FireEye – Before, During and After the Breach

Conoscenza dell'avversario, analisi del rischio, prioritizzazione degli allarmi, fruibilità, processi e predittività…..sono concetti che oggi è necessario prendere in considerazione (e possibilmente applicare) per affrontare in maniera adeguata l'attuale scenario della cyber security.

In questo articolo vedremo di analizzarli più in dettaglio e contestualizzarli.

Oggi gli attacchi informatici sono diventati molto più sofisticati e sono facilmente in grado di bypassare le difese tradizionali basate su signature, come i firewall di nuova generazione, gli IPS, gli antivirus, i web gateway, compromettendo la maggior parte delle reti aziendali.

La protezione da attacchi APT (Advanced Persistent Threat)/Zero Day necessita pertanto di soluzioni capaci di identificare in modo dinamico e bloccare gli attacchi informatici di nuova generazione in tempo reale, attraverso piattaforme in grado di collezionare e condividere informazioni sulle minacce a livello globale, che supportino le aziende dotate di sistemi informativi complessi, per proteggere i loro dati da tutti i principali vettori di minacce: web, via e-mail, file e attacchi informatici mobile-based o che sfruttino tecniche di social hacking.

Ultimamente il fenomeno dei ramsomware (i.e. Cryptolocker e sue varianti) ha aumentato la percezione delle organizzazioni sulla scarsa efficacia dei sistemi di difesa tradizionali.

E' necessario tuttavia fare un po' di chiarezza in quanto, sebbene le tecniche di attacco che sottendono sia agli attacchi APT sia ad attacchi ramsomware si siano notevolmente avvicinati nel corso degli ultimi anni, le differenze tra le due tipologie di attacco sono notevoli e legate soprattutto alle motivazioni degli attaccanti e agli obiettivi che gli stessi si prefiggono.

Oggi è abbastanza semplice far partire una campagna ramsomware anche per attaccanti non in possesso di capacità tecniche avanzate: è sufficiente infatti ottenere una lista corposa di indirizzi di posta elettronica, ricercare nel Dark Web (chi è che non ha un browser TOR?) un servizio RaaS (Ramsomware as a Service) e richiedere il servizio in cambio di una percentuale degli eventuali introiti, concordando le condizioni "commerciali" con il fornitore di servizio. Aggiungete la localizzazione della campagna (italiano) e argomenti d'interesse comune (le tasse, le bollette, etc.) e il gioco è fatto.

Chi sono i bersagli? Chiunque……aziende, istituzioni pubbliche e semplici cittadini.

Chi sono gli attaccanti in questo caso? Ovviamente organizzazioni di cyber criminali. In questo caso ha poca importanza la nazionalità degli attaccanti….i bitcoin non hanno confini!!!

Che scopo si prefiggono? Guadagnare soldi, sia per interesse personale sia per finanziare ulteriori attività illecite.

Quanto dura un attacco ramsomware? Solitamente poche settimane. Una volta che il "tema" della campagna diventa noto alla massa perde di efficacia.

Un attacco APT è invece perpetrato con presupposti completamente diversi rispetto ad un attacco ramsomware, sebbene possa utilizzare le medesime tecniche di attacco (ad es. mail di spear phishing).
Solitamente gli attacchi APT sfruttano exploit Zero Day creati appositamente per lo scopo, con l'obiettivo di sfruttare una vulnerabilità di un'applicazione, un sistema o un apparato di network e/o security prima ancora che essa sia nota oppure nell'arco di qualche ora/giorno dal momento della scoperta. In alcuni casi potrebbero passare diversi mesi prima che l'obiettivo target riesca ad accorgersi dei danni subiti. La vulnerabilità è quindi sfruttata dagli attaccanti prima che sia resa disponibile una soluzione o un processo di workaround.

Chi sono i bersagli? Principalmente aziende private in possesso di proprietà intellettuale, istituzioni pubbliche e infrastrutture critiche.

Chi sono gli attaccanti in questo caso? Stati esteri o organizzazioni di cyber espionage. In questo caso l'attribuzione dell'attaccante è molto più importante (si veda ad es. The 2016 Security Landscape - https://www2.fireeye.com/rs/848-DID-242/images/2016-Security-Landscape-RPT.pdf?mkt_tok=3RkMMJWWfF9wsRolvqzId%2B%2FhmjTEU5z17OkqXKexgokz2EFye%2BLIHETpodcMT8ZqPLHYDBceEJhqyQJxPr3NKNgN3tx5RhPmCg%3D%3D) perché l'attacco potrebbe comportate una risposta politica o cyber-militare da parte del bersaglio.

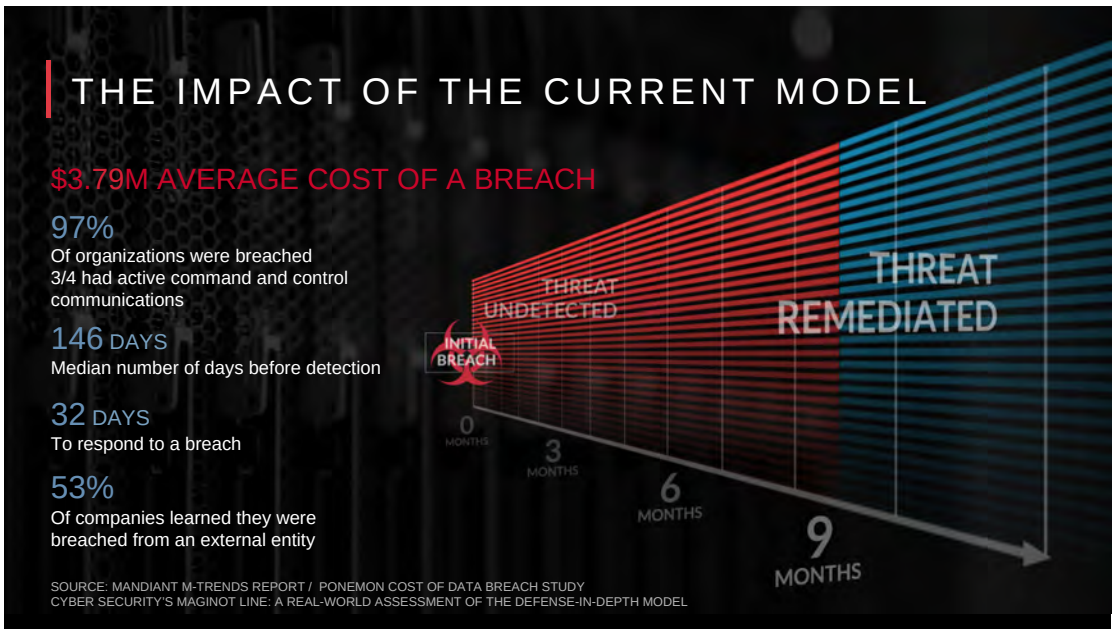
Che scopo si prefiggono? Rubare dati confidenziali che potrebbero compromettere un'azienda (segreti industriali) o una nazione (segreti di stato, dati riservati riguardanti il mondo politico, dati di magistratura, dati riguardanti la difesa, etc.) oppure bloccare le infrastrutture critiche di una nazione (si pensi agli attacchi portati a Dicembre 2015 alle centrali elettriche in Ucraina) oppure raccogliere le cosiddette PII (Personally Identifiable Information) per scopi di intelligence o fraudolenti.

Quanto dura un attacco APT? Il termine Persistente dell'acronimo APT è abbastanza auto-esplicativo in questo caso….l'obiettivo dell'attaccante è rimanere "nascosto" il più a lungo possibile per poter svolgere il suo "lavoro" e raccogliere quante più informazioni possibile o penetrare all'interno dell'organizzazione più in profondità. Si parla quindi di settimane e o mesi (nel peggiore dei casi siamo arrivati anche agli anni!!)

A tal proposito Mandiant pubblica ogni anno il proprio M-Trends Report (potete scaricare l'ultimo report qui: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html?utm_source=social&utm_medium=blog&utm_campaign=mtrends2016).

Si tratta di un report che riassume i dati rilevati dagli analisti Mandiant (a livello mondiale) a seguito di servizi di Incident Response svolti nel corso dell'anno precedente presso i clienti che hanno coinvolto Mandiant per l'analisi e risoluzione del breach. I dati riportati in questi report sono quindi dati reali.
Ebbene nel corso del 2015 il tempo medio che è intercorso tra il momento dell'attacco iniziale e il momento in cui il breach è stato scoperto è stato di 146 giorni (comunque in discesa rispetto ai 205 giorni del 2014 e ai 265 giorni del 2013).

Un altro dato interessante che emerge è che il 53% delle organizzazioni che ha coinvolto Mandiant ha scoperto di aver subito un breach da fonti esterne e non grazie a strumenti o personale interno.



Recentemente FireEye ha pubblicato il medesimo report per l'area EMEA (Europe, Middle East and Africa) (per ulteriori informazioni fate richiesta a paolo.cecchi@fireeye.com).

Ebbene la situazione nella ns. regione è decisamente peggiore. Ad esempio il tempo medio di cui sopra è pari a ben **469** giorni!!!

Questa lunga premessa ci permette quindi di entrare nel merito di come le organizzazioni dovrebbero prepararsi ad affrontare un attacco APT, con l'obiettivo di cercare di abbattere il tempo di detection e risposta ad un attacco informatico di questo tipo.

Ma quali sono le problematiche che oggi le organizzazioni si trovano a dover affrontare per dare una risposta efficace al problema?

Innanzitutto a seguito di un breach gli alti livelli dell'organizzazione non vogliono sapere i dettagli tecnici dell'attacco, ma le domande che pongono sono:

- Che dati sono stati esfiltrati?
- Chi ci ha atttaccato?
- Che impatto ha l'attacco sul ns. business/funzionamento dell'organizzazione?
- Come sono entrati?
- Sono ancora dentro?
- Che cosa abbiamo fatto per contenere l'attacco?

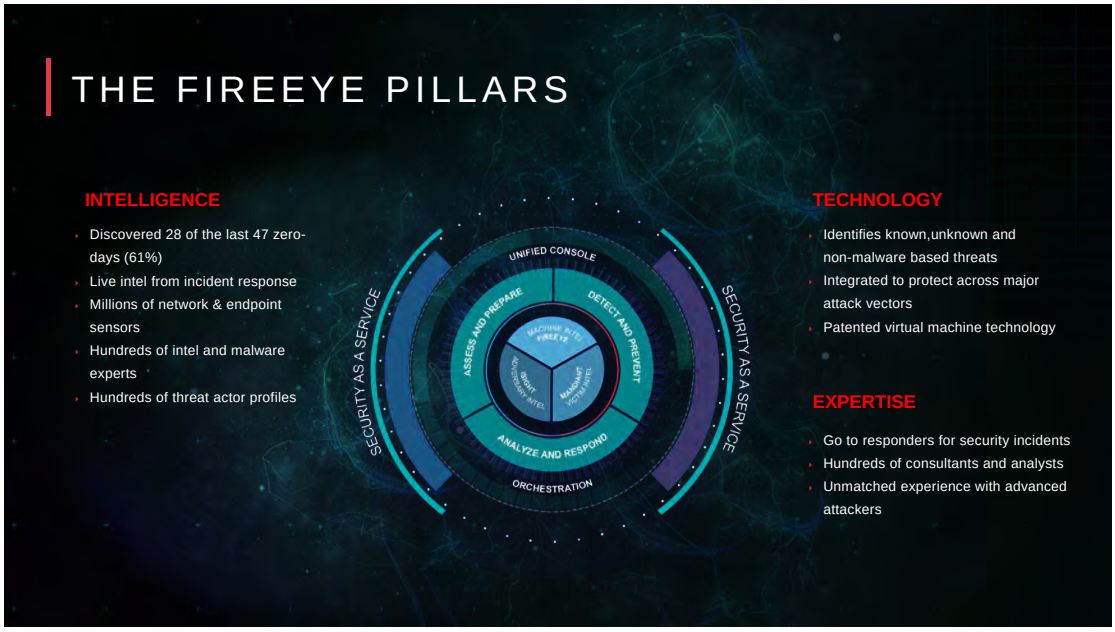
Solo con la tecnologia è estremamente difficile (se non impossibile) rispondere a queste domande e soprattutto i tempi di risposta rischiano di essere troppo lunghi.

Ad amplificare ulteriormente la difficoltà da parte di chi si occupa di cyber-security intervengono altri fattori quali ad esempio:

- difficoltà nel formare/trovare personale competente in materia e soprattutto nel trattenerlo all'interno dell'organizzazione (e questo è ancora più vero nell'ambito Difesa a causa dell'elevato turn over delle risorse)
- too many alerts: tutte le soluzioni di sicurezza implementate presso una qualsiasi organizzazione producono migliaia/decine di migliaia di alerts al giorno. Senza una contestualizzazione degli stessi diventa praticamente impossibile gestirli, anche per quelle organizzazioni dotate di strutture di sicurezza molto numerose (a cosa do priorità? Quanti sono i falsi positivi? Etc.)
- si combatte una battaglia asimmetrica: da una parte ci sono gli attaccanti, ben formati, ben finanziati, con un obiettivo ben preciso. Dall'altra ci sono i difensori, a cui spesso mancano gli strumenti minimi indispensabili per contrastare un ramsomware, figuriamoci un APT…
- tutti gli strumenti di sicurezza hanno le proprie console che spesso non si parlano tra di loro, e questo determina uno spreco di risorse enorme all'interno delle organizzazioni. Perfino i SIEM, che molti pensano essere la panacea per questo tipo di problematiche, vengono utilizzati dalla maggior parte delle organizzazioni come log collector (e allora perché non comprare un log collector che costa molto meno?) e quei pochi che li utilizzano per la correlazione degli eventi non sanno cosa dargli in pasto oppure non riescono ad analizzarne i dati.

E' necessario quindi che le organizzazioni ripensino il loro approccio alla cybersecurity non solo in termini di tecnologia, ma anche in termini di processi e persone. Per costruire una posture di sicurezza adeguata al nuovo scenario della cyber security occorre ragionare in termini di:

- tecnologie
- expertise
- intelligence



Ed è anche necessario accettare il fatto che la prevenzione non è più sufficiente a garantire la sicurezza della propria organizzazione, ma bisogno investire in capacità di "early detection" e "rapid response", come anche Gartner riporta:

"By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2013.

PETER FIRSTBROOK, NEIL MACDONALD
"MALWARE IS ALREADY INSIDE YOUR ORGANIZATION, DEAL WITH IT" (12 FEBRUARY 2014 - G00259857)

Ritornando quindi al "prima, durante e dopo" l'attacco vediamo come le organizzazioni dovrebbero prepararsi (Sun Tzu docet!).

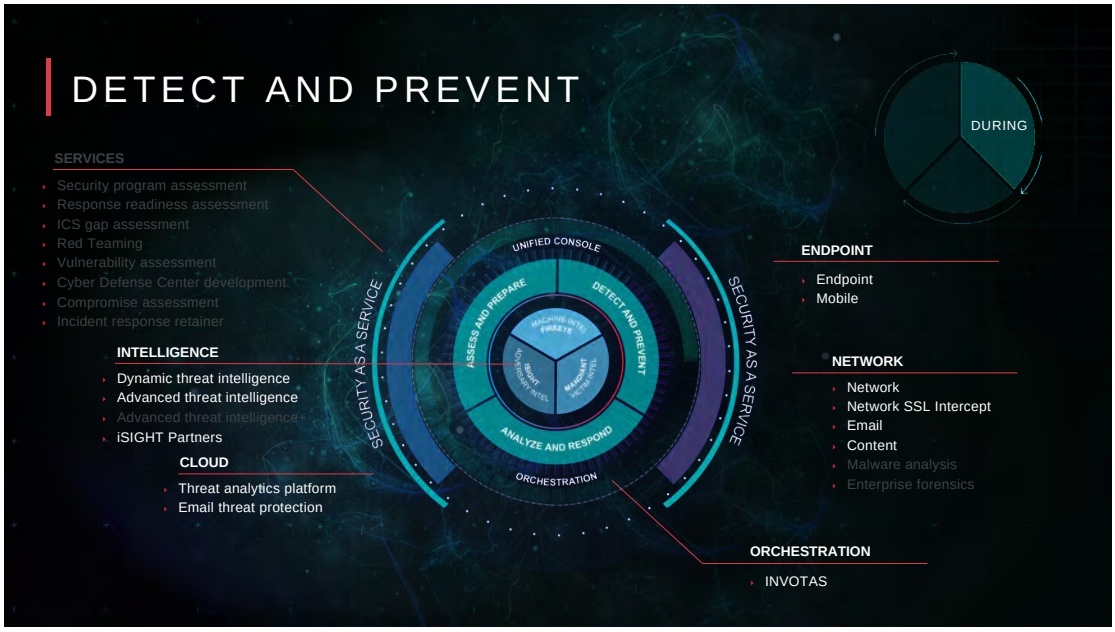
FASE 1: Prima dell'attacco - > Assess and prepare

In questa fase è necessario capire quanto la propria organizzazione è pronta ad affrontare un attacco cibernetico, quali sono i punti deboli sia in termini tecnologici sia in termini di processo, come si comportano gli attaccanti per poter intraprendere preventivamente le necessarie contromisure di difesa.

Entrano quindi in gioco alcuni servizi che permettono di rispondere ad alcune domande necessarie per migliorare la propria posture di sicurezza:

- Quali sono i miei punti deboli? -> Vulnerability Assessment e Red Teaming
- Quali sono i processi interni in caso di un attacco informatico e come posso migliorarli? -> Response Readiness Assessment, Security Program Assessment
- Sono compromesso in questo momento? -> Compromise Assessment
- Sono in grado di gestire da solo un breach o posso aver bisogno di qualcuno esterno? -> Incident Response Retainer
- Chi è che attacca il mio segmento di mercato? Stati, organizzazioni criminali, attivisti? Che tecniche utilizzano? -> Advanced Threat Intelligence +, iSight

<u>FASE 2: Durante l'attacco -> Detect and Prevent</u>



In questa fase è importante adottare soluzioni in grado di aumentare la capacità e velocità di detection di un attacco (ricordiamo i famosi 146/469 giorni in cui l'attaccante è dentro l'organizzazione prima di essere scoperto) e soprattutto contestualizzare l'attacco mediante l'intelligence. Queste due capabilities permettono di ridurre l'impatto dell'attacco: diminuendo il tempo in cui scopro di essere sotto attacco i danni subiti saranno minori e i costi della remediation saranno ridotti (pensiamo alla differenza che c'è tra lo scoprire un attacco in pochi minuti o ore rispetto a scoprirlo dopo 5 mesi!!).

In questa fase entrano in gioco quindi tecnologie e intelligence:

- cosa vogliamo proteggere? Quali sono i canali attraverso cui un attaccante può penetrare la ns. organizzazione? Abbiamo servizi in cloud?-> Ovviamente molteplici per cui devono essere prese in considerazione diverse soluzioni in grado di proteggere questi canali sia a livello perimetrale, sia a livello di endpoint sia nel caso di utilizzo di servizi in cloud, e in particolare:

  - Navigazione Web – NX (https://www.fireeye.com/products/nx-network-security-products.html)
  - Traffico Email -> EX (https://www.fireeye.com/products/ex-email-security-products.html)
  - Contenuti (file share, hybrid cloud, etc.) -> FX (https://www.fireeye.com/products/fx-content-security-products.html)
  - Endpoint (PC o Server) –> HX (https://www.fireeye.com/products/hx-endpoint-security-products.html)

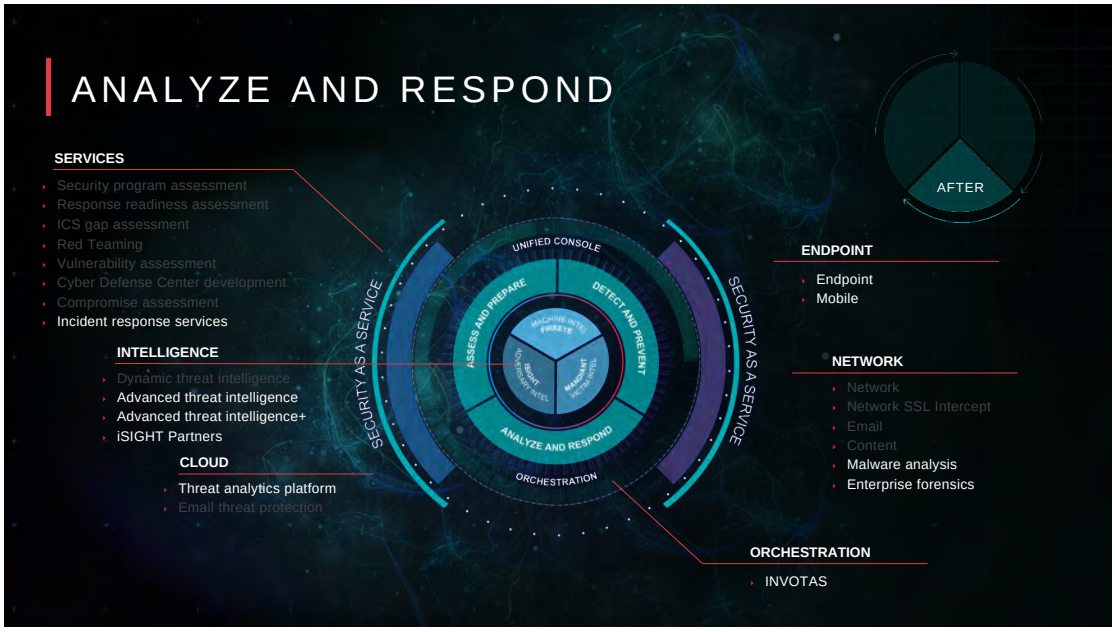
- Dispositivi mobili (smartphone e tablet) -> MTP/MX (https://www.fireeye.com/products/mobile-threat-protection-mobile-security-products.html)
- Traffico Email nel caso si utilizzino servizi in cloud (Office 365, Google mail) -> ETP (https://www.fireeye.com/products/ex-email-security-products.html)
- Analisi log (SIEM nel cloud) -> TAP (https://www.fireeye.com/products/threat-analytics-platform.html)

- Come posso gestire centralmente tutte queste soluzioni e abilitare capacità di correlazione in grado di affrontare anche attacchi multi-vettore (una prima parte via mail, l'altra via web ad esempio) -> CM (https://www.fireeye.com/products/central-management.html)

- Come posso fare prevention in uno scenario in cui gli attaccanti sono estremamente dinamici e cambiano le loro tecniche di attacco e/o il malware utilizzato per sferrare l'attacco? Come riesco a capire se è in corso un attacco se non viene utilizzato malware? -> Per agire in questo scenario occorre un approccio estremamente dinamico che permette di condividere le informazioni a livello mondiale ed in tempi estremamente rapidi, e qui viene in aiuto un sistema cloud di information sharing (DTI) e di nuovo l'intelligence con la licenza ATI (attribuzione, kill chain analysis) (https://www.fireeye.com/products/dynamic-threat-intelligence.html)

- Come posso ottimizzare tutte le risorse interne (sia tecnologiche sia umane) per poter gestire adeguatamente un breach? In un mondo di tecnologie che non si parlano tra di loro e di processi spesso scorrelati dalle stesse tecnologie servizi di automazione/orchestrazione diventano fondamentali. Gartner stima che il mercato delle soluzioni di automazione/orchestrazione vedrà un crescita a due digit nel corso dei prossimi anni. FireEye, con l'acquisizione di Invotas, è oggi in grado di proporre anche questo tipo di soluzioni (FireEye Security Orchestrator - https://www.fireeye.com/products/security-orchestrator.html)

FASE 3: Dopo l'attacco -> Analyze and Respond



In questa fase è necessario capire cosa sta accadendo, analizzare l'attacco e intraprendere le necessarie azioni per poter chiudere l'incidente nel modo più veloce e corretto possibile. Senza le necessarie informazioni (analyze) la risposta rischia di essere insufficiente e non definitiva. Purtroppo spesso quando Mandiant viene coinvolta sul campo a seguito di un breach una delle cose cui ci troviamo di fronte è la formattazione dei PC che si suppone siano stati compromessi. A ns. avviso si tratta di una delle azioni più deleterie che si possano fare, proprio perché operando in tal modo si perdono tutte le informazioni necessarie per capire meglio l'attacco e gli attaccanti.

Anche in questo caso si può ricorrere a soluzioni e servizi che permettono di gestire questa fase nella maniera più corretta, rispondendo ad alcune domande tipiche e in particolare:

- Cosa sta accadendo sui miei host (PC/server/dispositivi mobili)? Cosa sta facendo o ha fatto l'attaccante? -> sono necessarie capability di endpoint forensic, che le soluzioni HX e MTP/MX di cui sopra includono
- Cosa ha fatto l'attaccante all'interno della mia rete? Che comunicazioni ha attivato? Come si è spostato? Cosa ha preso? -> sono necessarie capability di network forensic, che la soluzione PX/IA (pensiamola come ad un registratore dei flussi di traffico dentro la rete) rende disponibili (https://www.fireeye.com/products/enterprise-forensics.html)
- Cosa fa quel malware che ho rilevato? E cosa avrebbe fatto se non lo avessi bloccato? -> è necessario aggiungere una capability di malware analysis (tipica dei SOC/CERT), che viene resa disponibile attraverso la soluzione AX (https://www.fireeye.com/products/malware-analysis.html)
- L'attaccante ha compromesso altri sistemi dentro la mia organizzazione che non siano PC, server o dispositivi mobili? Come posso sapere se ha compromesso ad esempio il mio sistema di videosorveglianza e di allarme

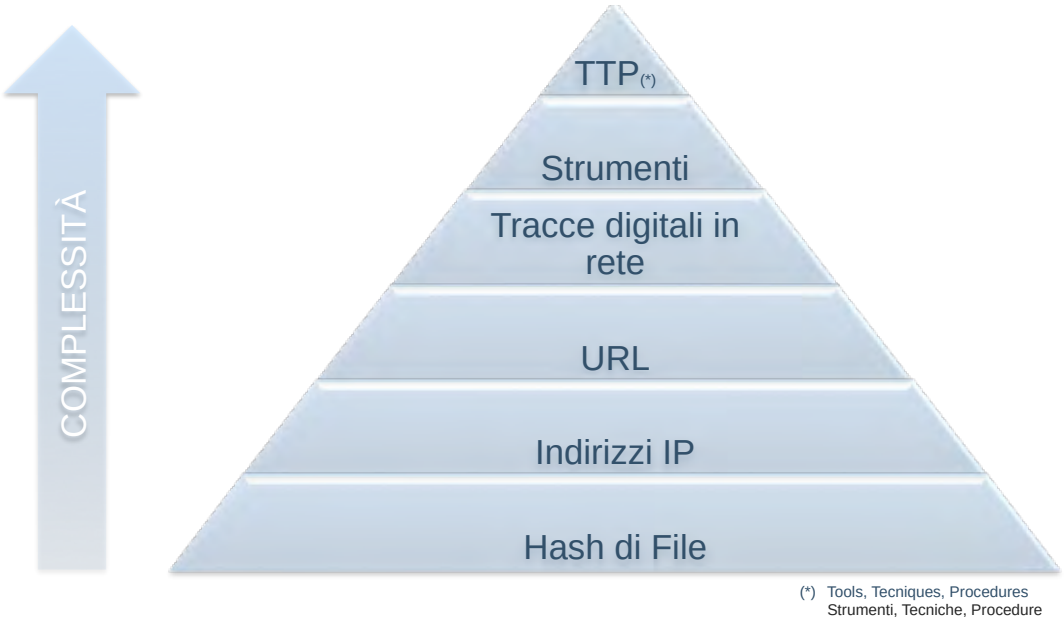
su IP e sarebbe quindi in grado di disabilitarli quando vuole? -> Di nuovo la soluzione di analisi dei log e di matching con la ns. intelligence (TAP) può rispondere a questo tipo di domande

- E se l'attaccante non sta più usando malware? Come faccio a capire dove si è mosso? -> Di nuovo l'intelligence (ATI, ATI+, iSight) rende disponibili informazioni in merito a strumenti, tecniche e procedure utilizzati dagli attaccanti
- Non sono in grado di gestire l'incidente da solo? Come posso fare? -> La risposta è il servizio di Incident Response (https://www.fireeye.com/services/mandiant-incident-response.html) di Mandiant, leader di mercato indiscusso in tale ambito

In maniera trasversale a tutto quanto sopra e per colmare la mancanza di risorse professionali interne che alcune organizzazioni possono avere si può ricorrere a FireEye as a Service (https://www.fireeye.com/products/fireeye-mssp-services.html). Si tratta di un servizio gestito delle soluzioni FireEye, che aggiunge, a quanto già presente all'interno dell'organizzazione, expertise e intelligence per la gestione pro-attiva degli incidenti.

Da quanto sopra emerge evidente come l'intelligence stia diventando sempre più importante nell'ambito della cyber-security. Proprio per ovviare alla mancanza di risorse e gestire decine di migliaia di alert (di cui spesso la maggior parte è costituita da falsi positivi) la conoscenza degli strumenti, tecniche e procedure di attacco e la contestualizzazione degli attaccanti costituisce un elemento imprescindibile per tutte le organizzazioni.

Il problema è capire bene di quale tipo di intelligence bisogna usufruire.



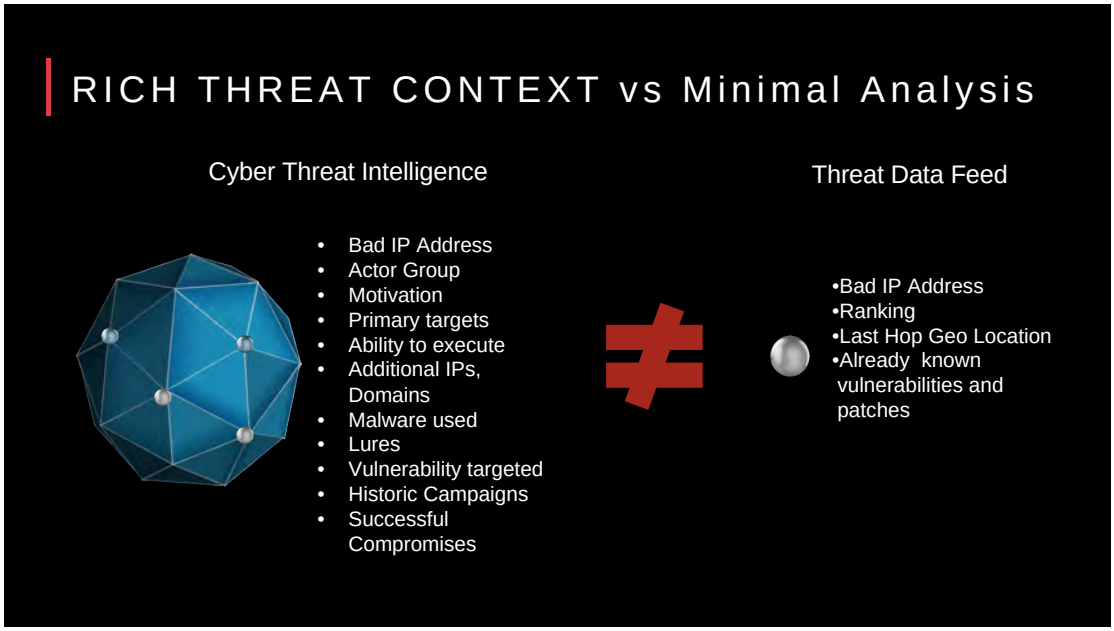
Oggi molte organizzazioni usufruiscono di servizi che rendono disponibili hash di file, indirizzi IP/URL malevoli, indicatori di compromissione (IoC) semplici, eventi di sicurezza generalisti. Questi dati vengono dati in pasto agli strumenti di sicurezza presenti all'interno dell'organizzazione (next-generation firewall, sistemi antimalware, antivirus, sistemi IDS/IPS, etc.) che generano gli alert che poi verranno raccolti da un sistema di centralizzazione degli allarmi (tipicamente un SIEM) e che verranno gestiti dal personale di sicurezza del SOC, laddove presente.
Gli analisti del SOC effettuano un triage sui sistemi sospetti e nel caso validino l'infezione possono ripulire gli stessi oppure coinvolgere il team di Incident Response (IR) per i casi più gravi.

Il problema di fondo di questo approccio è che i dati di cui sopra non sono contestualizzati (ovvero verificati ed associati all'attaccante) e questo determina un numero elevato di alert e numerosi falsi positivi che bloccano l'operatività dei SOC e aumentano il tempo di risposta all'attacco.

La Cyber Threat Intelligence dovrebbe invece fornire informazioni che, partendo dalla conoscenza degli avversari, delle loro motivazioni e delle metodologie che utilizzano, permetta di focalizzarsi su quanto realmente importante (protect what matters most) per la propria organizzazione ottimizzando al tempo stesso processi e risorse.

La Cyber Threat Intelligence dovrebbe quindi:

- Essere focalizzata sul rischio
- Riguardare gli avversari
- Essere actionable (ovvero immediatamente fruibile)
- Essere in grado di prioritizzare allarmi e azioni
- Essere basata su un processo preciso e focalizzato sulle esigenze di ciascuna organizzazione (definizione requisiti di intelligence, raccolta informazioni, analisi e propagazione, consumo)
- Essere predittiva (se so che stà partendo una campagna di attacco nel mio segmento di mercato posso prepararmi in anticipo)



FireEye, grazie all'acquisizione di iSight, è oggi in grado di fornire questo livello di Cyber Threat Intelligence ed aiutare le organizzazioni ad essere più efficaci nella lotta contro le minacce cyber.

Concludo ricordando una interessante definizione di che cosa è la cyber security che ho recentemente sentito ad un evento (tradotta in italiano):

"La cyber security è quell'insieme di tecnologie, processi e persone che permettono alle organizzazioni di garantire la confidenzialità, integrità e disponibilità dei dati sui propri sistemi informativi al fine di evitare che attacchi informatici possano causare la "distruzione" dell'organizzazione stessa".

Per garantire la sopravvivenza della propria organizzazione è quindi assolutamente necessario essere preparati e pronti!!!

Paolo Cecchi
FireEye Inc.

Paolo.cecchi@fireeye.com

Cyber Defence e Coordinamento esterno

Ruoli evolutivi dei CERT nella cooperazione tra Difesa, Amministrazioni, Agenzie e Infrastrutture Critiche

A cura di Fabio Battelli, Director – Deloitte ERS, Cyber Risk Services

Le capacità di Cyber Defence di una nazione sono intimamente legate all'abilità di attuare un coordinamento fattivo tra tutti i soggetti che fruiscono o erogano servizi attraverso lo spazio cibernetico. Tuttavia spesso tale coordinamento risulta immaturo o insufficiente a garantire un efficace contrasto della minaccia cyber su scala nazionale.

Secondo analisi e studi indipendenti a livello mondiale circa 30 dei 196 stati riconosciuti sovrani a livello internazionale hanno reso pubblica una propria strategia per la protezione dello spazio cibernetico; a questi vanno aggiunti i documenti strategici della NATO e dell'Unione Europea. Tuttavia, mettendo a fattor comune le diverse strategie esistenti, emergono alcuni aspetti comuni. Tra questi la necessità di rafforzare la condivisione delle informazioni (anche tra pubblico e privato), l'*early warning* e le capacità di *incident response*, considerati effettivamente come priorità strategiche da tutti gli Stati.

In linea con queste necessità la Commissione Europea nel 2013 ha concluso, attraverso la collaborazione con Deloitte, uno studio di fattibilità[1] per la realizzazione di un **European Early Warning e Response System** (EWRS), con l'obiettivo di fornire **supporto operativo** e di **facilitare la cooperazione** tra le principali strutture di *difesa* all'interno dell'EU, consentendo al contempo di:

- Migliorare la capacità di rilevare e identificare gli incidenti di sicurezza a livello globale;
- Fornire rapida notifica a tutti gli stakeolder interessati;
- Favorire una reazione coordinata agli incidenti ed alle emergenze.

Lo studio ha individuato immediatamente nel Computer Emergency Response Team (CERT) la funzione capace di raggiungere gli obiettivi sopra elencati, pur costatando numerose differenze ed approcci adottati nelle iniziative già avviate nel tempo dai singoli Stati Membri e che in qualche misura risultavano significative e pertinenti anche per lo sviluppo del EWRS. Le conclusioni dello Studio hanno portato all'identificazione di tre possibili scenari di implementazione della piattaforma EWRS in Europa:

- Piattaforma aperta di *information sharing* focalizzata sulla collaborazione e comunicazione attiva tra tutti gli Stati Membri;
- Piattaforma chiusa, accessibile solo ad un ristretto numero di stakeholder, con funzionalità di risposta coordinata agli incidenti cyber, in aggiunta alla capacità di infosharing tra soggetti accreditati;
- Piattaforma integrata e accessibile solo ad un insieme ristretto di stakeholder, che offre funzionalità di scambio informazioni, incident response e servizi di monitoraggio e individuazione delle minacce.

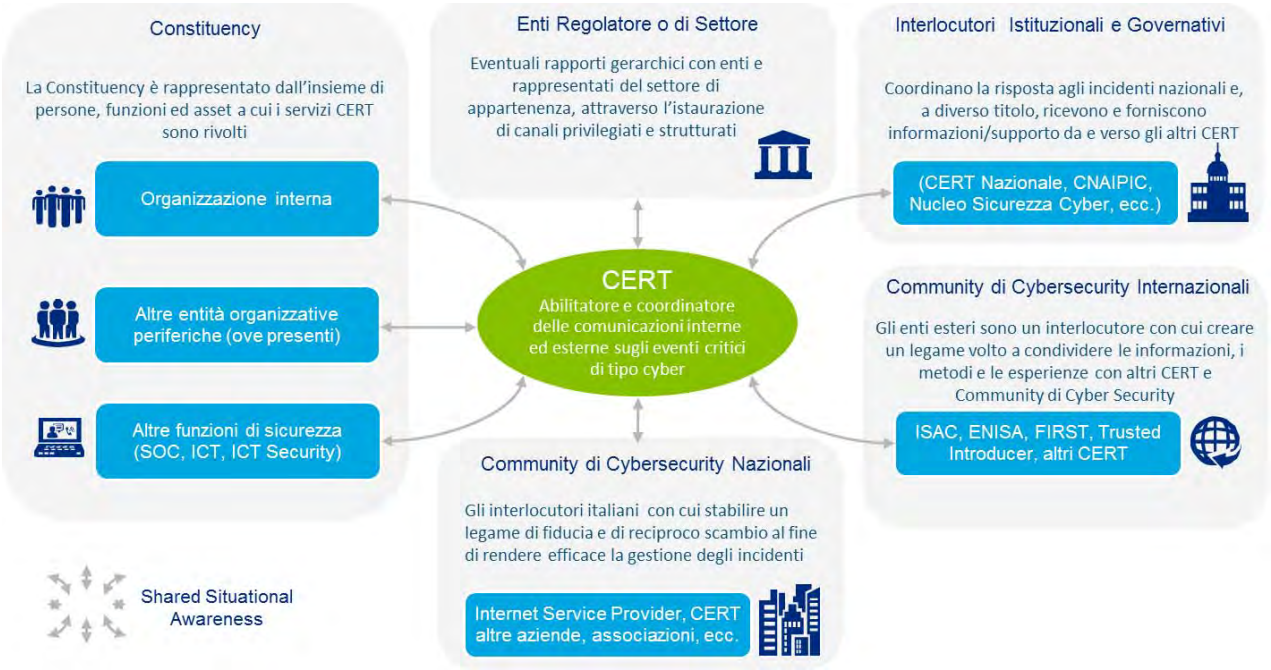
Indipendentemente dalle evoluzioni di questa piattaforma, appare chiaro ed urgente sia a livello di Commissione Europa, sia dei singoli Stati Membri, il ruolo chiave che il CERT può avere nel rafforzamento della Cyber Defence nazionale. Non a caso, anche la recente approvazione della direttiva NIS da parte del Parlamento Europeo, ha ulteriormente enfatizzato il ruolo strategico del CERT per la sicurezza nazionale dello spazio cibernetico.

Il CERT infatti si sta affermando, sia nel mondo pubblico, sia in quello privato, come il punto di contatto principale per la gestione degli incidenti critici e la prevenzione delle minacce nel cyber space.

---

1 Feasibility study and preparatory activities for the implementation of a European Early Warning and Response System against cyber-attacks and disruptions, European Commission and Deloitte

Figura 1 - Ruolo del CERT nella Cyber Defence



Tuttavia l'adozione del CERT come strumento reale e capace di rafforzare fattivamente la Cyber Defence su scala nazionale deve superare ancora sfide piuttosto importanti. In particolare, in termini di coordinamento e cooperazione tra gli stessi CERT è necessario individuare strategie nazionali e di settore in grado di rispondere almeno alle seguenti domande:

- Quale modello di cooperazione è richiesto ?
- Quali capacità minime devono essere attribuite a ciascun CERT ?
- Quali best practice e standard condivisi è possibile adottare ?
- Quali ruoli e responsabilità è necessario definire ?
- Quali strumenti comuni è possibile adottare ?

Interrogativi complessi che evidenziano chiaramente quanta strada ci sia ancora da percorre, soprattutto in termini di azione sistemica al problema. Volendo fare un passo indietro, precedente a quello della cooperazione e del coordinamento e considerando la specificità del contesto italiano, andrebbero preliminarmente indirizzati i seguenti aspetti:

- La maggior parte delle infrastrutture critiche nazionali non ha ancora formalmente costituito un CERT o sta cominciando adesso il percorso per la sua realizzazione;
- Lo scambio informativo su incidenti subiti e tecniche adottate è attuato ancora in casi sporadici e solo in alcuni ambiti/settori (vedi Pubblica Amministrazione attraverso CERT-PA)
- Molte organizzazioni (sia appartenenti al settore pubblico, sia a quello privato) non hanno ancora maturato una sensibilità specifica sull'effettiva necessità di contribuire attivamente alla Cyber Defence nazionale
- Nonostante le indicazioni e gli elementi forniti dalla NIS europea ed i passi avanti fatti dal Legislatore, mancano ancora dei regolamenti tecnici o di auto-disciplina che consentano di uniformare le aspettative e le necessità in materia di Cyber Defence nazionale.

Un primo passo fondamentale per indirizzare parte delle tematiche illustrate potrebbe arrivare dalla definizione di un insieme di CERT, volti a garantire cooperazione tra gli stessi **e** nell'ottica di favorire

un'adeguata strategia di **difesa nazionale.** Ciò può essere raggiunto ad esempio attraverso l'adozione di un **Framework Nazionale di Cyber Defence**, che possa da una parte uniformare le capacità richieste dai CERT e dall'altra favorire il coordinamento tra attori pubblici e privati, troppo spesso impegnati a fronteggiare le medesime minacce e risolvere analoghe problematiche.

L'impiego di tale framework comune andrebbe inoltre nella stessa direzione promossa nel **Cyber Defence Policy Framework emanato nel 2014 dalla Commissione Europea,** che alla base richiede "*Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector*"**.**

Altri vantaggi derivant dall'adozione di un framework di Cyber Defense comune possono essere così riassunti:

- **Trust**. Disponibilità di una rete di contatti fiduciari per l'intera community CERT/CSIRT, che faciliterebbe la cooperazione e lo scambio informativo
- **Prevenzione**. Condivisione proattiva e tempestiva delle minacce, basata sull'utilizzo di metodiche e strumenti comuni;
- **Reazione.** Riduzione degli impatti a livello di Sistema Paese in casi di incidente/crisi, grazie allo scambio informativo sulle minacce e le tecniche di risposta agli incidenti;
- **Situational Awareness.** Visibilità completa sullo stato della minaccia nazionale, grazie alla condivisione di dati e statistiche contestualizzate allo scenario italiano.
- **Baseline di Protezione**. Standardizzazione delle capacità di difesa, mediante la condivisione di un set specifico di standard operativi ed organizzativi
- **Competitività.** Maggiore credibilità e competitività Internazionale, grazie a misure concrete ed effettive di difesa nazionale;
- **Rilevanza sovranazionale**. Contributo fattivo alla sicurezza dello spazio cibernetico, globale per definizione.

Forcepoint: conoscere per proteggersi

Forward without fear: reazione immediata contro le minacce informatiche

Il cybercrime si evolve secondo logiche industriali e lo fa avendo a disposizione budget consistenti e ritorni vicini all'800% degli investimenti.

L'aumento della connettività e la digitalizzazione della vita quotidiana delle imprese e del pubblico portano ad uno sfruttamento maggiore dei sistemi di pagamento, del Cloud e dei dispositivi IOT, con un ulteriore aumento dell'esposizione dei nostri dati e delle nostre informazioni, anche finanziarie.

Inoltre, l'evoluzione e l'espansione di un Internet che sta rapidamente invecchiando, offrono significative possibilità di attacco e nello stesso tempo uno scoglio per i difensori.

La sicurezza informatica intelligente oggi non consiste più solo nel prevenire una violazione, ma nel costruire la resilienza e la flessibilità necessarie per rispondere ad essa e nel ridurre al minimo i potenziali danni della violazione stessa.

Per Forcepoint (nata dalla fusione di Websense, Raytheon Cyber Products e Stonesoft) prevenzione significa proteggere utenti, reti e dati, consentendo alle aziende di concentrarsi su ciò che conta di più per promuovere la propria attività e conseguire il proprio business con successo.

Proprio a questo punta la nostra vision, denominata *4D Security*: Difendere (Defend), Rilevare (Detect), Decidere (Decide) e Sconfiggere (Defeat).

Solo se le violazioni vengono identificate rapidamente i Security Manager sono in grado di reagire e decidere quali azioni sono necessarie per tornare altrettanto rapidamente alla normalità con un processo di bonifica efficace.

La piattaforma Forcepoint protegge contro le minacce provenienti da insider e outsider, individua rapidamente le infrazioni, riduce al minimo il "dwell time" - il periodo tra la compromissione delle macchine o delle reti e la risoluzione - e blocca il furto. Una piattaforma, dunque, che semplifica ed insieme rafforza la sicurezza come parte di una strategia olistica che comprende persone, processi e tecnologia.

Attacchi ai Sistemi SCADA, dalla teoria e dall'intelligence vista con Avex nel 2014 sono oggi passati all'azione, con l'attacco alle centrali elettriche Ucraine (BlackEnergy) che e' stato causa di un importante black out e l'attacco di qualche settimana fa alle aziende energetiche Israeliane, altrettanto pericoloso.

Un anno fa il Malware Carbanak e' entrato in modo subdolo attraverso un'attivita' di spear phishing nelle banche e si e' diffuso all'interno delle reti, rimanendo in ascolto per diversi mesi, fino all'attacco conclusivo sferrato nell'arco di una notte, che ha portato ad un potenziale danno di un miliardo di dollari.

Inoltre, mai come in questi mesi le minacce esterne vanno a sommarsi a quelle provenienti dall'interno dell'azienda, che siano involontarie o intenzionali.

Proprio per questi motivi l'approccio di Forcepoint risulta di grande interesse per i clienti, poiche' unisce le capacita' e le esperienze data-centric delle soluzioni storiche di Websense, tipicamente utilizzate nelle aziende del settore privato, ad un approccio molto spinto sull'analisi comportamentale, che deriva invece dall'approccio Raytheon, tipico del settore della difesa, fornendo cosi' alle aziende uno strumento completo e pervasivo che offria il meglio di entrambi i mondi.

La sicurezza nell'era del cognitive computing

di Nicoletta Armiraglio, Security Marketing Leader, IBM Italia

Per decenni siamo stati consapevoli della crescente rilevanza del cybercrime e delle sue implicazioni, ma mai come negli ultimi anni ci stiamo accorgendo della sua rapida evoluzione e trasformazione.

Oggi infatti la rivoluzione dell'Internet of Things, l'Indutry 4.0, i droni, le Smartcities, la robotica e la digitilazzazione che sta avvenendo in tutti i settori, hanno di fatto moltiplicato i punti di vulnerabilità del nostro sistema economico e sociale. In questo contesto gli hacker, che operano ormai da anni come vere e proprie organizzazioni a scopo di lucro, - si stima infatti che nel 2014 1 billion di record sia stato rubato (X-Force Threat Intelligence Quarterly 2015) generando più di $400B di profitti illegali (Center for Strategic and International Studies 2014) - sfruttano queste nuove vulnerabilità, aumentando così la pericolosità dei loro attacchi in termini di precisione ed efficacia.

Già nel 2014 i centri di ricerca IBM Security anticipavano alcuni trend rilevanti in ambito cybercrime (X-Force Threat Intelligence Quarterly 2016), quali ad esempio: Il superamento di ogni barriera geografica da parte degli attaccanti, un sempre più massivo utilizzo del Dark Web e di tecniche sofisticate di encryption, la nascita di nuove frodi per attuare nuovi schemi di pagamento e infine, la previsione che i dati biometrici diventeranno ben presto il nuovo target per i 'Bad Guys'. Tali trend non solo si sono materializzati ma hanno ad oggi superato ogni previsione. Basti pensare alle rapidissime evoluzioni che nel 2015 hanno avuti gli attacchi malware in ambito bancario, in vari paesi, dimostrando così come le organizzazioni criminali acquisiscono e spostano risorse da differenti parti nel mondo. Sempre nel 2015 abbiamo assistito anche all'aumento di incidenti caratterizzati da chiari effetti fisici scatenati da attacchi digitali. A dimostrazione del fatto che se ci eravamo abituati, parlando di cybercrime, a non considerare più le 'barriere geografiche' degli stati, oggi sono crollati anche i confini tra ciò che è digitale e ciò che è fisico.

Di fronte a tali trend è quindi evidente che la sicurezza informatica non può più prescindere da nuovi modelli di protezione integrati ed evoluti e da tecnologie ed esperienze all'avanguardia. In passato era sufficiente attuare difese statiche e perimetrali, e la sicurezza all'interno delle organizzazioni era spesso un esercizio di compliance. Oggi tale approccio non è più sufficiente: occorre mettere in campo una strategia di cybersecurity che consenta di creare un '**sistema immunitario**' di difesa, governato al centro dalla security intelligence. Ovvero da un sistema in grado di acquisire, normalizzare e analizzare, in tempo reale, i dati strutturati generati da utenti, applicazioni e infrastrutture. Fondamentali all'interno dell'infrastruttura di security intelligence sono i sistemi avanzati di analytics che, grazie alla capacità di analizzare enormi volumi di informazioni, sono in grado non solo di rilevare eventuali compromissioni in tempi rapidi, ma anche di ridurre i falsi positivi, risparmiando così tempo e risorse.

Se a tutti gli effetti nella sicurezza informatica abbiamo assistito al susseguirsi di due epoche distinte, quella dei 'controlli perimetrali' e quella più recente della 'security intelligence', oggi di fronte all'inarrestabile metamorfosi degli attacchi e a sempre più imprevedibili e nuovi metodi di elusione delle barriere difensive, per avere un reale vantaggio sul cybercrime e prevenire i danni, è necessario entrare in una nuova era della sicurezza informatica: l'era della 'cognitive security'.

La cognitive security, attraverso il recente annuncio di IBM Watson for Cyber Security, rappresenta una nuova frontiera tecnologica con la quale partendo dalla security intelligence e dai big data analytics, IBM Security sta formando una nuova generazione di sistemi in grado di comprendere, ragionare e apprendere le minacce in continua evoluzione. Con tali sistemi gli analisti avranno la possibilità di aumentare e persino automatizzare la loro comprensione di una minaccia, rendendo più rapida l'individuazione di connessioni tra dati, minacce emergenti e strategie correttive. Attraverso i sistemi cognitivi abbiamo infatti iniziato ad integrare comportamenti istintivi e competenze di sicurezza in nuovi strumenti difensivi, capaci di analizzare report di ricerca, testi web, dati sulle minacce e tutti i dati, strutturati e non strutturati, rilevanti per la sicurezza. Sarà possibile non solo analizzare i dati non strutturati – come blog, articoli, video, report, alert – che rappresentano oggi l'80% di tutti i dati presenti in internet e che non vengono intercettati dai sistemi di sicurezza tradizionali, ma anche elaborare in modo più rapido ed efficace il volume di dati immenso che ogni giorno gli analisiti security si trovano di fronte. Basti pensare che un'organizzazione di medie dimensioni deve valutare oltre 200.000 dati giornalieri relativi ad eventi di sicurezza e spendere, in media, 1,3 milioni di dollari all'anno solo per la gestione di "falsi positivi", sprecando oltre 21.000 ore di lavoro. Se a questo aggiungiamo oltre 75.000 vulnerabilità note in sistemi software, riportate nel National Vulnerability Database, 10.000 articoli e report pubblicati ogni anno e oltre 60.000 blog sulla sicurezza pubblicati ogni mese, si capisce quanto risulti impegnativo per gli analisti di sicurezza agire rapidamente e quanto nella lotta al moderno cyber crime sia imprescindibile avvalersi di tecnologie e competenze d'avanguardia.

2.Watson for Cyber Security will address the IT security skills gap of 1.5 million jobs by 2020, by augmenting the average analyst's capabilities to make sense of more than 200,000 security events a day.

3.To train Watson for Cyber Security, 15,000+ security documents will be fed to Watson each month, including reports and data from the IBM X-Force Exchange. A beta offering that infuses cognitive in QRadar is expected to be available later this year.

Robocop Vs Terminator
Un nuovo approccio alla Cyber Intelligence

L'esperienza pluriennale in tema di Offensive Security operata in contesti di alto profilo e security-critical ha permesso a InTheCyber di identificare alcuni fattori imprescindibili per ottimizzare le probabilità di riuscita di un attacco: tra di essi figurano la profilazione del target e l'ideazione e la conseguente adozione di una strategia di azione ad hoc. Noi crediamo che lo stesso genere di approccio debba essere utilizzato anche nel campo della Cyber-Intelligence.

In particolare, in questo specifico momento storico, la Cyber Intelligence, intesa come attività di reperimento di informazioni e monitoring tramite canali informatici, si trova a fronteggiare una tipologia di target nuovo, anomalo da un punto di vista di utilizzo del web.

In effetti, solitamente l'attività di Cyber Intelligence per il contrasto al del cyber-crime consta nello scovare informazioni nascoste negli angoli più remoti di Internet, spesso rovistando nei meandri dell'underground, siano essi forum chiusi o all'interno di hidden service in TOR. Ora invece, vi è la forte necessità di tracciare e monitorare le azioni sul web di una nuova tipologia di persone, che non si comportano secondo le usuali modalità dei cyber-criminali, ovvero non solo non nascondono le informazioni, ma cercano di condividerle il più possibile. Il riferimento va ovviamente agli adepti del cosiddetto stato islamico, che utilizzano i social network principali per effettuare una massiva azione di propaganda, necessaria per raggiungere quella massa critica di persone che possa costituire un sufficiente seguito al fine di attuare il loro piano di conquista. Questa grande diversità comportamentale porta a dover ridefinire le modalità con cui viene effettuato il monitoring, altrimenti si corre il grosso rischio di non riuscire a tenere efficacemente sotto controllo il fenomeno in oggetto.

Apparentemente, l'attività di intelligence diviene molto più facile, poiché l'informazione si trova con uno sforzo molto limitato. In realtà, si viene a generare un problema nuovo, ovvero la presenza di un surplus di dati che non danno reale valore aggiunto all'informazione. Il punto è che se da un lato può essere interessante verificare quante e quali persone siano simpatizzanti dello stato islamico o di gruppi radicali, dall'altro si rischia di perdere di vista l'obiettivo principale, che non consiste nell'effettuare un'analisi sociologica, ma nel verificare se qualcuno stia pianificando attentati.

Il problema dell'entropia causata da un surplus di dati non costituenti informazione è un problema molto serio nell'ambito di operazioni di Intelligence, poiché l'estrazione di ciò che rappresenta reale informazione nel mare magnum dei dati disponibili sul web è impresa davvero improba.

Per rendere l'idea dei numeri in gioco, si pensi che sul web risiedono circa 3.77 ZB di dati, ove uno ZB (ZettaByte) equivale a 1 migliaio di miliardi di GigaByte. Volendo circoscrivere l'analisi ai soli social network otteniamo comunque cifre astronomiche: a titolo di esempio consideriamo che ogni singolo secondo vengono pubblicati circa 7mila tweet, 50mila post su Facebook e 7 ore di video su YouTube.

Anche ipotizzando di poter analizzare tutti questi dati, riuscire ad estrapolarne informazione utile in modo completamente automatizzato salvaguardando un apprezzabile rapporto falsi positivi/falsi negativi, è problematica ardua da affrontare. Non esistono infatti delle "signature" per il linguaggio umano che identifichino una minaccia in modo sufficientemente preciso come avviene per malware ed attacchi informatici in genere.

Solitamente per risolvere questo genere di problemi si invoca l'analisi semantica come panacea di ogni male, mostrando come sia possibile distinguere l'utilizzo di una parola in una frase piuttosto che in un'altra. Ad esempio, con la semantica è possibile capire la differenza di utilizzo della parola bomba in frasi come "*A Parigi è esplosa una bomba*" o "Belen Rodriguez è una bomba".

Ma una frase tipo: "*Domani vado a mettere una bomba al parlamento*" è forse indice di un attacco imminente? Frasi come questa sono all'ordine del giorno al bar del paese, ove l'argomento di discussione può essere un ritocco dell'età pensionistica o l'inserimento del canone RAI in bolletta, e in quella sorta di "mega-bar" che è Facebook probabilmente verrà scritta da migliaia di persone al giorno. Oppure ancora: "*Oggi mi faccio saltare in aria*", è la frase di un kamikaze? Più probabilmente è la frase di una persona stressata dalla pesante giornata lavorativa.

Inghippi come questi possono far sorridere l'uomo, ma risulta estremamente difficile per la macchina dialogare con peculiarità linguistiche quali il sarcasmo o l'utilizzo di modi di dire e figure retoriche, senza considerare le complicazioni dovute all'utilizzo di particolari dialetti o alle difficoltà di traslitterazione e trascrizione fonetica di lingue come l'arabo, rappresentando quindi una seria difficoltà.

Questo è il punto, da un lato ho la necessità di reperire informazioni molto puntuali e precise, poiché ogni singola frase o commento potrebbero essere estremamente interessanti, dall'altro si rischia fortemente di rimanere schiacciati dai troppi dati, trovandosi in una condizione non dissimile dal non averli affatto.

Per questo a nostro avviso è necessario ricorrere ad un approccio diverso, che permetta di trovare solo le informazioni realmente utili, discernendole da tutto ciò che invece potrebbe generare solamente inutile entropia.

Per raggiungere tale obiettivo è innanzitutto necessario capire che un software non può e non deve sostituirsi all'operatore di intelligence, ma lo deve supportare,

aumentandone le capacità. Per fare un parallelo “fantascientifico”, il SW dovrebbe fungere più da esoscheletro per l’uomo anziché da robot indipendente.

È necessario infatti a nostro avviso demandare alla macchina quel lavoro che sa fare bene, ovvero compiere azioni velocemente, ripetutamente e instancabilmente, immagazzinando le informazioni utili identificate nel tempo, mantenendo invece nelle mani del cervello umano le responsabilità decisionali.

In quest’ottica, il SW deve aiutare l’operatore di Intelligence ad affinare le sue ricerche sulla base di informazioni già ottenute e validate, ove la validazione dell’informazione è un’operazione essenziale e delicata, che può fare solo l’uomo. Ad esempio, ad un certo istante di funzionamento del sistema, l’uomo può e deve decidere tra le informazioni individuate dallo strumento sulla base delle precedenti ricerche, che una specifica persona sia da monitorare, o che una specifica frase possa essere indice forte di appartenenza ad un gruppo e che quindi vada ricercata altrove, eccetera.

Affinché ciò avvenga in modo efficiente, il sistema può e deve avere memoria dello stato precedente e solo di quello, seguendo un processo che potremmo definire markoviano. In questo modo sarà possibile per l’operatore costruire una sorta di “percorso” che porta dalla conoscenza zero al raggiungimento dell’obiettivo, minimizzando il rischio di perdersi in una giungla di dati inutili che porterebbero fuori strada l’investigazione.

Ricapitolando, visto il differente approccio al web del nuovo target e la conseguente differente disponibilità dell'informazione che diviene enorme, occorre adottare un nuovo approccio nelle attività di intelligence, in cui l'informazione ottenuta possa essere consolidata tra varie fonti e validata dall’uomo in modo tale che essa possa essere utilizzata come base solida da cui identificare altra informazione utile, secondo un processo che potremmo definire markoviano. Per fare questo sono necessari nuovi software di supporto, che non analizzino big data per produrre altri big data, ma che permettano di districarsi tra i big data estrapolando i dati realmente interessanti da quelli che producono solo entropia.

IFI ADVISORY

INTELLIGENCE & FRAUD INVESTIGATION

Dopo l'Accordo sul nucleare: il nuovo cyber warfare iraniano

STEFANO LUPO

10 maggio 2016

IFI ADVISORY

INTELLIGENCE & FRAUD INVESTIGATION

Sommario

1. Approccio asimmetrico e Cyber Warfare....3
2. L'Iran nel contesto internazionale....5
3. Attacco e difesa Cyber nella logica strategica iraniana....7
4. L'accordo sul nucleare e il Cyber Warfare post sanzioni....12

1. Approccio asimmetrico e Cyber Warfare

La *information-dominance,* quella particolare congiuntura per la quale si dispone di una completa conoscenza dell'avversario mantenendo al contempo al riparo i propri dati sensibili più rilevanti, è al centro dell'analisi di John Arquilla[1], lo stesso autore, assieme a David Ronfeldt, di uno dei primi rilevanti studi sull'importanza del *cyberwar* nel contesto strategico.[2] Il dominio dell'informazione è una delle motivazioni cardine che spingono all'attività in campo cibernetico, specie per scopi riconducibili all'ambito bellico (*warfare*). E' certo che il *cyber warfare* si insinua nel quadro dell'*information warfare*, seppur in una nicchia di quest'ultimo, ma ben presentando quel duplice orientamento delle sue componenti basi, l'acquisizione e il diniego di accesso (assurance/denial) che fungono da piano principale di azione nel macro contesto informativo.[3] La conoscenza della rete, del *network,* abbinata alla capacità di controllo e comando, elementi fondamentali della *information dominance*, nello spazio cyber, inteso come quel network interdipendente di informazioni, infrastrutture tecnologiche (compreso Internet e le rete di comunicazione), sistemi computerizzati, quadri processuali e di controllo in siti industriali critici[4], acquista una valenza ancor più concreta.

Il *cyberspace*, ormai stabilmente considerato come quinto dominio dell'ambito bellico (congiuntamente alla terra, al mare, all'aria e allo spazio extra-atmosferico)[5], è il campo d'azione del *cyberwar,* da distinguere in maniera decisa dalla *cyber-criminality* e ancor più dal *cyber-terrorism* (sulla base degli obiettivi bersaglio dell'azione). Considerando gli episodi cyber storici fin qui corsi, come in Estonia nel 2007, in Georgia nel 2008 fino ad arrivare al grande caso di Stuxnet nel 2010 e confrontandoli con le analisi più rilevanti in materia[6], la valutazione di un *cyber attack* come di un atto tendente ad alterare, impedire o distruggere il corretto funzionamento sistemico di un computer o di un network o delle informazioni e dei programmi contenuti in essi, apre un interessato punto di indagine sulle caratteristiche precipue e sulla valenza internazionale dell'attività cyber e, in particolare, del *cyber warfare*, rafforzato dalla flessibilità, dal dinamismo e dai costi relativamente bassi del materiale necessario, in grado, tuttavia, di raggiungere una dimensione globale con una forza chiaramente moltiplicativa.[7]

1**John Arquilla**, "The Strategic Implication of Information Dominance", *Strategic Review,* Summer 1994.

2**John Arquilla, David Ronfeldt**, "Cyberwar is coming!", in *Comparative Strategy,* vol.12, N.2, Spring 1993, pp.141-165.

3NATO Allied Joint Publication (AJP)3.10, Allied Joint Doctrine for Information Operation, 23/01/2009

4"The White House Cyberspace Policy Review", 16 Maggio 2011 (NSPD-54/HSPD23), p.1

5US. Department of Defense, *The National Military Strategy for Cyberspace Operations,* 2006, p.3.

6Comm. On Offensive Information, Warfare, National Research Counil, Technology, Policy, Law and Ethics regarding US Acquisition and use of Cyber Attack Capabilities, 10-11 (2009)

7**C.S. Gray, G. Sloan**, *Geopolitics,, Geography and Strategy*, Cass, 1999, London, p.139

La valutazione dell'apporto cyber alle operazioni belliche standard, inquadrando l'apporto cibernetico come una sorta di moltiplicatore di potenza per le forze di superficie[8], si è concretizzata sia nella prassi storica sopra citata sia, ancor prima cronologicamente, nella ricerca di due generali cinesi sul contributo del *cyberspace* alle moderne sfide che un Paese si pone (si pensi alla lotta nell'Estremo Oriente per il possesso delle cosiddette "terre rare" o metalli strategici) [9] e su quali piani d'azione l'approccio cyber possa favorire un Paese rispetto a un altro. Accanto ai caratteri salienti dei punti di forza di un approccio cyber, quali l'assenza di impedimenti geografici-geopolitici e la rapidità di esecuzione, il dato rilevante risulta nell'analisi di chi si pone, sul piano internazionale, come *cyber-skilled*. La distribuzione delle sempre più riconoscibili *cyber-capabilities* evidenzia una propensione alla vulnerabilità agli attacchi non corrispondente all'attuale *status quo* per quanto concerne il livello di rilevanza internazionale di determinati attori globali, costruito, principalmente, attorno a misure ancora tradizionali come il potere militare ed economico. Questo elemento, unito a quello, dirimente, della possibilità di un uso sempre più marcato del cyber a scopo bellico per il sabotaggio o distruzione di infrastrutture, dati militari sensibili, congiuntamente alla creazione di confusione finanziaria[10], sembra essere alla base della marcata presa di coscienza dell'Amministrazione Obama per quanto riguarda il *cyberspace.*[11] La constatazione non potrebbe essere arrivata in un momento migliore, dal momento che molte delle potenze Cyber (Russia e Cina) o di quelle emergenti (Corea del Nord e Iran soprattutto) sono attori internazionali che non mirano al mantenimento dello *status quo* o, in alcuni casi- come per l'Iran- che aspirano al ruolo di potenza regionale[12], alimentando potenzialmente il clima di instabilità globale.

Le particolari caratteristiche del *cyberwar* ne fanno strumento gradito e congeniale per quei Paesi, non di primissimo piano, che sfruttano le peculiarità asimmetriche del *cyberspace*, che favoriscono l'attaccante rispetto al difensore, in termine di tempi e di costi di reazione, il tutto in un clima di incertezza che risulta più adatto a quegli attori in grado di non seguire necessariamente i rigidi canali della diplomazia o dei percorsi decisionali democratici nell'assunzione di determinate importanti prese di posizioni. La manifesta duttilità dell'approccio cyber, ben integrabile con vere e proprie azioni belliche cinetiche (come nel caso della preventiva manomissione dei radar siriani da parte di Israele prima del bombardamento di siti nucleari nel 2007), lo rende centrale nelle cosiddette *blended menace* (minacce miste) e richiede, nel contempo, un'assoluta capacità di resistenza, la

8**A. Fitsanakis,** "Cells Wars: the Changing Landscape of Communications Intelligence", RIEAS Research Paper, n.131, Maggio 2009

9Gen. **Qiaoling & Xiangsui**, *Unrestricted Warfare*, Beijing, 1999.

10Press Release, John Chipman, Dir-Gen &Chief Ex. International Institution for Strategic Studies, Military Balance 2010-Press Statement (feb.3 2010).

11The White House National Security Strategy 27 (2010).

12**Choe Sang-Hun & John Marxoff**, *Cyber Attacks Jam government and Commercial Web Sites in the US and South Korea*, New York Times

cyber deterrence[13], cioè un insieme di programmi, network, prassi e controlli, capace di minimizzare la minaccia cyber che poggia su costi bassissimi, soprattutto di *entry*, capacità di proliferazione indiscriminata (come si vedrà analizzando STUXNET), rapida possibilità di creare incertezza, anonimato e riequilibrio tra grandi e piccole potenze, con le prime (come gli USA) sfavorite in un diretto scontro cibernetico con medi attori internazionali, che meno hanno da perdere, in termini di strutture finanziarie, connessioni economiche, quadro amministrativo, come nel caso dell'Iran. In ultima istanza, si presenta come una reale possibilità operativa anche per i movimenti insurrezionali o gruppi della cosiddetta "società civile" che mirano a sovvertire lo status quo del proprio Paese[14], partendo dalla facilità di comunicazione, permeazione pressoché globale, accelerazione degli eventi e, in definitiva, il ruolo di "moltiplicatore di forza" che il cyber permette di dispiegare[15].

2. L'Iran nel contesto internazionale

Gli eventi intercorsi nel primo decennio del XXI Secolo in Medio Oriente, dall'attacco all'Afghanistan nel 2001 come conseguenza dell'atto terroristico delle Torri Gemelle dell'11 Settembre 2001, e l'invasione dell'Iraq di Saddam Hussein da parte di forze statunitensi, due anni dopo, hanno permesso all'Iran di un'importanza strategica di primo ordine, rafforzata anche dalla sovrapposizione sull'area geografica iraniana di due nevralgici punti d'interesse: all'*Hearthland* di Makinder, quell'area del Centro-Asia in grado di determinare gli equilibri e i domini mondiali e della quale l'Iran rappresenta la naturale porta di ingresso, si è andato a sovrapporre una sorta di *Heartsea* rappresentato dall'Oceano Indiano, dopo lo storico passaggio di potere dall'Oceano Atlantico in conseguenza del termine della guerra fredda e il *Rimland* di Skypman, la costa asiatica dell'Oceano Indiano stesso. Tale contingenza ha reso l'Iran il crocevia per eccellenza tra il grande Est Asiatico alla ricerca di fonti energetiche (Cina e India), con il serbatoio d'energia mondiale (Medio Oriente) e le grandi rotte verso il commercio mondiale attraverso i choke-points di Suez e del Capo di Buona Speranza (Europa e Americhe).

La rilevanza geopolitica, abbinata alla particolarità strutturale dell'Iran quale Repubblica Islamica, sciita duodecimana e a forte carico di ostilità nei confronti dei vicini che ne minacciano l'ascesa regionale, o meglio, la ripresa di quel ruolo di potenza regionale sempre detenuto dalla Persia, rende l'Iran una delle principali faglie di crisi del pianeta. Da un lato l'Arabia Saudita e i Paesi principali del Golfo Persico e membri del Gulf Cooperation Council (Bahrain, Qatar, Emirati Arabi, e in minima parte Oman) contestano

13**Trevor Moss**, "Is the Cyber War the New Cold War?" *The Diplomat*, 19 /04/2013.

14 **David J. Betz**, "Cyberspace and Insurgency" in **P.B.Rich, I. Duyvesteyn**, *The Routledge Handbook of Insurgency and Counterinsurgency*, London, New York, 2014.

15 **S. Livingston**, "Claryfing the CNN effect", Research Paper-18, Shorenstein Centre, Harvard University, 1997.

il ruolo iraniano sia in termini di leadership regionale sia come concausa dei disordini religiosi tra le due principali correnti musulmane. Dall'altro Israele continua a sentire come minaccia forte alla propria esistenza la possibilità che l'Iran si doti di armamento nucleare, nonostante l'Accordo implementato il 16 gennaio 2016 *(Joint Comprehensive Plan of Action)*, anzi ora più che mai, oltre alla continua azione destabilizzante persiana.[16] Analizzando il contesto e, di conseguenza, l'approccio strategico iraniano, si individuano situazioni di contrasto posizionate a distanza variabile dall'epicentro rappresentato da Teheran. Minacce interne, prossime, a media distanza, lontane, investono il regime degli Ayatollah, implicando diversi gradi e livelli di risposta da parte dell'establishment al potere. Ridottosi apparentemente e forse solo temporaneamente il grande "cappello di crisi" rappresentato dalla questione del nucleare iraniano, non sono da sottovalutare le crescenti interazioni di Teheran con la faglia di crisi principale presente al momento in Medio Oriente, vale a dire la guerra civile siriana, nella quale l'Iran si è posizionata, come era prevedibile, a fianco del regime governativo alawita di Bashar al-Assad, con la collaborazione, secondo i rispettivi livelli di interesse, di Russia e Cina. La minaccia rappresentata per la sicurezza di Teheran da parte dell'azione del sedicente Stato Islamico in Siria e Iraq ha dato modo di credere a una possibile, momentanea convergenza di interessi tra Iran e Stati Uniti, sebbene rimangono molte questioni e punti di divergenza, a partire dal futuro del Presidente Assad, all'auspicabile fine della minaccia dello Stato Islamico e del conflitto civile in Siria, che va avanti dal 2011. Altri dossier, inoltre, rimangono sul tavolo. Determinate congiunture rendono il contesto iraniano ancora instabile e temuto da attori regionali di primaria importanza, come Israele e Arabia Saudita, alleati sempre più scontenti di Washington. L'appoggio mirato ad Hamas e Hezbollah tra Palestina e Libano permette all'Iran di mantenere Israele in un perenne stato di tensione. In seconda battuta, la poco lungimirante azione americana dell'invasione dell'Iraq nel 2003, in una visione geopolitica di medio periodo, ha creato un vacuum politico religioso che sta premiando sempre più la forte componente sciita irachena, naturalmente e solidamente collegata e alleata al regime di Teheran, tassello fondamentale per la realizzazione di un collegamento strategico tra la capitale iraniana e il fronte Mediterraneo, passando appunto per l'Iraq, la Siria e il Libano, la cosiddetta mezzaluna sciita, unica vera proiezione di potenza, non solo economica, per il Paese persiano.

L'Iran, infatti, fin dal 1979, data dalla Rivoluzione che ha detronizzato lo Shah Reza Palhavi, e che quasi immediatamente ha preso una connotazione prettamente islamica, è dominato, sotto il profilo della sicurezza, da una costante sindrome di "accerchiamento" da parte di attori dotati di netta superiorità bellica. La strategia cardine delle forze iraniane per preservare la sicurezza nazionale ha dovuto necessariamente orientarsi sul contenimento della possibile minaccia esterna attraverso un'azione di deterrenza (quasi unicamente perseguibile attraverso modalità tipiche dell'asymmetric warfare.[17] La Repubblica Islamica dell'Iran, come si avrà modo di constatare nel corso della trattazione, è tutto fuorché un player geopolitico irrazionale: come attore geostrategico e geopolitico,

16 Comprehensive Plan of Action Joint Comprehensive Plan of Action, U.S. Department of State.

ha dimostrato più volte di essere in grado di adattare il proprio credo, politico, militare, culturale, alle contingenze del momento storico, dalla Rivoluzione alla guerra con l'Iraq tra 1980 e 1988, dalla prima guerra del Golfo del 1991 fino all'invasione dell'Iraq nel 2003, senza venir meno all'obiettivo primario dello Stato. Esso si può ben definire come la sua sopravvivenza, declinabile sia nel perpetuarsi del regime al governo, sia nella vera e propria continuazione fisica dello Stato stesso, inteso come tale (governo, territorio, cittadini). In tale contesto, l'arma relativamente nuova del cyber rappresenta una linea di azione assolutamente spendibile dall'Iran, sia sotto il profilo del *cyber espionage*, sia sotto quello dell'attacco vero e proprio, all'esterno o all'interno dei propri confini, aspetto decisamente prioritario per la tenuta del regime iraniano.

3. Attacco e difesa Cyber nella logica strategica iraniana

Il fronte interno resta la vera spina nel fianco, il settore concreto in cui l'Iran deve affrontare le problematiche più incombenti, in termini di prossimità geografica e di impatto effettivo sulla stabilità di governo, come le rivolte post-elettorali del 2009 e la repressione stringente hanno dimostrato, prima dell'elezione alla presidenza della Repubblica Islamica di Hassan Rouhani nel giugno 2013. Rouhani, infatti, conservatore pragmatico, è ben voluto dalla Guida Suprema Ali Khamenei, oltre che "apprezzato" per l'avvio di un'operazione, primariamente di immagine, che possa consentire all'Iran di muoversi sul piano internazionale in una condizione di isolamento inferiore rispetto a quello generato dalla Presidenza di Mahmoud Ahmadinejad. Si vedrà e si analizzerà come proprio le skills e l'expertise elaborate in termini di counter-revolution e di anti-rioting da parte degli organismi militari e di controllo del regime iraniano siano base fondante del crescente interesse di Teheran per le tecnologie cibernetiche e le applicazioni concernenti il monitoraggio della popolazione mediante ispezioni cyber e tracciabilità del malcontento tramite gli strumenti informatici. L'esperienza e la competenza guadagnate in ambito interno sono state e continueranno ad essere il motore della *cyber capability* iraniana anche sul fronte estero, ulteriormente stimolato da cyberattacks di grande impatto e clamore internazionale, come STUXNET, Flame e DuQu sono effettivamente risultati essere. A tutto questo si deve consapevolmente affiancare lo studio dell'asymmetric warfare, archetipo delle specificità iraniane nelle condotte belliche in campo terrestre e navale e perciò adatto, come si è visto, a prestarsi ad azioni cyber.

Il travagliato rapporto tra Media, Internet e popolazione in Iran si riflette ampiamente nella criticità periodiche quali le tornate elettorali, i commenti post-voto e le rimostranze pubbliche, quando cioè il livello di resistenza del regime raggiunge picchi di rilevante sforzo. Prima ancora di subire in pieno l'offensiva cibernetica rappresentata da STUXNET, Flame e DuQu, quindi l'azione combinata israelo-americana, l'entourage iraniano di

17 Asymmetric Warfare: scontro bellico tra due o più schieramenti i cui pesi militari o le strategie e tattiche, differiscono notevolmente (es: esercito regolare contro movimento di guerriglia).

vertice sperimentava un forse ancor più pericoloso attacco alla stabilità nazionale. Sin dalla fine del 2008 il corpo paramilitare governativo Basji e la Guardia della Rivoluzione (Sepah-e Pasdaran) avevano lanciato lo slogan dei "10000 blogs" al servizio delle idee della Repubblica Islamica, mentre nel marzo 2009 i reparti cibernetici dei Pasdaran individuarono l'utilità di un sistema, denominato Gerdab (vortice) capace di raccogliere foto e dati di eventuali arrestati e di pubblicare tali informazioni. Nelle rimostranze seguite alle proteste circa i brogli della rielezione di Mahmoud Ahmadinejad e nella conseguente dirompente esplosione del movimento dell'"Onda Verde" che chiedeva un cambiamento sostanziale, Gerdab non ha tardato ad essere utilizzato come lista online degli arrestati dai reparti di sicurezza. "Il monitoraggio della situazione nazionale tramite gli strumenti informatici è costante" sosteneva il Professor Abdolmohammadi dell'Università di Genova, intervistato nel 2013.[18] La capillarità del controllo da parte del FATA[19] dei siti sensibili durante l' "Onda Verde", come "mowjcamp.com", "radiozamaneh" si estrinsecava anche nella raccolta delle mailing list con i dati sensibili e, tramite attività di *political hacking* (hacktivists), nella manomissione vera e propria di alcuni siti riconducibili all'Onda Verde, come Jarash e Kalameh, e il vero e proprio hacking, il 18/12/2009, di Twitter, colpevole di essere la principale piattaforma di veicolo delle idee dei manifestanti.[20]

L'annuncio della Guida Suprema Khamenei, nel febbraio 2012[21], della costituzione di un *Supreme Cyber Council* e lo stanziamento complessivo di circa un miliardo di dollari negli ultimi cinque anni (a partire dal giugno 2011) allo scopo di finanziare l'elaborazione di nuove tecnologie e l'educazione del capitale umano, sono solo due delle numerose dimostrazioni della centralità assunta dal cyber in Iran. [22] I motivi del successo della *cyber technology* sono ascrivibili alla predisposizione iraniana, alla discreta presenza di una solida componente scientifica e soprattutto all'attenzione posta dal regime verso due principali direttive: la protezione tecnologica delle principali infrastrutture critiche del Paese da eventuali virus sul modello del passato STUXNET e la possibilità di interdire l'attività cyber dannosa per il regime proveniente sia dall'esterno sia, soprattutto, dall'interno del Paese.

Una volta scoperta la concreta pericolosità di un *cyber attack,* l'Iran ha iniziato a lavorare per migliorare la propria capacità di difesa in ambito cyberspace e ad effettuare attività d'intelligence per radunare le migliori potenzialità, anche a scopo offensivo. Il programma

18Intervista al Professor Pejman Abdolmohammadi, Università di Genova, 30/03/2013

19 "The Police for the Sphere of the Production and the Exchange of Information". Il capo della divisione cyber della polizia è stato sostituito dopo la morte, in carcere, del noto blogger attivista Sattar Behesti, il 3 novembre 2012, mentre era in stato di fermo in prigione.

20Ibidem.

21**Emily Alpert, Ramin Mostaghim**, "Iran's Supreme Leader calls for New Internet Oversight Council", Los Angeles Times, //03/2012.

22**Gabi Siboni & Sami KronenFeld** : " Iran and Cyberspace Warfare", Military and Strategi Affairs, v.4, n.3, Dec.2012

difensivo appare strutturato su un duplice livello: di prevenzione di nuovi attacchi (STUXNET) e di penetrazione d'intelligence (Flame e DuQu), congiuntamente a un'intensa attività di sostegno al regime attraverso sistemi di sorveglianza e di blocco delle informazioni.[23] Sul piano offensivo, la strategia cyber viene impiegata come elemento cardine della dottrina bellica asimmetrica e come strumento adatto a portare un significativo danno al nemico pur in condizioni di inferiorità geostrategica. [24] Se cruciale diventa la partership tecnologica con Paesi all'avanguardia nel controllo del dissenso, e la fornitura di sistemi ZMXT di sorveglianza della cinese ZTE Company ne è la riprova più concreta[25], fondamentale è la formazione dei quadri dirigenziali scientifici del comparto cyber che in Iran trova la sua naturale base negli Istituti e Università tecnologiche come la "Sharif University Technology" a Teheran, l'"Amkabir University", specializzata in *data security*, ma che giustamente non disdegna il finanziamento di compagnie private a partecipazione statale (principalmente del Ministero della Scienza) quali l'"Iran Telecommunication Research Center" o addirittura la realizzazione di parchi tecnologici per lo sfruttamento dell'economie di scala, come il "Pardis Technology Park", istituito a partire dal 2001, e il "Guilan Science and Technology Park", a supporto delle start up.[26] La base tecnologica fornita dai centri studi per l'elaborazione tra gli altri, di un programma di filtro dei dati di nome SEPAR e del ben più ambizioso programma, comunicato ad agosto 2012 dal ministro delle Comunicazioni Reza Taghipour, della realizzazione imminente di un proprio network internet controllato e indipendente da azioni esterne (nominato Halal)[27] , va di pari passo con la creazione e la ramificazione di corpi cyber autonomi ma interfacciati, in grado di ricoprire tutti gli incarichi di *surveillance & security* richiesti. A tal proposito, la realizzazione di un " National Cyber Center" risponde alla necessità di un organismo tecnico di coordinamento di tutte le attività cyber e di monitoraggio del "Cyber Council", che determina principalmente la politica cyber nazionale, lasciando a organismi tecnici come lo "Cyberspace Defense Command", che opera nel contesto della Difesa Passiva iraniana nel quadro dello Staff generale delle Forze Armate, l'elaborazione delle dottrine difensive per le Istituzioni nazionali assieme al Maher, il " Center for Information Security".[28]

A livello di *intra-iranian cyber activity,* il controllo più ramificato e capillare è attuato da due delle principali istituzioni cyber del Paese, vale a dire dal "Comittee to Identify Unauthorized Websites", istituito nel luglio del 2009, di cui fanno parte vari ministeri e soprattutto il Procuratore Generale e il capo della polizia, e dalla *cybercrime unit* della

23**Art Keller,** "The Greater Persian Firewall", *Foreign Policy,* Sept 2012, p.28.

24**Brian Ross**, "What will happen to Usa, if Israel Attacks Iran?" ABC News 5 Marzo 2012.

25**Steve Stecklow**, "Chinese firm helps Iran Spy on Citizens", Reuters, 22 Marzo 2012.

26 **Reza Marashi**, "The Islamic Republic's Emerging Cyberwar", National Iranian American Council, April 30/2011.

27 **Robert Tait**, "Iranian State Goes offline to dodge Cyberwar", The Telegraph, 5/8/2012.

28 "Iran is Formulating Strategic Cyber Defense Plan: Official", *Tehran Times*, 15 Giugno 2012.

polizia stessa, denominata FATA, predisposta soprattutto per contrastare i crimini cyber contro la sicurezza del Paese e per il monitoraggio di tutti i cyber nauti iraniani e colpevole in numerosi casi della morte di dissidenti[29].

L'impianto difensivo viene completato dai centinaia di blog gestiti da hackers affiliati al regime il cui ingaggio è diretto incarico del "Basji Cyber Council", che si occupa inoltre dell'inserimento di propaganda filo-governativa nei siti e sui media nazionali[30]; questo fatto dimostra la predisposizione del regime di Teheran a utilizzare, a fianco di organismi strutturati e istituzionalizzati, anche componenti autonome apparentemente prive di controllo ma capaci, proprio per il maggiore spazio di manovra a disposizione, di rendersi ancora più efficaci nelle singole *cyber operations*. Tale approccio è ancora più evidente se si analizza la componente predisposta all'offesa cibernetica, nella quale la Guardia della Rivoluzione ha il ruolo principale.[31] Le unità cyber dei Pasdaran sono predisposte principalmente allo sviluppo di software infetti progettando serie di codici malevoli, allo sviluppo di strumenti informatici adatti alla penetrazione cibernetica e a meccanismi di disturbo[32]. A tali unità va riconosciuto il merito di aver realizzato un sistema elettronico capace di bloccare i radar e le comunicazioni, segno dell'elevato sviluppo scientifico delle *cyberwarfare units* dei Pasdaran[33], il cui compito comprende però anche il coordinamento e l'*outsourcing* di hackers con compiti di offesa in ambito internazionale, di cui l'" Iranian Cyber Army" e l'" Ashiyane Digital Security Team" (famosa per l'inserimento di propaganda filo-iraniana sul web israeliano) e l'"Izz al-Din Al-Qassam Cyber Space Fighters" (il gruppo dell'attacco alla "Bank of America") sono gli esempi più conosciuti.[34] Ai gruppi più o meno istituzionalizzati si affiancano, necessariamente, le norme giuridiche e i quadri normativi preposti a proteggere l'impianto portante della Repubblica Islamica, ossia le istituzioni portanti del regime stesso. In quest'ambito si situa da tempo, oltre a tutta la riforma informatica predisposta per la modifica dei motori di ricerca e dei *web videos*, anche un controllo capillare di tutti i cyber cafès presenti nel Paese, numerosissimi, sia attraverso la registrazione dei dati anagrafici degli utilizzatori, sia attraverso un sistema di ripresa a telecamere a circuito chiuso da installare all'interno degli esercizi.[35] A completare il già strutturato piano cibernetico iraniano concorre la forte collaborazione, già citata in precedenza riguardo la Cina, con le macro realtà internazionali della

29 "Iran To Crack down on Web Censor-Beating Software", Hurriyet Daily News, Sept. 22/2012.

30 **Golnaz Esfandiari**, " Iran's Paramilitary Militia is recruiting Hackers", Forbes, 12/01/2011

31 **Iftadi Ian Amit**, "Cyber Crime War", Paper Presented at Defcon\18 Conference, 31/7/2010.

32 Iranian Internet Infrastructure and Policy Report, Small Media Report, novembre 2014.

33 **Frank, J. Ciluffo**, "The Iranian Cyber Threat to the US", Statement before the US Chamber of Representatives, 26 Aprile 2012.

34 **Scott Peterson**, "Iran Cyber Prowess: Could it really have cracked Drone Codes?" Christian Science Monitor, 24/04/2012.

35 Iran begins filter "Internet Access" BBC Monitoring International Reports, 12 Maggio 2003.

programmazione cyber e dell'elaborazione software, quali Russia e Cina, oltre allo studio delle tecniche di repressione del dissenso attraverso la manipolazione della strumentazione tecnologica tramite partnership con la Corea del Nord. Fin dai primi anni 2000, ad esempio, la collaborazione scientifico-accademica tra Iran e Russia è molto forte, come dimostrano la frequente partecipazione di studenti dell'Accademia delle Scienze dell'Iran a corsi in Russia[36] e sempre il Cremlino si è reso fortemente partecipe della crescita tecnologica dell'Iran, sia con la partecipazione di propri scienziati in siti nucleari sensibili come Busher e Natanz, sia con la costruzione del Satellite per le telecomunicazioni Zoreh.[37] Non può infine mancare un solido legame tecnologico tra l'Iran il subcontinente indiano, uno dei fari nel processo di sviluppo software, divenuto particolarmente importante per l'Iran in seguito all'embargo occidentale, che ha coinvolto inevitabilmente anche la componentistica informatica.[38]

L'attività cibernetica di hacking è stata anche subita, dal regime, a dimostrazione del livello di guardia sempre altissimo che le istituzioni cyber del regime devono mantenere in ogni istante, come ben hanno appreso elementi dei Basji, quando nel 2010 hanno realizzato che un proprio sito (moghavernat.ir) era sotto attacco della Green Cyber Army, riconducibile alla dissidenza. [39] Per questa e per altre dinamiche l'"Iranian High Council Of Informatics" ha evidenziato 543 compagnie informatiche da monitorare e ha plaudito alla realizzazione, *in fieri,* nel dicembre 2012, di Mehr, una sorta di Youtube locale, totalmente rispondente ai desideri del regime.[40] L'asse inevitabile di scontro cibernetico è e risulta essere il triangolo USA-Iran-Israele, con il Paese persiano costretto a correre ai ripari per sostenere la superiorità tecnologica e di inventiva dimostrate dal 2008 ad oggi da parte del Cyber Command americano e dalla celebre unità 8200 dell'Israel Defence Force, adibita alla *cyberwar.* Nel macro contesto dell'ostilità israelo-americana per la pretesa aspirazione iraniana a dotarsi di energia nucleare, con possibili risvolti bellici, si insinua il lungo mirato disegno americano di attacco cibernetico alle strutture iraniane del caso. L'obiettivo dell'Operazione "Olympic Games", ideata già nel 2006 dall'Amministrazione Bush ma portata avanti, dopo averla sposata appieno, da quella Obama, era quello di costringere il governo iraniano, con ripetuti attacchi ai quadri tecnologici e alla strumentazione del caso, a rinviare sine die il programma nucleare.[41] L'operazione era stata inizialmente decisa come un'azione integralmente e unicamente americana, ma le

36 **Alexei Kravchenco,** "Russia-Iran Cooperation is not a Tactical Move", TASS, March 2001, p.2

37 "Iranians Inspect Ruddis Telecom Plant", Asia Pulse (Mosca), 1/06/2001.

38 "Iran: President Khatami visits Information Technology Center in India" Financial Times Information, BBC Monitoring International Reports, 28/01/2003.

39Ibidem.

40**Golnaz Esfandiari**, "Iran developing smar control" Software for Social Networking Sites", *Radio Free Europe/Radio Liberty*, 5 Gennaio 2013.

41**David E. Sanger**, "Obama Order sped up wave of Cyberattacks against Iran", NYT, 1/06/2012.

continue minacce di azioni unilaterali israeliane nei confronti dei siti iraniani presto convinsero le amministrazioni americane a integrare anche i quadri di Tel Aviv, per renderli consapevoli e partecipi, di questo nuovo approccio bellico nei confronti di Teheran che presentava indubbi risvolti positivi. Ecco che il *malware* STUXNET, indirizzato alla manomissione delle centrifughe della centrale di Natanz ed entrato in azione nel finale del 2009 come *computer worm*[42] grazie al contagio tramite chiavetta USB(prima immune a qualsiasi visualizzazione esterna perchè presente solo a Natanz, poi improvvisamente propagatosi ad altri terminali simili a quelli di Natanz, di produzione Siemens, in Europa e in Asia e scoperto nel febbraio 2011 dalla società Symantec) viene seguito concettualmente da Flame, un *data mining virus* capace di rubare qualsiasi informazione trascritta in byte, virus anch'esso scoperto da una società d'analisi informatica, la bielorussa Kasperski, collaboratrice dell'International Telecomunication Union (ITU) e da DuQu, costruito su parte della base dati di STUXNET, un pericoloso *reconaissance virus*, pressochè invisibile e capace di aprire numerose *backdoors (*faglie per entrare nel sistema) di numerosi impianti informatici.[43]

Complessivamente l'operazione "Olympic Games" si può considerare solo un mezzo successo: essa ha effettivamente compromesso per alcuni anni alcune centrifughe dell'impianto di Natanz, ma ha oltremodo innalzato l'asticella dello scontro cibernetico, che Teheran viveva, fino al 2009, come un *affaire* interno per monitorare la propria dissidenza. Così le squadre cibernetiche iraniane, una volta raggiunta una certa soglia di padronanza tecnologica, hanno portato a termine una serie di *cyberattacks* prima nei confronti di due *data security companies* nel 2011 (caso Diginotar e Comodo)[44], poi, nel 2012, in rapida successione nell'Agosto 2012 il virus "Shamoon", rozzo ma efficace, ha condotto un attacco coronato dal successo contro i *company operational and control systems* della compagnia petrolifera Saudita Aramco e della compagnia di gas naturale del Qatar Resgas[45] in rappresaglia al contributo saudita e dei Paesi del Golfo alla causa ribelle siriana osteggiata dal filo-iraniano governo di Al- Assad. Neanche un mese dopo, nel settembre 2012, gli Al-Qassam Cyber Fighters, con il pretesto dell'ingiuria all'Islam da parte della pellicola americana "The Innocence of Muhammad" hanno attaccato alcune istituzioni finanziarie americane, quali la Bank of America, Morgan Chase, Citi Group (operazione Ababail), con il vero e dichiarato obiettivo di attuare una ritorsione per le sanzioni comminate al regime di Teheran.[46] L'escalation cibernetica innescata da "Olympic Games", per quanto è noto, ha inasprito il rapporto con Teheran anche sul piano tecnologico,

42**James Farwell & Rafal Rohozinski** (2011): Stuxnet and the future of Cyberwar", Survival: Global Politics and Strategy, 53: 1, 23-40

43CSIS- Middle East Program- Cyber Conflict In the Gulf, Nov. 14/2012.

44**Eva Galperin, Seth Schoen, Peter Eckesley**; "A Post Mortem On the Iraniana Diginotar Attack", Electronic Frontier Foundation, Sep.13 2011

45J**im Finkle, "**Exclusive: insiders suspected in Saudi Cyber-Attack", Reuters, 7/09/2012.

46**Gerry Smith**, "Cyber Attacks Against US Banks Sponsored by Iran, Lieberman Says," Huffington Post, 09/09/2012.

portando sì qualche risultato di breve periodo ma anche causando, ad ampio spettro, alcuni scivoloni come l'abbattimento di un drone da ricognizione americano RQ 170 in volo da Kandahar in Afghanistan sui cieli iraniani, si pensa per un riuscito *cyberattack* di manomissione dei codici di volo del drone da parte delle *cyber units* iraniane, un risultato ancor più peggiore per gli americani perché nell'Aprile 2012 la Guardia della Rivoluzione ha confermato la decodifica dei dati contenuti nel drone.[47]

4. L'accordo sul nucleare e il Cyber Warfare post sanzioni

Sono sensibili le preoccupazioni di quanti avversano l'accordo JCPOA (Joint Comprehensive Plan of Action) raggiunto il 14 luglio 2015, poi implementato il 16 gennaio 2016, dal gruppo detto dei P5+1 (USA, Regno Unito, Cina, Russia, Francia, più la Germania) con l'Iran e la partecipazione dell'Unione europea. Fra queste, vi è quella di un Iran favorito non solo dalle condizioni che ritardano, sì, il suo programma nucleare, senza tuttavia interromperlo, ma anche dalle positive ricadute economiche che, come si vedrà, potrebbero portare a un effetto cascata per le casse di Teheran, dopo circa 6 mesi di attento monitoraggio degli obblighi imposti al Paese persiano dal JCPOA stesso. Ad esse si combina inoltre la forte pressione dei Paesi europei che, come Italia, Francia, Germania e Regno Unito, ben più degli Stati Uniti sono desiderosi di riprendere il forte legame commerciale con l'Iran. Dati inequivocabili dimostrano come dopo neanche 6 mesi dall'implementazione del JCPOA, l'export petrolifero iraniano, prima frenato dalle sanzioni, sia aumentato del 90%, conferendo una proiezioni, ai prezzi petroliferi attuali, di circa 21 miliardi di dollari di entrate entro la fine del 2016. A questi, si vanno ad aggiungere, all'incirca, 100 miliardi di dollari precedentemente congelati nel mercato internazionale (frutto dell'export iraniano pre sanzioni) che, come detto sopra, dovrebbero essere destinati a Teheran qualora, dopo sei mesi dall'implementazione del JCPOA, i controlli internazionali evidenziassero il corretto rispetto dell'Iran delle misure imposte dall'accordo sul nucleare[48]. L'amministrazione Obama, negli USA, è particolarmente sotto attacco, nel clima pre elettorale per le presidenziali, da parte dei policy makers repubblicani, che l'accusano di eccessiva accondiscendenza nei confronti del regime degli Ayatollah, che anzi, avrebbe chiesto ulteriori facilitazioni, come l'accesso, almeno parziale, al sistema finanziario americano, fin qui ancora interdetto all'Iran[49].

E' ritenuto molto probabile, dati alla mano, come il JCPOA, tra concessioni e facilitazioni annesse, possa portare a Teheran, entro la fine del 2016, quasi 130 miliardi di dollari. Una

47 **Ilan Berman**, "The Iranian Cyber Threat to the US Homeland", April 26, 2012, Statement Before the House of Representatives.

48 A Nuclear Deal with Iran. Managing the Consequences. Reports of the American Foreign Policy Council Task Force, Ottobre 2015.

49 **I.Berman**, "Obama's Iran Sanctions Bait-and-Swifth", *National Review Online*, 5 Aprile 2016

cifra che rappresenterebbe circa ¼ dell'intero Prodotto Interno Lordo (PIL) iraniano del 2014 (415 miliardi di dollari), iniettando nel sistema economico persiano le liquidità necessarie per l'aumento del PIL di circa 2,6% per il 2016, e di circa il 4% per il 2017[50]. Per un Paese come l'Iran, rimasto isolato per anni e soprattutto obbligato, per i suoi dettami strategici, a continui finanziamenti alle sue principali proxies nell'area del Medio Oriente (100-200 milioni annui a Hezbollah, 10 ad Hamas, 2 al Jihad Islamico Palestinese), il flusso monetario rappresenta l'opportunità di ammodernare le proprie infrastrutture, a partire da quelle del settore delle telecomunicazioni, ancora ampiamente obsolete e ovviamente del comparto cyber. A beneficiarne, inoltre, sarebbero quei colossi e conglomerati economici, come Khatam-al-Anbiya, attivo soprattutto nel settore delle costruzioni, controllato dal corpo dei Pasdaran e principale punto di inserimento e di ramificazione del corpo stesso all'interno del sistema commerciale iraniano[51].

Come si inserisce questa, si pensa, positiva congiuntura economica, nell'arco del quadro strategico iraniano e, più precisamente, all'interno del programma cyber di Teheran? La situazione complessiva nella regione (crisi siriana, confronto in Iraq, presenza dello Stato Islamico, tensione continua con Israele, plurimo scontro con l'Arabia Saudita, a partire dal fronte dello Yemen) non permette di dire che l'Iran abbandonerà, alla luce delle facilitazioni e dell'accordo JCPOA, la sua politica assertiva, che gli impone un ruolo da potenza regionale. In tale ottica, il contributo dato dal cyber, a partire dalle possibilità concesse al gruppo Basji di permeare con politiche di propaganda scenari come Siria e Iraq per raccogliere, tramite mirato indottrinamento, un maggior numero di adesioni alla causa sciita[52], è considerato vitale. Dall'elezione di Hassan Rouhani, nel giugno 2013, ad oggi, inoltre, la cyber confrontation tra Iran e il resto del mondo, a partire dagli USA, da Israele e dall'Arabia Saudita, non si è affatto spenta, anzi. Ha assunto connotazioni ben specifiche che permettono, forse, di comprendere quale possa essere un probabile scenario di medio periodo sul piano cyber.

Due sono i principali episodi da esporre per meglio comprendere la dimensione dello scontro cyber e, quindi, i possibili risvolti del confronto cibernetico tra l'Iran e i suoi principali competitors nel periodo post sanzioni. Nel maggio 2014 la security firm Isight Partners scopriva una campagna di attacchi cyber, condotta per circa 3 anni, dal 2011, su oltre 2000 personal computer, da parte, si suppone, di hackers iraniani, a esponenti politici e militari americani, oltre che a diplomatici, giornalisti, lobbisti. L'operazione, ribattezzata da Isight "Newscaster", era basata su profili falsi sui principali social media (Facebook, Twitter, LinkedIn) e su un falso sito di notizie registrato a Teheran (Newsonair.org) che,

50 **J.C. Zarate**, "The Implications of Sanctions Relief Under the Iranian Agreement", Statement before the Senate Committee on Banking, Housing and Urban Affairs, 5 Agosto 2015.

51 Il conglomerato controlla circa 5000 compagnie sussidiarie e, al momento (primavera 2016) ha contratti nel Paese per oltre 50 miliardi di dollari.

52 American Enterprise Institute, "Basji Organization Enters Cyber Operations", 2016. Si riportano infatti le parole del comandante del corpo, generale Ali Fazli, propenso all'utilizzo dei media per permeare l'opinione pubblica siriana, irachena e libanese.

attraverso link di phishing, rilasciavano malware non molto sofisticati ma comunque in grado di essere utilizzati per l'efiltrazione di dati (aspetto che evidenzia l'acquisita capacità degli hackers iraniani, su standard simili a quelli di russi e cinesi, primari rivali cyber, fino ad ora, degli Stati Uniti[53]). Gli aspetti primari da considerare riguardo a Newscaster sono sia il ruolo sempre più fondamentale dei social media, utile canale di comunicazione ma ancor più efficiente sistema e punto di inserimento per attività di cyber espionage, sia l'ampiezza strutturale messa in atto dagli iraniani, con una campagna offensiva più complessa e allo stesso tempo più longeva di quelle normalmente organizzate dai cinesi. Isight ha rilevato come l'attività di cyber espionage iraniano abbia subito un'evoluzione incerta e si sia adattata, in un certo qual modo, al corso del negoziato diplomatico sul programma nucleare iraniano e sulla minaccia rappresentata dallo Stato Islamico. A un'intensificazione dell'azione cyber del maggio 2014, poco prima del reale inizio del colloqui sul nucleare iraniano, è seguita una fase di quasi silenzio, nei confronti soprattutto degli USA, man mano che le possibilità di accordo sul nucleare aumentavano (parimenti cresceva invece il focus iraniano contro Israele e Stato Islamico). Dopo l'estate 2015, ad accordo raggiunto, gli attacchi sono ripresi anche nei confronti di Washington.

Il secondo caso da riportare evidenzia come l'Iran non solo sia in grado, oramai, di effettuare importanti operazioni di cyber espionage, ma abbia anche le capacità per cyber attack a rete infrastrutturali di primaria importanza. Cylance, importante security firm, in un report del 2014 ha evidenziato una serie di attacchi cibernetici di provenienza iraniana a infrastrutture critiche, punti nodali per la diffusione di energia, università (nessun danno SCADA, Supervisory Control And Data Acquisition, è stato tuttavia segnalato), compresa l'infiltrazione nella rete di comandi della diga di Bowman, a Rye, nello stato di New York[54].

L'Iran è ormai non più una potenza di secondo rango nel panorama cyber global, essendo in grado, come visto, di operare efficacemente sia sotto il profilo dello spionaggio sia sotto quello più direttamente operativo, a danno di infrastrutture o bersagli di alto valore simbolico. Sotto il profilo della difesa, non è chiaro fino a che punto l'Iran possa sostenere un attacco cibernetico coordinato e di lungo periodo. Analizzando le singole situazioni, si individua tuttavia quella specificità iraniana di grande abilità nella lotta impari, anche cibernetica che, come detto, premia nel breve termine l'attore più debole. Le risposte iraniane agli attacchi americani e israeliani, pur notevolmente meno sofisticate, hanno ad ogni modo ottenuto un valido risultato, quanto meno sul piano del clamore internazionale e della manifestazione della presenza iraniana anche sul piano cibernetico, una presenza

53 **E. Nakashima**, Iranian hackers are targeting U.S. officials through social networks, report says, 29 maggio 2014, The Washington Post https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html

54 Cylance, "Operation Cleaver", Cylance, Dicembre 2014, http://www.cylance.com. Un hacker iraniano è finite sotto indagine nel 2015 per l'attacco alla diga. Si segnala inoltre che 7 iraniani, che lavoravano per due società collegate allo stato persiano e, direttamente, al corpo dei Pasdaran, sono finite sotto inchiesta, nella primavera 2016, per altri attacchi negli USA.

che Washington, alla luce della lunga esperienza persiana in campo interno, avrebbe dovuto tenere in maggiore considerazione. La valutazione degli impatti negativi di uno scontro con l'Iran, capace anche di influire dal punto di vista cibernetico sia sui suoi attori *proxy* Hezbollah e Hamas (e le prove di decodifica del linguaggio criptato dell'IDF- Vered Harim durante la guerra in Libano dell'estate 2006- da parte di Hezbollah dimostrano una certa competenza acquisita) sia sul governo azero, suo vicino, indicano che Washington e Tel Aviv necessitano di una più accurata *cyber threat intelligence*, se vogliono mantenere la carta cibernetica come valevole opzione di dissuasione per il medio periodo contro l'Iran. La fase post sanzioni potrebbe pertanto vedere un Iran assertivo con i principali rivali regionali, come Israele e Arabia Saudita, contro i quali non sono da escludere attacchi cyber compiuti contro direttrici infrastrutturali, sicuramente accompagnati da attente operazioni di cyber espionage, in particolare nei confronti di Tel Aviv. Per quanto riguarda il confronto con gli Stati Uniti, l'Iran potrebbe passare da essere un "nemico dichiarato", come qualche anno fa, a un "avversario collaborativo", come potrebbe essere nei casi di Russia e Cina. L'attività di spionaggio cyber non cesserà sicuramente e anzi potrebbe diventare il principale e più continuo canale di confronto tra Washington e Teheran, almeno nel medio periodo, in attesa che il nodo di rischio regionale in Medio Oriente, la presenza del cosiddetto Stato Islamico, possa trovare una sua soluzione definitiva, con tutto quello che ne comporterebbe per gli equilibri regionali. Viene in mente in primo luogo il futuro della Siria e del suo presidente Al Assad, tanto caro a Teheran. I dossier di confronto e scontro tra l'Iran e la comunità internazionale, nella sua componente occidentale, quindi, sono e rimarranno ancora numerosi.

Polizia Postale e delle Comunicazioni
Obiettivi e strategie

*Giorgio Bacilieri

La Polizia Postale e delle Comunicazioni, settore specialistico della Polizia di Stato isituito con la legge di riforma dell'Amministrazione della Pubblica Sicurezza, è principalmente impegnata a prevenire e contrastare la criminalità informatica, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

Il Servizio Centrale, vertice della struttura, è stato istituito con decreto ministeriale dell'1 marzo 1998 come organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione e punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della Specialità.
Il flusso di tutte le informazioni rilevanti in materia di *cybercrime* consente al Servizio di svolgere, fra l'altro, un'efficace e mirata azione nel campo della cooperazione internazionale.
La presenza sul territorio è assicurata attualmente da 20 Compartimenti e 80 Sezioni.

Avvalendosi della professionalità dei suoi tre Centri di eccellenza (CNCPO – Centro Nazionale per il Contrasto della Pedopornografia *online*, CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – Commissariato di PS online), il Servizio Centrale assicura un'efficace azione di raccordo operativo con gli uffici territoriali, in particolare nelle quattro macroaree criminali di interesse prioritario:
- pedopornografia *online*;
- *hacking* e crimini informatici;
- *financial cybercrime*;
- *cyberterrorismo*.

Fra le attribuzioni e le competenze delle diramazioni territoriali vanno aggiunte:
- la tutela dei servizi postali, di bancoposta e di telecomunicazione;
- la prevenzione e repressione dei reati legati al commercio elettronico;
- il concorso nel contrasto delle violazioni del diritto d'autore per quanto attiene agli aspetti telematici;
- il raccordo operativo con gli Ispettorati Territoriali del Ministero dello Sviluppo Economico nelle attività di controllo amministrativo di comune interesse.

Il CNCPO è stato istituito dalla legge 6 febbraio 2006, n. 38, con il compito di raccogliere tutte le segnalazioni provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori, avvalendosi della rete *Internet* e di altre reti di comunicazione.
A tale scopo il Centro alimenta il CETS – *Child Exploitation Tracking System*, una banca dati utilizzata da numerosi Paesi del mondo, che consente di tracciare i tentativi di adescamento e di condivisione di materiale pedopornografico da parte dei pedofili *online*, permettendo di raccogliere, elaborare ed analizzare i dati e le prove.
L'Italia è tra i primi Paesi europei a mettere in atto sistemi di protezione della navigazione in Rete attraverso il blocco o il filtraggio dei contenuti pedopornografici. I provider italiani accedono quotidianamente alla *black list* in modalità certificata e provvedono ad apporre filtri alla navigazione.
Quanto al contrasto, va detto che la legge 3 agosto 1998, n. 269 (successivamente la legge 16 marzo 2006, n. 146) ha consentito al personale della Specialità di intraprendere indagini *undercover*, utilizzare indicazioni di copertura, anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero partecipare ad esse.

La direttiva del Ministro dell'Interno, in data 28 aprile 2006, recante il “Riassetto dei comparti di specialità delle Forze di polizia”, rimette alla competenza primaria della Polizia di Stato garantire, in via generale, l'integrità e la funzionalità della rete informatica, ivi compresa la protezione delle infrastrutture critiche informatizzate, nonché la prevenzione ed il contrasto degli attacchi di livello informatico alle strutture di livello strategico per il Paese.
L'individuazione delle infrastrutture critiche informatiche di interesse nazionale è intervenuta con decreto ministeriale del 9 gennaio 2008.
Anche se di fatto già operante dal 2005, il CNAIPIC è stato istituito formalmente con decreto del Capo della Polizia – Direttore Generale della Pubblica Sicurezza del 7 agosto 2008. Avvalendosi di tecnologie di elevato livello e di personale altamente qualificato, è incaricato della prevenzione e del contrasto della minaccia informatica di matrice terroristica o criminale che ha per obiettivo le infrastrutture critiche informatiche di interesse nazionale.
I servizi di protezione informatica sono erogati sulla base di apposite convenzioni con i responsabili delle strutture interessate, con le quali si realizza in tale particolare settore un rapporto di partnership pubblico-privato.
Presso il CNAIPIC, inoltre, è inserito il Punto di contatto italiano per le emergenze tecnico-operative connesse al verificarsi di episodi di criminalità transnazionale, secondo quanto stabilito dalla Convenzione sul *cybercrime* sottoscritta a Budapest il 23 novembre 2001.
Il Punto di contatto opera 24 ore su 24 e 7 giorni su 7 all'interno della rete *High Tech Crime* costituita in ambito G7 e successivamente estesa al Consiglio d'Europa.

Al fine di prevenire turbative e pericoli per l'ordine e la sicurezza pubblica, la Polizia Postale e delle Comunicazioni provvede al costante monitoraggio della Rete per individuare attività illecite di proselitismo concernenti iniziative di carattere razzista, xenofoba, sessuofobica o comunque ispirata a reati di odio.
La Specialità concorre, inoltre, con altri organi di polizia specializzati in indagini tecniche di particolare complessità, su fenomeni di eversione e terrorismo, a livello nazionale ed internazionale, quando vengano messi in atto attraverso strumenti informatici e di comunicazione telematica.
In particolare per quanto concerne le minacce provenienti da gruppi/organizzazioni riconducibili al fondamentalismo religioso islamico, il Servizio Centrale, unitamente a 9 Compartimenti pilota, effettua un costante monitoraggio della Rete anche con l'ausilio di interpreti madrelingua.
Dall'1 luglio 2015, il Servizio Centrale costituisce il Punto di contatto nazionale per le attività di *Internet Referral Unit* (IRU), istituito presso *Europol*, che ha come compito quello di individuare contenuti rilevanti in tema di terrorismo, coordinare e condividere in maniera rapida le informazioni con gli Stati membri, in stretta collaborazione con le compagnie ed i provider.
Quanto al contrasto, va detto che la legge 16 marzo 2006, n. 146 (modificata dalla legge 13 agosto 2010, n. 136) ha consentito al personale della Specialità di intraprendere indagini sottocopertura.

Il Compartimento Polizia Postale e delle Comunicazioni per la Liguria è inserito fra i Compartimenti pilota per l'espletamento di attività di prevenzione e contrasto al *cyberterrorismo* ed ai reati d'odio.
La particolare vivacità investigativa ha formato spunto per l'emanazione della “*Direttiva inerente gli approfondimenti investigativi aventi ad oggetto condotte poste in essere attraverso la Rete ed astrattamente riconducibili all'ipotesi di cui all'articolo 414, comma 4, del Codice Penale*” del 13 ottobre 2015, da parte della Procura della Repubblica presso il Tribunale di Genova (Procura Distrettuale) indirizzata a tutte le Forze di polizia.
Oltre alla configurazione del delitto di istigazione o apologia aggravata dall'attinenza a vicende di terrorismo o crimini contro l'umanità, sono state formulate indicazioni in merito alle previsioni dell'articolo 2, commi 3 e 4, del decreto legge 18 febbraio 2015, n. 7, convertito dalla legge 17 aprile 2015, n. 43, relative all'inibizione di accesso a siti e/o rimozione dei contenuti degli stessi, che vede protagonista il Servizio Centrale, secondo un sistema di blocco o filtraggio (*black list*) simile a quello adottato per la materia della pornografia minorile.

La sinergia in atto con il mondo accademico, in particolare il protocollo con l'Università di Genova, oltre a contemplare attività di formazione per il personale, ha consentito di realizzare un *software* dedicato che, basandosi sull'*open source intelligence*, costituisce prezioso ed efficace strumento di monitoraggio delle informazioni pubblicate su un noto *social network*.
Inoltre, è in fase ormai conclusiva la sottoscrizione di un importante protocollo d'intesa per la prevenzione e contrasto dei crimini informatici sui sistemi informativi "sensibili" a livello regionale, secondo linee operative impartite da parte del Servizio Centrale, che costituisce novità assoluta ed ha la finalità di replicare sul territorio il modello convenzionale codificato a livello CNAIPIC.

In conclusione, si può affermare che, l'efficacia delle attività investigative specialistiche attribuite alla Specialità debba essere perseguita almeno attraverso sei obiettivi e/o strategie:
- la cooperazione internazionale (giudiziaria e di polizia);
- il modello convenzionale finalizzato alla tutela delle infrastrutture critiche e "sensibili";
- le sinergie tra settore pubblico e privato (già in atto tra Polizia di Stato e: principali realtà bancarie rappresentate dall'Associazione Bancaria Italiana – ABI, nonché lo stesso gruppo Poste; società di *e-commerce*; gestori di *social network*; SIAE; ecc.);
- l'utilizzo di banche dati specifiche che costituiscano una comune rete di *information sharing* (per quanto concerne il contrasto al *financial cybercrime*, va detto che, in considerazione degli ottimi risultati raggiunti durante il primo periodo di sua operatività, la piattaforma OF2CEN sta per essere esportata in Europa con il nome di EU OF2CEN, secondo un progetto che vede l'Italia come *leading country* e la Polizia Postale e delle Comunicazioni come *driver*);
- le sinergie con il mondo accademico;
- il rispetto del modello organizzativo del coordinamento da parte di tutti gli uffici e organi investigativi (ognuno secondo le proprie attribuzioni e competenze).

*Vice Questore Aggiunto della Polizia di Stato
Dirigente Supplente del Compartimento Polizia Postale
e delle Comunicazioni per la Liguria

Intervento tenuto in Chiavari (GE) l'11 maggio 2016
in occasione del *V Cyber Defence Symposium*
organizzato dalla Scuola Telecomunicazioni Forze Armate

I nuovi scenari della sicurezza tra Internet of Things e Smart Cities

Una conferenza tenutasi a Singapore iniziava così: Congratulazioni. Perché secondo una ricerca dell'Economist, Singapore è risultata la seconda città tra le più sicure al mondo. Secondo una ricerca nella quale si è andati ad analizzare diversi oggetti nell'ambito della sicurezza della città, quindi l'aspetto tecnologico, sanitario, dell'infrastruttura e anche della sicurezza personale. Possiamo farci anche noi le congratulazioni? Non rientriamo nelle prime 20, nessuna città italiana nelle prime 20, 25° Roma-26° Milano. La cosa non migliora nemmeno sotto l'aspetto europeo, perché risultiamo quart'ultimi e terz'ultimi, precediamo Istanbul e Mosca. Questa è la situazione che stiamo affrontando, ovvero il discorso sicurezza in senso complessivo del sistema Paese. Dati questi fatti, vediamo se possiamo proteggerci e da cosa possiamo proteggerci perché il problema principale che vediamo oggi è che quello che conoscevamo delle architetture IT non esiste più, è completamente cambiato. Abbiamo strumenti che si collegano di qualsiasi forma e natura, oltre a cellulari, pc e tablet anche gli elettrodomestici e tutto quello che ha un indirizzo IP, droni e molto altro ancora. La prima cosa che abbiamo fatto e stata dare un nome, abbiamo chiamato tutto questo Internet of Things o nel momento in cui viene inserita nelle città diventa la Smart City. Bellissimo, tutto sta funzionando, più o meno, ma apre dei problemi di sicurezza giganteschi. In una Smart City dalle pompe di benzina ai sistemi di comunicazione al controllo del traffico è tutto connesso, ma sono tutte finestre che noi apriamo in termini di problematiche relative alla sicurezza. Per dare un'idea, una macchina connessa, non una a guida automatica, una macchina connessa a internet che scambia informazioni con la casa madre, genera circa 20 GB di dati l'ora, massa di dati che deve essere controllata. Il problema esiste. Potremmo considerare l'Internet of Things come il network dei network, ma questa rete mano mano che ne stiamo sfruttando le capacità, si sta dimostrando immatura e sperimentale. Chi sta guidando l'espansione è più il marketing, il consumatore, vengono prodotti nuovi oggetti interconnessi ma nel momento in cui si progettano non si pensa alla sicurezza, è più importante metterli sul mercato, la sicurezza verrà dopo. Qualsiasi cosa che è connessa ad internet oggi può essere hackerata, compromessa, dobbiamo conoscere il nostro nemico per combatterlo ma uno degli altri aspetti che si sta verificando è che c'è un cambiamento degli attori della guerra, si stanno generando anche dei commerci e dei settori alternativi e abbiamo avuto anche casi in Italia. Il mercato è abbastanza florido, un progettino per andare ad analizzare, a sniffare, a prelevare dei dati costa circa mezzo milione di euro. Ma oltre questo è nato chi sfrutta queste situazioni, il mercato underground, dove è possibile comprare servizi anche per chi è uno sponsor del cloud computing, non si deve nemmeno mettere in piedi l'infrastruttura, ma si ha la possibilità di pagare in pay per use, e riconoscono una percentuale in base agli introiti fatti in base all'attacco. Dove è possibile acquistare sia il toolkit sia i servizi manutenzione, sono delle vere e proprie società commerciali che non girano nella parte pubblica del web, ma nel deep web dove si può entrare tranquillamente e tranquillamente acquistare servizi. Ne esistono anche di pubblici. Chi conosce Shodan? È un motore di ricerca che consente di trovare alla stregua di Google tutte le informazioni degli apparati presenti in rete e individua quali sono le porte aperte, come sono aperte, quali sono i sevizi attivi ed è pubblico. Funziona sulla geo localizzazione, riesce a circoscrivere un'area e a fornire le informazioni sui dispositivi presenti, posso fare tipologie di ricerca fino ad arrivare a trovare quelli che possono essere apparati, abbiamo trovato ad esempio centrali d'acquedotto e sistemi di controllo di impiantistica importanti. Da ricerche che abbiamo fatto come Trend Micro per capire chi è il nostro nemico, quali sono le piattaforme che il nemico può attaccare, cosa significa oggi cybernetica? Un problema critical infrastructure è su chi può attaccare quelli che sono gli apparati DCS-SCADA. Abbiamo una rete di honeypots dove andiamo a verificare queste cose e la guerra allo scenario è globale. Facciamo ricerche anche su tecnologie che vengono utilizzate: IES per esempio, un protocollo per il controllo di posizionamento, viene dalla tecnologia analogica portata sul digitale, ma la cosa carina è sui provider che forniscono questo tipo di servizi. Su youtube si trova un video dove dimostriamo come con tre righe di comando è possibile spostare navi sui sistemi di plottaggio, quindi possiamo far apparire davanti a un porto una flotta di imbarcazioni o farne sparire contemporaneamente un'altra o avvicinarsi a una petroliera e comunicare che c'è qualcuno vicino. Tutto con tre righe di comando. Parliamo poi delle auto, stiamo studiando il concetto delle scatole nere per le assicurazioni mettendo sulla nostra macchina un gateway internet, quindi anche lì si apre tutta una serie di scenari e problematiche. Ma come possiamo prevedere queste cose? Ci

deve necessariamente essere collaborazione tra pubblico e privato e università, perché gli scenari cambiano in continuazione. Sennò è veramente difficile vincere.

Gastone Nencini, Country Manager Trend Micro Italia