber, con l'obiettivo di sviluppare strategie preventive di difesa, efficaci rispetto ai vari tipi di minacce che affiorano. Di seguito viene discusso un focus su due filtri applicabili al processo di analisi, effettuabile a partire dal patrimonio informativo Web di cui sopra:

- Focus sull'analisi di tipo comportamentale;
- Focus sull'analisi di tipo geopolitico.

3.3 Focus sull'analisi di tipo comportamentale

Le fonti informative su citate acquisiscono particolare valore per la rilevazione, l'analisi, il confronto ed il riconoscimento di variabili socio-comportamentali riferibili ai cyber criminali poiché dall'altro lato dei devices, quali vettori di attacco, si nasconde un essere umano, con la tendenza innata a personalizzare l'ambiente con cui interagisce, e a lasciare, anche inconsciamente, tracce digitali distintive ed associabili alla propria identità "virtuale",

Di conseguenza l'approccio ed i principi della tecnica investigativa del "*Psychological Profiling*"[9], integrati con le logiche dell'Informatica Forense, consentono di elaborare specifici profili e modelli comportamentali, quali punti di partenza per la riconduzione dell'identità digitale dell'offender alla sua identità reale.

Il "*Digital Profiling*" rappresenta dunque l'applicazione, al contesto cyber, della metodologia di riferimento per il "*Psychological Profiling",* al fine di definire e/o convalidare specifici profili e modelli comportamentali riconducibili agli offender che popolano ed operano nel Cyberspace. Questo in ottica di fornire elementi di valore a supporto dell'attività investigativa per l'identificazione dell'offender stesso.

In una prima fase dell'approccio viene portata avanti l'acquisizione di evidenze di natura:

[9] Tecnica elaborata dall'Unità Speciale di Scienze Comportamentali dell'FBI per l'identificazione degli autori seriali di crimini tradizionali

- *Tecnica*, derivanti dalle proprietà di un attacco informatico e riconducibili a specifici modus operandi (vettori, tecniche di attacco, metodologia…)
- *Socio-comportamentale*, riferibili all'offender (livello di competenza e capacità tecniche, signature, linguaggio, simbolismo, immagini, motivazione…) ed alla vittima (target) dell'attacco medesimo.

La "Vittimologia", quale studio delle caratteristiche distintive della vittima di reato (es. sesso, categoria sociale di appartenenza, professione…), fornisce infatti importanti contributi e spunti per l'attività di analisi, al fine di identificare potenziali collegamenti con l'identità criminale, ed in primis, con le motivazioni (curiosità, vendetta, profitto economico, notorietà e visibilità personale) quali componenti direzionali di orientamento di un comportamento verso uno specifico obiettivo.

E' importante sottolineare come, diversamente dalla tecnica del "*Psychological Profiling*", per i reati informatici risulta di difficile applicazione il principio relativo all'invariare nel tempo delle modalità di attacco. Ciò coerentemente con la consapevolezza che l'evoluzione tecnologica e la diffusione e condivisione di informazioni "devianti" nel cyberspace, consentono ad un offender di potenziare le proprie competenze, ponendo in essere attacchi sempre più complessi e differenziati.

Ciò che tende però a rimanere costante nel tempo, è la tendenza da parte dell'offender a personalizzare il proprio operato, mediante per esempio il ricorso a specifici segni di riconoscimento quali, simboli, immagini o specifici messaggi lasciati a seguito dell'esecuzione di un attacco. E' dunque questo il valore aggiunto dell'analisi comportamentale applicata al contesto digitale.

Alla prima fase di acquisizione delle evidenze, segue un'attività di loro confronto (sistema linking) con dati storicizzati, derivanti dall'analisi di attacchi informatici perpetrati in passato. Questo, al fine di rilevare potenziali connessioni e modelli ripetuti, verso cui focalizzare l'attenzione.

Nel dettaglio, il confronto con tale base dati potrebbe fornire concreti spunti investigativi per indirizzare ulteriori attività di ricerca, a carattere "proattivo", in considerazione del contesto digitale di riferimento dell'offender (es. canale IRC), dove, mediante l'interazione personale o automatizzata, sarà possibile raccogliere ulteriori variabili socio-comportamentali riferibili alla sua identità "virtuale" e "reale" (età, gruppo di appartenenza, ruolo e specializzazione, motivazione…).

Risulta dunque propedeutico a tal fine, la previsione di database strutturati, in continuo aggiornamento, ed alimentabili con informazioni provenienti da fonti diversificate (Forze dell'Ordine, Enti accreditati, fonti OSINT, forum specialistici…).

Tra le fonti OSINT è importante sottolineare la presenza sul mercato di tool, nati e pensati per finalità che esulano da attività di profilazione, ma che presentano al contempo funzionalità adottabili nell'ambito delle attività di ricerca ed analisi connesse alla definizione di un profilo criminale. Ne è un esempio la piattaforma Hootsuite[10] le cui funzionalità, consentirebbero per esempio, di individuare utenti "*influencer*" (tramite ricerca per attribuzione di punteggio) relativamente a tematiche sensibili discusse sui "Social Network" ed al contempo, gli "hot spot" corrispondenti, ovvero, aree geografiche (es. Milano Centro) dove le medesime sono principalmente oggetto di interesse.

La reale potenzialità di tale strumento, non risiede però nel suo utilizzo singolo, ma al ricorso, in concomitanza, di altre piattaforme OSINT (es. Cree.py, Foca, Maltego, UCINET…) al fine di acquisire ed incrociare una pluralità di dati di natura diversificata e potenzialmente riconducibili ad un medesimo evento criminoso.

Al termine delle attività di raccolta ed analisi dati, potrà essere delineato uno specifico modello comportamentale, riconducibile ad un profilo deviante consolidato (Wannabe, Script Kiddie, Cracker, Ethical Hacker, Hacktivist, Cyber Warrior/Mercenary, Industrial Spy Hacker, Military Hacker/State-sponsored attacker, Cyberterrorist…), o indicativo della presenza di una nuova figura deviante non ancora categorizzata.

[10] Hootsuite – Social Media Management Dashboard, https://hootsuite.com/it

In conclusione è possibile sottolineare la peculiarità della tecnica del profilo psicologico, quale tassello di un approccio multidisciplinare che riconosce l'importanza di analizzare le dinamiche del Cyberspace senza prescindere dalla componente umana, e quale strumento per indirizzare, accanto a risposte passive ad attacchi informatici, interventi proattivi di contrasto a potenziali minacce cyber.

3.4 Focus sull'analisi di tipo geopolitico

Il rapido sviluppo del cyberspace ha avuto impatti anche sui tradizionali paradigmi della geopolitica, i quali sono venuti progressivamente meno, determinando uno stravolgimento delle dinamiche di difesa e sicurezza. In primo luogo, al contrario delle altre minacce quella cyber è asimmetrica, multipolare e anonima. Il cyberspace stesso è un luogo in cui le identità si scompongono, facendo sì che a un'identità personale corrispondano infinite identità digitali, non sempre riconducibili alla prima. In secondo luogo, nel cyberspazio viene meno il concetto geopolitico di *limes* (confine), sostituito da concetti come aterritorialità e anarchia. Infine, anche il tradizionale concetto di guerra viene radicalmente ripensato, in quanto la cyber war è un tipo di conflitto che non si svolge su un territorio definito, tra fazioni riconosciute e con armi convenzionali: sul web chiunque può essere potenzialmente colpito da un attacco informatico, ovunque nel mondo e in qualsiasi momento.

In questo contesto il Web assume una rilevanza più profonda di quella che ha avuto dalla sua nascita ad oggi. Non è più considerabile come solo veicolo di comunicazione. Si va arricchendo di una dimensione interattiva che consente agli utenti di entrare in un'altra dimensione, governata da costumi propri e che determina dinamiche che influenzano anche la vita reale. In quanto tale, essa assume rilevanza dal punto di vista innanzitutto socio-politico: gli eventi accaduti o in fase di accadimento, non vengono più esclusivamente comunicati o notiziati sul web, in esso avviene anche la fase dell'organizzazione degli stessi. Si pensi, ad esempio, al recente fenomeno del reclutamento, a opera dell'organizzazione terroristica ISIS, di combattenti sui Social Network. Il Web fornisce anche una serie di elementi che aiutano nella comprensione delle intenzioni degli utenti engagées attivamente nella vita sul web. In esso è possibile, infatti, innanzitutto, rinvenire *rumors* che diano il sentore di ciò che sta accadendo nell'ambiente, ma anche determinare il *sentiment* diffuso. Ciò sposta il piano su cui si giocano le relazioni diplomatiche e internazionali su un altro livello. Di elementi di questo tipo devono tener conto i servizi di Intelligence nazionale nella protezione degli asset statali.

Inoltre, la pervasività della tecnologia e del web fa sì che da un lato, gli attacchi cyber colpiscono non solamente gli apparati tecnologici ma impattano anche la sfera personale, delle organizzazioni e di un intero paese. Dall'altro le motivazioni e gli obiettivi da raggiungere a livello sociale, politico e economico possono costituire i presupposti per compiere azioni benevole o malevole nel cyberspazio.

Per interpretare correttamente gli attacchi cyber si rende dunque necessario studiarne la natura, le modalità con cui vengono eseguiti e le motivazioni sottese. Il Web consente, in questo senso, di avere un vasto patrimonio informativo e una serie di indicatori utili al lavoro dell'analista:

- **Politica**: considerare elementi quali l'andamento politico del paese di interesse, la sua posizione e i suoi interessi strategici in campo internazionale, i paesi competitor e quelli alleati, le organizzazioni e i panel internazionali di cui fa parte, i conflitti in cui è coinvolto più o meno direttamente e i fattori di destabilizzazione interni e esterni;
- **Economica**: considerare l'andamento economico dell'organizzazione di riferimento, eventuali investimenti, fusioni o acquisizioni, i suoi competitor, le countries e i settori strategici, l'andamento dell'economia del paese in cui l'organizzazione si trova, l'area economica di cui il paese fa parte ed eventuali investimenti e/o accordi economici con altri paesi o società straniere;
- **Sociale**: considerare elementi quali l'orientamento dell'opinione pubblica, il sentiment, i fattori di malcontento, le proteste sociali in corso, le disuguaglianze tra fasce sociali;

- **Culturale / Religiosa**: considerare gli usi, i costumi e l'orientamento religioso del paese in cui l'azienda si trova e di tutti quelli con cui ha accordi economici/commerciali o ha fatto investimenti, eventuali minoranze etniche e/o religiose, il loro livello di integrazione nella società civile, eventuali emarginazioni, radicalizzazioni e intolleranze.

Un evento che può rappresentare un esempio di interconnessione tra gli indicatori di cui sopra e la componente cyber, è l'attacco perpetrato nei confronti delle infrastrutture critiche ucraine mediante il trojan Black Energy[11], nel Dicembre 2015. L'evento ha provocato un black out della rete energetica del paese lasciando al buio circa 225.000 cittadini. Analisi di settore hanno consentito di dimostrare una plausibile relazione tra l'evento descritto e la situazione geopolitica contemporanea che vede coinvolte Ucraina e Russia. Ciò evidenzia la necessità dell'intervento di specifiche competenze per l'interpretazione di eventi che sempre più si allontanano dalla sfera prettamente tecnologica e informatica e che impattano , invece, sulle relazioni internazionali.

Un'analisi complessa, effettuabile attivando tali direttrici, ma che tenga fortemente conto degli elementi sopra esposti di cui il web è pervaso, fornisce un prodotto completo che non solo consenta la difesa ma anche e soprattutto la prevenzione da attacchi cyber, rivolti sia alla dimensione pubblica che a quella privata, in modo tale da identificare mandanti, motivazioni e obiettivi a questi correlati.

Conclusione

La Web-based Intelligence ha assunto un ruolo primario nello sviluppo di un modello di Adaptive Cyber Security che permetta un'azione predittiva efficace nei confronti delle minacce cyber.

Il modello proposto, andando oltre la tradizionale e unica dimensione IT, beneficia di una forte integrazione tra le tecnologie esponenziali, l'analisi comportamentale e SPEC, permettendo di incrementare l'accuratezza, ridurre l'annoso problema dei falsi positivi e identificare quindi azioni complesse in termini di preparazione e tentativi di attacco veri e propri.

Le nuove componenti si basano su specifiche capacità multidisciplinari tradizionalmente esterne alle aree dell'Information Technology, da cui scaturisce il vantaggio competitivo di nuove prospettive di analisi e riconoscimento.

L'evoluzione verso tale nuovo modello suggerisce quindi che l'investimento tecnologico sia affiancato dall'integrazione della componente altamente qualificata di tipo umano necessaria all'analisi della dimensione comportamentale e SPEC.

Come abbiamo visto, l'informazione rilevante, rapida e precisa ha un valore inestimabile: ogni realtà, aziendale e non, anche a fronte di tecnologie e modelli avanzati potrà agire su perimetri limitati e circoscritti. Pertanto emerge che proprio la collaborazione tra ogni realtà, sia a livello pubblico che privato, può beneficiare di sinergie in cui mettere a fattor comune pratiche, skills e informazioni strategiche che solo combinate possono fornire un seria azione predittiva di contrasto al cybercrime, in continua e sempre più veloce evoluzione.

11 Cyber attacco nei confronti dell'infrastruttura energetica ucraina Ukrenergo attraverso il trojan Black Energy che ha interrotto il servizio a centinaia di migliaia di utenti per circa 75 minuti nella notte tra il 23 ed il 24 dicembre 2015. "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents" in https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

Bibliografia

World Economic Forum, *The Global Risks Landscape 2016*

ENISA, *National/governmental CERTs - ENISA's recommendations on baseline capabilities 2015*

R.A. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, P.A. Laplante, *Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political*

A. Sharma, R. Gandhi, Q. Zhu, W. Mahoney and W. Sousan, *A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference*

S. Das, T. Nayak, *Impact of Cyber Crime: Issues and challenges*

Policy Department External Policies, European Parliament, *Cyber Security and politically, socially and religiously motivated cyber attacks*

A. Karatzogianni, *Cyber-Conflict and Global Politics*

N. Naghshineh, *HUMINT OR WEBINT? Concept Study on possible routes for improving knowledge discovery within organizations*

T. Stevens, *Cyber Security and the Politics of Time*

M.D. Cavelty, *Cyber Security and Threat Politcs*

T. M. Cheung, D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*

A. Teti, *Cyber Intelligence e Cyber Espionage*

T. Townsend, M. Ludwick, J. McAllister, A.O. Mellinger, K.A. Sereno, *SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project*

A. Vivaldi, *Cultural Intelligence - Geopolitica, intelligence e scienze umane*

M. Caligiuri, *Cyber intelligence, la sfida dei data scientist*

M. Mayer, L. Martino, P. Mazurier, G. Tzvetkova, *How would you define Cyberspace?*

K. Geers, D. Kindlund, N. Moran, R. Rachwald, *WORLD WAR C: Understanding Nation-State Motives, Behind Today's Advanced Cyber Attacks*

Intelligence and National Security Alliance, *Strategic Cyber Intelligence*

Politique Etrangère, *The Incomplete Governance of the Internet*

A. Lamanna, *La cyber-geopolitica e le sue rappresentazioni*

M. Mayer, N. De Scalzi, I. Chiarughi, *La politica internazionale nell'era digitale: dispersione o concentrazione del potere?*

J.E. Douglas, A. E. Burgess, *Criminal Profiling. A viable Investigate Tool Against Violent Crime*

Payments UK, *Cyber Threat Intelligence: Criminological Review*

Italian Team for Security, Terrorism Issues & Managing emergencies, Sicurezza, Terrorismo e società

Roberto Baldoni, Luca Montanari (a cura di), *Framework Nazionale di Cyber Security*

NIST, *Framework for Improving Critical Infrastructure Cybersecurity*

ISO-IEC 27004:2009 *Information Technology-Security Techniques-Information Security Management-Measurement*

ISO-IEC 27032:2012 *Information technology -- Security techniques -- Guidelines for cybersecurity*

NIST 800-55 Rev.1, *Performance Measurement Guide for Information Security*

FireEye, *Cyber attacks on the Ukrainian grid: what you should know*

Mihaela Teodor, Bogdan-Alexandru Teodor, *Cyber Threats in Hybrid Warfare: the Ukrainian Case* in *Countering Hybrid Threats: Lessons Learned from Ukraine*, 2016, IOS Press

ICS-CERT, *Cyber-Attack against Ukrainian Critical Infrastructure*

A.Toti, *Open source, intelligence & cyberspace. La nuova frontiera della conoscenza*

GReAT, Kaspersky Lab's Global Research & Analysis Team, *BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents* in https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

M.E. Bonfanti, A.P. Rabera, *Internet-based Intelligence: Prediction or Foreknowledge? in E. Mordini, M. Green, Internet-based Intelligence in Public health emergencies*, 2013, IOS Press.