Atti Convegno Cyber Crime Conference 2018 - Tavola Rotonda

Author : Redazione

Date : 28 maggio 2018

Sistemi di Machine Learning, Blockchain, IoT e Big Data nelle mani dei Cyber Criminali - Come evolve il Cyber Terrorismo e quali sono i nuovi rischi per Stati ed Industria

Pierluigi Paganini: Buongiorno a tutti e, innanzitutto, grazie per essere qui; voglio ringraziare anche l'organizzazione per l'invito che ha voluto farmi. Sono Pierluigi Paganini, attualmente rivesto diverse cariche - sono membro del gruppo analisi minacce dell'Enisa, sono coautore delle norme di comportamento tra Stati nel cyber spazio approvata nel corso del G7 Summit tenutosi in Italia e sono CTO dell'azienda Cybersec. Oggi sono qui con alcuni colleghi e amici con cui cercheremo di capire come stia mutando lo scenario tecnologico, con particolare riferimento allo scenario delle minacce - proprio in relazione all'evoluzione di queste nuove tecnologie - e di come stiano ampliando quella che, in gergo, definiamo la nostra “superficie di attacco”: per comprendere che benefici portino queste nuove tecnologie, ma anche per dare una serie di *alert* legati al loro utilizzo talvolta improprio che espone governi, cittadini e infrastrutture critiche a minacce di cui poi leggiamo sui giornali. Tali minacce talvolta risultano devastanti arrivando a mettono a rischio persino il concetto di democrazia su cui si fondano gli Stati.

Oggi sono con me - li presento e poi, nel corso della Tavola, porrò a ciascuno di loro alcune domande - il **Colonnello Giovanni Reccia**, Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza; il **dottor Francesco Taverna**, Direttore Tecnico Principale della Polizia di Stato; Il **professor Andrea Margelletti**, presidente del Centro Studi internazionali (Ce.SI); l'amico **Andrea Rigoni**, *advisor* internazionale ed esperto di Cyber Defence; e infine il **dottor Gregorio D'Agostino** del centro Enea Casaccia, con cui approfondiremo alcune tematiche di ricerca.

Andrei subito nel vivo con le domande, partendo dal Col. Reccia: Colonnello, nell'attuale scenario stiamo assistendo a un incremento significativo delle minacce; ma quello che preoccupa maggiormente è, secondo me, il livello di complessità di tali minacce. Qual è

secondo lei la fenomenologia criminale che sta impattando maggiormente gli utenti, le aziende e gli stati?

Col. Giovanni Reccia: Sotto il profilo degli attacchi informatici noi abbiamo una visione riferita agli aspetti economico-finanziari, fondamentali per lo sviluppo del Paese. Principalmente le frodi informatiche che cerchiamo di individuare vanno a impattare su due piani: quello, a carattere sociale, dei cittadini - è evidente che quando si va a colpire un risparmiatore che subisce un’esfiltrazione di dati tramite ad esempio una carta di credito clonata, ciò può avere effetti negativi sull'intero sistema bancario del Paese - e dall’altro sul sistema imprenditoriale. Infatti un imprenditore può trovarsi davanti ad un’esfiltrazione di documenti, magari relativi a brevetti, determinando anche problemi di concorrenza sleale, oppure, ad esempio, rispetto agli strumenti di ingegneria sociale mirati ad individuare e capire che tipo di operazioni economiche stia per intraprendere l'imprenditore, come negli attacchi *man-in-the-middle* in cui qualcuno assume l'identità digitale di una delle parti ed effettua una serie di operazioni per conto della vittima: anche questo ha naturalmente degli effetti negativi e può essere distorsivo del sistema economico legale.

Diciamo però che, sotto il profilo della fenomenologia che noi ci troviamo ad affrontare quotidianamente, è il Dark Web a influire sull’intero sistema. Di recente sono stato a Milano per discutere di *e-commerce* legale e delle problematiche legate ai siti web d’impresa, ma esiste anche un *e-commerce* assolutamente illegale: avete tutti presente la figura contenente l'iceberg

a cui si ricorre spesso anche a livello internazionale per distinguere il *Clear web* (la parte emersa) da tutto quel mondo sommerso rappresentato da Deep Web e Dark web. Ebbene nella parte sottostante fiorisce un commercio illegale di armi, stupefacenti ma anche di informazioni, servizi illegali e vere e proprie guide per effettuare attacchi informatici a danno di privati e aziende. In questo senso il sistema tradizionale di controllo del web è “saltato” ed è necessario individuare nuovi strumenti d’intervento. Sappiamo che il principale browser di accesso al Dark web è TOR, The Onion Router, che presenta notevoli difficoltà di individuazione dei soggetti operanti grazie alle tecniche di anonimizzazione degli utenti e crittografia della comunicazione/segnale. Questo comporta una serie di necessità: da un lato trovare nuovi strumenti tecnologici su cui confrontarsi soprattutto con le aziende e gli istituti di ricerca, con cui abbiamo intrapreso rapporti per trovare soluzioni operative di carattere tecnologico; dall'altro lato ci sono esigenze più prettamente di polizia, in cui si prova a intervenire attraverso le cosiddette “operazioni sotto copertura”. Tra questi due estremi dovremmo provare comunque a cercare altri strumenti, come normative condivise e forme di cooperazione tra Stati soprattutto nello scambio di informazioni: probabilmente è così che in futuro dovremo agire tutti insieme.

Pierluigi Paganini: Sposo *in toto* quanto lei ha detto e aggiungo qualche altro elemento. Di recente ho pubblicato il mio ultimo libro, che riguarda proprio le tematiche legate al Dark web. Nel raccogliere le necessarie informazioni mi sono confrontato spesso con il potenziale del Dark web, un dominio in cui abbiamo diverse tipologie di attori: attori *Nation State,* sindacati criminali - badate bene, parliamo di organizzazioni complesse, strutturate in maniera gerarchica, in cui a ciascun livello è assegnata una specifica funzione - ma quello che mi ha più spaventato è che, in taluni casi, ho trovato giovani, ragazzi, che in maniera più o meno cosciente accedevano facilmente a questa parte oscura del web e con altrettanta facilità scaricavano di tutto, dal *malware* spia per il telefonino a codici malevoli di altro tipo; c'è poi ovviamente il mercato degli stupefacenti e in particolare il fenomeno - in preoccupante aumento - che riguarda la vendita di sostanze anabolizzanti.

Col. Giovanni Reccia: direi che il profilo del *vendor* nel Dark web è decisamente eterogeneo; non sono da escludere - anzi, ci sono sicuramente - collegamenti con la criminalità organizzata, che nell'arco di 20-25 anni ha scelto di “modernizzarsi” anche spostando, in molti casi, la propria “piazza” illegale dalla città al *Dark web*.

Pierluigi Paganini: Grazie, Colonnello. Passiamo ora la parola al dottor Taverna, con cui vorrei discutere di un altro aspetto. Il tema di questa Tavola, a cui abbiamo già accennato, sono le nuove tecnologie - parliamo di *blockchain*, internet delle cose, tecnologia *mobile*, intelligenza artificiale: secondo lei in che modo queste tecnologie stanno mutando in maniera rapida lo scenario delle minacce e qual è quella che maggiormente preoccupa, alla luce dei fenomeni che state osservando in questo periodo?

Francesco Taverna: Innanzitutto vi ringrazio per avermi invitato in questo autorevole consesso. Rispondo chiarendo da subito che il panorama delle minacce cyber è complesso, non solo per i cittadini fruitori della tecnologia, ma anche per gli attori istituzionali che i cittadini hanno il dovere di proteggerli.

Da un lato il legislatore è stato costretto a un cambio di passo nel tentativo di adeguare la

normativa vigente - in particolare il diritto penale - alla tutela di nuovi beni giuridici, quali la privacy e la sicurezza informatica; dall'altra noi operatori di polizia siamo costretti ad una continua rincorsa, nel tentativo di colmare il *gap* culturale che ci separa dalla conoscenza minima necessaria per comprendere i nuovi fenomeni cybercriminali e farvi fronte nella maniera più adeguata possibile. Ovviamente parliamo di uno scenario molto complesso: quello che stiamo constatando in particolare è una crescita asimmetrica tra la tecnologia e la consapevolezza del suo corretto utilizzo. Oserei dire che, se la prima cresce in modo esponenziale, l'*awareness* - sia sul fronte della tutela della privacy che su quello della sicurezza dei dati - ha un andamento al massimo lineare. Cito ad esempio la superficialità con cui l'utente medio della tecnologia condivide le proprie informazioni personali sui social network, prestando il fianco non solo alle *Big Companies* che sfruttano questi dati per fini commerciali, ma anche ai cybercriminali che, attraverso tecniche di *social engineering*, si ritrovano così in mano una miriade di informazioni utili per sferrare attacchi sempre più astuti e mirati. Un altro problema, a mio avviso, è la tecnologia a basso costo che ha semplificato la vita di molte piccole e medie imprese ma che ha portato con sé, come corollario, enormi rischi per la sicurezza. Mi riferisco a tutte quelle aziende che optano per soluzioni economiche *in house* - ad esempio sviluppando il proprio sito web o la propria Web Application utilizzando i *plugin* di un CMS gratuito, magari reperito sul web - che probabilmente offrono un risultato, dal punto di vista qualitativo e funzionale, non molto differente da quello di un prodotto professionale, ma sicuramente più povero in termini di sicurezza. Così, ancora oggi, ci troviamo ad affrontare minacce che speravamo di non dover più riscontrare: sono ancora numerose le segnalazioni di attacchi di tipo *SQL injection* - sembra assurdo ma è così - finalizzate al *dump* dei dati o semplicemente al *defacement* per scopi dimostrativi. A tal proposito l'*hactivismo* ha cambiato pelle: non ci troviamo più ad affrontare *crew* criminali dotate di enormi *skill*, perché la facilità con cui è possibile reperire in rete *tool* automatici finalizzati a *penetration testing* - ma che all'occorrenza possono essere convertiti in strumenti offensivi - fa sì che gli hacker scandaglino la rete alla ricerca di falle nella sicurezza e colpiscano il primo sito web vulnerabile, incontrato in modo quasi casuale, per poi rivendicare capziosamente l'attacco come fosse l'esito vittorioso di una campagna mirata.

Da un punto di vista statistico sono molte le segnalazioni che ci arrivano di attacchi DoS e DDoS, anche con finalità estorsive (mi riferisco al DDoS for Bitcoin): lo scorso anno sono stati 49 gli episodi di *denial of service* che ci hanno denunciato le infrastrutture informatiche che noi monitoriamo. I numeri sono costanti - abbiamo avuto sette episodi nel solo mese di marzo - ma ci preoccupa più che altro il potenziale impatto economico di questo tipo di attacchi: come diceva il colonnello Reccia, oggi sul mercato nero è possibile addirittura noleggiare intere *botnet* - costituite anche da dispositivi IoT compromessi, il caso *Mirai* ne è stato un esempio - che riescono a sferrare attacchi TCP o UDP *flooding* anche a diverse centinaia di Gigabit per secondo; quindi parliamo di numeri importanti. Diciamo che, se le infezioni da Ransomware sono diminuite - in questo senso abbiamo un dato confortante, anche in virtù del fatto che cittadini e imprese sono sempre meno disposti a cedere ai ricatti degli estorsori - constatiamo invece un incremento delle minacce APT che colpiscono le grandi organizzazioni; peraltro siamo convinti che i numeri che abbiamo siano una stima per difetto dei dati reali. Questo perché le grandi aziende spesso non denunciano di essere rimaste vittime di questa tipologia di attacco per timore di un danno reputazionale. Auspichiamo che con l'entrata in vigore del GDPR il prossimo 25 maggio e poi con il recepimento della direttiva NIS qualcosa cambi e che gli

obblighi di notifica (con il conseguente regime sanzionatorio previsto per gli inadempienti) costituiscano un deterrente alla reticenza degli attori coinvolti nel denunciare gli attacchi subìti.

Pierluigi Paganini: Lei ha citato il GDPR. Cosa immagina possa accadere da Maggio in poi: uno scenario in cui una serie di attacchi clamorosi possano effettivamente portare alla luce realtà scomode - una gestione non oculata del patrimonio informativo di un'impresa, l'esposizione più o meno approssimativa di tutto gli *asset* aziendali - oppure pensa che ci sarà un progressivo adeguamento e quindi bisogna "correre" prima che accada l'incidente?

Francesco Taverna: Mi auguro che il GDPR segni uno spartiacque, ma temo non sarà così immediato. Noi, dal punto di vista delle forze di polizia, non possiamo far altro che aumentare le nostre attività preventive: quindi spingere le imprese e gli enti pubblici che monitoriamo attraverso il nostro centro di controllo delle Infrastrutture critiche (C.N.A.I.P.I.C.) a uscire allo scoperto e rivelare gli attacchi subìti, perché appunto la diffusione delle informazioni e la condivisione di esperienze e *best practice* rappresentano il terreno su cui dobbiamo continuare a muoverci, non solo a livello nazionale ma ovviamente anche internazionale. Aggiungo, a questo proposito, che è in procinto di partire un progetto che estenderà la logica del C.N.A.I.P.I.C. a livello territoriale, con l'individuazione di alcuni centri di eccellenza nei compartimenti regionali che avranno facoltà di stipulare, a loro volta, convenzioni con enti pubblici e privati locali, in modo da aumentare la pervasività della nostra azione sul territorio: il fine è quello di convogliare e diramare le informazioni relative a vulnerabilità, attacchi e minacce dal centro verso la periferia - e in direzione opposta.

Pierluigi Paganini: La ringrazio. Parliamo di impresa e in questo senso voglio chiedere ad Andrea Rigoni: quanto è importante oggi una Cyber strategia di impresa e qual è la situazione effettiva che ci troviamo davanti quando parliamo di aziende italiane, con particolare riferimento alle piccole e medie aziende ma considerando anche la grande impresa? Quanto sono pronte a recepire il concetto di Cyber strategia?

Andrea Rigoni: Le aziende non sono pronte, in senso assoluto. Alcune stanno senz'altro prestando più attenzione, il problema è che con la crescita esponenziale sia dei profili di vulnerabilità sia della complessità della minaccia, l'attenzione - che è stata molto ritardata, di fatto l'Italia parte con un programma istituzionale nel 2013 (l'Inghilterra è partita nel 1986) e di riflesso anche il settore privato ha iniziato ad essere sensibilizzato in ritardo - dicevo: la crescita di vulnerabilità, minacce e del conseguente impatto, gli ingredienti fondamentali con cui costruiamo la torta del rischio, crescono in maniera esponenziale. Secondo me abbiamo già raggiunto il punto in cui la crescita delle nostre capacità di protezione e governo del rischio non sono sufficienti. Ripeto, non ci vuole un futurologo per comprenderlo: se da una parte cominciamo a muovere i primi, timidi passi verso iniziative legate alla robotizzazione e all'*Artificial intelligence*, dall'altro è evidente che questi strumenti, per organizzazioni e attori molto motivati, sono già oggetto di forte attenzione. Pensiamo anche ai temi legati alla *blockchain* e alle criptovalute: diventano un'opportunità per il business, ma lo sono anche dal lato delle minacce. Immaginiamo, quindi, come un'organizzazione possa oggi, con gli strumenti limitati che ha, difendersi e fronteggiare questi scenari. Diventa quindi fondamentale - né più nemmeno di come viene fatto sulla difesa nazionale o la salute pubblica - un intervento coordinato da una strategia che collochi precisamente il ruolo di ciascun attore. Qui spendo due parole: da una parte, c'è anche nel titolo del nostro *Panel*, l'introduzione di nuove tecnologie vengono sfornate a ritmi che nemmeno gli esperti specifici di settore riescono più a sostenere. Ogni giorno ci sono, non tanto nuovi prodotti ma nuovi algoritmi e nuovi approcci, la cui adozione da parte del mercato è ormai scellerata; lo si vede banalmente da qualche dato

statistico, come il numero di utenti che utilizzano software Beta sulle proprie piattaforme - non solo personali ma anche professionali - e l'adozione di nuovi strumenti (se guardiamo le applicazioni aziendali e personali che utilizziamo oggi non sono certo quelle di 3 o 5 anni fa). Il business oggi - penso al business del settore finanziario, dei trasporti, dell'Industria - tira a una velocità impressionante, e chi non tiene quella velocità è *out*. Non si possono porre dei limiti, rinunciare ad adottare nuove tecnologie: non proporre, ad esempio, l'*home banking* perché non è sicuro è assolutamente impensabile in una logica di mercato. Queste nuove tecnologie però sono prone, ovviamente, a nuove classi di vulnerabilità: mentre vent'anni fa, se un termostato aveva un collegamento telefonico, riuscivamo a imporre all'azienda di fare dei test, oggi non c'è predicibilità degli scenari di uso e, evidentemente, uno scenario che non riesco a prevedere diventa molto più difficile da tutelare.

Trasliamo questo dall'altra parte: come accennavo queste tecnologie non solo creano una vulnerabilità, ma alimentano le minacce. Quello che ci preoccupa di più sono gli attori che hanno risorse economiche e di capitale umano ingenti - quindi attori statuali, che come sappiamo stanno investendo molto su questo tipo di approcci. Quindi, ad esempio, l'utilizzo dell'intelligenza artificiale e degli RPA ci porrà presto le stesse sfide che oggi affrontiamo con i "super batteri".

Mi chiedevi delle aziende: è ovvio che le aziende debbano aumentare i loro livelli di attenzione ma, da sole, non possono fronteggiare minacce di questo genere. Sarebbe come chiedere a una famiglia di predisporre, con gli strumenti che ha a disposizione, la terapia contro una nuova malattia. Qui subentra il ruolo di istituzioni, organizzazioni e governi che devono costruire una strategia intorno a questi temi. È possibile che incentiviamo la digitalizzazione dimenticandoci che la sicurezza deve esserne una caratteristica fondamentale? Perché quando abbiamo fatto il piano Industria 4.0 non abbiamo obbligato ad adottare misure minime di Cyber Security? È chiaro che, una volta che ho costruito un aeroplano non sicuro, metterlo in sicurezza a posteriori è impossibile anche per un ingegnere aeronautico: non posso concepire un aereo che trasporta passeggeri o merci pensato senza componenti di *safety* e *security*. La stessa cosa ormai vale per le imprese: è impossibile pensare di costruire un nuovo processo, un nuovo servizio o una nuova applicazione senza forti caratteristiche di sicurezza. Ripeto come non sia sufficiente l'*awareness* - " Fallo in modo sicuro" - ma servono norme smart (un po' quello che ha cominciato a vedersi con il GDPR, ma che non è ancora sufficiente) - e dall'altra parte servono approcci sistemici. Se un'azienda punta tutto sull'Industria 4.0, va sul mercato e compra soluzioni intrinsecamente vulnerabili, noi possiamo anche dirgli che è obbligato a predisporre un piano di sicurezza, ma se quella tecnologia non è stata pensata - nemmeno a livello di prodotto, probabilmente a livello di ecosistema - in modo sicuro, cosa può fare il povero imprenditore?

Probabilmente dovremmo inserire anche l'agenda di ricerca - che nominalmente c'è nella nostra strategia nazionale ma bisogna farlo nella pratica, sviluppando queste componenti non solo a livello nazionale - perché bisogna cominciare ad aiutare anche il mercato ad andare in quella soluzione. È anacronistico, in un mercato globale, che un Paese come l'Italia (ma anche l'Unione Europea) pensi di regolare da sola l'*Internet of Things*: non si può fare da soli, bisogna cominciare a ragionare in termini di ecosistema. Una volta bastava mettersi d'accordo con l'FCC, la *Federal Communication Commission* degli Stati Uniti, il cui parere negativo diventava un grosso ostacolo all'introduzione del prodotto sul mercato globale perché quello statunitense

era il primo mercato: ora che la maggior parte dei prodotti, anche quelli disegnati negli Stati Uniti, vengono prodotti in Asia e c'è molta più innovazione e tecnologia che proviene dal continente asiatico, con la conseguente frammentazione regolatoria, le cose sono molto diverse.

Per concludere, ottima l'attenzione che viene sollevata dai nuovi regolamenti ma attenzione al rischio boomerang del GDPR, lo dico senza timore di smentita e ne riparleremo fra un anno o due. Prevedibilmente c'è stata una corsa agli adempimenti: peccato che il GDPR non sia un adempimento ma una filosofia che un'azienda dovrebbe approcciare abbracciare in modo molto più ampio sulla Cyber Security e, purtroppo, abbiamo una *regulation* che prende solo un piccolo pezzo. Vedo in giro, anche nelle aziende più grandi e mature, dotate di capacità e competenze, grosse difficoltà nel dover trattare - come sta avvenendo - un aspetto unico in maniera disomogenea.

Pierluigi Paganini: Grazie, Andrea. Passo la parola al dottor D'Agostino: finora abbiamo parlato di attacchi sempre nell'ottica dei potenziali danni legati all'esfiltrazione di informazioni e dati, o dei rischi per chi cada vittima di una frode. Però c'è, ovviamente, un altro risvolto della medaglia quando parliamo di attacchi cyber, ovvero la possibilità che comportino effetti fisici sulla realtà che quotidianamente viviamo. Ci può dire di più? Qual è il livello di separazione tra effetti logici ed effetti fisici di un attacco cibernetico?

Gregorio D'Agostino: Innanzitutto buongiorno a tutti e grazie per l'invito. La ringrazio molto per questa domanda perché, se ci riflettiamo, nel nome di questa conferenza c'è la parola *cyber***:** questo termine, in senso stretto e "didattico" - io insegno Sicurezza Informatica a Tor Vergata, oltre a occuparmi di infrastrutture critiche presso l'Enea - dovrebbe riferirsi esclusivamente a quegli effetti informatici che producono, appunto, effetti fisici sulle infrastrutture. Poi, a causa dell'indistricabilità di questi mondi (il mondo della sicurezza informatica e il mondo della sicurezza cyber) di fatto vengono usati come sinonimi, come anche oggi abbiamo ampiamente visto. Parlando di infrastrutture critiche, uno dei problemi più importanti è proprio in quale misura sia possibile, con mezzi puramente informatici, causare degli effetti fisici - e viceversa come, tramite delle vulnerabilità di tipo fisico, possiamo accedere a elementi conoscitivi di tipo strettamente informatico (essenzialmente risorse di calcolo o dati). Effettivamente, si tratta di due piani assolutamente indistricabili.

Per dimostrarlo ricordo due eventi storici: il primo (che è stato per me l'occasione in cui mi sono posto più chiaramente questo problema) è Stuxnet, forse l'esempio più maturo - c'erano stati casi precedenti, ma meno eclatanti - in cui un soggetto è riuscito, con un'azione deliberata, a colpire e inabilitare temporaneamente le centrifughe per l'arricchimento dell'uranio in Iran per ritardare i programmi di sviluppo nucleare di quel Paese, considerato ostile da questi soggetti. È molto interessante che lo si sia fatto utilizzando tutti gli strumenti che abbiamo citato oggi: ingegneria sociale (termine assolutamente non evocativo, perché non si tratta di altro che della conoscenza del mondo umano), vulnerabilità di tipo strettamente informatico - in maniera molto piena - e infine si è usata, ed è l'interessante concetto che richiamava ora Andrea Rigoni, un'innovazione tecnologica. In realtà l'attacco non si sarebbe potuto realizzare se i PLC di queste centrifughe fossero rimasti quelli vecchi perché i PLC in uso al momento dell'attacco erano riprogrammabili in maniera informatica, cosa che non si poteva fare nelle precedenti versioni. Quindi, cosa è successo? Nella manutenzione è stato riprogrammato il *firmware* in modo che si credesse che le centrifughe andassero a una velocità più alta, così ottenendo un effetto fisico con metodi puramente informatici. Questo è un esempio classico, interessantissimo in tema di armi perché si trattava di un'arma cyber selettiva e in grado di programmare il target: ci sono molti aspetti interessanti che ora non abbiamo modo di sviscerare, però si è trattato senz'altro di un evento importante. Quindi il concetto che richiamava Andrea è fondamentale: ogni volta in cui incontriamo un'innovazione tecnologica abbiamo nuove vulnerabilità e dobbiamo stare molto attenti a fornire simultaneamente tutti gli elementi di sicurezza necessari affinché quelle nuove vulnerabilità non si tramutino in un disastro. Questo è un *warning* che vale per qualunque cosa. Guardate, è lo stesso problema dei nuovi *meltdown* e dei recenti problemi con i processori: qualche soggetto molto intelligente in termini di programmazione *hardware* si è detto "sono in grado di prevedere ragionevolmente il flusso delle richieste e quindi uso questa conoscenza per accelerare la velocità del mio processo". Piccolo particolare, facendo questo violo dei criteri legati alle autorizzazioni; anche lì stessa cosa, un'innovazione e subito un problema. Ma, dicevo, il tema è anche l'inverso: non si può pensare di realizzare la sicurezza cyber senza la sicurezza fisica. Questo, lo dico sempre ai miei studenti, è una tecnica avanzatissima di crittografia chiamata *rubber hose cryptography*, che consiste sostanzialmente nell'avvolgere intorno al collo di una persona un tubo di gomma per estorcerle con la tortura le informazioni necessarie per acquisire l'accesso alla risorsa o al dato di nostro interesse. Essenzialmente, se qualunque oggetto - sia esso un dato o una risorsa informatica - è accessibile per un soggetto, vuol dire che intrinsecamente esiste una procedura

con cui possiamo forzare quell’accesso.

L’esperienza di qualche anno fa all’Osservatorio Nazionale, dove c'era anche il professor Margelletti, ci fa capire come questa disciplina coinvolga tutte le altre: non esiste un campo isolato dagli altri, l'aspetto fisico va insieme a quello informatico, legale, sociale, politico, di *decision making*. È un'unica battaglia, che bisogna combattere tutti insieme: questo per me è molto importante dal momento che mi occupo di scienza delle complessità. Un fenomeno importantissimo - emerso soprattutto in campo finanziario - è che a volte tutti i componenti di un sistema sono singolarmente funzionanti ma a livello sistemico presentano delle anomalie: questo si sta presentando anche nel campo cyber, per cui la battaglia si presenta complessa ma anche molto stimolante.

Pierluigi Paganini: La ringrazio. Bene, chiudo questo primo giro passando la parola al professor Margelletti. Parliamo di nuove tecnologie - mi viene in mente il mondo dei social network, ma non solo - e parliamo di un altro tipo di minaccia, il terrorismo: come sta cambiando, cosa è accaduto nell'ultimo decennio? In che modo i gruppi terroristici di tutto il mondo - non pensiamo soltanto allo Stato Islamico - utilizzano la tecnologia per aumentare l’efficacia dell’azione di propaganda e delle proprie operazioni? Chiedo al professore, che si occupa di queste tematiche all'interno del suo Centro Studi, come stia cambiando il fenomeno del terrorismo in ragione dell’introduzione delle nuove tecnologie.

Prof. Andrea Margelletti: Grazie, buongiorno a tutti. È per me un privilegio essere in questo *parterre de rois* di straordinario livello; è una gioia provare a imparare e io ce la metto tutta. Prima di iniziare, lasciatemi dire che quanto tratteggerò questa mattina è frutto delle conversazioni con il mio esperto cyber, il dottor Francesco Tosato (responsabile Area Difesa e Sicurezza dell'Istituto) che saluto e ringrazio: grazie per provare - spesso inutilmente - a far capire a un uomo analogico come sia il mondo digitale.

Allora, come stanno cambiando le cose? Prima di tutto faccio un esempio che vi parrà lontano del tempo, ma che mi aiuta ad avere un *framework* per comprendere meglio le cose di cui stiamo parlando. Per trent’anni, i palestinesi hanno condotto attacchi contro gli israeliani. Nessuno meglio di voi sa come la realtà sia infinitamente meno importante della percezione: per cui se io colpisco degli atleti alle Olimpiadi, oppure dirotto un aereo, sono indiscutibilmente un terrorista. I risultati dell’OLP, in 30 anni e rotti di guerra con Israele, sono stati sostanzialmente nulli. Poi è arrivata una nuova generazione, quella di Hamas: l’iconica l'immagine del ragazzino che lancia una pietra contro il carro armato israeliano è diventata parte dell'immaginario come quella dello studente a Piazza Tienanmen con le buste della spesa, percepito non come un terrorista ma come un combattente per la libertà; e questo per la prima volta nel 1993 porta gli israeliani al tavolo della pace con i palestinesi. Qual è la differenza strategica tra 30 anni di attentati con risultati zero e i risultati incredibili raggiunti in un anno (al prezzo di sacrificare una generazione?) Che l’OLP era nato nell'epoca della radio, Hamas nell'epoca della televisione: quindi conosceva perfettamente la potenza dell'immagine nel trasmettere un messaggio. La *leadership* del nuovo jihadismo - soprattutto quella nata dalla metà degli anni ‘90 - appartiene all'epoca della rete. Noi ci troviamo fondamentalmente oggi davanti a tre *pillars*: proselitismo, capacità di azione e realtà del mondo virtuale. Le tre cose sono assolutamente interconnesse. Poi c'è tutto l'aspetto che riguarda il finanziamento, che però è ancora molto confuso.

Il proselitismo: se vi chiedo quanti terroristi occidentali siano andati a far parte di Al Qaeda la vostra risposta sarà “non ne ho idea”, perché sono così pochi da non essere rilevanti; ma se vi chiedo quanti siano andati a combattere per l'Isis la risposta sarà “migliaia”. Dov'è la differenza? In un approccio completamente diverso: Al Qaeda era una realtà terroristica classica, l’Isis e le nuove organizzazioni jihadiste sono realtà ad architettura aperta a cui prendono parte anche persone con ruoli diversi, dal poliziotto al medico all’esperto cyber. Ed è completamente diversa la strategia di comunicazione. Uno degli uomini che meglio conosceva Il mondo jihadista era il fondatore del movimento talebano, il famoso mullah Omar che, riferendosi agli occidentali, diceva “Voi avete gli orologi, noi abbiamo il tempo”. Ebbene, le attività di proselitismo - ed è la vera grande battaglia che quotidianamente conducono le forze dell'ordine e i miei amici dell'*intelligence*, in prima fila il Dipartimento per le Informazioni e la Sicurezza - sono dirette a bambini di 6 o 7 anni, lasciati soli dai genitori con una baby-sitter che prima era reale ma oggi è spesso virtuale. Se andate nel Dark web vi troverete davanti, più che al gioco *Call of Duty*, ad una vera *Call of Jihad*. Questo passa non solo per i canali social, ma anche attraverso i sistemi di messaggistica istantanea (recentemente DIGOS e Polizia Postale hanno colpito a Trieste una realtà di questo tipo).

Secondo punto, la pianificazione: nei video dei jihadisti sul web trovate regolarmente microdroni o Google Maps (strumenti ormai accessibili a chiunque), quindi la capacità di geolocalizzare e individuare i bersagli con estrema precisione - cosa che fu fatta già, a uno stadio larvale, l’11 settembre 2001 - è ormai parte integrante della pianificazione terroristica.

Infine, i cyber attacchi: In questo momento non c'è organizzazione terroristica che sia in grado di condurre un attacco Cyber della stessa portata di una realtà statuale, ma non vi è dubbio che la capacità di colpire la qualità della vita terrorizzando con un camioncino o un pullman le strade delle nostre città sia parte dominante delle conversazioni jihadiste. Non più colpire i palazzi del potere ma la quotidianità, negando a tutti noi l’accesso a beni primari o cambiando radicalmente il nostro stile di vita: se Al Qaeda puntava sull’atomica sporca, i jihadisti d'oggi - gente di vent'anni o anche meno - puntano ad attaccare i nodi di qualità della nostra esistenza.

Pierluigi Paganini: Chiudiamo la Tavola Rotonda (per poi proseguire con una serie di interessanti riflessioni che si svilupperanno nell’arco della giornata) con un pensiero che mi sembra riassuma quello che ci siamo detti finora. Sicuramente le nuove tecnologie - che siano sistemi di *Machine Learning*, *blockchain*, *big data, Internet of Things* - stanno modificando profondamente la nostra società e il modo di operare di chi ne abusa. Tra le tecnologie che ho appena menzionato, personalmente quella che mi preoccupa di più è legata al potenziale abuso dei sistemi di *Machine learning*, strumenti di autoapprendimento che, se da un lato possono sicuramente servire a una difesa sempre più automatizzata, dall'altro possono essere usati per condurre attacchi di capacità superiore proprio grazie alla possibilità di offendere in funzione della risposta che ci si trova davanti. Grazie!