Cyber Warfare 2014

Armi cibernetiche, sicurezza nazionale e difesa del business

a cura di Umberto Gori
e Serena Lisi

CWC 2015 CYBER WARFARE CONFERENCE

FrancoAngeli

Cyber Defense, Cyber Intelligence e relative armi: Casi di collaborazione tra pubblica amministrazione, industria e ricerca finanziata dalla Commissione Europea

di *Alessandro Zanasi*[1]

Introduzione

In quello che è diventato un film culto degli anni '80, *War Games*, il regista John Badham ipotizzava lo scenario in cui un giovane pirata informatico alle prime armi penetrasse all'interno di un computer della Difesa USA e, da qui, mettesse in atto azioni in grado di spingere il mondo verso il baratro di un conflitto termonucleare tra le due superpotenze di allora. A 30 anni di distanza dall'uscita del film, questo scenario rimane ancora lontano dalla realtà. Ma non così tanto quanto si potrebbe pensare. La diffusione su larga scala di Internet, il suo utilizzo nei settori sia civile che militare, unitamente alle innovazioni tecnologiche che hanno portato la maggior parte delle infrastrutture critiche dei Paesi occidentali ad essere connesse alla rete, ha fatto sì che quello cibernetico sia oggi considerato un dominio estremamente sensibile in chiave sicurezza.

Anche se non in grado di scatenare un'apocalisse nucleare, un malintenzionato ha la possibilità, attraverso la rete Internet, di provocare disservizi su larga scala, potenzialmente in grado di mettere in ginocchio un Paese bersaglio. Per farlo non può però muoversi da solo. Lo sviluppo degli strumenti necessari a questo fine, le armi cibernetiche (*cyber weapon*), richiede competenze specialistiche di altissimo livello, grandi risorse a disposizione, nonché importanti capacità di coordinamento per la mobilitazione dei vari attori necessari per raggiungere l'obiettivo.

Le medesime esigenze sono quelle necessarie a chi deve occuparsi del problema opposto, ovvero garantire la (cyber) sicurezza di fronte alle minacce presenti nel cyberspace. La Commissione Europea (CE),

---

[1] Fondatore e CEO di Zanasi & Partners (Z&P), società specializzata in sicurezza ed intelligence, formata da ricercatori e consulenti con competenze ed esperienze acquisite lavorando presso la Commissione Europea (ESRAB ed ESRIF), in società informatiche (IBM) e nucleari (Ansaldo), in centri di ricerca (in Francia, Stati Uniti e Italia), nelle forze dell'ordine (Carabinieri) e svolgendo attività accademiche (in Francia, Regno Unito ed Italia).
Sito web: http://www.zanasi-alessandro.eu

attraverso diverse linee di finanziamento alla ricerca in materia di sicurezza, si pone l'obiettivo di aiutare le imprese, le università e i centri di ricerca a sviluppare le misure di protezione necessarie per garantire all'intero continente un adeguato livello di cyber security.

1. Il mito romantico della Cyber War

Una certa visione romanzata della tecnologia ha spesso lasciato intendere che azioni di guerra cibernetica possano essere condotte da singoli individui, lupi solitari i quali, mossi da motivazioni idealistiche o di altro genere, abbiano la capacità, con pochi clic, di mettere in ginocchio le infrastrutture critiche (IC) di un Paese bersaglio. Niente di più sbagliato. Certamente la storia recente ha dimostrato come singoli individui o gruppi di hacker di piccole dimensioni possano ottenere risultati di forte impatto: dal defacing di siti web[2], alla sottrazione di account sui principali social media[3], al furto ed esposizione di dati riservati (password di accesso a servizi web, piuttosto che email e documenti privati di varia natura)[4]. Operazioni molto appariscenti ma che raramente hanno avuto un impatto tangibile in termini di sicurezza. E che, anche per questo motivo, non possono essere considerati atti di cyber war ma ben più semplici attacchi cibernetici di basso livello.

In che cosa consiste la differenza tra le due categorie? Diversi operatori e studiosi del settore propongono una definizione piuttosto estensiva di cyber war. Richard Clarke, ad esempio, la definisce come un insieme di generiche "azioni da parte di uno stato-nazione per penetrare i computer o le reti di un'altra nazione allo scopo di causare danni o malfunzionamenti" (Clarke, 2010). Più stringente è invece Thomas Rid, secondo il quale, per essere considerato un atto di guerra (quindi di cyber war), un attacco cibernetico deve soddisfare tre requisiti: essere violento, strumentale e avere una connotazione di carattere politico (Rid, 2012). In entrambi i casi, che si adotti una definizione estensiva piuttosto che una restrittiva, le operazioni citate sopra, le quali possono essere portate avanti da attori dalle dimensioni e dalle risorse a disposizione limitate, non rientrano nella fattispecie della cyber war.

---

[2] La letteratura in questo senso è sterminata.

[3] Noto come takeover, questo genere di operazioni è stato condotto molto spesso dal Syrian Electronic Army. Esemplare fu il takeover contro l'account Twitter della Associated Press, utilizzato per pubblicare una (falsa) notizia circa esplosioni alla Casa Bianca e provocare conseguentemente una violenta turbolenza sui mercati borsistici (http://www.reuters.com/article/2013/04/23/markets-global-idUSL2N0DA1X620130423).

[4] Il furto e l'esposizione di dati riservati sono parte integrante del modus operandi dei gruppi di "hacktivist" (ad esempio: Anonymous).

Quel che è ormai certo, infatti, è che lo sviluppo di capacità di cyber war richiede un enorme sforzo da parte di un ampio numero di risorse altamente qualificate, aventi accesso a tecnologie avanzate che solo un attore-stato può permettersi di coordinare. La guerra cibernetica si combatte attraverso armi apposite. Si tratte delle cyber weapon, le quali possono essere definite come "software usato, o disegnato per essere utilizzato, al fine di minacciare o creare un danno fisico, funzionale o psicologico a strutture, sistemi o esseri umani" (Rid & McBurney, 2012). Queste armi cibernetiche sono strumenti in grado di sfruttare vulnerabilità presenti in software e componenti hardware bersaglio al fine di guadagnare l'accesso ad un obiettivo critico[5]. Sono necessarie grandi capacità di coordinamento, di intelligence e di cyber intelligence per scovare queste vulnerabilità[6], nonché ingenti investimenti finanziari per sviluppare le cyber weapon.

Facendo un parallelo con le armi spaziali, anche nel mondo cibernetico possiamo riconoscere il vettore (una email, una pagina web, un dispositivo hardware portatile) della cyber weapon il quale, una volta superate le difese nemiche ed avendo avvicinato l'obiettivo, può rilasciare il payload (estrazione di quanto contenuto in memoria, rimozione/danneggiamento di un software o sua occultata alterazione), obiettivo finale dell'operazione. Lo studio del funzionamento di queste armi e delle possibili misure di protezione nei confronti di esse rientra a pieno titolo nei campi della cyber defense, della cyber intelligence e della cyber security.

Come mai questa preoccupazione in merito alla cyber war? La guerra cibernetica si combatte all'interno del cyberspace, un dominio caratterizzato dall'utilizzo dell'elettronica e dello spettro elettromagnetico per immagazzinare, modificare e scambiare informazioni attraverso dispositivi collegati a reti informatiche interconnesse. Oggigiorno, cyberspace è spesso utilizzato quale sinonimo di Internet. Ciò che rende la guerra cibernetica una minaccia così grave per la sicurezza delle società moderne è il fatto che i cittadini, le attività commerciali e le amministrazioni pubbliche sono sempre più dipendenti da Internet e dalle tecnologie informatiche per lo svolgimento delle loro attività quotidiane. L'adozione di tali strumenti ha consentito di aumentare la produttività, promuovere l'innovazione, favorire gli scambi commerciali, fino a costituire un volano per veri e propri cambiamenti sociali. Internet ha trovato applicazione pressoché in ogni settore, ivi inclusi quelli legati alla fornitura di servizi vitali per un Paese. La velocità di crescita del cyberspace ha però preso in contropiede la ricerca sulla sicurezza. Il risultato è che il non adeguato livello di protezione delle tecnologie digitali pone ora un forte freno all'economia e allo sviluppo sociale dell'Europa. Le stesse innovazioni tecnologiche che hanno portato innumerevoli benefici al

[5] Vulnerabilità che possono essere dovute ad errori di programmazione/progettazione, oppure essere state inserite di proposito all'interno di software e/o dispositivi hardware (es. "backdoor" e "logic bomb").
[6] In particolare quando si tratta di vulnerabilità non note ("*zero-day*").

continente possono oggi essere sfruttate da Paesi nemici per compiere atti di cyber war dalle nefaste conseguenze. Si pensi ad esempio agli effetti catastrofici che potrebbero originarsi da attacchi mirati ai sistemi di controllo (ad esempio SCADA: Supervisory Control and Data Acquisition) delle infrastrutture critiche di un Paese: le reti di distribuzione idrica ed elettrica, di telecomunicazioni, del trasporto ferroviario e aereo, ecc.

Da diverso tempo il Pentagono considera il cyberspace quale uno dei cinque domini della conflittualità, accanto ai più tradizionali terra, mare, aria e spazio (Lynn, 2010; Martino, 2013). L'obiettivo perseguito dalla difesa USA è di arrivare a sviluppare anche per la cyber war una dottrina bellica equivalente a quella in vigore negli altri domini. L'importanza strategica del cyberspace non può infatti essere trascurata. Vi è inoltre da tenere in considerazione la natura asimmetrica della guerra cibernetica. Nonostante l'entità di tale asimmetria sia stata negli ultimi anni sicuramente esagerata, portando a prestare eccessiva attenzione a fenomeni di semplice cyber attivismo e cyber vandalismo, ciò non toglie che la cyber war fornisca, a Paesi militarmente di seconda fascia, l'opportunità di colmare il gap dalle grandi potenze in merito alle capacità offensive[7]. Ne consegue che le minacce alla sicurezza si moltiplicano. La cyber security, orientata soprattutto alla protezione delle infrastrutture critiche, è diventata un'assoluta priorità politica ed economica per l'Unione Europea, nonché una sfida per assicurare la sicurezza e la libertà dei suoi cittadini.

Uno degli aspetti che rende particolarmente complicato il garantire la sicurezza delle IC è però dovuto al fatto che, mentre la sicurezza dei cittadini è a carico delle agenzie di law enforcement, molte infrastrutture critiche appartengono e sono gestite dal mondo privato. Lo sviluppo di una partnership pubblico-privato è pertanto necessario: l'obiettivo di raggiungere un adeguato livello di cyber security può essere perseguito soltanto nell'ambito di un'ampia e proattiva collaborazione tra tutti gli stakeholder del settore. È questo, unito ad una forte spinta alla ricerca in materia di cyber security, ciò che l'Unione Europea deve favorire.

2. Collaborazione in Europa: coordinamento e investimenti

Lo sviluppo delle tecnologie di cyber security necessarie per la protezione delle IC richiede una forte collaborazione tra industrie, centri di ricerca e istituzioni nonché ingenti investimenti in particolare nel settore della ricerca. Per questo motivo è forte il rischio che nessuno stato europeo,

[7] Basti pensare, in questo senso, agli investimenti in capacità offensive di cyber warfare fatti dalla Corea del Nord (http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/08/why-cyber-armies-are-a-good-investment-for-countries-like-north-korea/).

da solo, abbia le risorse e le competenze necessarie sia per promuovere e coordinare queste collaborazioni, sia per erogare i finanziamenti necessari per essere all'avanguardia rispetto alle minacce cibernetiche alla sicurezza.

La tematica fu inizialmente affrontata da ESRAB (European Security Research Advisory Board), un comitato istituito nel 2005 dalla Commissione Europea e costituito da 50 esperti di sicurezza provenienti da autorità pubbliche (BKA, EDA, ministeri, ecc.), industrie (Thales, Finmeccanica, ecc.) e noti ricercatori e consulenti. ESRAB nacque con lo scopo di tracciare le linee guida della ricerca in materia di sicurezza (e della cyber security) e dei relativi finanziamenti. Gli sforzi fattisi in ESRAB proseguirono in ESRIF (European Security Research Innovation Forum), un forum attivo tra il 2007 e il 2009 e composto da 64 advisor indicati dai propri governi e nominati dalla Commissione Europea, rappresentanti di aziende europee di sicurezza (per esempio: Thales, Finmeccanica, EADS/Airbus Group, Saab, Sagem, Smiths, Z&P, ecc.), ministeri (Interno, Difesa), agenzie governative (EUROPOL, BKA, EDA). Tale forum, inoltre, si occupò di creare alleanze strategiche tra end-user e fornitori a livello europeo, cioè garantì un dialogo tra i mondi diversi ma imprescindibili della ricerca, scienza, industria, operatori di infrastrutture critiche e autorità responsabili della sicurezza informatica.
Lo scrivente è stato membro sia di ESRAB che di ESRIF.

I progetti di ricerca e sviluppo prioritari da perseguire, riguardanti il settore della sicurezza e identificati durante le attività di questi due tavoli, furono poi finanziati nel contesto del Settimo programma quadro (FP7), iniziato nel 2007 e concluso nel 2013, ai quali potevano aderire le istituzioni pubbliche e private dei Paesi membri, e proseguito attraverso Horizon 2020 (dal 2014 al 2020).

3. Ricerca in materia di sicurezza in Europa: casi di successo

A titolo di esempio si introducono di seguito alcuni casi di successo di progetti di ricerca, legati ai temi della cyber security, cui Z&P ha partecipato grazie ai programmi di finanziamento della Commissione Europea.

3.1. SCADA LAB

Principali partecipanti:
INTECO/INCIBE (Spagna, Ministero dell'Industria, del Turismo e del Commercio);
CNPIC (Spagna, Ministero dell'Interno).

Gli apparati SCADA, fattispecie della più ampia categoria degli ICS (Industrial Control System), sono sistemi informatici adibiti al controllo di processi industriali. Essendo spesso accessibili attraverso la rete Internet, tali sistemi rappresentano uno degli obiettivi più appetibili per l'attacco di una cyber weapon. La presa in controllo dell'infrastruttura SCADA di un impianto di produzione potrebbe dare la possibilità ad un malintenzionato di alterarne i parametri di regolazione, eseguire operazioni non previste e comprometterne l'integrità. Un esempio in tal senso risale al 2010, quando l'Iran scoprì che da diverso tempo un malware denominato Stuxnet stava sabotando con successo i sistemi SCADA della centrale nucleare situata nella città di Natanz, riuscendo a provocare danneggiamenti a circa il 20% delle centrifughe utilizzate per l'arricchimento dell'uranio.

Obiettivo del progetto SCADA LAB (SCADA LABoratory and test bed for critical infrastructure protection) è quello di realizzare un laboratorio fisico in cui testare la sicurezza delle tecnologie SCADA per ridurne la vulnerabilità nei confronti di minacce cibernetiche, nonchè sperimentare nuove soluzioni che possano prevenire e mitigare gli effetti di tali attacchi contro infrastrutture critiche.

3.2. CloudCERT

Principali partecipanti:

INTECO/INCIBE (Spagna, Ministero dell'Industria, del Turismo e del Commercio);

CNPIC (Spagna, Ministero dell'Interno);

Fondazione ICSA (Italia).

In Europa, buona parte delle infrastrutture critiche è, interamente o in parte, posseduta e gestita da operatori privati, i quali spesso non hanno incentivi sufficienti ad investire nella loro sicurezza, lasciandole così esposte ad atti di terrorismo, disastri naturali, incidenti, azioni di criminalità informatica e di altro genere. I CERT (Computer Emergency Response Team) sono organizzazioni che monitorano quel che accade nel cyberspace allo scopo di analizzarne lo stato di sicurezza e la vulnerabilità nei confronti delle minacce cibernetiche, raccolgono segnalazioni di eventuali attacchi e predispongono procedure di risposta. I CERT europei recensiti a dicembre 2014 sono 251 (ENISA, 2014). Queste organizzazioni condividono raramente informazioni tra loro, il che comporta un inefficiente utilizzo di risorse a livello di sistema.

La finalità del progetto CloudCERT (Testbed Framework to Exercise Critical Infrastructure Protection) è quella di sviluppare

una piattaforma comune per la condivisione di informazioni riguardanti minacce e vulnerabilità, di allarmi e avvisi per la protezione delle IC, in maniera rapida ed efficiente tra i CERT dei vari Paesi europei ed i gestori delle IC del continente.

3.3. LEILA

Principali partecipanti:
National Defense University (Romania, Ministero della Difesa);
KEMEA (Grecia, Ministero dell'Interno).

I fallimenti dell'intelligence sono purtroppo uno dei temi di discussione principali trattati negli ultimi anni da chi si occupa di sicurezza. La mancata identificazione dei piani che hanno portato all'11 settembre, i grossolani errori commessi nell'individuare la "smoking gun" che ha portato alla seconda guerra del golfo, fino ad arrivare alla riuscita del recente attacco alla redazione di Charlie Hebdo, sono tutti esempi di come non sempre le agenzie di intelligence siano in grado di operare adeguatamente. La necessità di evitare in futuro il ripetersi di questi errori costituisce una spinta allo sviluppo di programmi di training sempre più efficienti. Una delle direzioni nelle quali il mondo del training si sta muovendo è quella dei serious games, "videogiochi" interattivi finalizzati non tanto all'intrattenimento, quanto piuttosto alla formazione dell'utente/giocatore.

Tra gli errori commessi più di frequente dagli analisti di intelligence particolare importanza rivestono quelli indotti dai cosiddetti "bias cognitivi", la cui riduzione è stata l'oggetto di un altro progetto europeo: RECOBIA (Reduction of Cognitive Biases in Intelligence Analysis). Tali automatismi mentali sono scorciatoie di pensiero che provocano l'involontario allontanamento dell'analista da quello che è un processamento logico e razionale delle informazioni a disposizione. Il progetto LEILA (Law Enforcement Intelligence Learning Applications) mira a sviluppare serious game dedicati agli analisti di intelligence e finalizzati alla mitigazione degli effetti dei bias cognitivi di cui questi possono soffrire. Attraverso un approccio olistico che combina tra loro diverse materie psicosociologiche, il giocatore partecipa a simulazioni di situazioni reali, dove si trova alle prese con le varie dinamiche cognitive che entrano in gioco nella realtà durante il processo di decision making in condizioni non favorevoli (sotto stress, in una situazione di emergenza, quando sono presenti incertezze, ecc.). Attraverso un tutoraggio diretto ed un sistema di valutazione del comportamento adottato, il giocatore impara a riconoscere gli errori cognitivi nei quali incorre e ad elaborare appropriate strategie di mitigazione.

3.4. SECRET

Principali partecipanti:
ALSTOM Transport SA (Francia);
Politecnico di Torino (Italia);
SNCF (Francia);
UIC (Internazionale).

Nel 2011 le forze di sicurezza iraniane catturarono un RQ-170 Sentinel ("La bestia di Kandahar"), un drone statunitense operato dalla CIA. Per impossessarsi del velivolo, al drone venne "accecato" il sistema di comunicazione e localizzazione (operazione che prende il nome di jamming) e gli furono fornite false istruzioni di volo (spoofing) convincendolo ad atterrare in suolo ostile. Simili attacchi possono essere condotti anche contro altri mezzi di trasporto non necessariamente militari. Si pensi ad esempio a uno scenario in cui una rete ferroviaria è vittima di un attacco cibernetico attraverso il quale il malintenzionato conquista la possibilità di riuscire a controllare i deviatoi e manovrare così il tragitto dei treni (Newton, 2002). A una tale azione potrebbero conseguire ingenti danni, economici ma anche in termini di vite umane: si immagini una collisione fra due o più treni o il deragliamento di un treno merci che trasporta sostanze chimiche tossiche.

Fra i diversi tipo di attacco di natura elettromagnetica che possono essere sferrati contro la rete ferroviaria, il progetto SECRET è volto a valutare il rischio di quelli posti in essere attraverso tecniche di jamming. SECRET mira a valutare le conseguenze di un attacco di questo genere, identificare misure preventive, protettive, resilienti e di ripristino, al fine di sviluppare nuove soluzioni a tutela della sicurezza delle linee ferroviarie europee.

3.5. iSAR+ e SOTERIA

Principali partecipanti:
Thales (Francia);
Guarda Nacional Republicana (Portugal);
North Yorkshire Police Authority (Regno Unito).

Ogni giorno condividiamo avvenimenti, pensieri e file attraverso i social media generando un'enorme mole di dati. Le rivelazioni di Snowden hanno reso pubblico quanto attentamente NSA e GCHQ monitorano le piattaforme di comunicazione a fini di cyber intelligence. Tuttavia un simile approccio di analisi dell'informazione reperibile dai social media potrebbe divenire

estremamente importante in situazioni di emergenza. È sempre più frequente che, all'occorrere di una grave emergenza (disastro naturale, attentato ecc.), gli utenti della rete chiedano aiuto o assicurino i propri conoscenti sul loro stato di salute utilizzando queste piattaforme di social networking [8]. Tali informazioni potranno essere rese disponibili per supportare il personale coinvolto nelle operazioni di soccorso (ad esempio le forze dell'ordine e la protezione civile) per l'intero perdurare dello stato di emergenza. Lo scambio effettivo ed efficace di tali informazioni critiche potrebbe favorire la pianificazione dell'intervento da parte della macchina dei soccorsi.

Da queste considerazione nascono i due progetti, denominati iSAR+ (Online Mobile Communications for Crisis Response and Search and Rescue) e SOTERIA (Online Mobile Communications for Emergencies). Entrambi concorrono a sviluppare tecniche di raccolta automatica di dati dai social media (social media monitoring), per classificarli e analizzarli in maniera automatica mediante applicazioni di Big Data Analytics: Data e Video Mining e Text Mining multi-lingua.

3.6. BODEGA

Principali partecipanti:
VTT (Finlandia);
Thales (Francia);
CEA - Commissariat à l'énergie atomique et aux énergies alternatives (Francia);
Atos (Spagna);
Agenzia dei Monopoli e delle Dogane (Italia);
UIC (Internazionale).

In un mondo sempre più globalizzato, il numero di persone che ogni giorno varcano le frontiere che separano Paesi diversi è in continuo aumento. I viaggiatori sono spesso obbligati a sottoporsi a lunghe attese, risultato delle lente procedure di identificazione adottate dal personale che si occupa di border control. Un tema particolarmente sentito è quello della semplificazione di tali procedure di controllo in modo tale da ridurre i tempi d'attesa, senza che questo vada però a scapito della sicurezza.

Il progetto BODEGA (BOrDErGuArd: Proactive Enhancement of Human Performance in Border Control) ha l'obiettivo di sviluppare una profonda comprensione dei fattori di natura psicologica presenti in viaggiatori e guardie di frontiera durante le operazioni di

[8] http://www.theguardian.com/technology/2014/oct/17/facebook-safety-check-friends-disasters

controllo documenti. Nel corso del suo lavoro, l'operatore potrebbe infatti essere influenzato da bias cognitivi che lo portano ad effettuare decisioni non dettate dalla logica e dal raziocinio. Per effetto di stereotipi culturali, ad esempio, un agente potrebbe nutrire istintivamente maggiori sospetti su soggetti aventi una carnagione scura o un aspetto trasandato piuttosto che su persone dai tratti caucasici o vestite in maniera elegante. Allo stesso modo BODEGA mira a migliorare la comprensione delle reazioni fisiche di origine psicologica, quali segni di stress o nervosismo che potrebbero tradire le reali intenzioni di un viaggiatore. Una volta identificate queste reazioni somatiche sarà possibile modellarle al fine di sviluppare sistemi di monitoraggio video con integrate funzioni di image processing in grado di segnalare tempestivamente la loro comparsa tra i viaggiatori in attesa di essere controllati. Tali sistemi permetteranno di monitorare efficacemente aree ampie ed affollate, migliorando l'efficienza dei controlli. Le soluzioni che scaturiranno dal progetto dovranno essere eticamente e socialmente accettabili, così come affidabili ed user friendly per gli operatori. Queste soluzioni integreranno metodi, strumenti, linee guida e raccomandazioni, mettendoli a disposizione degli operatori del settore. I risultati di BODEGA contribuiranno all'implementazione dell'iniziativa europea nota come "Smart borders" finalizzata a diminuire i disagi dei viaggiatori, garantendo standard di sicurezza più elevati da parte delle forze dell'ordine.

4. Nuovi programmi di finanziamento in materia di sicurezza

Le opportunità di ricerca e innovazione sono proseguiti grazie al nuovo programma di finanziamento europeo Horizon 2020, avviato il 1° gennaio 2014 e destinato a terminare il 31 dicembre 2020, e che convoglia al suo interno gli antecedenti FP7, il Programma quadro per la competitività e l'innovazione (CIP) e l'Istituto europeo di innovazione e tecnologia (EIT). Il budget stanziato per Horizon 2020 è di 78,6 miliardi di euro e fornirà ai ricercatori le risorse necessarie per condurre i propri studi, contribuendo all'innovazione tecnologica del continente. Uno dei pilastri su cui si fonda Horizon 2020 è quello della leadership industriale così da aiutare le aziende del continente nella loro trasformazione verso una leadership mondiale.

Per quanto concerne la materia della sicurezza, Horizon 2020 propone un Work Programme apposito (Secure Societies) attraverso il quale veicolare proposte di progetti dedicati alla protezione del cyberspace e delle IC, incentivando la ricerca in tema di cyber security e di lotta al cyber crime e cyber terrorismo, assicurando la protezione della libertà e la sicurezza dei Paesi dell'Unione Europea e dei suoi cittadini.

A titolo di esempio, oltre alla precedente descrizione di BODEGA (finanziato attraverso H2020), si fornisce di seguito la traccia di due dei bandi per progetti di ricerca sulla sicurezza in scadenza nel corso del 2015.

4.1. DRS-12-2015: Critical Infrastructure "smart grid" protection and resilience under "smart meters" threats

Gli smart meter, dispositivi che trovano il loro impiego principale nelle infrastrutture di distribuzione dell'elettricità basate su smart grid, misurano il consumo di una risorsa (ad esempio quella elettrica) ad intervalli temporali prestabiliti e comunicano tale informazione al fornitore del servizio. Oltre ad agevolare la fatturazione, questa informazione permette che sulla smart grid diventi possibile un'allocazione dinamica, on-demand, della risorsa, evitando inutili sprechi e rendendo più efficiente l'intero sistema di approvvigionamento. Gli smart meter sono spesso dotati di un'interfaccia WiFi che permette di collegarli alla rete LAN domestica, in maniera tale da poter consultare le informazioni contenute in essi (ad esempio statistiche relative ai consumi) da un computer oppure attraverso dispositivi dedicati noti come "in-home displays". A questa interessante possibilità fa da contraltare un rischio per la sicurezza. In caso di vulnerabilità, lo smart meter potrebbe costituire una testa di ponte per l'accesso di un cyber attacker all'intera rete LAN cui il dispositivo è connesso, garantendogli il controllo su un insieme di apparati che operano su di essa, quali computer, tablet e telefoni ma anche impianti di riscaldamento, frigoriferi, sistemi di videosorveglianza, ecc. ("Internet of things").

L'obiettivo del bando è quello di analizzare le nuove minacce insite nell'utilizzo degli smart meter e proporre soluzioni concrete per mitigare i rischi associati e ridurre di conseguenza le vulnerabilità (anche a fronte di attacchi cibernetici).

4.2. FCT-1-2015: Forensics topics: Tools and infrastructure for the fusion, exchange and analysis of big data including cyber-offences generated data for forensic investigation

Le informazioni che le agenzie di law enforcement sono oggigiorno in grado di raccogliere durante le loro investigazioni su crimini di varia natura (incluso il cybercrime) sono innumerevoli e di natura solitamente eterogenea.

Quelle prodotte durante i cyber attack sono particolarmente interessanti sia per la repressione del crimine informatico sia per

sviluppare soluzioni di "attacco" più sicure. Tale risultato può essere perseguito attraverso la realizzazione di una piattaforma per la raccolta, analisi, interpretazione, fusione, salvataggio e condivisione dei dati, in grado di processare informazioni di diversa natura, strutturate e non-strutturate, ed estrarre da queste "valore". Ci si aspetta che l'utilizzo di tecniche avanzate di Big Data Analytics come Data e Video Mining e Text Mining, consentirà alla piattaforma di velocizzare e rendere estremamente più accurate rispetto al passato tutte le operazioni di analisi, con ovvie conseguenze benefiche per quel che riguarda la sicurezza della società nel suo complesso.

Conclusioni

L'esigenza di una maggiore protezione dalla minaccia cibernetica sta divenendo sempre più pressante per i Paesi dell'Unione Europea. Il proliferare dei rischi di sicurezza legati a nuove e sempre più letali cyber weapon pone tutti i Paesi moderni in una situazione potenzialmente molto pericolosa. Una risposta efficace può essere elaborata soltanto attraverso l'attiva cooperazione tra tutti gli operatori, pubblici e privati, esposti al rischio.

La Commissione Europea si pone l'obiettivo di coadiuvare tale processo di collaborazione attraverso il varo di diverse linee di finanziamento dedicate a progetti di ricerca e sviluppo nel campo della cyber security. Zanasi & Partners, forte delle sue competenze e della sua esperienza in progetti europei, sta operando attivamente in questo contesto.

Bibliografia

Lynn, W.J. (2010). Defending a new domain. The Pentagon's Cyberstrategy. Foreign Affairs, 89(5).

Clarke, R.A., & Knake, R. (2010). Cyber War. The Next Threat to National Security and What to Do About It. Manhattan, NY: Ecco Press.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. The RUSI Journal, 157(1), 6–13.

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32.

Martino, L. (2013). La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica. Reperibile all'indirizzo: http://www.cssi.unifi.it/upload/sub/Martino La quinta dimensione.2.pdf

ENISA. (2014). Inventory of CERT teams and activites in Europe. Reperibile all'indirizzo: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Scott, A.N. (2002). Can cyberterrorists actually kill people? Reperibile all'indirizzo: http://www.sans.org/reading-room/whitepapers/warfare/cyberterrorists-kill-people-820

FrancoAngeli
Scienza Politica
e Relazioni Internazionali

Cyber Warfare 2014

La quinta Conferenza Nazionale sulla Cyber Warfare si è svolta con una nuova formula, in due edizioni: la prima, "Lo Sviluppo delle Armi Cibernetiche" (Roma, 11 ottobre 2014), dedicata ad un approccio strategico e la seconda, "L'utilizzo della Cyber Intelligence per la Difesa del Business" (Milano 13 ottobre 2014), dedicata a problematiche economiche. Il progressivo aumento della frequenza di attacchi informatici sempre più sofisticati e dirompenti rende prioritaria l'introduzione di innovazioni politico-strategiche, organizzative, tecnologiche e culturali affinché i decisori politici ed aziendali siano costantemente aggiornati e pronti ad interagire in tempi brevissimi garantendo, come già affermato nelle scorse edizioni, una stretta collaborazione tra mondo civile, militare e accademico. L'evento è stato ideato dal Centro Interdipartimentale Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università di Firenze, dall'Istituto per gli Studi di Previsione (ISPRI), dal Centro Studi Difesa e Sicurezza (CESTUDIS) e dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) de "La Sapienza" di Roma, d'intesa con Maglan Group – Information Defense and Technologies. La Conferenza ha avuto l'adesione del Presidente della Repubblica e sua Medaglia di Rappresentanza ed il patrocinio di Senato della Repubblica, Ministero della Difesa e Ministero dello Sviluppo Economico.

Umberto Gori, professore emerito dell'Università degli Studi di Firenze, è presidente del Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII) e direttore dell'Istituto per gli Studi di Previsione e le Ricerche Internazionali (ISPRI).

Serena Lisi è docente a contratto di Analisi e Pianificazione delle Operazioni di Pace all'Università degli Studi di Firenze.

MAGLAN
Information Defense & Intelligence

FrancoAngeli
La passione per le conoscenze

ISBN 978-88-917-1425-1