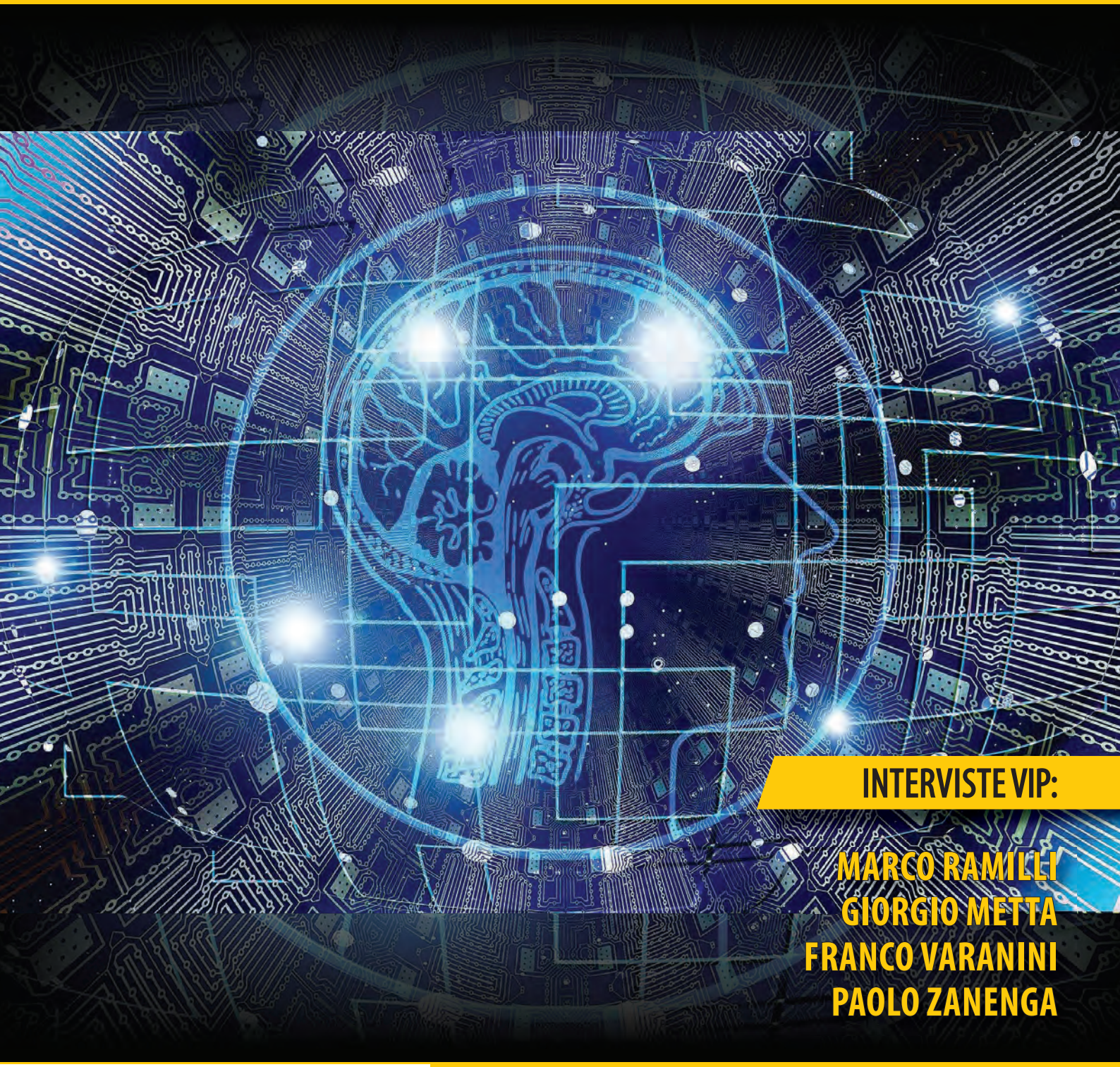
Cybersecurity Trends

Edizione italiana, N. 3 / 2020



INTERVISTE VIP:

MARCO RAMILLI
GIORGIO METTA
FRANCO VARANINI
PAOLO ZANENGA

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Folder centrale: Machine Learning & Threat Hunting

Global Cyber Security

La Fondazione GCSEC è un'organizzazione senza scopo di lucro, creata per promuovere la sicurezza informatica in Italia e nel resto del mondo. Il Centro, fondato e finanziato da Poste Italiane, ha sede a Roma e collabora con Istituzioni Italiane e Internazionali Governative, enti privati, istituti di ricerca e organismi internazionali.
La missione della Fondazione è quella di sviluppare e diffondere la conoscenza e la consapevolezza sulla sicurezza informatica, creando le condizioni per migliorare le capacità, le competenze, la cooperazione e la comunicazione tra i diversi attori coinvolti nell'uso e nella protezione di Internet.

Information Sharing
Creazione di modelli di information sharing pubblico - privato

Threat Intelligence
Analisi di modelli di attacco e delle tecnologie necessarie a velocizzare l'analisi stessa

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione e corsi di specializzazione e master

Fondazione Global Cyber Security Center
Viale Europa, 175 – 00144 Roma
www.gcsec.org

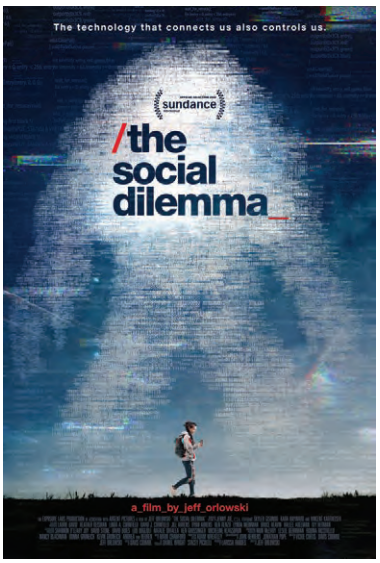
GLOBAL CYBER SECURITY CENTER

Indice

Essere responsabili non è più un'opzione

Autore: Nicola Sotira

In questi giorni si è discusso molto nei blog ed in rete sul film "The Social Dilemma" disponibile sulla piattaforma Netflix, inoltre, ho ritrovato, molto spesso, le citazioni del film anche nei convegni dove il film viene usato in modo strumentale. Il film, grazie ad una serie di racconti di operatori della Silicon Valley che hanno lavorato negli



OTT, ci espone retroscena riguardanti le piattaforme digitali che, lavorando sulle nostre vulnerabilità, ci *"manipolerebbero"* in nome del profitto. The Social Dilemma si muove su alcuni assi principali: la trasformazione digitale, manipolazione/persuasione, noi visti come un prodotto e non ultimo la sorveglianza digitale con la bravissima Shoshana Zuboff.

Uno dei temi nel film è quello della trasformazione e metamorfosi digitale, l'accelerazione della tecnologia che non va di pari passo al nostro apprendimento, le nostre difficoltà nello stare al passo della crescente innovazione. Inoltre, si cerca di mettere in luce anche il lato oscuro: da un lato gli enormi cambiamenti, assolutamente positivi, a livello globale e dall'altro la nostra dipendenza e l'utilizzo ossessivo delle diverse piattaforme digitali. L'analisi si sviluppa, successivamente, sul tema del profitto e di come viene generato; un profitto basato su dati, analisi e previsioni dove il prodotto è il consumatore delle piattaforme. Il teorema che viene enunciato è che non siamo più in un mercato basato sulla vendita di prodotti e servizi, ma in uno scenario dove i nostri dati, arricchiti dalle nostre abitudini e comportamenti in rete, sono i nuovi features.

Ovviamente il tutto gestito da una rete di algoritmi che usano il genere umano come una cavia da laboratorio. In ultimo il film analizza i temi della persuasione e delle *fake news*; le tesi puntano il dito sull'utilizzo di tecnologie sofisticate e sull'uso dei social per la persuasione degli utenti che vengono, pertanto, indotti ad acquisti mirati oltre a influenzare scelte politiche e gestire movimenti di opinione. Lo scenario dipinto è quello di una rete utilizzata come strumento di dubbia moralità. Un'arma digitale in grado di

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

determinare conseguenze rilevanti nel campo sociale e politico di un paese. Quest'ultimo aspetto è poi connesso alle *fake news* e all'allarmismo creato artificialmente dagli algoritmi che gestiscono le piattaforme digitali. Il film sostiene la tesi per la quale la manipolazione digitale ha sia scopi puramente commerciali, quindi con un'ottica di puro profitto, che l'obiettivo di orientare gli utenti della rete in un modo impercettibile ma costante influenzando quindi la società, la politica e l'economia.

Questa disinformazione verrebbe amplificata a dismisura grazie all'utilizzo crescente dei social network sino a generare, in casi estremi anche disordini sociali. Abbiamo visto tutti, per esempio, il ruolo che ha giocato la disinformazione sul tema COVID. Che cosa fare quindi per arginare questo dominio, almeno come viene presentato nel film? Sicuramente il digitale e lo sviluppo della tecnologia sta contribuendo allo sviluppo economico della società e contribuisce anche a migliorare la nostra qualità di vita. Certamente ci sono anche aspetti negativi, che vanno contrastati con la cultura, l'investimento sulla scuola e la formazione.

L'utilizzo consapevole di questi strumenti e la cultura digitale deve fare parte della formazione delle nuove generazioni e non solo. Abbiamo anche, però, un tema di responsabilità che spetta solamente a noi, se in rete spopola un movimento che cerca proseliti e vuole convincerci che la terra è piatta probabilmente la responsabilità delle piattaforme sta nel diffonderla, ma noi possiamo non aderire né promuoverla sapendo che è una discussione anacronistica e forse poteva avere un senso ai tempi di Galileo, ma oggi è paradossale. Lo stesso atteggiamento che dobbiamo avere nell'indossare responsabilmente i dispositivi di protezione individuale per contrastare la

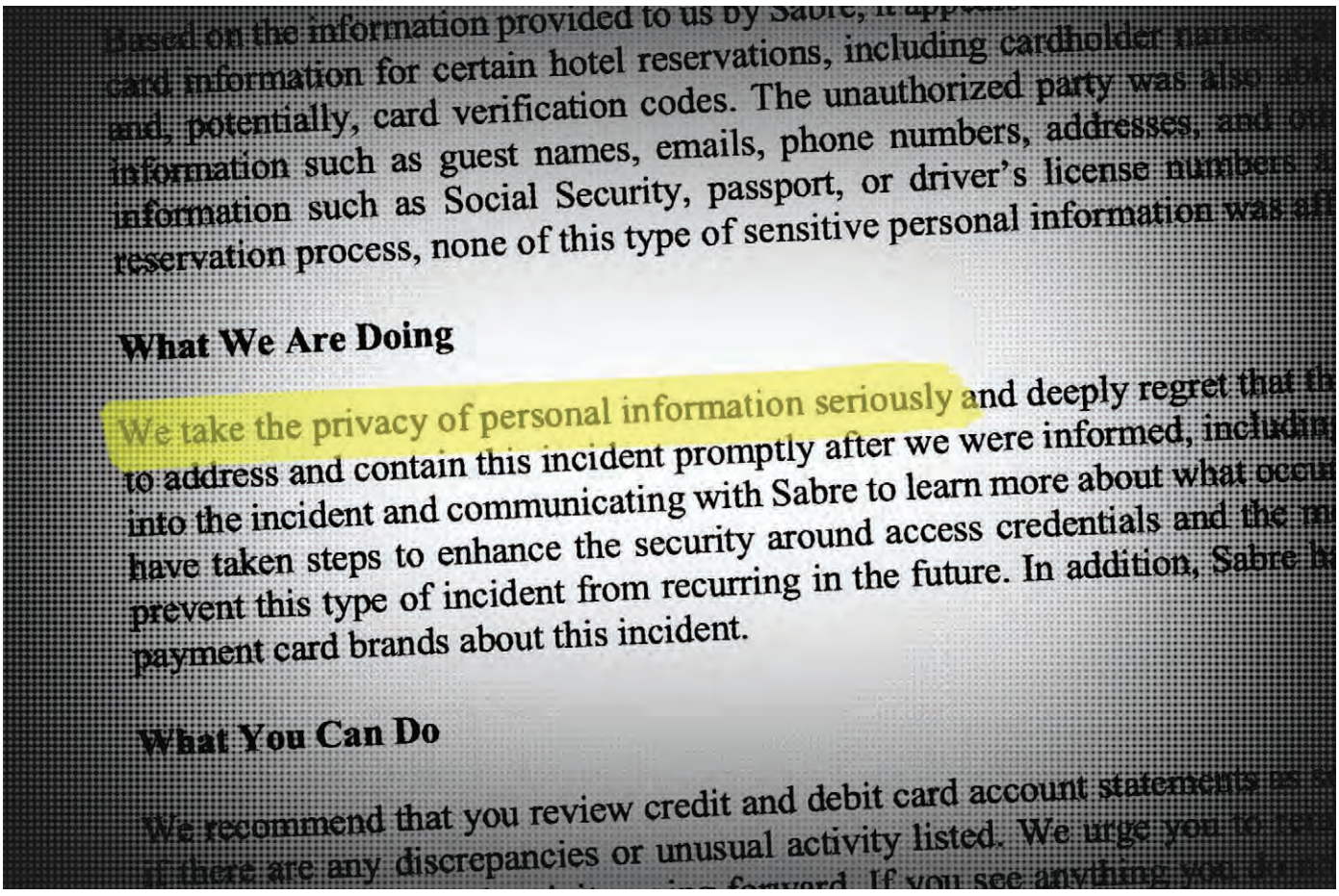
diffusione del COVID, stesso atteggiamento sull'utilizzo del monopattino elettrico che sembra si parcheggi da solo sulle strisce pedonali.

In questo contesto NOI facciamo la differenza ed il nostro comportamento responsabile gioca un ruolo fondamentale.

Social e piattaforme digitali, come presentato nel film, sono popolati di algoritmi, che scriviamo e progettiamo NOI, sempre NOI clicchiamo e utilizziamo queste piattaforme.

NOI siamo il motore del possibile cambiamento e NOI dobbiamo contribuire ad uno sviluppo etico anche con i nostri comportamenti.

Se diventiamo consumatori etici e responsabili anche gli OTT inseguiranno questa tendenza solamente perché genererà loro profitto. ■


Based on the information provided to us by Sabre, it appe
card information for certain hotel reservations, including cardholder
and, potentially, card verification codes. The unauthorized party was also
information such as guest names, emails, phone numbers, addresses, and
information such as Social Security, passport, or driver's license numbers
reservation process, none of this type of sensitive personal information was af

What We Are Doing

We take the privacy of personal information seriously and deeply regret that th
to address and contain this incident promptly after we were informed, includin
into the incident and communicating with Sabre to learn more about what occu
have taken steps to enhance the security around access credentials and the
prevent this type of incident from recurring in the future. In addition, Sabre h
payment card brands about this incident.

What You Can Do

We recommend that you review credit and debit card account statements
there are any discrepancies or unusual activity listed. We urge you

La bionica porterà un cambiamento così radicale da farci interrogare sul *significatio* stesso della vita

Intervista VIP a Marco Ramilli

Autore: Massimiliano Cannata

Ing. Ramilli, la diffusione della IA è un tema che interessa e affascina sempre di più non solo gli addetti ai lavori. Nei giorni scorsi se ne è parlato anche al festival della filosofia che si svolge a Modena Carpi e Sassuolo. Macchinazione il titolo. Come ha spiegato Il filosofo Roberto Esposito nel suo intervento introduttivo, l'uomo si è sempre servito di strumenti sempre più potenti per tentare di aggirare e dominare la natura. Quali sono le opportunità e i rischi di questo nuovo orizzonte che il rapporto uomo e robot apre?

Le opportunità che si manifestano grazie all'utilizzo di tecnologie avanzate come per esempio, la diffusione dei Robot sono ampissime. Siamo alla vigilia di una nuova era, di un nuovo scatto evolutivo. Grazie a questi strumenti sarà possibile ridurre il lavoro fisico dell'essere umano, ridurre la percezione della "fatica", durante le nostre vite, potremmo illuderci di avere più tempo da passare con i nostri cari, riducendo le ore di permanenza in ufficio. Grazie alla bionica risulterà possibile "amplificare il nostro corpo", donandoci capacità che oggi a stento sogniamo. Potremo inoltre sostituire parti di noi stessi con componenti meccatronici (arti meccanici, orecchio artificiale, etc.), che ci permetteranno una vita più lunga. Tale tecnologia, quando sarà a regime, introdurrà un cambiamento cosi radicale da dover rivalutare il significato stesso della vita e di conseguenza del genere umano.

Siamo insomma di fronte, come ha scritto Roberto Cingolani, a una "terza specie" con cui dobbiamo imparare a fare i conti?

Mi trovo in accordo con Roberto Cingolani nel pensare che avremo "a che fare" con una nuova specie, ma la cosa che ancora più mi affascina di questa nuova specie è la sua unicità nell'arco della storia. Infatti ogni evoluzione epocale, che ha segnato un'era geologica o antropologica non è mai stata "voluta" direttamente dall'uomo. Tutte sono state influenzate dall'uomo - certamente - ma non direttamente volute. Non è mai esistito un *"homo erectus"* che ha deciso spontaneamente di trasformarsi in un *"homo neanderthalensis"* o un *"homo neanderthalensis"* in *"homo sapiens"*. Invece alla vigilia di questa nuova era un *"homo sapiens"* può decidere di trasformarsi in *"cyborg"* cambiando cosi la propria specie.

BIO

Marco Ramilli, CEO e fondatore di Yoroi, è tra i massimi esperti a livello internazionale di Cybersecurity. In questa intervista analizza l'eccezionale strumento del *machine learning*, inserendo quella che si può considerare come una fenomenologia importante del cambiamento nella visione generale del rapporto uomo - macchina. Dicotomia, quest'ultima, irriducibile che ha caratterizzato la storia della civiltà fin dal suo primo sorgere, ed è facile prevedere che tale binomio farà sentire ancora di più i suoi effetti nell'era del *"post-umano"*.

Affascinante e nello stesso temo sconvolgente, non crede?

Tutte le volte che ci penso, invece che essere felice provo una sensazione di amarezza. Cosa significa decidere di appartenere ad una nuova specie? Cosa significa non essere più umani ma umanoidi? Ma se tutti decidessero di diventare umanoidi, abbagliati dalla speranza di vita eterna (o molto lunga) grazie alla continua sostituzione di pezzi di "noi", che significato avrebbe la vita? L'uomo non è fatto per vivere in eterno ed i suoi difetti, proprio come le sue caratteristiche lo identificano e lo distinguono da tutto il resto del creato. Non è forse la scarsità di una risorsa che ne determina il suo valore? Quale valore attribuire alla vita se la sua scarsità si riducesse? Varrebbe ancora la pena di vivere oppure ci sentiremo come incatenati in un perenne purgatorio? Personalmente non vedo rischi relativi a conflitti di specie: "X mens" VS "Uomini" ma piuttosto vedo rischi relativi alla perdita di identità, alla perdita della capacità di agire, alla perdita nel "divertirsi", perdendo così capacita di sognare e di soffrire. Queste ultime credo siano abilità molto importanti per noi esseri umani, perché danno sapore all'esistenza.

La cyber security si serve molto della IA. Quali sono le ragioni e i vantaggi sul piano della protezione degli asset produttivi e sull'individuazione delle vulnerabilità organizzative?

L'intelligenza artificiale meglio coniugata come Machine Learning (ML) aiuta notevolmente gli analisti sotto due principali aspetti. In primo luogo nella riduzione del rumore di fondo, abbassando il numero di falsi positivi. Gli eventi da analizzare sono sempre un numero molto elevato, a tal punto da essere impossibile leggerli tutti. Grazie a tecniche di ML gli eventi sospetti possono essere presi in considerazione, ridotti al minimo e presentati all'analista per la sua ultima ed autorevole analisi. In secondo luogo ed in maniera duale il ML aiuta l'analista nell'individuazione dei "piccoli segnali", movimenti impercettibili all'occhio umano che, discostandosi dalla normalità, destano sospetto. Anche in questo caso il ML pre-processa tali eventi e decide, autonomamente o in modalità supervisionata, quali siano quelli da presentare all'analista che, in caso di positività, decide a sua volta di prendere in carico l'incidente e di gestirlo autonomamente.

L'autonomia delle macchine una minaccia per l'uomo?

Un aspetto che preoccupa è la possibile sostituzione dell'uomo da parte di macchine sempre più performanti. È un pericolo reale? Esistono dei correttivi che possono tutelare gli spazi di azione e intervento dell'uomo nelle organizzazioni produttive?

Non credo sia affatto possibile la sostituzione dell'essere umano nel processo decisionale. L'intelligenza artificiale, per com'è studiata e progettata, presenta un carattere specifico e non generalista. Cerco di spiegarmi meglio. I sistemi di intelligenza artificiale sono capaci di prendere decisioni contestualmente al luogo/ambiente in cui essi sono stati "addestrati". Qualora si utilizza un algoritmo addestrato a trovare delle irregolarità sulla superfice della lamiera per riconoscere il volto di un essere umano, si può verificare che l'algoritmo non riesce a fare questa operazione. Questo perché l'AI "ragiona" secondo modelli logici esclusivamente "verticali", anziché orizzontali, come fa l'uomo. E' vero che già esistono dei progetti che tendono a insegnare alle intelligenze artificiali la cooperazione attraverso un cloud organizzato e quindi ad utilizzare il «modello artificiale» specifico al momento giusto. Contestualmente esistono protocolli che ambiscono all'addestramento di un modello atto a «imparare» in modo generale e non specifico, simulando cosi la mente umana. Si tratta però di prime sperimentazioni che non devono destare alcuna preoccupazione, almeno nell'immediato.

Quali sono le tecniche ed i principali algoritmi di machine learning maggiormente utilizzati nell'ambito della sicurezza informatica?

Sono molteplici le tecniche e gli algoritmi di Machine Learning utilizzati nell'ambito cybersec. Provo a riassumere i principali. Regressioni lineare, come per esempio i "Decision Trees" oppure i Suport Vector Regression (SVR) sono ampiamente utilizzati per effettuare azioni di predizione. In altre parole vengono impiegati questi algoritmi per decidere se una attività possa essere malevola o meno. Per esempio nei sistemi EDR (Endpoint Detection and Response) le regressioni lineari vengono implementate per comprendere se l'«n» richiesta a sistema (syscall) possa essere malevola o meno in funzione di uno storico «n-t» ed un modello che segue una data funzone f preventivamente addestrata sul sistema. La Classificazione, come per esempio Support Vector Machine (SVM) e Decision Tree Classification (DTC) sono utilizzati principalmente in modo supervisionato per classificare attacchi

basandosi su un insieme precondiviso. Per esempio, nella nostra Yomi (la Open Sandbox realizzata da Yoroi, oggi disponibile gratuitamente sia su Virustotal sia attraverso il il proprio portale web) vengono utilizzati algoritmi di SVM per classificare i Malware all'interno di un numero prestabilito di comportamenti malevoli come per esempio: Ransomware, Trojan, RAT, Dropper, InfoStealer, etc. Il Clustering, come per esempio K-mins, Gaussian Mixture Model e Mistured Models vengono utilizzati, tipicamente in fase di analisi per la costruzione dei modelli che poi saranno utilizzati in produzione sui vari prodotti, come per esempio: sonde di rete, EDR o sistemi di Hunting. Oltre a quelli elencati vi sono algoritmi denominati «generativi» come per esempio: le catene di Markov e algoritmi genetici che non sono molto frequenti nell'ambito della cybersecurity anche se a volte vengono impiegati per calibrare le attività di testing delle tecnologie più diffuse.

Etica, scienza e tecnologia: il futuro in questo trinomio

La tecnologia non è certo neutrale come erroneamente si crede dipende molto dall'uso che se ne fa. Un errore va scongiurato quello della supponenza, che richiama il mito di Prometeo che ruba il fuoco agli dei o di Icaro che vuole avvicinarsi troppo al sole e per questo gli si bruciano le ali. Etica scienza e tecnologia possono trovare un punto di incontro?

Sono d'accordo su questa visione. La tecnologia e in modo particolare l'Intelligenza Artificiale non può essere considerata neutrale e per questo non deve essere messa alla guida di decisioni strategiche (aziendali, politiche, istituzionali), pensando che possiede i requisiti per prendere decisioni imparziali e «giuste» per tutti. Questo perché il trend decisionale dipende in modo strutturale dal modello architetturale su cui l'IA si fonda ed in modo particolare dal training che ha ricevuto tale modello. Ne consegue che se a un modello perfettamente neutro (difficile da realizzare, ma non impossibile), gli viene insegnato (attraverso training) un determinato comportamento, anche in modo quasi impercettibile ad un ipotetico arbitrio umano, esso avrà al suo interno un piccolo pregiudizio *(bias)* che con il tempo si manifesterà in modo sempre più eclatante fino a raggiungere paradossali decisioni. In quel momento sarà necessario prevedere un sistema di "Reset" o di "Stop" di quell'intelligenza perché diventerà presupponente, prenderà perciò decisioni sbagliate, che non sarà possibile correggere. Questo mi è personalmente accaduto adottando un modello che, nonostante le numerose correzioni da parte di più analisti, continuava a pretendere di aver ragione su un evidente errore. L'algoritmo è stato resettato nel 2017, abbiamo così consegnato al passato un'esperienza che ricorderemo e che continua a farci riflettere ogni qual volta ci misuriamo con l'universo mirabolante dell'innovazione, che pone ogni giorno delle sfide che non ammettono tentennamenti. ■

I robot sono la "chiave" per conoscere meglio l'uomo

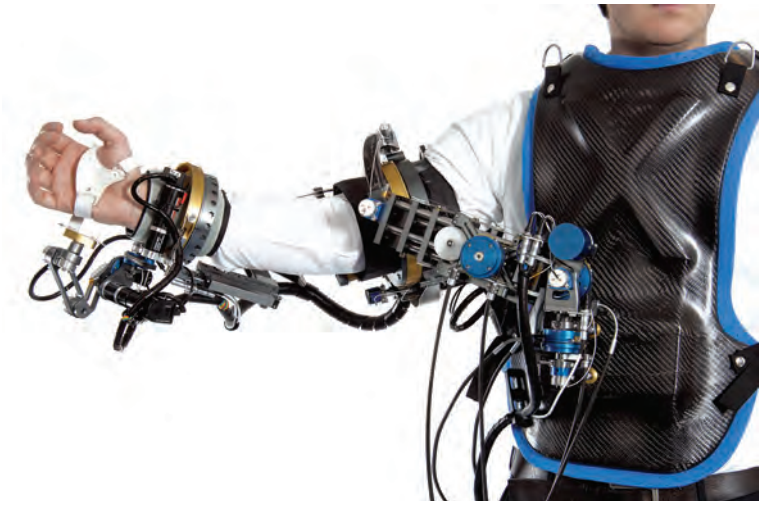
Intervista VIP a Giorgio Metta

Autore: Massimiliano Cannata

Internet e AI presto saranno comandati dal cervello umano. È solo una delle ultime provocazioni che la ricerca scientifica e tecnologica ci pone di fronte. Prove di umanità futura qualcuno potrà osservare, in realtà come spiega molto bene Giorgio Metta nell'intervista che ci ha concesso, al di là delle fascinazioni superficiali che lasciano il tempo che trovano, dovremo imparare a servirci con equilibrio e razionalità dei robot, non tanto per alimentare fuorvianti analogie, quanto per conoscere meglio quella straordinaria e per molti aspetti misteriosa facoltà che è l'intelligenza umana

"Siamo tutti un po' robot". ***Direttore partirei da questa affermazione ricavata da un recente confronto che ha avuto con l'atleta paralimpica Bepe Vio, pubblicato dal*** **Corriere Innovazione** ***che disegna molto bene il futuro prossimo, per chiederle: a quali livelli di interazione tra uomo e macchina siamo arrivati oggi e cosa dobbiamo aspettarci da questa necessaria ma anche difficile convivenza, che sollecita analisi e riflessioni di varia natura: epistemologica, filosofica, sociologica oltre che tecnico - ingegneristica?***

Non credo che si possa parlare di difficile convivenza. Il robot è uno strumento e come tale disegnato da noi e per noi. I robot come prima il martello, la pala, il motore a vapore e poi quello a combustione interna e così tante altre invenzioni sono solo l'evoluzione della nostra capacità di inventare oggetti che ci permettano di vivere meglio. I robot – forse intelligenti – servono proprio a questo scopo. Dove siamo? Sfortunatamente non abbastanza avanti. Siamo un'umanità che invecchia piuttosto velocemente e avremo sempre più bisogno di macchine che ci consentano di fare meno lavoro. I robot di oggi non sono abbastanza flessibili da sostituirci nei lavori più complessi o pericolosi. Il campo più promettente nel breve termine è proprio quello dei robot "indossabili" come le protesi o gli esoscheletri. Questa è un'ottima opportunità per aiutarci sia nel riacquisire capacità perdute, sia per ridurre gli incidenti sul lavoro. Per i robot completamente autonomi purtroppo ci vorrà più tempo.



Abbiamo a disposizione strumenti sempre più potenti, dotati di capacità biomeccaniche e sensoristiche molto avanzate. Siamo di fronte a un'"altra specie" (cito il titolo di un recente libro – intervista di Roberto Cingolani, ed. Il Mulino), di "alieni" che vivono a tutti gli effetti tra noi, con uno specifico corredo di linguaggi e di comportamenti che dobbiamo imparare a conoscere sempre meglio?

Dal punto di vista filosofico e con un po' di sguardo al futuro possiamo immaginare di doverci "relazionare" con un'altra specie. Più pragmaticamente direi che oggi possiamo fare cose eccezionali ma con dei limiti ben precisi. Un mondo di tecnica dove tutto sommato troviamo poca filosofia. Se guardiamo al futuro, credo che sia necessario pensare a definire e conoscere quella facoltà superiore che chiamiamo intelligenza. Un collega molto famoso del MIT mi ha detto una volta: "se risolviamo il problema

BIO

Giorgio Metta è il direttore scientifico dell'Istituto Italiano di Tecnologia (IIT). Laureato in ingegneria elettronica con lode (1994), ha ottenuto un PhD (2000) dall'Università di Genova. Dal 2001 al 2002 è stato postdoc presso il prestigioso AI-Lab del Massachusetts Institute of Technology (MIT). Ha lavorato all'Università di Genova e dal 2012 è anche Professore di Robotica Cognitiva presso l'università di Plymouth (UK). Ha gestito per conto di IIT i rapporti con gli enti finanziatori e le relazioni internazionali, ed in questo ruolo è stato membro del consiglio di amministrazione di euRobotics aisbl, l'associazione di riferimento per la robotica europea. Ha curato la partecipazione a due dei centri di competenza del Ministero dello Sviluppo Economico per l'industria 4.0 (ARTES4.0, START4.0). È stato uno dei tre rappresentanti italiani al forum G7 sull'intelligenza artificiale del 2018 e, più recentemente, uno degli autori dell'Agenda Strategica Italiana sull'Intelligenza Artificiale. Ha coordinato lo sviluppo del robot iCub per oltre un decennio rendendolo, di fatto, la piattaforma di riferimento per la ricerca nell'IA. Attualmente, ci sono più di 40 robot nel mondo, in laboratori di ricerca di paesi quali Giappone, Cina, Singapore, Germania, Spagna, Regno Unito e Stati Uniti. Le sue attività di ricerca si svolgono nel campo dei sistemi bio-ispirati e della robotica umanoide, con particolare riferimento alla progettazione di macchine che possano imparare dall'esperienza. E' autore o co-autore di più di 300 pubblicazioni scientifiche ed ha lavorato come PI in circa una dozzina di progetti di ricerca internazionali ed industriali.

dell'intelligenza, possiamo poi risolvere qualsiasi altro problema". Credo che sia giusto. Una volta realizzati robot e sistemi intelligenti molto potenti, potremo chiedere a queste macchine di aiutarci a risolvere i problemi globali del nostro pianeta: ambiente, energia, malattie, esplorazione spaziale per citarne alcuni. Stiamo affrontando problemi molto complessi e uno strumento straordinario come l'AI servirebbe per raccogliere e interpretare i dati che esaminiamo giorno per giorno nella ricerca scientifica affinché questa poi abbia un impatto concreto sulla nostra vita quotidiana.

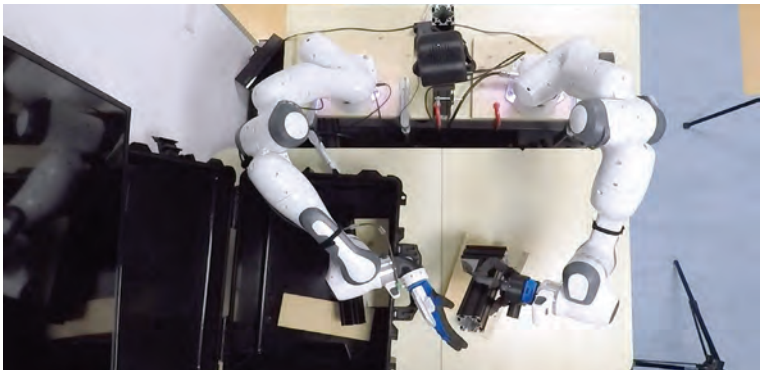
Tentare di tracciare delle analogie tra l'intelligenza artificiale e l'intelligenza umana è un esercizio utile, anche se può rischiare di diventare fuorviante se non si ha un approccio rigoroso. Esiste, a suo giudizio, una "razionalità", che potremmo definire digitale, che si distacca dalla tradizione della logica occidentale di matrice aristotelica?

Credo che più che di un'analogia – piuttosto lontana dalla realtà tecnologica – possiamo e dobbiamo capire l'intelligenza umana. Lo scopo è duplice, certamente quello più evidente è che dalla comprensione dell'intelligenza biologica deriva la possibilità di progettare macchine sempre più efficienti; in seconda battuta, ma non meno importante, l'intelligenza artificiale può essere il mezzo per capire quella biologica. Parafrasando Feynman "quello che non so costruire, non lo posso neanche capire".

I robot nella quarta rivoluzione

La "quarta rivoluzione" ci ha proiettato nell'infosfera. Robot e macchine intelligenti determineranno un salto di paradigma. Quali saranno gli ambiti di maggiore diffusione di questi strumenti e quali aspetti della nostra vita saranno maggiormente sconvolti e (speriamo tutti) migliorati dall'avvento di applicazioni informatiche e apparati che ci seguiranno ovunque, accompagnando ogni gesto della nostra quotidianità?

Il cambio di paradigma per quanto molto impattante avrà dei tempi medio-lunghi. È vero che il digitale ha una penetrazione di mercato molto rapida, i robot – parliamo quindi di hardware – però sono qualcosa di più complicato. Richiedono un'infrastruttura dedicata e investimenti importanti. Vedremo prima applicazioni molto specifiche soprattutto nel mondo delle imprese, vedremo probabilmente un'automazione ancora più spinta dove si integra la meccanica con i processi software. Per trovare però i robot nella vita quotidiana ci vorrà più tempo. Dipende anche da quali sono le nostre aspettative. Se parliamo di oggetti semplici – come i robot per la pulizia della casa oppure gli assistenti cognitivi e perché no i robot per l'intrattenimento – questi sono già con noi. Io vedo però altre possibilità come i robot per l'assistenza che purtroppo come dicevo richiedono ancora del tempo prima di essere tecnicamente realizzabili e commercialmente convenienti.



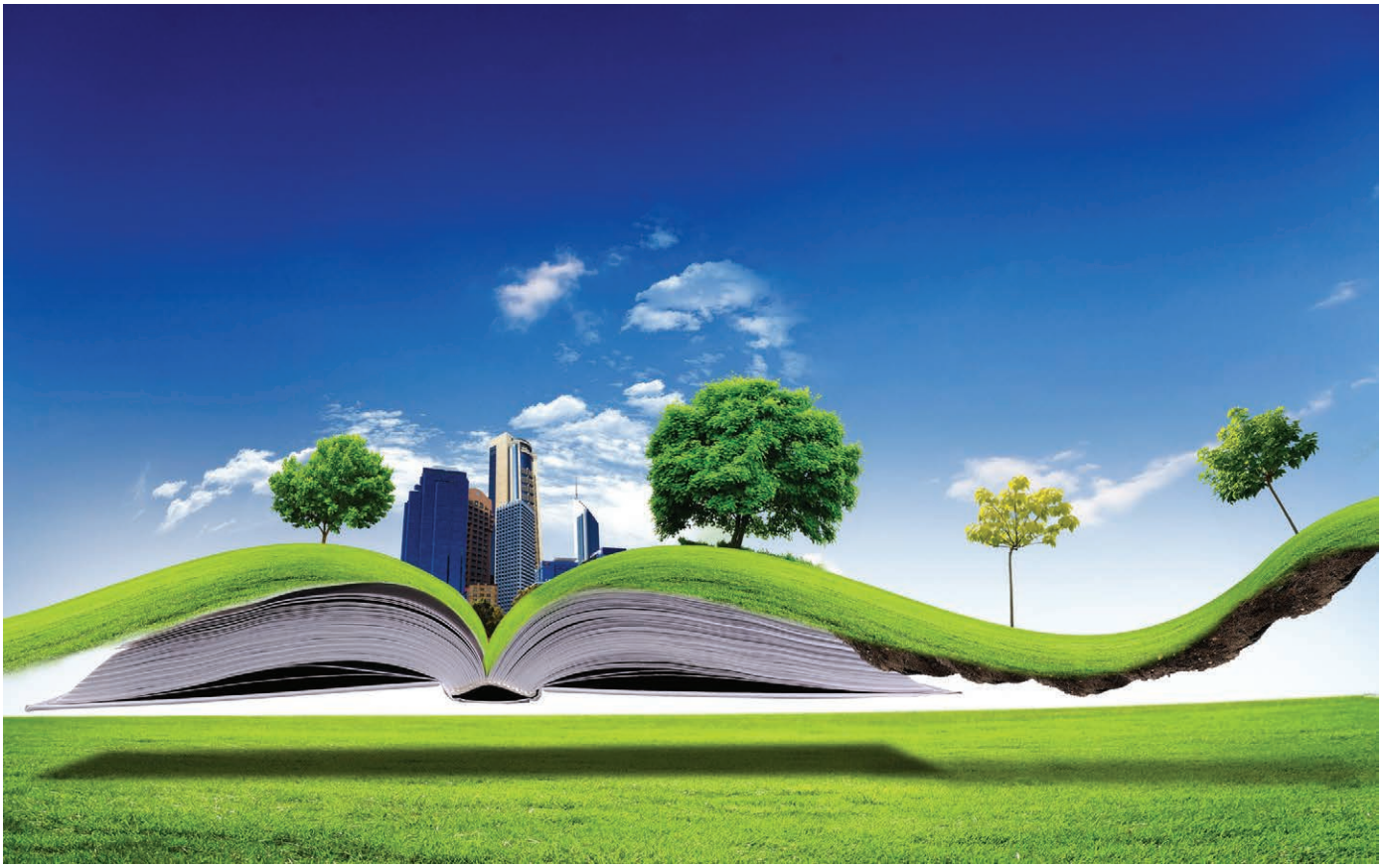
Il tema dell'autonomia e della decisione, facoltà tipicamente umane è quello che suscita maggiori interrogativi di carattere etico - filosofico. I robot potranno probabilmente spingersi a fare delle scelte al posto nostro. Abbiamo le conoscenze e le capacità per governare la forza di questa* "intelligenza globale" *che ha già determinato un cambiamento radicale e senza precedenti nella storia dell'umanità?

L'intelligenza artificiale – per quanto possiamo alla luce delle conoscenze di cui oggi disponiamo – non prende veramente "decisioni" se non quelle derivate dal modo in cui è progettata. Ricordiamoci che è sempre, in ultima analisi, il progettista umano che setta i parametri di funzionamento dell'algoritmo. Dal punto di vista dell'utente, questi parametri potrebbero essere sconosciuti, per cui si pone il problema di realizzare dispositivi che siano anche in grado di spiegare come e perché raggiungano una certa "decisione". Esiste quindi un problema etico-filosofico che è più legato a come i produttori realizzeranno le applicazioni di IA, piuttosto che un problema di controllabilità in senso stretto. Se dovessimo pensare a delle regole, di fatto dobbiamo chiedere che l'IA non ci inganni (per volontà del produttore) e svolga dei compiti in maniera non conforme a quello che ci viene indicato nel "manuale di istruzioni".

La necessità di riorganizzare saperi e competenze

La pandemia ha messo a nudo la grande esigenza di trovare un punto di interconnessine dei saperi. Anche gli epidemiologi devono conoscere gli algoritmi e le scienze computazionali, così come i politici che hanno bisogno della scienza per affrontare i livelli di complessità della "società del rischio" in cui gli eventi "eccezionali" sono divenuti la norma. Creare nuove professionalità dal profilo sfaccettato ed eclettico sarà una sfida importante per il futuro. Da un punto di osservazione prestigioso come l'IIT di Genova come vede questo problema che ha a che fare con i metodi della formazione, ma anche con la capacità di divulgare i risultati della scienza e le conquiste della tecnologia?

Sarà necessario sempre più, come si fa normalmente nel mondo scientifico, saper "contaminare" diversi saperi, prescindendo dalle barriere disciplinari tradizionali. Questo non vuol dire che non esisterà la specializzazione ma semplicemente che per affrontare le grandi sfide dell'umanità dovremo necessariamente mettere a fattor



comune il mondo digitale con quello dell'hardware, le scienze della vita con quelle dei materiali, la robotica insieme alla neuroscienza. Quindi una formazione con un'apertura verso la sperimentazione di "combinazioni" nuove sarà essenziale. Non dimentichiamoci che la pandemia è stata un evento eccezionale – soprattutto perché nonostante alcuni segnali del recente passato, non eravamo pronti – ma il problema del cambiamento climatico era ormai noto da anni. Per affrontarlo dobbiamo allo stesso tempo agire sull'approvvigionamento energetico, a partire dal modo in cui usiamo l'energia, sui trasporti, sulla produzione e sfortunatamente dobbiamo mettere comunque in conto la possibilità che qualche effetto dell'innalzamento della temperatura sarà inevitabile. Avere persone capaci di ragionare su questi problemi sarà cruciale.

Cybersecurity Trends ***si rivolge al mondo della cybersecurity. Sotto questo specifico profilo, l'automazione, la catena di montaggio robotizzata e più in generale le applicazioni della robotica in ambiti delicati come la medicina e l'assistenza socio-sanitaria sono strumenti che hanno generato trasformazioni organizzative e di processo e che di fatto stanno modificando l'universo del lavoro. Vi sono fattori di rischio in questa innegabile "rivoluzione"?***

I rischi sono intrinseci di ogni nuova tecnologia e come tali vanno analizzati e gestiti. L'automazione presenta rischi legati alla mera sicurezza tecnica (minimizzabili e a volte annullabili) ma anche quelli sociali – pensiamo all'impatto sul mondo del lavoro. Per i rischi di natura tecnica esistono soluzioni adeguate in fase di progettazione, regolamentazione, protezione dell'infrastruttura. Non è tutto perfetto ma non ci sono problemi insormontabili. Per quelli sociali, includendo in questi anche quelli relativi al cattivo uso della tecnologia, non possiamo che agire analizzandoli e ponendo in essere delle misure di controllo, di governance, e mitigazione dei rischi possibili.

Proviamo in conclusione a guardare oltre: case intelligenti, **smart city, remote working,** ***automobili che percorrono da sole le nostre autostrade. I contesti urbani, così come gli spazi dell'abitare, stanno rapidamente mutando profilo. La frontiera, che molti definiscono ancora in maniera vaga, del "post umano" che sembianze assumerà?***

Sono ottimista, mi piace vedere gli aspetti positivi dell'innovazione. Dobbiamo avere coraggio perché non possiamo tornare indietro. Abbiamo intrapreso un cammino verso il futuro dove la tecnologia diventa un componente essenziale della nostra qualità della vita. Abbiamo il dovere di farlo in maniera responsabile e sostenibile. Io spero di vedere un mondo in equilibrio con l'ambiente dove l'apporto dell'uomo sia principalmente improntato all'esercizio del "pensiero", lasciando il resto all'intervento di infrastruttura di tipo automatico o meccanico. Un mondo dove avremo finalmente controllato (e capito) i bit, gli atomi, i neuroni e i geni, in cui sapremo sfruttare queste conoscenze acquisite per aggiustare il nostro corpo come pure il nostro pianeta. Con queste stesse componenti magari potremo andare anche oltre il nostro pianeta, per aprire pagine nuove e affascinanti di quel cammino dell'uomo verso il progresso, che non avrà mai fine. ■

Distinguere, giudicare, scegliere: come "essere umani tramite la tecnica"

Intervista VIP a Franco Varanini

Autore: Massimiliano Cannata

Cinque leggi *(non siamo inforg, non siamo robot, non siamo algoritmi, non siamo macchine, siamo esseri umani)* da osservare ma anche da trasgredire per comprendere, per usare una celebre immagine di Emanuele Severino: *"La tendenza fondamentale del nostro tempo"*.

Francesco Varanini etnografo, critico letterario, esperto di innovazione, coniuga l'esperienza del ricercatore sociale con un'importante conoscenza del mondo aziendale. Il suo originale eclettismo emerge molto bene nel bel saggio: *"Le cinque leggi bronzee dell'era digitale"* (ed. Guerini e associati).

Professore, come si vede molto bene nel suo scritto la civiltà delle macchine apre un nuovo orizzonte. Quali sono i rischi e le opportunità?

Credo non basti parlare di civiltà delle macchine. Il cambiamento significativo, non sta tra una precedente civiltà e la civiltà delle macchine. La discontinuità rilevante è interna alla civiltà delle macchine. Il tempo che possiamo definire tempo della civiltà delle macchine, grosso modo dall'Illuminismo e dalla Rivoluzione Industriale in poi, mostra un passaggio chiave. Possiamo far data al primo articolo di Alan Turing, 1936, dove viene descritto per la prima volta il computer; o possiamo far data alla metà del secolo scorso, quando si afferma il concetto di automazione in ambito industriale, anni in cui Turing scrive a proposito delle macchine che pensano.

Prima di allora cosa succedeva?

C'erano macchine che accompagnavano l'uomo nel lavoro, ne alleviavano la fatica – non esistevano però strumenti progettati e costruiti con il proposito di sostituire in toto l'uomo nel lavoro. Oggi si accettano come cose normali previsioni nelle quali si afferma che entro cinquant'anni ogni lavoro umano potrà essere sostituito dal lavoro di una macchina. Non importa se la previsione è sbagliata: può darsi che i tempi siano più lunghi. Ciò che è importante è che l'affermazione sia tecnicamente fondata.

Tornando al bilanciamento tra rischi e opportunità cosa dobbiamo aspettarci?

Che gli esseri umani siano privati della possibilità di lavorare, con il rischio che ci venga sottratta la nostra stessa identità, che nel lavoro trova una sua esplicazione e realizzazione. L'opportunità consiste nel fatto che la nuova situazione è una sfida, che dobbiamo affrontare. Ci troviamo a convivere con macchine sempre più autonome, che impongono di riflettere su noi stessi, su chi veramente siamo.

Goethe e Leopardi ci spiegano la sostenibilità

Goethe e Leopardi. Perché ha scelto riferimenti così importanti per parlare di robotica e* machine learning*?

Sono grandi poeti e pensatori, seppero cogliere con grande acume le novità del tempo in cui vissero. Vivevano al tempo dell'Illuminismo e della Rivoluzione Industriale. Dobbiamo chiederci se noi sappiamo leggere il

nostro tempo così bene come loro seppero leggere il loro. La forza incontrastabile di leggi superiori è l'alibi che forniamo a noi stessi per non assumerci nessuna responsabilità. Eppure, ci ricorda Goethe, le leggi sono ammonimenti che ci spingono ad essere con forza e convinzione e piena consapevolezza coloro che possiamo essere. Di fronte a macchine, intelligenze artificiali, siamo così spinti ad essere più pienamente umani.

E Leopardi, per quale ragione viene chiamato in causa?

Basta ricordare un'immagine. Scrive: "Le macchine al cielo emulatrici / crebbero, e tanto cresceranno al tempo / che seguirà". Difficile dare una definizione migliore riguardo a strumenti sempre più potenti ed autonomi rispetto a noi umani. Questi grandi scrittori ci ricordano che il progresso non ci condurrà da nessuna parte se dimentichiamo la storia, se rinunciamo alla saggezza. Potremmo addirittura intravedere in queste affermazioni, un'anticipazione ovviamente *ante litteram* del termine 'sostenibilità'.

Le* leggi bronzee dell'era digitale *enunciate nel suo scritto fanno venire in mente il contrasto evocato da un recente lavoro di Vittorino Andreoli che parla della strana condizione dell' homo stupidus stupidus nella società dell'informazione. E' un parallelismo corretto?

Istupidito più che stupido direi. Le cinque leggi che descrivo mettono a fuoco cinque modi, cinque vie tramite le quali noi umani ci siamo appunto "istupiditi". Siamo cittadini dotati di diritti, ma nell'era digitale finiamo per essere sudditi di sovrani che decidono per noi. Prendiamo il caso di Zuckerberg che al pari di un sovrano assoluto decide le leggi che vigono in Facebook, che tutti siamo costretti a subire. Le leggi di cui parlo sanciscono di fatto la privazione della libertà. Il conoscerle, appunto, apre la strada al trasgredirle. Sta poi ai cittadini saper usare gli strumenti digitali come strumenti di libertà.

Siamo ancora in tempo per fissare un limite entro cui le macchine intelligenti devono di fatto muoversi?

È vano cercare di mettere un limite, così come è difficile mettere un freno ai tecnici e ai progettisti che operano nel settore. E se poi mai (anche se credo che non ci convenga spingerci sul terreno di questa ipotesi) le macchine svilupperanno una propria intelligenza, e quindi una determinata autonomia rispetto agli umani, saranno in grado di andare oltre qualsiasi limite imposto loro. Questo comunque non deve preoccuparci perché la presenza di macchine sempre più potenti e autonome, e magari intelligenti, è lo stimolo che ci spingerà a sviluppare le nostre capacità, a riscoprire la nostra saggezza. Paradossalmente più potenti sono gli strumenti a nostra disposizione, maggiore è la spinta ad esprimere la nostra umanità.

Esiste un limite della ricerca?

Distinguere, giudicare, scegliere: il titolo di uno dei capitoli. Non sono verbi entrati in disuso per essere sostituiti dalla cosiddetta* trinity *della blue economy: velocità, immaterialità, interconnessione?

Distinguere, giudicare, scegliere è, non a caso, il titolo conclusivo del saggio. Il messaggio è molto chiaro: proviamo a trasgredire le leggi alle quali, nel tempo in cui viviamo, dobbiamo sottostare. Velocità, immaterialità, interconnessione costituiscono uno stile di vita che ci viene imposto, leggi che ci vengono imposte: che vuol dire fare qualsiasi cosa alla massima velocità, essere sempre connessi alla Rete... Si tratta di aspetti positivi a patto di saperli viverle con saggezza, con moderazione, con spirito critico. Tornare a leggere letteratura, a godere dell'arte, della musica, potrà aiutarci in questo che è un percorso di recupero di una dimensione umana che stavamo, proprio disorientati dalla frenesia, perdendo per strada.

Le due culture, analogica e digitale appaiono oggi in conflitto. Esiste la possibilità che possano convivere?

Non credo esista una radicale discontinuità tra cultura analogica e cultura digitale. Nel mio saggio cerco di far vedere come ciò che chiamiamo cultura digitale nasce con l'Illuminismo e la Rivoluzione Industriale. Attenzione: parlare di *Disruption*, di rottura, di discontinuità, nasconde un messaggio politico pericoloso: è come se qualcuno ci dicesse: dimentica chi sei,

considera superati i tuoi valori, la tua storia, affidati ai nuovi guru, ai tecnici, ai profeti dell'innovazione acritica. È proprio ciò che non dobbiamo fare. Tutti i cittadini sono oggi più che mai chiamati a distinguere, giudicare, scegliere in prima persona.

"Essere umani tramite la tecnica", Lei scrive molto opportunamente. Siamo preparati per accogliere questo decisivo messaggio?

Purtroppo no. Ma possiamo prepararci. Voglio dare un messaggio di speranza, di fiducia. Fiducia in noi stessi. C'è però un passaggio chiave che va sottolineato: la tecnica non è in mano ai cittadini. È in mano ai tecnici. L'esempio più semplice e chiaro penso sia questo. Le macchine digitali funzionano in base a un codice, un programma. Chi è in grado di scrivere questo codice? Chi sa cosa c'è scritto nel codice che fa funzionare le macchine? Solo i tecnici, non certo i cittadini. È proprio questa impossibilità di leggere il codice che può trasformare i cittadini in sudditi, che potremmo definire con una parola più adatta: utente. Per ritrovare un giusto equilibrio la tecnica non deve chiudersi in una torre d'avorio ostentando superiorità, nel contempo il comune cittadino deve aprirsi all'innovazione, non sacrificando nulla della sfera di quei diritti conquistati al prezzo di tante lotte e rivendicazioni.

Epidemia e pandemia per nulla sinonimi

In questo momento certamente difficile per la storia dell'umanità, quale deve essere il compito dell'impresa (si pensa di solito solo allo stato e ai soggetti pubblici) perché si possa riavviare un futuro di crescita uscendo dal buio della notte di questa terribile pandemia?

Le parole hanno un peso e un senso al quale non sempre poniamo attenzione. Ci sono due termini, che in questi giorni penosi e terribili abbiamo usato considerandoli come sinonimi: *epidemia* e *pandemia*. In realtà questa parole raccontano storie ben diverse. *Epidemia* è un antica parola greca che parla di qualcuno o qualcosa venuto tra noi. Ospite desiderato o indesiderato. La parola nel suo significato originario non parla di malattia o di pericolo. Parla della necessaria attenzione che dobbiamo tributare rispetto a qualcuno o qualcosa che arriva nel nostro paese, nella nostra città, nella nostra casa. *Pandemia* è invece una parola che ha una radice tecno-scientifica, coniata dai medici verso la metà dell'Ottocento. La caratteristica distintiva della pandemia è il suo essere dichiarata da un'autorità. La pandemia esiste quando un'autorità ne afferma la presenza. Il cittadino di conseguenza finisce con l'assumere un atteggiamento dipendente: attende regole, cure, protezione. Tutto ciò ha un valore, a patto di non tralasciare la radice etimologica dell'altro lemma: epidemia, che invita a un atteggiamento responsabile ogni singola persona. Guardando al mondo dell'impresa per rispondere alla sua sollecitazione, si potrebbe dire che quello che serve è una crescente responsabilità sociale. In parallelo anche ogni singolo soggetto dell'organizzazione deve maturare un atteggiamento coerente alle sfide che una società complessa pone ad ogni cittadino. Siamo, infatti, sulla stessa barca, nessuno può chiamarsi fuori, questo il messaggio di fondo su cui vorrei confrontarmi con i lettori. ■

BIO

Francesco Varanini, nato a Pisa nel 1949, laureato in Scienze Politiche. Negli Anni Settanta è stato antropologo in America Latina. Negli Anni Ottanta presso Arnoldo Mondadori Editore ha ricoperto posizioni di responsabilità nell'area del Personale, dell'Organizzazione, dei Sistemi Informativi, dell'Innovazione di mercato e di prodotto. Tra l'altro ha guidato il progetto di digitalizzazione degli archivi e di banca dati full text degli articoli pubblicati sui periodici Mondadori e su *Repubblica*. Successivamente è stato direttore generale della casa editrice del settimanale *Cuore*, e poi co-fondatore del settimanale *Internazionale* e amministratore delegato della relativa casa editrice.

Formatore e consulente dalla metà degli Anni Novanta, si occupa in particolare di processi di cambiamento. Cercando un punto di incontro tra la cultura umanistica e il 'management', tra le dinamiche relazionali e gli approcci sistemici-informatici. Ha insegnato (dal 2003) per dodici anni come docente a contratto presso il Corso di laurea Interfacoltà in Informatica Umanistica dell'Università di Pisa. Successivamente ha tenuto cicli di seminari presso l'Università di Udine. Ha fondato (nel 2004) e dirige, presso la casa editrice Este, la rivista *Persone & Conoscenze*, rivista mensile rivolta ai professionisti delle Risorse Umane.

E' progettista e chairman di convegni promossi dalla casa e dalla rivista: Risorse Umane & non Umane, il Convivio, Formare e Formarsi, EssereDigitale. E' socio fondatore (nel 2002) e Direttore Scientifico di Assoetica, associazione per la diffusione di atteggiamenti etici nel mondo del lavoro e delle organizzazioni. E' membro del Comitato Scientifico della rivista *Sviluppo & Organizzazione*. Dal luglio 2013 al novembre 2015 è Presidente per la Lombardia dell'Associazione Italiana Formatori (AIF). Ha organizzato e curato, in quanto Direttore Scientifico, il XXVII Convegno Nazionale dell'Associazione Italiana Formatori (AIF): 'Liberare la formazione', Milano, 13-14 novembre 2015.

È autore du numerosissime pubblicazioni, curatore del sito www.bloom.it e del blog www.diecichilidiperle.blogspot.com. In una vita parallela è saggista e critico letterario, con una particolare attenzione per la letteratura e la cultura ispanoamericana. Racconta di sé su www.francescovaranini.it.

Le nuove frontiere della Cyber Threat Intelligence

Autore: Andrea Pompili

Il gioco della cyber security è sempre stato guidato dall'esigenza di evolvere da un approccio puramente reattivo ad uno proattivo o, addirittura, predittivo, aumentando il significato dei segnali deboli provenienti dall'infrastruttura informatica e cogliendo le intenzioni di un avversario prima che raggiunga il proprio obiettivo.

Il limite principale di questa necessità è insito nell'esigenza stessa: anche gli attaccanti diventano sempre più preparati e strutturati, aumentando la capacità di nascondersi sfruttando l'entropia tipica delle comunicazioni informatiche, variando velocemente le modalità di compromissione grazie ad un perimetro sempre più dissolto e interconnesso.

BIO

Andrea Pompili è un informatico che da tempo si occupa di sicurezza.Molto giovane, entra a far parte del mondo del computer con uno dei giochi italiani più famosi basato sulla piattaforma C64. Una volta laureato, si è occupato prima di sviluppo software su portali Web Based e piattaforme di calcolo distribuito, quindi di sicurezza informatica lavorando anche per le più grandi compagnie Telefoniche su piattaforme di cyber security in ambito ICT e industriale, assessment di sicurezza e ricerca vulnerabilità, computer forensic, malware reverse engineering. Attualmente Andrea è Chief Scientist Officer presso CY4Ggate e si propone di scoprire e integrare soluzioni e idee innovative per garantire la sicurezza per questo mondo interconnesso.

In particolare l'avvento degli APT (Advanced Persistent Threat) ha spinto tutte le aziende a ripensare il concetto di protezione spostando l'attenzione dalle vulnerabilità agli attaccanti, cercando di comprendere i limiti operativi e, soprattutto, i passaggi logici seguiti nelle varie fasi della compromissione: dalla modalità di ingresso alla strategia di identificazione dei target, dalle tecniche per garantire la persistenza a quelle per esfiltrare i dati o controllare le operazioni.

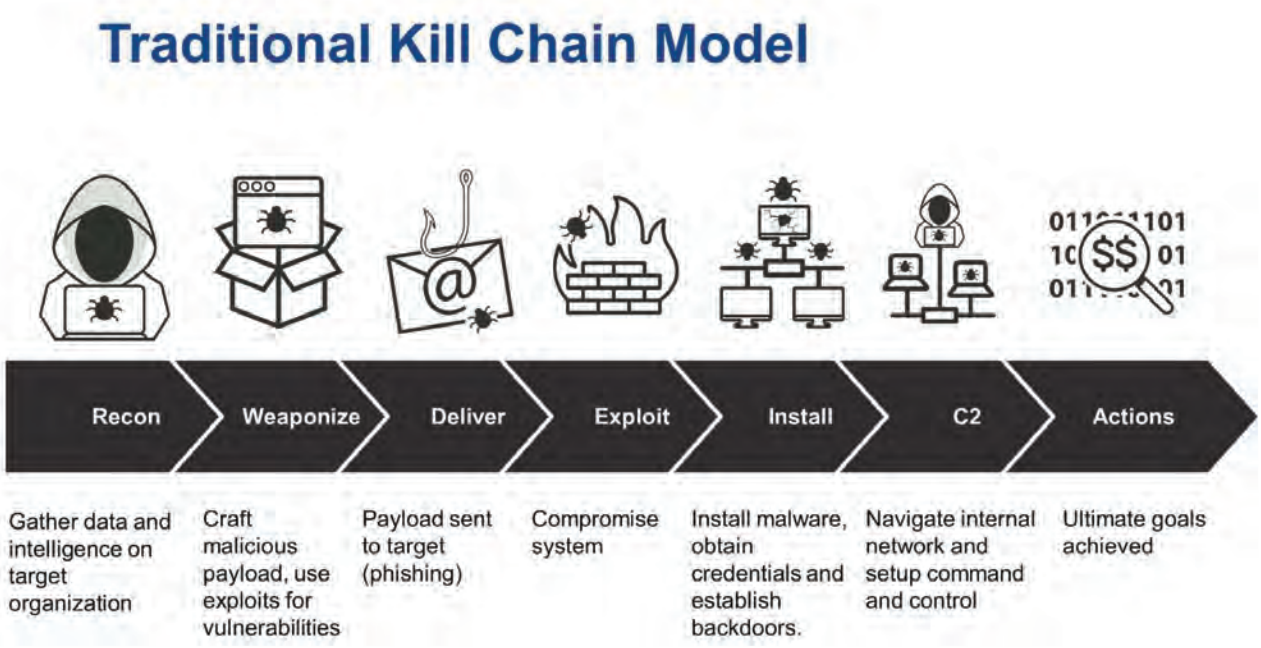
Ciò significa che un APT può essere considerato come una "catena di attività" che combina una sequenza di azioni e attacchi informatici eseguiti partendo da uno o più servizi esposti come la posta elettronica, un sito web esposto, etc., con lo scopo di creare un impatto all'interno di uno o più sottosistemi interni e ottenere quindi un "vantaggio" strategico in funzione degli obiettivi dell'attaccante.

Tale concetto è chiamato **kill-chain**, ed è praticamente una sequenza di **tattiche** e **tecniche** di attacco tipicamente seguite da un attaccante per compromettere un sistema complesso.

Il concetto **"Tattiche, tecniche e procedure" (TTP)** è piuttosto noto nel mondo dell'intelligence, e più in generale in ambito militare. È stato creato per identificare il modo in cui i threat actor orchestrano e gestiscono attacchi complessi ai danni di uno specifico obiettivo.

Le tattiche rappresentano il "perché" una tecnica specifica viene utilizzata all'interno di una kill-chain. Rappresenta l'obiettivo tattico dell'avversario in termini dell'eventuale vantaggio che vuole ottenere una volta applicata. Le tattiche sono definite come categorie contestuali che includono una o più tecniche e sono caratterizzate dall'effettivo scopo dell'avversario, come: "essere persistente", "scoprire un'informazione", "spostarsi lateralmente", "eseguire qualcosa" o "raccogliere ed esfiltrare dati".

Le tecniche invece rappresentano il "come" un avversario può raggiungere l'obiettivo tattico di riferimento: è l'approccio di attacco specifico che può essere utilizzato per ottenere l'obiettivo desiderato. Per alcuni tipi di tattiche, le tecniche rappresentano anche "cosa" l'avversario guadagnerà una volta che avrà eseguito l'azione corrispondente. Ad esempio per le tattiche orientate alla raccolta dati (Collection) e all'information gathering (Discovery), le tecniche specificano cosa effettivamente può essere raccolto per le successive fasi della kill-chain o per il completamento della stessa.



Ad esempio, un avversario può estrarre delle credenziali valide da un software utilizzato all'interno del dominio per raccogliere quindi informazioni sugli utenti configurati nel sistema: il "come" è analizzare il software per trovare delle credenziali utile, il "cosa" è l'elenco degli utenti abilitati sul sistema.

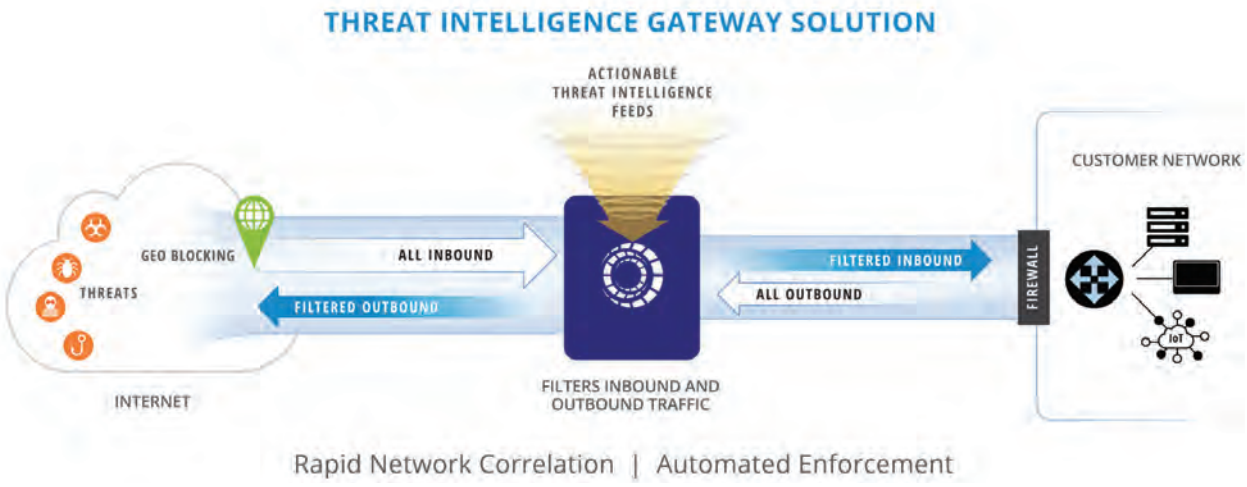
Infine, le procedure sono strettamente legate alle tecniche perché rappresentano l'implementazione specifica che un avversario adotta per ottenere il risultato desiderato della tecnica. Una determinata procedura è lo "strumento" utilizzato per eseguire la tecnica, caratterizza l'avversario in una specifica campagna di attacco ed è solitamente utilizzata per estrarre una "firma" che può essere poi utilizzata dalle contromisure di sicurezza presenti nel dominio.

Tale approccio rientra sotto il cappello delle *"actionable threat intelligence"*, ossia la capacità di razionalizzare le informazioni relative alla natura degli avversari e al loro modo di agire, per costruire i dataset necessari per la loro rilevazione automatica da parte delle contromisure.

Uno dei sistemi più noti per definire una informazione di intelligence "actionable" è quello degli IoC (Indicator of Compromise) con il suo standard aperto di riferimento OpenIOC, che è ormai gestibile nativamente da quasi tutti i dispositivi di protezione attiva, in quanto consente di identificare un'azione come malevola riconoscendone le caratteristiche tecniche comuni ad attacchi già noti (es. Il nome di dominio usato per le comunicazioni di commando e controllo o l'hash di uno dei payload utilizzati) e quindi neutralizzarla in tempo reale.

La cattiva notizia relative alle procedure è che il loro ciclo di vita è piuttosto breve a tal punto che, per kill-chain complesse di tipo multi-stadio e multi-target, queste potrebbero essere utilizzate una sola volta.

Si pensi infatti ad una vulnerabilità di tipo 0-day che consenta di eseguire del codice arbitrario: questa è una procedura ad alto valore che può essere utilizzata, ad esempio, per implementare la tecnica "Exploitation of Remote Services", orientata a soddisfare la tattica "Lateral Movement", ossia spostarsi da un Sistema ad un



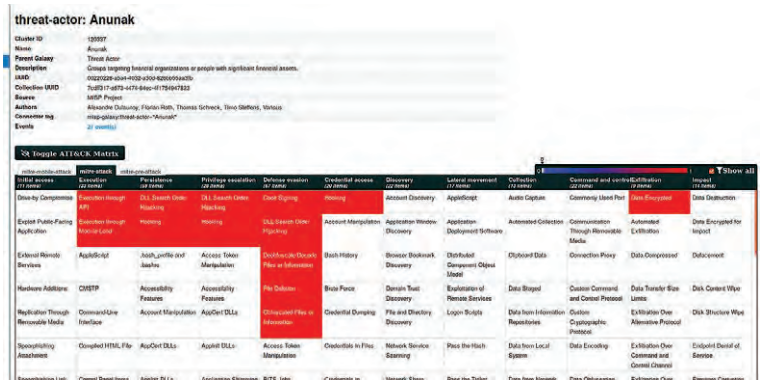
altro attaccando uno dei servizi esposti se vulnerabile a questa procedura.

Questa procedura, tuttavia, è valida solo per la prima e unica volta in cui viene utilizzata, perché una volta che l'attacco è stato eseguito, i difensori studieranno questa nuova procedura, identificheranno una firma valida per poterla rilevare e, allo stesso tempo, avviseranno il produttore del software per risolvere il problema. Ciò significa che dal punto di vista dell'avversario questa procedura può essere utilizzata solo nell'intorno temporale della campagna di attacco, e deve essere sostituita da procedure analoghe in un'attività di attacco successiva.

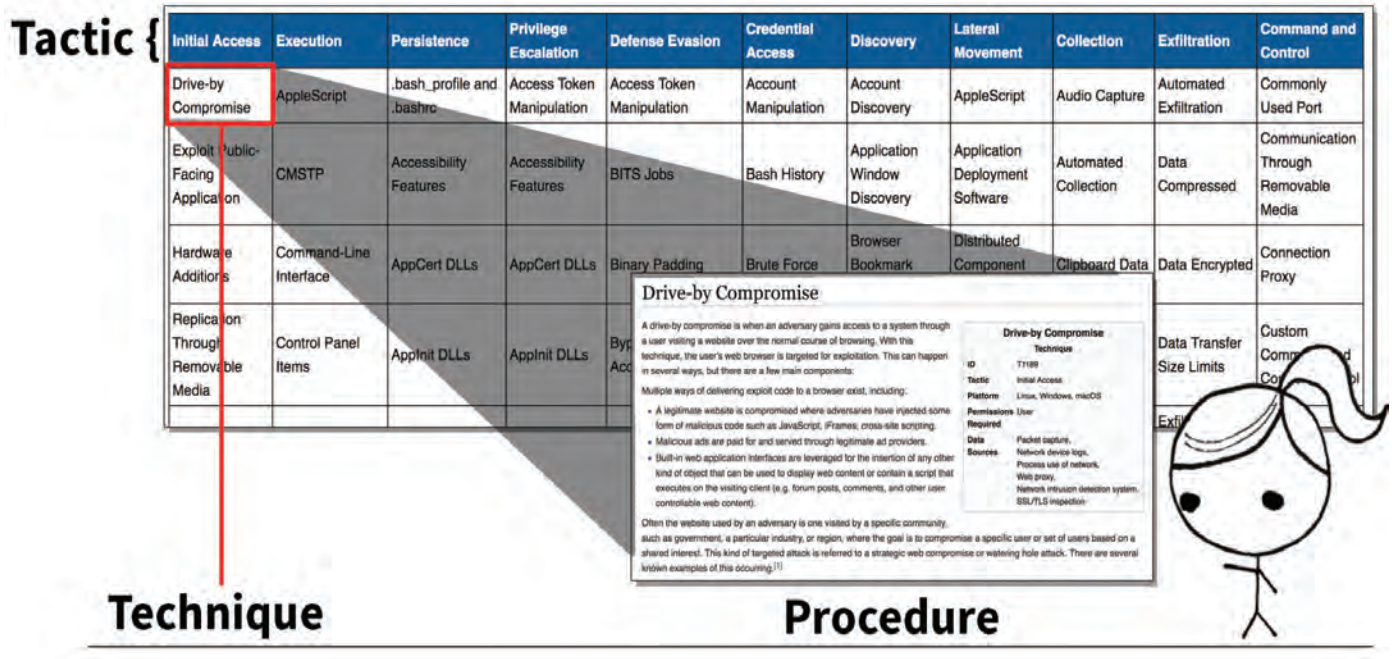
Le tattiche e le tecniche, invece, sono legate al modus operandi dell'avversario, quindi indipendenti dalle effettive vulnerabilità o configurazioni errate sfruttate in una vera e propria kill-chain. La maggior parte degli avversari è infatti interessata esclusivamente all'esfiltrazione di dati sensibili, altri sono interessati al controllo di infrastrutture critiche industriali, altri ai defacement e così via.

Negli ultimi anni, quindi, tutti gli strumenti di cyber response e le practice di incident management hanno iniziato ad utilizzare il modello TTP per le seguenti funzioni:

- Triage rapido e contestualizzazione di un attacco correlando le informazioni con le TTP tipiche di uno o più threat actor noti;
- Supportare la ricostruzione della kill-chain a partire dalle evidenze raccolte e riconoscendo le TTP utilizzate in una campagna o attacco già eseguita da uno dei threat actor noti;
- Identificare possibili sorgenti o vettori di attacco basati sulle TTP;
- Supportare la risposta proattiva e i processi di contenimento degli incidenti di sicurezza, individuando quali sistemi o funzionalità potrebbero essere successivamente compromesse una volta identificata uno specifica kill-chain attraverso le TTP osservate;
- Validare l'ffettiva capacità di detection delle contromisure di sicurezza esistenti testando eventuali nuove TTP o combinazioni di kill-chain.



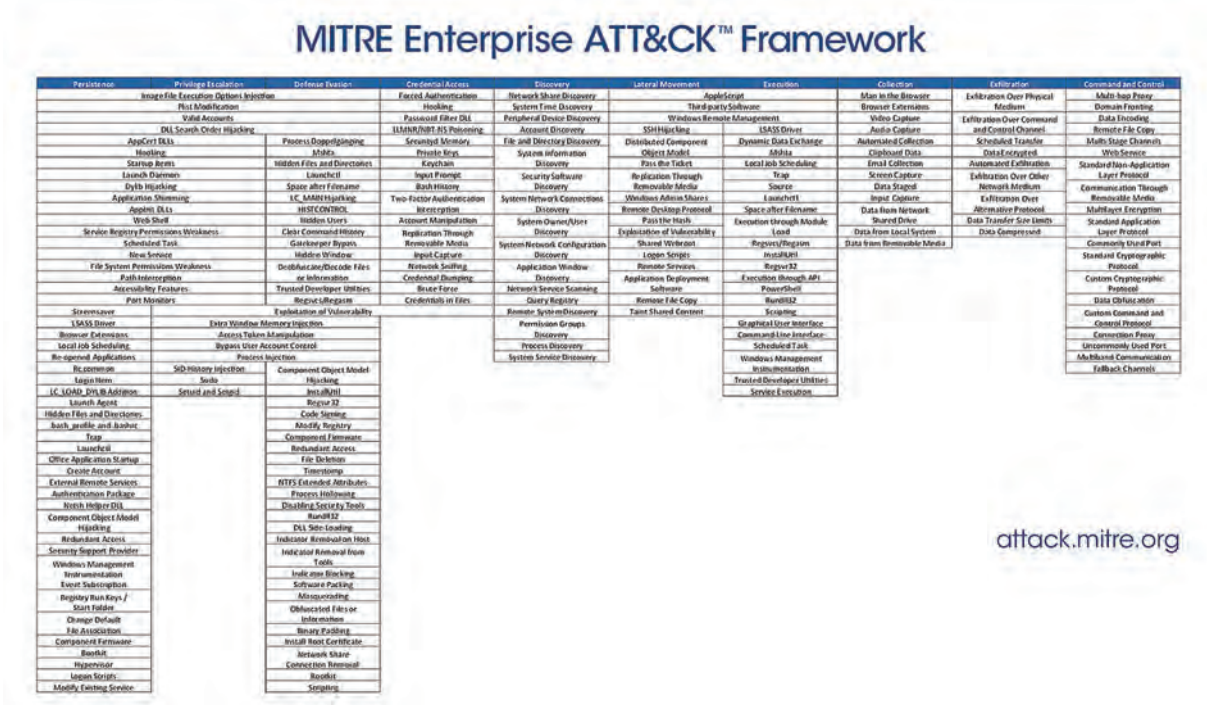
Esistono diverse mappature TTP applicabili nel dominio cyber. La più nota è la MITRE Att&ck Matrix, che sta diventando lo standard "de-facto" per la cyber security ed è attualmente integrate nella maggior parte dei sistemi di rilevamento degli attacchi informatici.

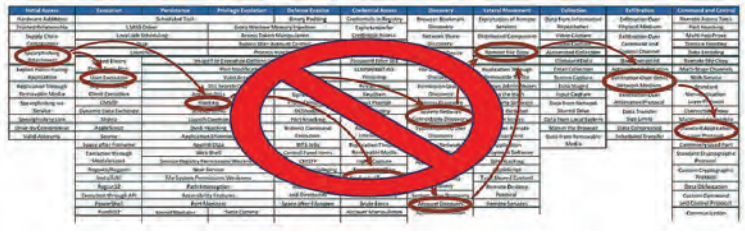


Tale modello si basa sull'astrazione del "modus operandi" di un attaccante, descrivendolo attraverso I concetti di tecniche e tattiche. Questo sistema consente di superare l'approccio reattivo tipico delle contromisure di sicurezza, consentendo di rilevare un eventuale avversario seguendo il suo comportamento tipico, una volta che l'uso delle tecniche corrispondenti sia stato identificato per il dominio sotto monitoraggio.

La stessa mappatura può essere utilizzata non solo per la detection, ma anche per supportare le attività di verifica della sicurezza, simulando uno specifico avversario all'interno di un dominio e misurando le capacità di detection e protezione effettivamente offerte dalle contromisure di sicurezza implementate.

Le tattiche definite nel modello sono state progettate per coprire anche lo scopo finale di una kill-chain, ovvero classificando e descrivendo tattiche specifiche orientate, per esempio, ad una esfiltrazione di dati sensibili (definite nelle categorie Collection ed Exfiltration) o a violare l'integrità o la disponibilità del target (definite nella categoria Impact). Ciò significa che la matrice MITRE Att&ck può essere utilizzata per modellare l'intera kill-chain di un attacco informatico incluso l'effetto finale che deve essere generato sul target, che poi è ciò che rappresenta la motivazione effettiva di un attacco: il vero legame tra le specifiche attività cyber e il concetto di operazione cyber.





Un'altra caratteristica della MITRE Att&ck matrix è il forte orientamento all'"espandibilità ". La mappatura è infatti stata definita sin dall'inizio come un concetto che può essere esteso o potenziato per includere nuove tattiche, tecniche e procedure, definendo in dettaglio quando questa estensione può essere fatta e come deve essere gestita e definita per garantire la coerenza dell'intero modello.

Questa possibilità è fondamentale quando si estende il concetto di attacco informatico con vulnerabilità e attività che riguardano le comunicazioni via radio, come le CEMA (Cyber Electro-Magnetic Activities). Una CEMA richiede infatti un approccio diverso alle esigenze di identificazione o riconoscimento di un attaccante, perché le kill-chain possono includere anche tecniche e procedure dedicate ai canali radio come il jamming o l'intercettazione attiva o passiva del canale, che devono essere coordinate o combinate per raggiungere o semplicemente influenzare le applicazioni e i servizi informatici basati su tali tipi di comunicazioni.

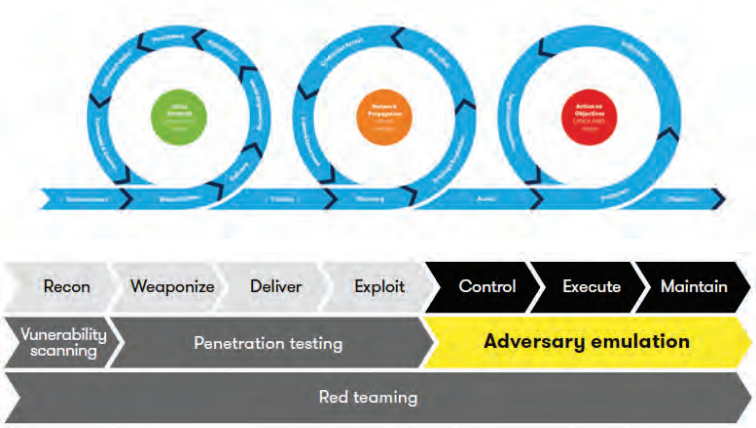
Questa possibilità può aprire la strada a nuove tattiche, tecniche e procedure che devono indirizzare non solo le vulnerabilità tecniche note legate ad errori nel software o nelle configurazione dei servizi esposti da un endpoint di tipo wireless (e.g. un access point o un comunicatore satellitare), ma anche a vulnerabilità funzionali basate, ad esempio, sulla mancata sincronizzazione tra gli endpoint causata da un attacco via radio sul protocollo, sulla loro mancata disponibilità mediante jamming o sulla violazione della segretezza delle informazioni scambiate sul canale.

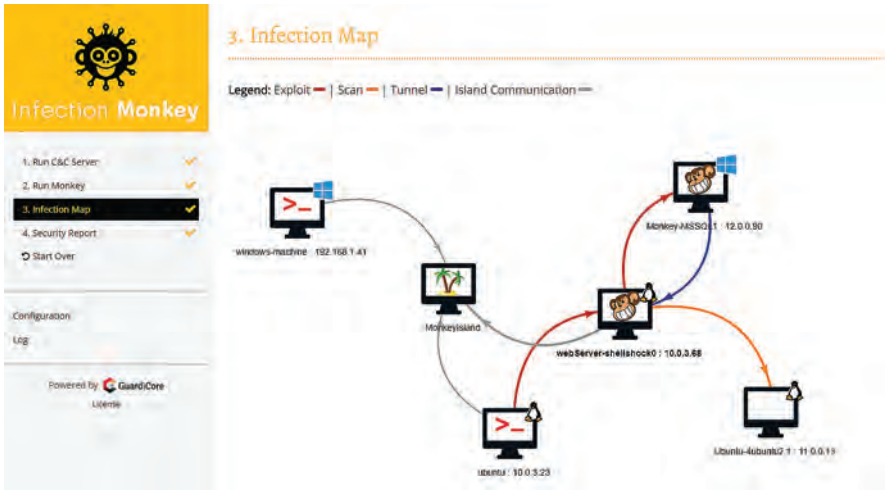
Come sfruttare questo nuovo paradigma? La soluzione più semplice e nota è quella della Adversary Emulation, ossia la possibilità di sintetizzare kill-chain non predicibili a partire dalla MITRE Att&ck Matrix, combinando procedure note in forza a soluzioni o tool più o meno aperte come Metasploit o Mimikatz. Tali

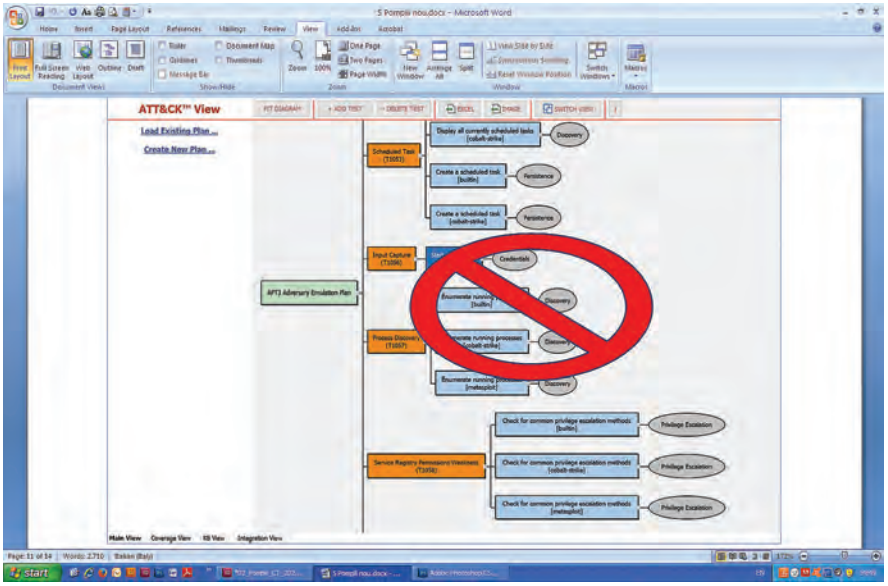
emulatori automatizzano il processo di un attaccante "programmato" per combinare le tattiche e le procedure desiderate, scegliendo la catena di attacco e gli obiettivi da colpire con algoritmi di pianificazione più o meno deterministici. Esempi di tali soluzioni sono CALDERA, Red Canary o Infection Monkey.

Tali strumenti possono migliorare il processo di validazione della sicurezza o il test di resilienza delle soluzioni di protezione aggiungendo ai tipici tool automatici di scansione un processo di "attacco" più vicino alla realtà dei fatti, avvicinandosi alle attività tipiche di un avversario. Questo approccio indirizza in maniera adeguata il limite descritto all'inizio dell'articolo, in quanto il sistema non viene più validato esclusivamente rispetto alle vulnerabilità delle singole componenti, ma rispetto ad una kill-chain, pesando quindi il concetto di sicurezza rispetto all'impatto finale effettivamente ottenibile.

Ma questo aspetto è solo l'inizio. Ultimamente si parla sempre più appunto di actionable threat intelligence, e la MITRE Att&ck Matrix è un perfetto candidato per supportare sistemi di protezione comportamentali come le soluzioni UEBA (User&Entity Behavioural Analytics) o i SIEM di nuova generazione. In tale scenario si potrebbe definire il concetto di Cyber Threat Intelligence Mapping ossia, data una informazione di intelligence relativa ad un attaccante e alle sue modalità, identificare la sua mappatura sulla matrice MITRE, evidenziando le







TTP specifiche per la campagna di attacco o per il threat actor di riferimento.

Tale mappatura può essere quindi utilizzata da sistemi comportamentali per "seguire il filo" di un attacco, magari partendo da segnali anche possibili falsi positivi, ma che se riconosciuti in una sequenza possono certificare l'attacco in corso e, oltretutto, offrire una attribution significativa. Attenzione: questa strategia implica che le regole di correlazione o identificazione per la rilevazione delle eventuali procedure, tecniche o tattiche non deve essere eccessivamente precisa, ma può anche gestire un certo livello di imperfezione in quanto il suo rischio sarà comunque pesato rispetto a rilevazioni successive coerenti con le kill-chain di interesse. Una semplificazione piuttosto forte, che cambia il processo tipico dell'ingegneria del monitoraggio usata per i SIEM, per esempio, in cui i falsi positivi sono sempre stati la principale fonte di preoccupazione e lunghe nottate di fixing all'interno dei SOC.

Rimane il problema di come gestire in maniera efficace tali mappature, sia in termini di condivisione, sia in termini di formato. La soluzione più idonea è quella di sfruttare le capacità offerte dalla piattaforma MISP, soluzione aperta nata per la condivisione di informazioni cyber tra gruppi di cyber defence, che nell'ultimo periodo sta sempre più assumendo un ruolo prominente proprio nella Cyber Threat Intelligence grazie alla sua struttura modulare e facilmente estendibile, nonché alle integrazioni

già esistenti per il concetto di actionable threat intelligence con le varie contromisure di sicurezza come IDS/IPS o SIEM.

Il MISP concettualmente è piuttosto semplice e intuitivo, ogni elemento informativo è strutturato come un "evento" con delle entità di base utili per la sua classificazione e per identificarne la natura, a cui possono essere aggiunte ulteriori entità, denominate Galaxy, che consentono di arricchire l'espressività dell'evento con ulteriori caratterizzazioni.

Tra le varie Galaxy figura anche la mappatura MITRE Att&ck, ossia è possibile inserire in un evento anche le TTP specifiche che lo caratterizzano, entità che poi possono essere segnate come esportabili e quindi trasmesse ad un qualunque sistema in grado di gestirle una volta richieste.

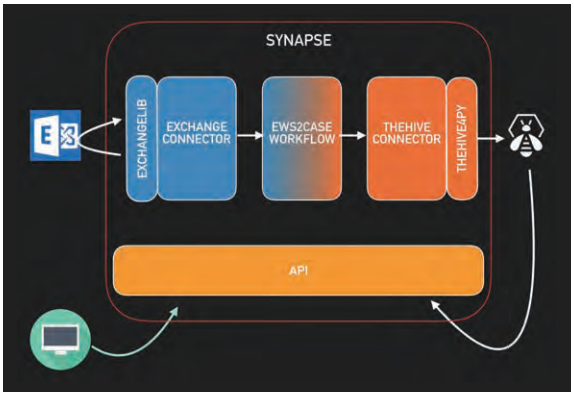
Abbiamo quindi un'architettura di riferimento estremamente interessante, aperta e, soprattutto, già pensata per garantire l'interoperabilità necessaria a raggiungere gli obiettivi descritti. Un SIEM evoluto potrebbe a questo punto interrogare ciclicamente un repository MISP e aggiornare la lista dei threat actor e delle TTP di riferimento, per poi provare a identificarle seguendo i pattern comportamentali delle anomalie rilevate.

Ma c'è di più. Come già accennato, il MISP è una piattaforma di condivisione nata per la cooperazione tra team di difesa. Per questa ragione gli eventi potrebbero seguire un workflow interno di creazione, arricchimento e pubblicazione in funzione dello stato di classificazione, analisi e validazione che il team di difesa, SOC o CERT, tipicamente segue. Questo significa che il MISP potrebbe essere utilizzato dagli analisti di sicurezza anche durante un processo di gestione di un incidente, sia nella fase di triage, sia nella fase di response.

E se si sfruttasse il triage per identificare non solo l'impatto di un attacco, ma anche le tecniche e tattiche riconosciute? Da qui un'ulteriore evoluzione del concetto: usare la procedura di incident response per generare ulteriori mappature TTP che potrebbero essere poi pubblicate per garantire il loro riconoscimento assistito da parte delle contromisure di sicurezza immediatamente dopo la loro rilevazione.

Questo approccio non è completamente nuovo. Le regole YARA sono nate per questo, ossia, una volta compresi gli indicatori tipici di una compromissione o di un attacco, costruire una regola utilizzabile immediatamente dalle contromisure in essere. Analogamente si può pensare di integrare le informazioni di classificazione di un incidente con le TTP osservate e da queste generare un evento MISP adeguatamente inizializzato e arricchito che le piattaforme di sicurezza potrebbero immediatamente consumare e utilizzare per riconoscere, da quel momento in poi, pattern di attacco compatibili.

Su questo principio sono state realizzate alcune soluzioni interessanti come **TheHive Project**, il cui scopo è proprio quello di integrare le tipiche funzioni di un case management con le potenzialità degli eventi MISP. La piattaforma consente infatti di gestire il tipico processo di incident management organizzando l'attività in task, entità da osservare, evidenze da collezionare e mappature da validare rispetto alle TTP, per poi generare eventi MISP adeguatamente strutturati sfruttando tutte le informazioni raccolte.



In conclusione, abbiamo compiuto un lungo viaggio attraverso le nuove frontiere della Cyber Threat Intelligence, in cui abbiamo compreso le potenzialità delle mappature basate su tattiche, tecniche e procedure. Abbiamo cercato quindi di capire come integrare tale approccio per gestire un processo di rilevazione incidenti più efficace e proattivo, fino a sfruttare tale espressività anche per semplificare le attività di adeguamento necessarie per garantire una risposta tempestiva ed efficace ad un attacco complesso. Molta strada va ancora percorsa in termini di:

- automazione della mappatura delle TTP sulle informazioni disponibili, anche non struturate;
- effettivo riconoscimento delle singole tecniche o tattiche da parte delle componenti in grado di osservare gli eventi di Sistema;
- capacità di riconoscere in maniera efficace kill-chain anche mai utilizzate a partire dalle TTP di riferimento, o effettuare una attribution automatizzata in funzione delle scelte operative dei vari avversari.

Ciò non toglie che le prospettive di integrazione e i benefici operativi derivanti da tale approccio siano inevitabilmente importanti, al punto da dover valutare investimenti o spunti di ricerca sempre più significativi proprio in questa direzione. ■

Machine learning: strumento insidioso se nelle mani del cyber crimine

Autore: Elena Mena Agresti

Machine learning (ML) è un termine divenuto ormai di uso corrente. Applicati nella logistica, nell"healthcare, nella finanza, nell'insurance, nel retail, gli algoritmi di *machine learning* macinano quantità enormi di dati che vengono prodotti quotidianamente dagli utenti e dalle organizzazioni. Se proviamo, più in particolare, a osservare quello che oggi avviene nella *cyber security*, settore che più ci interessa, bisogna precisare che tali algoritmi vengono utilizzati in massima parte come strumento a supporto della capacità di difesa delle organizzazioni. Esempio lampante le attività di *Threat Intelligence* che sfruttano il ML al fine di profilare gli attaccanti in maniera dinamica, seguire il passo dell'evoluzione delle minacce, prevedere attacchi, anticipare le mosse di possibili intrusi, fino a identificare i vettori che potrebbero essere utilizzati. Tramite i meccanismi di auto-apprendimento, gli algoritmi di *machine learning*, si rilevano inoltre come un aiuto prezioso per rilevare i pattern delle minacce e sviluppare le strategie offensive e difensive più adeguate in relazione al contesto specifico di riferimento.

L'interrogativo, che però, deve maggiormente allarmarci, a fronte di una così sofisticata e accelerata evoluzione, è molto semplice: se gli attaccanti stessi decidessero di utilizzare lo strumento del *machine learning* per superare le difese dell'azienda cosa succederebbe? Gli attacchi che si avvalgono delle forme più avanzate di Intelligenza Artificiale saranno più temibili? Le tecniche di difesa "intelligente" adottate dalle aziende, sarebbero capaci di riconoscere un attaccante anch'esso "intelligente" e tanto più insidioso perché in grado di adattare il proprio comportamento in base al contesto dello specifico momento aziendale?

BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e il CERT di Poste Italiane.
Esperta di compliance, standard internazionali, governancedell'information security, gestione dei rischi, security audit, formazione eawareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane eattualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

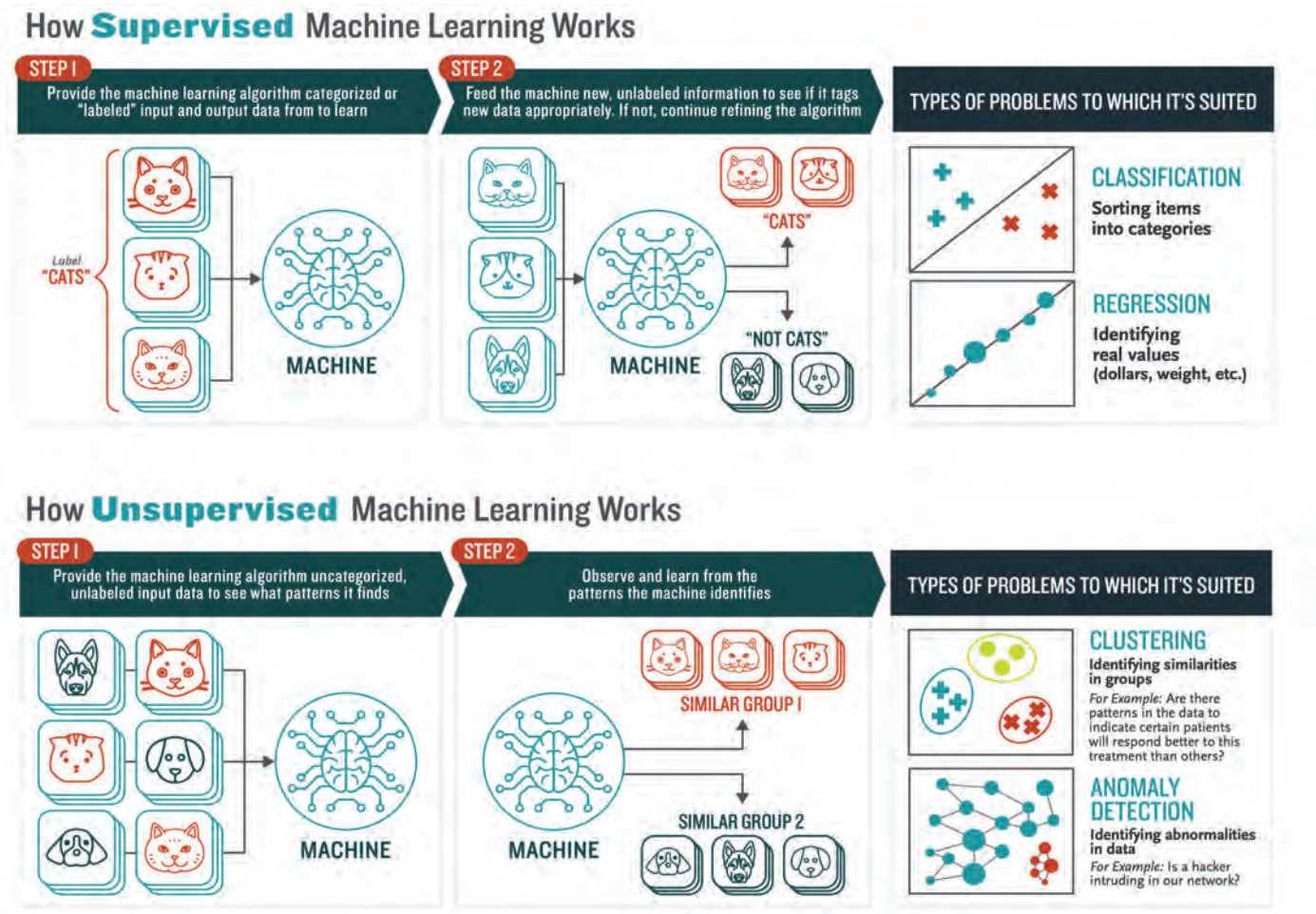
Le capacità predittive messe a rischio dalla "minaccia intelligente"

Difficile dare un risposta definitiva, la cosa più grave risiede, probabilmente nel fatto, per nulla improbabile, che le stesse capacità predittive elaborate dalle aziende, potrebbero risultare vane e inefficaci. Alla luce delle nostre conoscenze una cosa è certa: le piattaforme basate su algoritmi supervisionati sono destinate a non durare molto a lungo. Per comprendere al meglio lo scenario, è bene distinguere due macro-categorie di algoritmi di *machine learning*, i cosiddetti "supervisionati" e "non supervisionati". I primi, come si può comprendere dallo stesso nome, utilizzano esempi completi, forniti dall'operatore, per eseguire le attività richieste e vengono utilizzati nel caso di *pattern* e di comportamenti noti. Per loro natura, questi algoritmi, presentano grandi difficoltà nell'individuare modelli di attacco intelligenti in continuo mutamento. Gli algoritmi non supervisionati invece non ricevo alcuna tipologia di "aiuto", non partono da uno schema predefinito ma creano in autonomia, attraverso l'analisi costante di dati e grazie alle capacità di autoapprendimento, un modello comportamentale della minaccia. Tali algoritmi di fatto si caratterizzano per una maggiore efficacia, anche se al momento richiedono, purtroppo, un tempo molto lungo nella fase di apprendimento, soprattutto all'inizio della loro implementazione. Questo spiega il motivo pe cui sono, in molte situazioni, affiancati da soluzioni di difesa tradizionali.

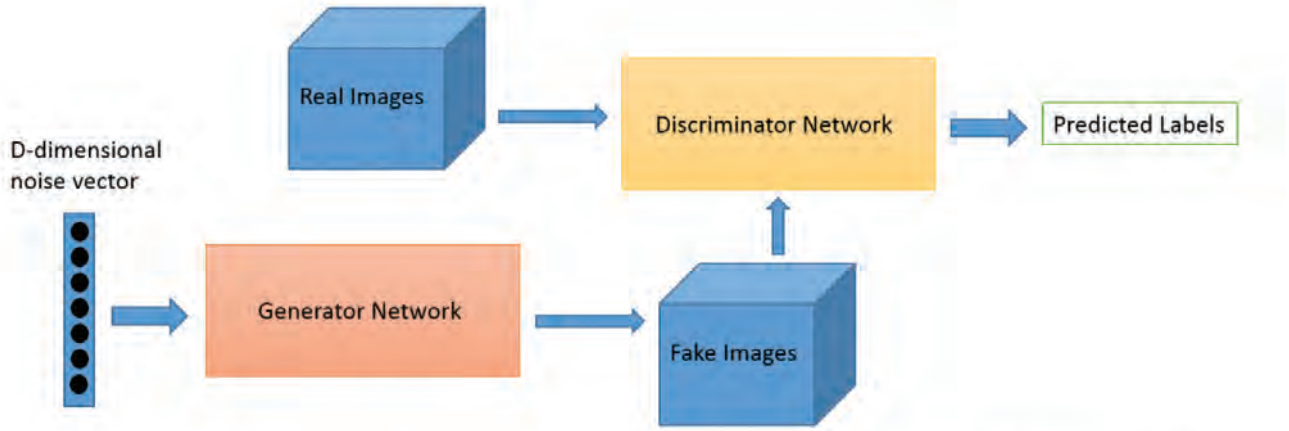
Esiste già da tempo la cosiddetta IA antagonista, si tratta di tecniche pensate per perturbare i dati, fuorviare l'algoritmo e indurlo a prendere decisioni sbagliate a vantaggio dell'attaccante. Sono diversi gli esperimenti compiuti in questo campo. Dalla modifica ad arte di piccoli pixel in un'immagine può far sì che una immagine sia classificata in modo errato ad attacchi perpetrati via telefono, attraverso l'utilizzo di frammenti di voci registrate per raggirare sistemi di sicurezza vocale o effettuare attacchi di *social engineering*, sotto le mentite spoglie di persone di fiducia, quando non addirittura autorevoli.

Una palestra per gli "algoritmi"

I nuovi algoritmi dovranno essere pensati per far fronte all'IA antagonista. Ad oggi sono in sperimentazione l'applicazione di dati ibridi, dati perturbati e dati reali per aiutare l'IA a riconoscere e risponde ad eventuali attacchi, tanto che sembra opportuno parlare di una sorta di "palestra" per gli algoritmi. Da alcuni anni sono state sviluppate le *Generative Adversarial Networks*



Sistemi "supervisionati" e "non supervisionati". Infografica © Booz, Allen, Hamilton



Simplified visualization of a GAN. Image source: "Generative Adversarial Networks for Beginners," O'Reilly.

(GANs), letteralmente reti antagoniste generative, basate su algoritmi di machine learning non supervisionati. L'architettura è costituita da due reti neurali distinte concorrenti che si sfidano l'una con l'altra. Le GAN hanno ultimamente fatto registrare diverse applicazioni nel campo della cyber security come nell'ambito del riconoscimento facciale, del furto di credenziali, della creazione di malware, finalizzati all'elusione dei sistemi di detection[1]. Più in generale appare opportuno prendere in esame due approcci nell'utilizzo delle GAN. Il primo in cui la rete GAN viene utilizzata per generare nuovi campioni attendibili che possono quindi servire come dati di addestramento per altri modelli di apprendimento automatico. Il secondo che prevede un vero e proprio "addestramento" della rete GAN, con l'obiettivo di generare dati antagonisti, dal profilo realistico, perciò particolarmente adatti ad ingannare i sistema di sicurezza.[2]

Altra caratteristica importante che non va tralasciata: gli attacchi basati sull'intelligenza artificiale possono non avere successo al primo tentativo, per poi riuscire con particolare efficacia a centrare il loro obiettivo negli attacchi successivi, questo grazie alle capacità di apprendimento e adattabilità. Sono già in circolazione dei malware "intelligenti" in grado di apprendere automaticamente l'ambiente IT, di identificare i sistemi meno protetti o imitare componenti di sistemi autorizzati e, in caso di rilevamento e blocco, di modificare il proprio comportamento, in modo da avere successo nelle azioni successive.

La frontiera "mobile" delle minacce

Ma i pericoli non finiscono qui. Sono stati sviluppati sistemi intelligenti per la violazione di captcha e password, di Virtual Humint automatizzation o di analisi di vulnerabilità in grado di identificare potenzialmente

anche le vulnerabilità zero day da sfruttare. Anche gli attacchi di social engineering e spam intelligente stanno diventando sempre più pericolosi. L'intento è quello di inviare una mail che ha come "finto" mittente il Direttore o il capo ufficio, replicandone il modo di scrivere, persino il linguaggio… Un lavoro perfetto, da far sembrare tutto lecito e customizzato per l'ignaro destinatario. Allo stesso modo siamo oggi in grado di simulare una conversazione con un essere umano attraverso gli algoritmi di NLP (Natural Language Processing, elaborazione del linguaggio umano), grazie all'applicazione dello strumento del *machine learning*. La frontiera dell'innovazione è aperta, per questa ragione bisogna rafforzare i sistema di tutela e di protezione delle reti, che riguardano non solo le attività di business, ma anche la nostra stessa vita, in tutte le manifestazioni del quotidiano.

Ripensare i nostri sistemi di difesa che dovranno essere sempre più orientati a rispondere a minacce "intelligenti" in grado di attuare le stesse logiche adottate per proteggere i nostri sistemi, diventa in quest'ottica un imperativo categorico, cui nessuno potrà sfuggire. ■

1 https://www.cs.tufts.edu/comp/116/archive/fall2018/tklimek.pdf
2 https://www.researchgate.net/publication/333552600_A_review_of_generative_adversarial_networks_and_its_application_in_cybersecurity

Threat Hunting e Machine Learning

Autore: Emanuele Gentili

L'attività di raccolta e di analisi delle informazioni da fonti esterne al proprio perimetro ha da sempre giocato un ruolo chiave in tutte le battaglie, siano esse quelle fisiche che quelle digitali.

L'importanza della Cyber Threat Intelligence e della conoscenza della minaccia permette da tempo alle varie organizzazioni che si dotano di questa capacità, di poter individuare, attribuire e rispondere, a volte anche in modo preventivo, ad incursioni cibernetiche da parte di avversari più o meno strutturati.

Effettuare l'identificazione di minacce cibernetiche, tuttavia, non è cosa semplice, se si pensa alle continue evoluzioni sia in termini di Operational Security (OPSEC) che di antimalware evasion, prontamente messe in campo dagli avversari strutturati in risposta alle metodologie e tecniche di "detection" implementate in soluzioni software o dettagliate all'interno di whitepaper dai vendor di cyber security.

BIO

Fondatore e SVP of Threat Intelligence in TS-WAY, ha maturato una lunga esperienza nell'analisi e nell'identificazione di minacce cibernetiche complesse. Advisor di realtà pubbliche e private, è Co-Direttore delle Iniziative di Cyber Security della Fondazione ICSA, membro del consiglio direttivo della COVID19 Cyber Threat Coalition. E' stato parte integrante del Nucleo di Analisi Nazionale nelle esercitazioni di guerra cibernetica NATO e svolge attività di ricerca per la produzione di algoritmi predittivi e metodologie di detection finalizzate all'identificazione di minacce cibernetiche complesse.

È bene tener presente che, almeno una parte consistente degli avversari strutturati leggono i report rilasciati online dai vendor di cyber security con l'obiettivo di apprendere come gli stessi siano stati in grado di identificare la minaccia. Ulteriore azione tipicamente svolta è quella di verificare la "detection" degli strumenti offensivi prima di lanciare una nuova campagna, al fine di avere un buon grado di confidenza che gli stessi non vengano rilevati né in formula di analisi dinamica né in quella di analisi statica.

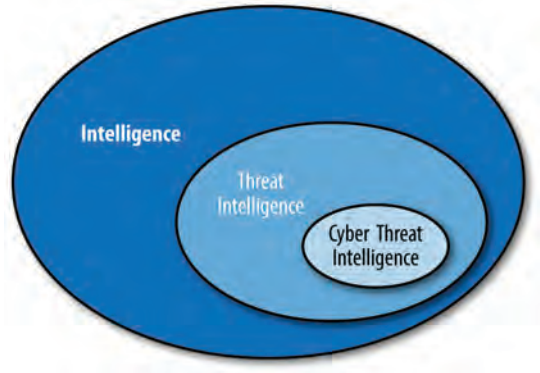
Una battaglia costante e ciclica

Ma le azioni correttive applicate dagli avversari generalmente non sono drastiche, bensì si limitano alla modifica delle sole aree critiche che permettono il riconoscimento ed il blocco della minaccia stessa. Va considerato infatti che dietro la manutenzione e lo sviluppo di un impianto malware ci sono investimenti, se non direttamente economici quantomeno equivalenti in tempo/effort che come per ogni software prevedono progettazione, sviluppo, testing e bug fixing.

Dall'ottica degli avversari è quindi di fondamentale importanza cercare di limitare l'identificazione dei propri strumenti offensivi con operazioni di

modifica chirurgica, che non richiedano progettazione e sviluppo ex novo di nuovi malware implant all'identificazione degli stessi.

Questo approccio, fortunatamente estremamente difficile da sorpassare, rende possibile agli analisti, da un punto di vista di Cyber Threat Intelligence, il tracciamento nel tempo dell'avversario dei suoi strumenti e delle relative evoluzioni.



Un'analisi approfondita degli strumenti offensivi e delle relative TTP (Tattiche, Tecniche e Procedure) associate all'avversario, con un'ottica di Threat Intelligence permette infatti di poter evincere dei "pattern" compositi e complessi, sia di tipo tecnologico che comportamentale, da poter utilizzare a proprio vantaggio per attività di Threat Hunting.

Pur non essendo una panacea, il Machine Learning trova interessanti modelli di applicazione all'interno

delle attività di Threat Hunting quale supporto agli analisti e ricercatori di minacce cibernetiche.

Partendo da una buona base informativa di Cyber Threat Intelligence, in termini di qualità e quantità di informazioni necessarie per svolgere attività di "training", sono stati implementati nel tempo vari modelli capaci di classificare minacce cibernetiche e di supportare ad esempio la fase di triage degli stessi, rendendo notevolmente la vita più semplice agli analisti di cyber security.

Altri approcci che stanno fornendo importanti risultati, vedono l'utilizzo di modelli di Machine Learning finalizzati alla generazione di "clusters" di similarità a partire da un insieme di malware non omogenei, altra capacità molto utile in chiave tecnica e strategica quando si possiede un'importante base dati di malware samples e si ha la necessità di investigare l'evoluzione di uno specifico avversario e/o di uno specifico malware nel tempo.

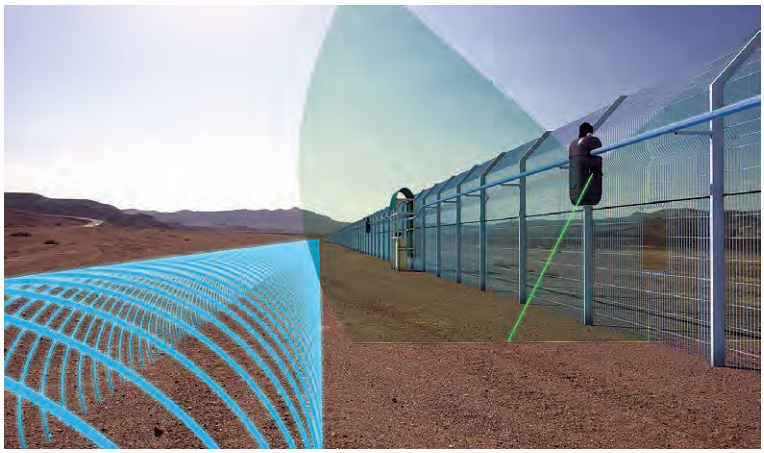
Come spesso accade la tecnologia viene in aiuto all'essere umano, ma attenzione a non considerarla la soluzione per ogni problema. ■

ML, AI, IoT: perché è importante riflettere

Autore: Laurent Chrzanovski

Da un primo sguardo possiamo osservare che i temi proposti dalle multinazionali, doverosamente affrontati sia dalle varie riviste non specifiche del settore sia dalla nostra rivista con spirito analitico e da altre con scopi simili, sono identici a quelli che hanno preceduto i due anni "persi" a discutere quasi esclusivamente sull'implementazione del GDPR e sulle misure che dovrebbero essere adottate dalle aziende.

Recentemente assistiamo ad un evidente paradosso. Per ovvi motivi di guerra economica globale, il tema del 5G e dei nuovi approcci di sicurezza necessari a qualsiasi azienda che deciderà di passare "dal cavo all'onda" sembrano essere diventati un tabù.



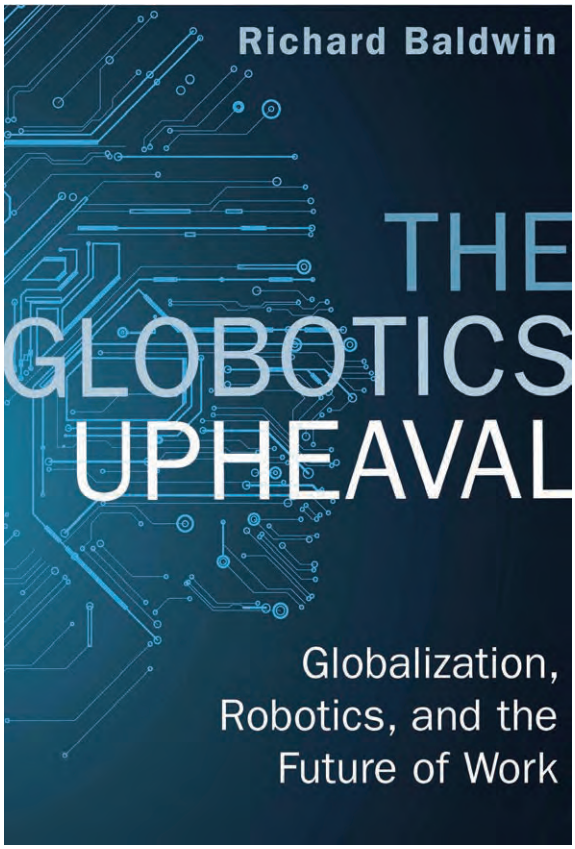
Ora il passaggio da una difesa perimetrale ad una difesa globale rappresenta un vero salto quantico che include l'utilizzo di nuove tecnologie e nuove formazioni: non si tratta più di difendere una struttura *intra muros,* con i suoi strumenti IT ed i suoi lavoratori, ma si devono ormai includere tutti gli impiegati, oggetti, macchinari e utenti connessi a distanza. In questo senso, discutere di ML, AI e IoT è vano e prematuro, proprio perché il 5G è l'anello ultimo e alquanto indispensabile per permettere la finalizzazione della quarta rivoluzione industriale, che include tutto quanto racchiuso nei tre acronimi ben noti. Arrivando quindi al *Machine Learning*, ormai inscindibile dall'Intelligenza artificiale, possiamo osservare due attitudini e due realtà in pieno contrasto tra di loro.

L'attitudine progressista

Il capolavoro di Richard Baldwin, *The Globotics Hupheaval,* pubblicato dalla Oxford University Press e appena edito in lingua italiana sotto il titolo *"Rivoluzione globotica. Globalizzazione, robotica e futuro del lavoro"* (ed. Il Mulino, Bologna 2020), è l'interpretazione perfetta del punto di vista dell'economia, trascritto dalla penna di uno dei più celebri professori di

BIO

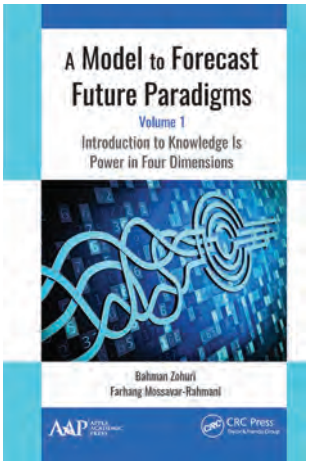
Laurent è professore di Archeologia e Storia Antica presso la Scuola dottorale e postdottorale dell'Universita' Statale di Sibiu. Tiene regolarmente corsi post-dottorato in Università di prestigio in diversi paesi dell'UE, in primis a Varsavia. E' autore/redattore di 40 libri, di oltre 150 articoli scientifici e di altrettanti articoli destinati al grande pubblico. Nel campo della cybersecurity, Laurent è membro del gruppo di esperti dell'ITU. Ha fondato e gestisce ogni anno il trittico di congressi PPP "Cybersecurity Dialogues" (Romania, Svizzera, Italia) organizzati in collaborazione con un grande numero di istituzioni specializzate, internazionali e nazionali. Con lo stesso, ha fondato ed è redattore capo di Cybersecurity Trends, la prima rivista trimestrale di sensibilizzazione alla sicurezza informatica per adulti, pubblicata in quattro varianti adattate ad altrettanti ecosistemi lingusitsici e culturali. Il suo campo di studio è focalizzato sulla relazione tra i comportamenti umani versus il mondo digitale, in cybersecurity e non solo.



questo campo. I robot non potranno funzionare correttamente se non saranno dotati di *machine learning* e di intelligenza artificiale, che a sua volta per non dare risultati controproducenti hanno bisogno di potenti infrastrutture globali che ne garantiscono il buon funzionamento, la difesa e ne limitano al massimo i danni.

Ci ritroviamo quindi di nuovo davanti ad un'altra "nicchia" monopolistica come quella delle GAFAM, e lo si vede nel piccolo numero di fornitori nel settore della robotica avanzata per i siti di logistica (4 giganti: un giapponese, un tedesco e due americani). Il libro, celebrato dal Sunday Times come *"Un manifesto come prova del futuro dei nostri impieghi e della nostra prosperità"*, spiega a che punto siamo con queste tecnologie, a che punto saremo a breve e medio termine, e quanti vantaggi ne potrebbero trarre le nostre società.

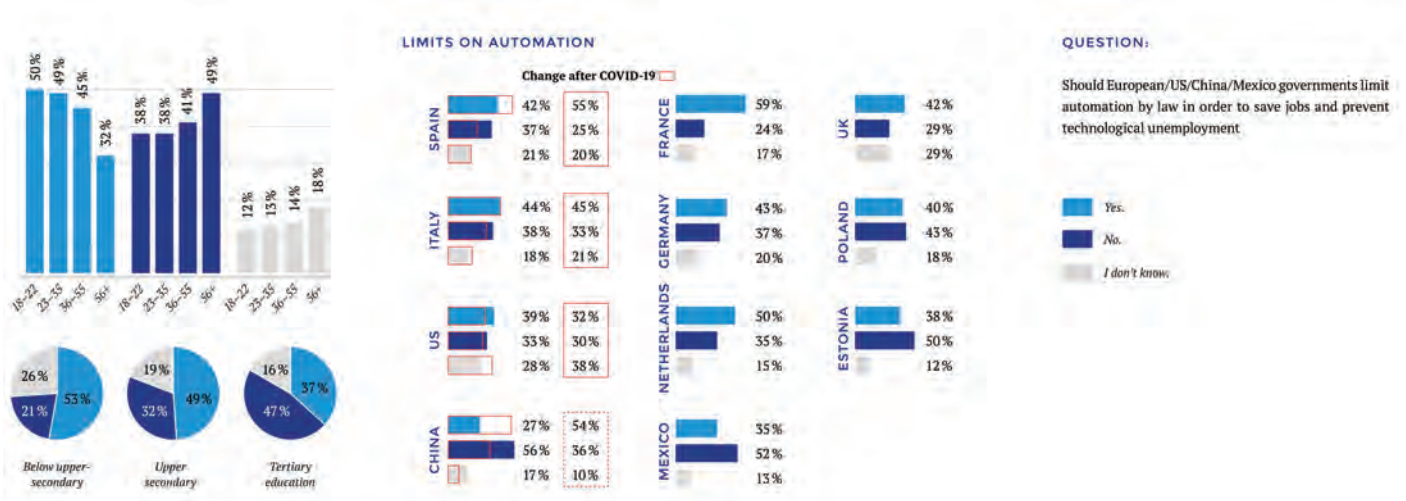
L'attitudine realista di specialisti e popolazione



Riassumendo molti articoli e libri, fra cui il più importante *"Knowledge Is Power in Four Dimensions"* dei ricercatori indiani Bahman Zohuri e Fahrang Mossavar-Rahmani (2 volumi, Apple Acedemic Press, 2019 e 2020) che dimostra come i risultati del ML e AI possono essere utili solo combinati all'intervento umano che li analizza e li perfeziona, ci limiteremo a citare il titolo dell'articolo che riassume la ricerca di Hannah Kerner, ricercatrice e specialista di Machine Learning per alimenti e agricoltura per il "Harvest Program" della NASA: ***"Too many AI researchers think real-world problems are not relevant. The community's hyperfocus on novel methods ignores what's really important."*** (MIT review, 8 agosto 2020). Ancor più incisiva la testata del secondo capitolo ***"More harm than good"***, la quale dimostra fino a che punto chi inventa i prodotti AI del domani è lontano da ogni realtà. Perché, come magistralmente dimostrato nella ricerca di Gary Marcus della New York University intitolata *"Deep Learning: A Critical Appraisal"* (White paper, NYU, 2018), i ricercatori si

basano su un ecosistema completamente stabile (motivo del loro successo in viticoltura o nella prevenzione di aritmie cardiache per malati cronici). La maggior parte dei prodotti AI non colgono, però, il "noise" dei *fake data* e si sono dimostrati completamente inefficaci per le strategie di business o lo sviluppo IT. Questo a causa della loro incapacità di comprendere lingue e culture diverse, in un mondo sempre più diversificato proprio in quegli aspetti necessari ad una corretta comprensione del singolo paese (potenziale militare, cyber, geo-strategico, economico e politico).

Da parte dei cittadini osserviamo una sana dose di scetticismo, accentuata anche da una vera e propria paura. La richiesta di adottare normative che regolamentano e limitano l'attività dei robot e l'AI è ormai un'esigenza comune alla maggior parte degli europei, come abbiamo già scritto in un numero precedente della rivista. Il rapporto annuo del 2019 di *Mapping European Attitudes to Technological Change and its Governance* dimostrava che *"la maggior parte degli europei ritiene che i governi dovrebbero intervenire immediatamente per limitare l'automazione e affrontare gli effetti negativi sulla società".*



Nel rapporto del 2020, appena uscito, si osserva che l'urgente richiesta di un intervento da parte dello Stato per adottare norme che limitano l'utilizzo dei robot e dell'automazione è aumentata di quasi un terzo dall'inizio della pandemia del COVID-19. Ad esempio, in Cina si sono raggiunti livelli massimi, dove ormai il 54% dei cittadini chiedono rapide misure di intervento da parte Stato, mentre nel 2019 erano solo il 27%. [1]

La realtà pragmatica del mondo economico:

Da un punto di vista economico, oggi ogni euro rimpatriato conta. Un'azienda pur di aumentare la propria competitività non si preoccuperebbe di sostituire centinaia di uomini, donne e bambini (lì dove la legge permette il lavoro sin dai 12 anni) sottopagati nel terzo mondo con un parco di robot in Europa, nonostante i danni che potrebbe apportare ai paesi con la chiusura delle fabbriche. A questo proposito, la Banca Mondiale (press release del 7 ottobre) ha appena denunciato che, tra molti fattori, saranno *in primis* l'AI e la robotica i responsabili del raggiungimento della soglia di povertà assoluta di più di 170 milioni di persone (meno di 1.69 US/giorno) entro il prossimo gennaio – l'IA avrà un impatto più grande nei paesi più ricchi, la robotica, invece soprattutto in Asia.

La realtà pragmatica del mondo della sicurezza:

Le soluzioni AI in materia di sicurezza, che hanno lo scopo di sostituire tutti i mezzi tecnologici e umani usati finora, sono ancora completamente immature. Come tali sono state rifiutate da tutti i servizi essenziali alla sicurezza dello Stato. In solo due campi l'AI offre risultati utilissimi. Il primo settore è quello delle tecnologie implementate con l'AI, queste venendo utilizzate per segnalare e affrontare gli APMT *(Advanced Persistent & Mutant Threat)* – la "M" è stata aggiunta da più di un anno – ed è proprio perché queste mutazioni sono delle aggiunte o delle modifiche ad un malware già noto che l'AI può riconoscerle e rispondere più rapidamente che l'umano. Il secondo è lo smistamento dei dati, perché

la creazione dei dati su base oraria è tale che non può essere gestita dall'uomo. L'AI permette agli analisti di focalizzarsi sulle minacce più gravi e più urgenti, a condizione – contrariamente all'AI onnisapiente venduta da alcune aziende – di non eliminare nulla, perché è proprio dalla massa dei dati scartati che lo specialista esperto può estrarre i "segnali deboli", possibile segnale di un attacco gravissimo che verrà attuato solo mesi o anni dopo (vedasi l'attacco del dicembre 2015 alla centrale elettrica di Ivano-Frankivsk, Ucraina, cominciato con operazioni "banali" sulle reti social e telefoniche di impiegati, manager, fornitori, etc. sin dall'aprile 2014).

Come sottolineato da Giorgio Metta in questo numero, gli esoscheletri hanno un grande potenziale. Come tali, sono già parte dell'arsenale d'assalto utilizzato su campi di battaglia reali (Afghanistan, Siria) dagli eserciti americani e russi. Ma nessun esercito ha intenzione di usare robot al posto di soldati. Tutti i prototipi testati dalla *United States Army* e dalla *Вооружённые силы Российской Федерации* sono risultati incapaci di distinguere l'amico dal nemico nelle guerre moderne, che ormai sono tutte ibride, e ancor peggio, in un contesto urbano con scarsa visibilità (polvere di sabbia in particolare), non sono in grado di distinguere un civile che tiene in mano un sasso da un terrorista che tiene una granata. I due eserciti che si sono espressi, uno attraverso il portavoce del DARPA e l'altro direttamente tramite il presidente Putin, hanno però scelto due opzioni diverse: il Pentagono, dopo test catastrofici, ha rifiutato (ufficialmente) di continuare a sostenere le ricerche sugli *"autonomous robot killers"* – ma è entrata in una "guerra verbale" con la *Cina su chi avrà il primo battaglione robotico (Times, 13 novembre 2019: China and the U.S Are Fighting a Major Battle Over Killer Robots and the Future of AI)*; Mosca che ha riscontrato grandi successi in Siria con mini-tank semi-autonomi (teleguidati ma con programmi di AI) vuole dotarsi di diversi prototipi di robot di attacco ma pienamente funzionali da usare esclusivamente su ordine presidenziale e solo in una guerra tra robot, metafora di guerra terrestre (locale, regionale o totale) tra grandi potenze (Interfax, 22 novembre 2019: *Путин велел увеличить количество боевых роботов и лазерного оружия)*.

Siria: il robot russo «Uran-6» (antimina) in azione.

Perché una pausa è obbligatoria:

È lo stesso Professor Baldwin a rivelare con la dovuta serietà accademica che viviamo proprio tutto il contrario di un qualsiasi progresso. Non solo afferma che *"il problema risiede nella velocità inumana dei cambiamenti, o, più precisamente, della confusione tra la rapidità di distruzione di impieghi versus la lentissima creazione di nuovi posti di lavoro"* (p. 187). Peggio, sottolinea che grazie alla "globotica", associata al peso e all'implicazione delle GAFAM, la ***"Job destruction IS the Business Model"***, come definito nel titolo del capitolo successivo alla citazione indicata.

Le conclusioni del libro - e i suoi pesanti non detti, sono più che preoccupanti. L'autore afferma con modestia che, non essendo uno specialista, si aspetta in tempi rapidi di ottenere un riscontro politico, sociologico, antropologico e un modello tassativo prima di celebrare la "globotica" come un progresso. In effetti, citando quasi cento fonti diverse, Baldwin pone la creazione di un modello socio-comunitario basato sulla flessibilità degli impiegati a cambiare città, regione o paese e anche sulla disponibilità ad imparare un nuovo lavoro come condizione sine qua non l'implementazione della "globotica". L'autore, inoltre, cita l'esempio della *"flexicurity"* danese che si basa non sulla difesa del posto di lavoro ma dell'impiego. Tale modello non solo sarebbe impossibile da adottare in paesi dalla dimensione dell'Italia (in Danimarca cambiare posto di lavoro non implica cambiare domicilio, visto la qualità e la rapidità dei mezzi pubblici) ma sarebbe pure incompatibile con i modelli degli ammortizzatori sociali come l'indennità di disoccupazione dell' 80% dei paesi membri dell'UE, che non hanno il sostegno formativo previsto dallo stato danese tramite massicci aiuti privati che garantisce un cambio positivo di categoria e anche del settore d'impiego.

In Francia, dove la giustizia non ha ancora dato il suo verdetto sul caso Amazon, il Presidente Emanuel Macron ha concluso un accordo con il gigante delle GAFAM permettendogli di estendere la sua presenza, questo dopo un accordo con il Presidente Donald Trump su di una tassazione *ad minimam* dei GAFAM (ma non dei robot come da tempo auspicava Bill Gates).

Ora i gruppi di ricerca del CNRS hanno dimostrato che ogni impiego generato da Amazon ne sopprime 2.8 altrove. La realtà sarebbe oltre i 5 posti di lavoro persi per 1 creato da Amazon se non ci fossero gli *"schiavi della strada"* (traduzione letterale). La politica di Amazon in Francia è stata quella di scegliere zone non lontane da grandi reti autostradali ma con un alto tasso di disoccupazione. Ed è così che la riserva archeologica e naturale del Pont-du-Gard si ritrova con un livello di particelle sottili pari a quello di una metropoli: per un mega deposito, che ha creato soli 220 posti di lavoro (ovvero 70 x 3 turni x 7 giorni), i municipi e le provincia hanno dovuto investire 6.6 milioni di euro per creare nuove reti di viabilità che consentissero un rapido

2008, Aldo Calvini Benedetti

collegamento dall'autostrada al deposito per scarico e carico di centinaia di TIR e camion più piccoli ogni giorno. Con i nuovi depositi in costruzione, sempre secondo i ricercatori del CNRS, la Francia dovrà sin dal 2021 comperare da altri paesi 12% addizionali di emissioni di CO_2, emissioni nuove che risultano dall'aumento del traffico stradale di merci generato esclusivamente dai magazzini del gigante GAFAM.

Oltre all'ecologia c'è un ultimo aspetto che non convince: il modello proposto da Baldwin si basa sulla creazione di nuovi *"job types"* di tipo comunitario basati su etica, empatia, cuore e abilità (secondo Baldwin queste sono qualità più equamente distribuite che il sapere e l'esperienza). Questi dovranno sostituire i vecchi CV basati su propensioni, curriculum universitari – oggi da considerarsi arcaici secondo l'autore – ed esperienze professionali. Ora se si siamo convinti della veridicità dell'espressione *"mens sana in corpore sano"* non possiamo immaginare cuore e empatia senza mente come *"job requirement"*.

"Mens sana in corpore sano ***cum cordam****"* sarebbe la giusta misura. Ma per avere una mens sana ci vuole giustamente tutta l'esperienza e la conoscenza che Baldwin ritiene inutile perché sarà sorpassata dal sapere dell'IA. Ed a causa dell' ignoranza e della mancanza di cultura che notiamo, in società sempre più individualista, che l'empatia viene abbandonata a favore di un'altra espressione del "cuore": l'odio e la violenza a "favore" di una "causa nobile", come ormai osserviamo da parecchi mesi negli Stati Uniti.

Dai gruppi storicamente pacifisti e colti, dai difensori delle minoranze e dai gruppi promotori di una condanna ferma – ma ancorata nella sua contestualizzazione storica – degli orrori della schiavitù, siamo passati alle distruzioni vandalistiche e alle guerriglie urbane con la "motivazione" *LGBT, Black Life Matters, Antifa…*

Le GAFAM stanno finendo di uccidere, oltre la cultura e la storia, il libero arbitrio basato sulla conoscenza di FATTI, la sola che permette di avere un DIBATTITO sulla loro interpretazione. Non permettiamo loro di farci credere che col CUORE ritroveremo uni impiego rubato da un robot o da un centinaio di algoritmi… gli stessi che hanno già rubato la democrazia in 42 elezioni in altrettanti paesi.

Nel *Mapping European Attitudes to Technological Change and its Governance* 2020, c'è un testo di Carl Benedikt Frey, direttore del programma *"Future of Work"* dell'Università di Oxford. Non vi è nessun dubbio. Regolamentazione o no, ci sarà marchia indietro a piena velocità - spiega lo specialista - con una frase limpidissima ***"When automation accelerates during a downturn, a techlash is likely to follow".***

Volendo ricordare (ad uso dei governanti europei?) una frase celebre del Presidente Roosevelt estratta dal suo discorso di State of The Union del 3 gennaio 1940, in piena crisi mondiale: ***"To face the task of finding jobs faster than invention can take them away - (this) is not defeatism"…*** un anno prima di Pearl Harbour, la distruzione di impiego da parte della tecnologia era già di pesante attualità… ■

1 (European Tech Insights, Center for the Governance of Change: www.ie.edu)

GLOBAL CYBER SECURITY CENTER

L'impatto del cyber risk sul mercato finanziario

Case Studies

Il nuovo studio della Fondazione GCSEC volto alla comprensione degli effetti di un attacco cyber sul valore azionario di un'azienda, a cura di Massimo Cappelli e Marika Mazza.

Disponibile gratuitamente previa registrazione su: www.gcsec.org

Il destino dei saperi politecnici nella società digitale

Intervista VIP a Paolo Zanenga, presidente della Diotima Society

Autore: Massimiliano Cannata

"Il futuro dei saperi politecnici" (vol. 1.2.3.) pubblicati dalla Fondazione Francesco Fabbri con la collaborazione di Diotima Society, Fondazione Giannino Bassetti e Centro Europa Ricerche è il condensato di molteplici esperienze, interpretazioni, idee e suggestioni emerse in occasione di una serie di incontri che si sono tenuti a Venezia, Milano e Roma. La riflessione su quello che si può considerare uno dei grandi temi del nostro tempo proseguirà nei prossimi mesi, con particolare focus sul rapporto tra saperi e lavoro, saperi e cultura del diritto, senza trascurare le implicazioni di natura semiotica e filosofica generate dal profondo processo di trasformazione dall'industriale al digitale, che sta cambiando non solo gli assetti di sistema, ma anche il nostro modo di vivere e di intendere le relazioni e il lavoro. Presidente oltre che fondatore di *Diotima Society*, abbiamo chiesto a Paolo Zanenga di aiutarci a capire le connotazioni di questo mondo digitale, che ci avvolge, con cui dobbiamo prendere le misure per affrontare al meglio le sfide future.

BIO

Paolo Zanenga è ingegnere e teorico dei sistemi cognitivi, saggista. Dopo aver partecipato alla rivoluzione manageriale tra gli anni '80 e '90 negli Stati Uniti, ha condotto progetti di innovazione strategica con importanti global company in Europa e negli Stati Uniti e con istituzioni governative. È titolare del corso "Complessità della conoscenza e reti dell'innovazione" alla Scuola di Dottorato del Politecnico di Torino e docente al master in "Filosofia del Digitale" all'Università di Udine. Tra le sue pubblicazioni, "Le Reti di Diotima" (Carocci 2010) e "Emersione - Oltre la Disruption" (2020). Visiting lecturer in altre università italiane e internazionali. Presidente oltre che fondatore di Diotima Society, gli abbiamo chiesto di aiutarci a capire le connotazioni di questo mondo digitale, che ci avvolge, con cui dobbiamo prendere le misure per affrontare al meglio le sfide future.

Prof. Zanenga la Diotima Society in collaborazione con istituti di ricerca, Università e con le aziende più aperte all'innovazione sta portando avanti un'analisi approfondita sulle trasformazioni sociali ed economiche di una realtà fluida, e in continua mutazione. Di che cosa si è parlato e soprattutto di cosa parlerete in questo ciclo di seminari che da Nord a Sud stanno coinvolgendo una porzione importante della classe dirigente e della classe manageriale?

Partirei da un dato di fondo, che investe tutte le categorie sociali senza distinzioni: la rivoluzione di quelli che abbiamo definito per intenderci "saperi politecnici". I saperi disciplinari, l'università humboldtiana e lo stato borghese costituiscono un combinato che nasce con la risposta prussiana alla Francia post-napoleonica e alle *Grandes Écoles* francesi, e che riconosce alle università uno status speciale e strategico per lo sviluppo dello stato nazione. Questo modello è quello che si è evoluto nel '900 attraverso il confronto col modello americano. Alle spalle sta un sistema di produzione di valore agganciato al principio di razionalità e all'organizzazione, che aveva come fine l'estrazione del valore dalla natura o dal lavoro. La natura era considerata come risorsa da cui estrarre valore: era a disposizione, compreso l'uomo. Le due parole chiave erano ordine e linearità. In questo scenario i saperi politecnici erano indispensabili per lo sviluppo tecnologico del

"sistema – stato" (ferrovie, metallurgia, ecc.) in una fase in cui anche le arti e le *humanities* erano servite a definire i lineamenti della "nazione".

Quali sono state le conseguenze di questo modello?

La storia è stata riscritta e risistemata secondo questi principi, teniamo conto che è stato in questo particolare periodo che si è aperta una voragine tra le due culture caratterizzata dalla profonda ignoranza, accompagnata spesso da un certo disprezzo, degli studiosi di *humanities* nei confronti della scienza e della tecnologia. Disprezzo a parti invertite ricambiato, più che dagli scienziati, dal mondo dell'economia e del business nei confronti degli umanisti.

Dopo la pubblicazione del celebre scritto del Nobel per la chimica e gli studi sulla termodinamica di Ilya Prigogine* La nuova alleanza*, si è compreso che non esistevano due culture. Un passo avanti importante anche se tardivo non crede?

Sicuramente decisivo. Il passaggio dal paradigma industriale a quello digitale è stato ed è il catalizzatore di questa trasformazione perché richiede, per continuare ad alimentarsi, un approccio non solo interdisciplinare, ma adisciplinare e complesso, necessario per mettere a fattore comune contributi di conoscenze diverse. Il sapere condiviso non richiede più trasferimento da persona a persona, è per definizione aperto, quindi a disposizione di tutti. C'è capitalismo dove c'è asimmetria di saperi, dunque il nuovo capitalismo deve mettere al centro l'innovazione. Una centralità che era stata auspicata da Schumpeter, che sosteneva che l'impresa dovesse essere per definizione innovativa: l'imprenditore, se non fa innovazione, non è tale.

"Viviamo – per citare il grande sociologo francese Edgar Morin – in un universo di partecipazione" segnato dall'interdipendenza di reti e sistemi e dalla complessità. Come ci si può orientare in questo nuovo orizzonte?

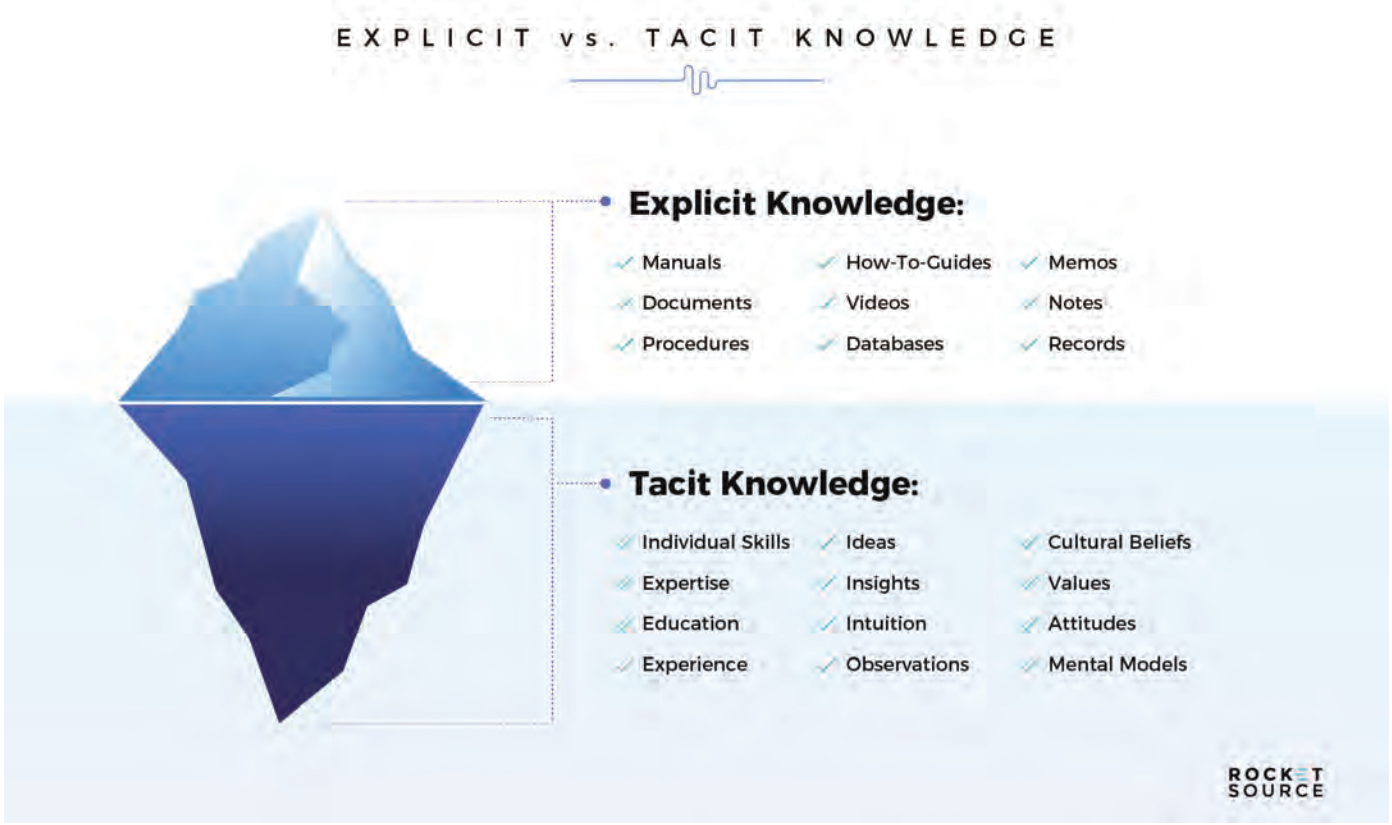
Il passaggio al digitale è connesso al passaggio da un contesto di sistemi chiusi a uno di sistemi aperti, che vivono di relazioni, non più di accentramento e proprietà, di *distressed assets* o *sticky resources:* non ha più senso investire in capitali fissi impegnati in un'economia di tipo storico. La finanza va verso imprese il cui nucleo è fatto di dati, immateriali ma capaci di condizionare il mondo. Un recente articolo in McKinsey spiega come oggi per il CEO di una global company fare strategia voglia dire non investire, ma disinvestire. Ciò che crea ricchezza deve essere disaccoppiato da ciò che non la crea. Le grandi multinazionali hanno ben compreso tutto questo come dimostra il tentativo di scardinare il diritto d'autore, al fine di sottrarre il sapere a chi ne potrebbe detenere o rivendicare la proprietà. Le piattaforme digitali come è noto estraggono dagli utenti informazioni per usarle, ma queste non diventano loro proprietà, non sono rese esclusive. Direi di più: la stessa idea di pubblico e privato si è modificata profondamente rispetto a quella maturata nella logica del sistema industriale.

Stiamo parlando di trasformazioni radicali che investono tutti gli ambiti della società. Se non rafforziamo gli investimenti in formazione non corriamo il rischio, molto concreto, di perdere la bussola del progresso e di imboccare la strada di un declino irreversibile?

Se ci riferiamo all'Italia, credo che dobbiamo reagire in fretta non facendoci spiazzare dal divenire in atto. I *bias* che frenano questo sviluppo dell'educazione sono molto radicati e articolati, per cui un'azione efficace per una migliore educazione deve essere pensata e attuata per superarli senza rimanervi incagliata. Vediamone alcuni: la focalizzazione sull'occupabilità, che privilegia competenze destinate a obsolescenza accelerata; una professionalizzazione centrata su competenze standardizzate, che penalizza i saperi taciti; l'immagine anacronistica della società, dell'economia e dei relativi valori che viene trasmessa ai giovani in ambito familiare e scolastico. Dobbiamo in sintesi renderci conto che

i saperi non sono uno strumento per fare cose, non sono più competenze, ma sono direttamente ricchezza; non strumento, ma fine. Tutto questo si riverbera inevitabilmente sull'inadeguatezza dell'insegnamento attuale, con il paradosso di docenti travet che non possono fare altro che correggere errori di persone ormai analfabete, che in futuro potrebbero diventare a loro volta insegnanti.

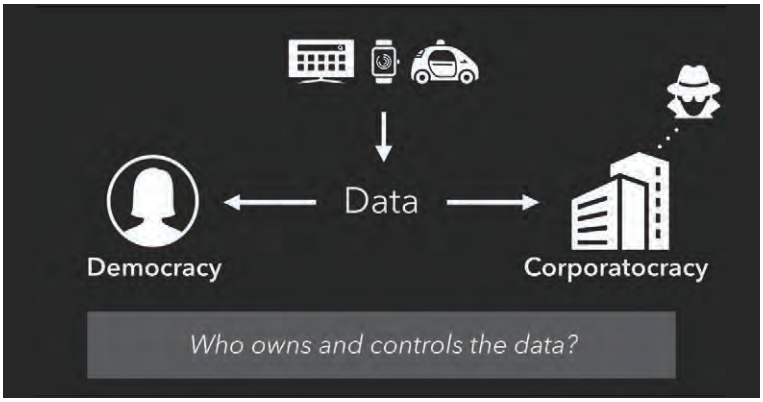
rete, emergono infiniti e diversi disegni della realtà, qualcosa che nessuno sarebbe stato in grado né di vedere, né di concepire. Quello che sappiamo è che l'applicazione del *data analytics* genera un'iperconoscenza che è insita nel dato e a noi resta ignota. Negli ultimi quindici-venti anni in Occidente questo fenomeno ha creato un oligopolio; non è detto che si tratti di un assetto definitivo. La legge di potenza dice che nelle reti *"the winner takes all"*. Tuttavia, i campi in cui può emergere un vincitore sono teoricamente infiniti, non limitati, come erano i settori dell'economia che conoscevamo.



"Verso la democrazia dei dati" è stato una delle problematiche al centro del dibattito che si è sviluppato attorno al festival internazionale della filosofia che si è appena concluso a Mantova, Carpi e Sassuolo dedicato al tema delle "macchinazioni". Qual è il suo parere in merito?

Nel paradigma digitale, la materia prima è il dato. Se prima un bene era unico e indivisibile, spesso rivale, e occupava uno spazio fisico definito, ora il bene ha un'identità molteplice, replicabile e replicata, è ovunque. Prima si faceva economia di scala se si produceva tutto in un punto o luogo circoscritto, oggi si ottengono economie di scala se vengono concentrati tutti i dati in un punto.

È dunque la capacità di estrarre significato dal dato che diventa un valore che oggi si concentra in un unico punto, un unico computer che elabora i dati raccolti da server distribuiti in tutto il mondo. A seconda dei criteri con cui si selezionano e si connettono i dati, i punti della



Questa linea di progresso non nasconde insidiosi pericoli?

Ampliando l'angolo di visuale potremmo dire che siamo di fronte alla realizzazione in via sperimentale, ma in via di estensione all'intero territorio, di un immenso Panopticon, il sistema carcerario ideato da Jeremy Bentham in cui tutto è visibile. Il potere deve avere tutto sotto controllo, vedere tutto. In tempi di coronavirus questo sistema ha funzionato bene, e ha mostrato la capacità di estendersi anche fuori dalla Cina, anche in stati democratici e

liberali. La dimensione del diritto peraltro non è più statale, nazionale, ma planetaria e sovranazionale, basato non più sull'atto bensì sul rapporto. Anche nel campo del diritto bisognerà considerare che la macchina (da questo punto di vista considero illuminata la scelta di un tema per il festival della filosofia che si colloca nel punto di convergenza tra intelligenza umana e artificiale) occuperà ruoli crescenti rispetto ai giudici umani.

Lo scenario fin qui tratteggiato impone un interrogativo: l'uomo ha ancora uno spazio di manovra nella società delle macchine digitali e dei robot?

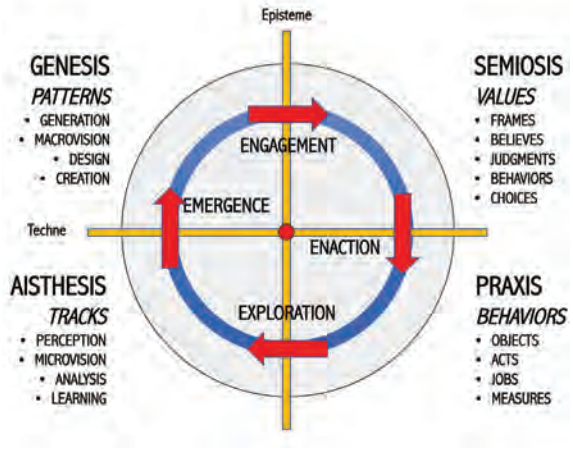
Se la macchina diventa l'interfaccia dell'uomo, i saperi di quest'ultimo devono essere in grado di gestire la relazione, la comunicazione e l'astrazione. Se il concetto di privacy è destinato ad essere superato da una trasparenza generalizzata, la capacità di immaginare, di guardare oltre l'immediato devono poter modificare di continuo la norma, il cui valore ricordiamocelo deve rimanere relativo. Quello che serve un aggiornamento e un'estensione del principio dell'*habeas corpus.*

Sembra di capire dal suo ragionamento che la tecnica non è tutto. Il fattore umano e la prospettiva etica assumono una valenza molto forte. Non pensa che si impone un'esigenza di* governance *non solo culturale ma anche politica di indirizzo della scienza che dovrà essere colmata con competenze all'altezza?

Il ruolo attivo degli attori nelle reti, cioè fondamentalmente dei loro processi cognitivi, per essere efficace deve iscriversi in una ristrutturazione dei fini e dei valori, in un contratto sociale di tipo nuovo, al cui centro non possono più essere istituzioni basate sulla loro permanenza, ma al contrario sulla loro impermanenza. La produzione di valori e la scelta dei fini avverrà attraverso intelligenza e creatività individuali e collettive, che diventano anche le fonti prime, e complementari ai dati, di un'economia che non è più centrata sul lavoro, ma sulla vita: un'economia politica che si fa biopolitica. Oggi, nel momento in cui il digitale sussume tutto il pensiero calcolante risulta ancora più evidente come la Tecnica (o la Tecnologia) abbia vita propria; ma è altrettanto evidente che (penso all'insegnamento di Heidegger su questo specifico aspetto) il pensiero dà senso ai dati fino a esorcizzare la Tecnica e a renderla benefica. A ciò corrisponde una visione diversa della realtà, non descrivibile in modo esaustivo da una scienza calcolante, ma sempre ricreata da un pensiero interpretante e significante.

Possiamo fare qualche esempio concreto di questo fitto intreccio che intercorre tra il pensiero e la tecnica?

Considerando che ci rivolgiamo a un pubblico che conosce molto bene i temi della sicurezza un esempio interessante di saperi e poteri che si creano



nel "caos generativo" è quello degli hacker. Il pensiero degli hacker rispetto alla determinazione dei fini è un pensiero senza corpo, senza un'esplicita dichiarazione di alterità non solo nei confronti del potere costituito ma anche della società nel suo complesso. Non a caso il mondo degli hacker viene catturato dai poteri della finanza: l'incorporeità sociale li avvicina all'altra forma di superamento dello stato, la finanza internazionale. Quello che stiamo descrivendo ci pone di fronte al superamento del determinismo. Possiamo, infatti dire, che non esiste alcun fenomeno culturale o economico che possa essere descritto in termini lineari: sono tutti fenomeni catastrofici, legati alle matematiche del caos, cui facevo prima riferimento.

Nel ringraziarla per questa interessante* overview *che ha offerto ai lettori di CST Le chiedo: il linguaggio ha un peso nella dinamica del cambiamento in atto?

Il pensiero significante diventa il dispositivo per rigenerare le parole che usiamo. Il che vuol dire discutere non solo dei valori, ma del senso delle parole che li definiscono. Parole come comunità, identità, competenza, classe, democrazia, moneta, stato, stanno andando tutte incontro a una probabile rigenerazione. Ciò che qualifica l'uomo è la capacità di inventare il mondo: nominare è inventare. Il linguaggio è invenzione di mondi. Si passa dal potere dell'agire al potere del definire. Habermas, un filosofo che rappresenta un pensiero ancora *mainstream*, collega alla produzione il lavoro e l'economia, mentre il potere di "definire" i termini del sapere erano riservati alla scienza, al diritto, alla politica (sfera pubblica). Nel momento in cui non è più la produzione al centro dell'economia, ma la conoscenza, la sfera economica e politica non saranno più separabili. In qualche modo l'economia è "costretta" a includere la politica sul terreno della responsabilità e della sostenibilità, e si fa strada sempre più pressante l'esigenza di aprire la nuova frontiera di un benessere costruito sulla fecondità dell'ecosistema, e non sul suo sfruttamento sistematico. ■

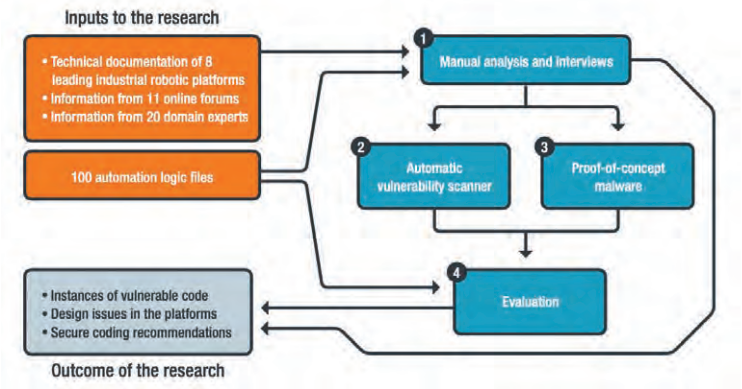
Industria 4.0: la vulnerabilità degli ambienti di programmazione per la robotica industriale

Una ricerca di Trend Micro e del Politecnico di Milano rivela alcune pericolose funzionalità nei linguaggi di programmazione per robotica industriale e stila, nel contempo, una guida pratica per ridurre la superficie di attacco grazie a un codice più sicuro, riducendo così le interruzioni di business negli ambienti OT.

"Rogue Automation: Vulnerable and Malicious Code in Industrial Programming", è il titolo dello studio condotto dall'italiano Federico Maggi di Trend Micro Research, in collaborazione con Marcello Pogliani del gruppo di sicurezza informatica del Politecnico di Milano. La ricerca descrive come alcune caratteristiche - fino ad oggi poco dibattute nel mondo della cybersecurity - dei linguaggi di programmazione per robotica industriale possano portare a programmi di automazione vulnerabili, permettendo, inoltre, ai potenziali aggressori di creare nuove tipologie di malware persistente. Quel che è più grave è dato dal fatto che questi punti deboli possono consentire agli attaccanti di prendere il controllo dei robot industriali al fine di danneggiare linee di produzione o impossessarsi di proprietà intellettuale.

Come viene rilevato dallo studio il mondo dell'automazione potrebbe essere impreparato a rilevare e prevenire queste criticità, perché finora non sono mai state affrontate. Inoltre, è fondamentale che il settore inizi ad adottare e seguire le *best practices*, per mettere in sicurezza il codice, che sono state condivise con gli *industry leader* come risultato di questa ricerca.

"Una volta che i sistemi OT sono collegati alla rete, applicare patch o aggiornamenti è quasi impossibile ed è per questo che una sicurezza a priori diventa un fattore critico". Ha

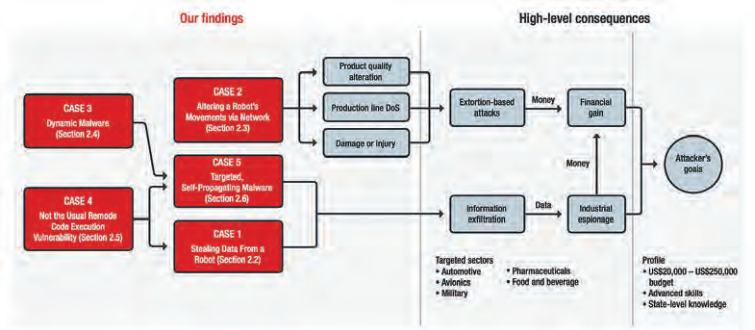


affermato Bill Malik, vice president of infrastructure strategies for Trend Micro. "Al giorno d'oggi, la spina dorsale dell'automazione industriale si basa su tecnologie legacy che troppo spesso contengono vulnerabilità latenti come Urgent/11 e Ripple20, o varietà di difetti nell'architettura come ad esempio Y2K. Non vogliamo limitarci a sottolineare queste sfide, ma ancora una volta assumere la guida della security nell'Industry 4.0, offrendo una guida concreta per la progettazione, la scrittura del codice, la verifica e la manutenzione attraverso strumenti in grado di scansionare e bloccare codici maligni e vulnerabilità".

Linguaggi di programmazione che possiamo considerare "legacy"- in quanto cuore delle moderne catene di produzione - come ad esempio RAPID, KRL, AS, PDL2 e PacScript sono stati progettati senza considerare un aggressore attivo. Sviluppati decenni fa, sono ora diventati essenziali per le attività critiche di automazione nei settori automotive come nelle filiere alimentari e nell'industria farmaceutica, ma non possono essere messi al sicuro facilmente.

Nuove tipologie di malware

Le vulnerabilità non sono l'unica preoccupazione nei programmi di automazione che utilizzano questi linguaggi. I ricercatori hanno dimostrato



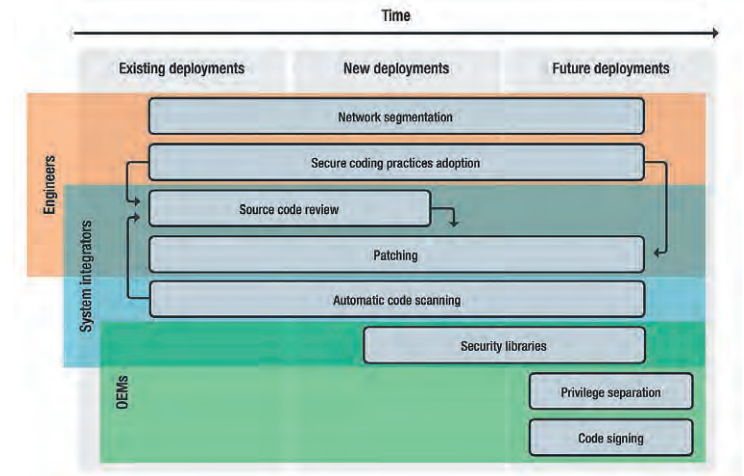
come una nuova tipologia di malware in grado di auto-propagarsi potrebbe essere creata utilizzando uno di questi linguaggi come esempio. In questa ottica Trend Micro Research ha lavorato a stretto contatto con il Robotic Operating System (ROS) Industrial Consortium - un'autorità internazionale in campo di robotica industriale - per proporre delle raccomandazioni con l'obiettivo di ridurre l'impatto delle criticità identificate[1]. "Molti robot industriali sono progettati per reti di produzione isolate e utilizzano linguaggi di programmazione legacy - spiega Christoph Hellmann Santos, Program Manager, ROS-Industrial Consortium Europe. "Possono essere vulnerabili agli attacchi nel momento in cui sono connessi a una rete IT. Per questa ragione, ROS-Industrial e Trend Micro hanno collaborato per sviluppare delle line guida per un corretto e sicuro settaggio delle reti per il controllo dei robot idustriali, attraverso il Robotic Operating System".

"Lavorare con questi sistemi è un po' come fare un tuffo nel passato: vulnerabilità adesso rare nei tradizionali sistemi IT (come le applicazioni web, ad esempio), si ripresentano attraverso questi linguaggi di programmazione, poco conosciuti ma estremamente critici", aggiunge Federico Maggi. "Nei prossimi anni il mondo dell'automazione industriale dovrà affrontare le sfide delle vulnerabilità che il mondo IT ha gestito negli ultimi 20 anni."

Linee guida e strategie di contrasto

Come dimostrano le linee guida, i programmi di automazione industriale, seppur basati su linguaggi "legacy", possono essere scritti in diversi modi per ridurne i rischi. Di seguito la checklist essenziale che Trend Micro e Politecnico di Milano propongono per la scrittura di programmi di automazione industriale sicuri:

- Trattare i macchinari industriali come se fossero computer e i task program come codice sorgente potenzialmente pericoloso;



- Autenticare ogni comunicazione;
- Implementare policy per il controllo degli accessi;
- Eseguire sempre la validazione degli input;
- Eseguire sempre la sanificazione degli output;
- Implementare una gestione degli errori senza esporre i dettagli;
- Implementare una configurazione appropriata e procedure di deployment.

Trend Micro Research e Politecnico di Milano hanno inoltre sviluppato uno strumento per rilevare codice maligno o vulnerabilità all'interno dei *task program*, prevenendo eventuali danni al momento della loro esecuzione.

Come risultato di questa ricerca, sono state identificate feature critiche per la sicurezza nelle principali otto piattaforme di programmazione di robot industriali e un totale di 40 istanze di vulnerabilità di codice open source. Un vendor ha rimosso il proprio programma di automazione vulnerabile e altri due sono stati avvisati, dando il via a discussioni per migliorare i propri strumenti. I dettagli delle vulnerabilità sono stati condivisi anche dal ICS-CERT alla propria community, attraverso un alert[2]. I risultati di questa ricerca sono stati presentati il 5 agosto scorso al Black Hat Usa e verranno illustrati anche alla conferenza ACM AsiaCCS Conference a Taipei nel mese di ottobre.

Il report completo è disponibile su: https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/unveiling-the-hidden-risks-of-industrial-automation-programming ■

1 https://rosindustrial.org/news/2020/6/23/how-to-securely-control-your-robot-with-ros-industrial
2 https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-20-217-01

I gateway industriali mettono a rischio gli ambienti industriali 4.0

Una nuova classe di vulnerabilità nei gateway industriali è stata messa in evidenza da un'interessante studio di Trend Micro. *"Lost in Translation: When Industrial Protocol Translation Goes Wrong"*, questo il titolo della ricerca che annovera, tra gli autori, l'italiano Marco Balduzzi.

Conosciuti anche come traduttori di protocolli, i gateway industriali permettono ai macchinari, ai sensori e ai computer che operano nelle fabbriche di comunicare tra di loro e con i sistemi IT, sempre più connessi a questi ambienti.

"I gateway industriali danno poco nell'occhio, ma hanno un'importanza significativa per gli ambienti Industry 4.0 e potrebbero essere identificati dai cyber criminali come un punto debole dell'infrastruttura" commenta Bill Malik, *vice president of infrastructure strategy* di Trend Micro.

La multinazionale giapponese non è nuova a questo tipo di "imprese". Sono una decina le vulnerabilità zero-day scoperte in questo settore. Non a caso Trend Micro è considerata un'azienda leader nel campo della sicurezza degli ambienti OT. Sono cinque i gateway industriali analizzati dalla ricerca, focalizzati sulla traduzione di Modbus, che è uno dei protocolli per sistemi di controllo industriale (ICS) maggiormente utilizzati al mondo.

Come far fronte alle principali vulnerabilità

Più in particolare le vulnerabilità e le debolezze identificate in questi dispositivi includono:

- Vulnerabilità nelle autenticazioni che permettono accessi non autorizzati;
- Crittografia debole che permette di avere accesso alle configurazioni dei dispositivi;
- Deboli meccanismi di confidenzialità dei dati che danno accesso a informazioni sensibili;
- Condizioni di denial of service;
- Difetti nelle funzioni di traduzione che possono essere utilizzati per operazioni di sabotaggio.

"Gli attacchi che sfruttano queste problematiche potrebbero permettere di ottenere dati sensibili, sabotare o manipolare importanti processi industriali, attraverso messaggi di attacco che vengono appositamente camuffati in modo da apparire come legittimi, e quindi più difficilmente identificabili dai tradizionali sistemi di detection" spiega Marco Balduzzi, Senior Research Scientist di Trend Micro Research.

Cosa fare? Sintetico *vademecum* per gli addetti ai lavori

La ricerca fornisce anche una serie di importanti raccomandazioni per venditori, installatori e gli utilizzatori dei gateway industriali industriali:

- Considerare con attenzione il design del prodotto e assicurarsi che abbia adeguate funzionalità di sicurezza, in modo che i dispositivi non siano soggetti a errori di traduzione o denial of service
- Non fare affidamento su un unico punto di controllo per la sicurezza della rete. Combinare firewall ICS con il monitoraggio del traffico
- Dedicare tempo a configurare e proteggere i gateway, utilizzando credenziali forti, togliendo i servizi non necessari e abilitando la crittografia dove supportata
- Applicare la gestione della security ai gateway industriali e a tutti gli asset OT critici. Per esempio, svolgere valutazioni sulle errate configurazioni o vulnerabilità e provvedere a un patching regolare

I risultati di questa ricerca sono stati presentati il 5 agosto in occasione del Black Hat.

Per chi vuole saperne di più informazioni sono disponibili su: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/lost-in-translation-when-industrial-protocol-translation-goes-wrong ■

Perché il crimine informatico rimane un fattore di preoccupazione per le aziende in un mondo fiaccato dal lockdown

In questo momento in cui le aziende italiane combattono per affrontare gli effetti causati dalla pandemia del COVID-19, è imperativo non dimenticare l'altra minaccia che può provocare effetti dirompenti e massicce perdite finanziarie: il crimine informatico.

Mentre le aziende lavoravano per consentire al personale di operare in smart working e riprogettavano i processi aziendali, i criminali informatici hanno intensificato i loro attacchi dando vita ad armi e strategie di attacco sempre

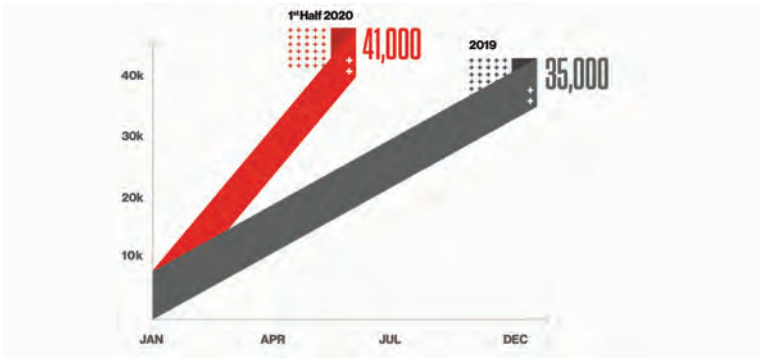
più mirate e sofisticate in grado di sfruttare l'aumentata esposizione alle minacce a cui la forza lavoro remota poteva essere sottoposta. I crimini informatici vengono perpetrati essenzialmente da due categorie di attaccanti: i cybercriminali e gruppi di hacking sponsorizzati da nazioni ostili.

I cybercriminali perseguono perlopiù il profitto economico, mentre i criminali sponsorizzati da nazioni ostili agiscono per impadronirsi di proprietà intellettuali di settori specifici, come le telecomunicazioni, la finanza e la sanità, adottando solitamente un approccio mirato a lungo termine.

Di tutte le attività informatiche malevole registrate nel paese, è il cybercrimine quello che ha avuto l'incremento più rapido dalla comparsa del coronavirus all'inizio di quest'anno, tanto che il team Threat Intelligence di CrowdStrike ha rilevato un'impennata del 330% del cybercrimine rispetto al 2019.

Adottare la "regola 1-10-60"

Per difendersi da avversari e armi sofisticate è necessario disporre di processi strutturati in grado di prevenire, rilevare e rispondere alle minacce in modo rapido e agile. Per combattere in modo efficace minacce sempre più complesse,

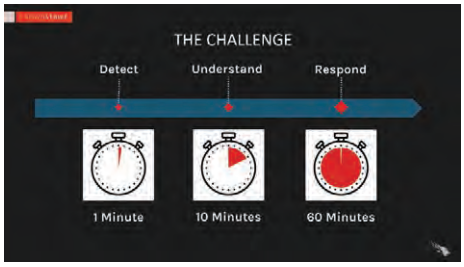


CrowdStrike sollecita le aziende ad adottare la "regola 1-10-60":

- Rilevare le intrusioni entro 1 minuto.
- Analizzare e identificare le minacce entro 10 minuti.
- Contenere e neutralizzare un attacco nel giro di 60 minuti.

Le aziende che riescono a rispettare la "regola 1-10-60" hanno molte più probabilità di espellere l'aggressore prima che l'attacco si diffonda oltre il punto di ingresso iniziale e di contenere l'impatto e la portata dell'intrusione. Per far fronte a questa sfida è necessario investire in strumenti che assicurino visibilità approfondita e funzionalità di analisi e *remediation* automatiche per l'intero ambiente aziendale, grazie i quali i responsabili della sicurezza possano interpretare le minacce e reagire in modo rapido e decisivo eliminando ogni complessità.

In definitiva, per ogni azienda è fondamentale considerare l'efficacia delle



proprie misure protettive attuali che tenga conto di una forza lavoro distribuita geograficamente e mettere in atto ulteriori misure per rafforzare le difese. Passeranno dei mesi prima che l'Europa torni a una situazione vagamente normale, ma la minaccia del crimine informatico non svanirà. Agire ora per capire come stanno evolvendo le minacce informatiche significa mettersi in una posizione di vantaggio per prevenire gli attacchi. ■

Lo sviluppo dell'IA impone nuove strategie di cybersecurity

Autore: Fabio Sammartino,
Head of Pre-Sales di Kaspersky Lab Italia

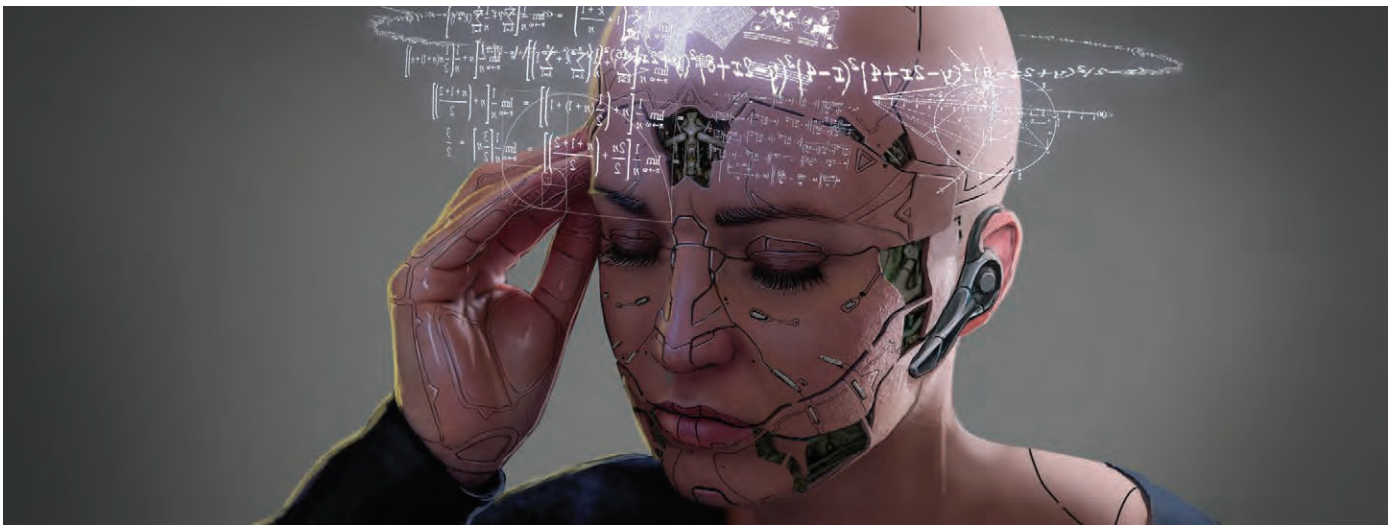
L'importante diffusione recente dell'IA ha reso "popolare", uno strumento fino a ieri conosciuto solo nella letteratura fantascientifica. Le applicazioni aziendali, sono in particolare, quelle che vanno osservate con maggiore interesse. Il motivo può essere imputato a diversi fattori. Innanzitutto esistono, come mai prima d'ora, molti più dati per il "training" degli algoritmi di IA, in secondo luogo la disponibilità di hardware di elaborazione più potente permette prestazioni più elevate, e infine le soluzioni di IA basate sul cloud hanno reso la tecnologia più accessibile e conveniente per le aziende di tutte le dimensioni. L'insieme di questi fattori hanno portato alla conoscenza dei più questo potente strumento, che di fatto ha trasformato le dinamiche del business, oltre che l'esperienza dei clienti. In questo intervento ci soffermeremo in maniera più diretta sul Machine Learning, tecnologia giustamente annoverata tra i principali disruptor nel business. Oggi alla base di molte applicazioni basate sull'Intelligenza Artificiale, il *machine learning* permette di insegnare ai computer a riconoscere i pattern all'interno di una grande serie di dati.

Grazie alla sua applicazione le organizzazioni aziendali sono in grado di prendere decisioni "intelligenti" e più "consapevoli, riuscendo nel contempo a migliorare il loro livello di protezione dagli attacchi informatici, attraverso l'adozione di misure sofisticate, quali la *threat modeling* e *l'intelligence*. Un sottoinsieme del *machine learning* si può considerare il *Deep learning*. Dal punto di vista strettamente computazionale siamo di fronte a un "sistema intensivo", perché utilizza reti neurali artificiali avanzate che permettono ai computer di imparare dai propri errori e migliorare continuamente le proprie funzionalità, silurando comportamenti che sono tipici del cervello umano. Profonde e importanti appaiono le implicazioni sul fronte dell'automazione aziendale, in quanto questa metodologia permette di ridurre l'errore umano in aree critiche come la sicurezza informatica.

Giova poi ricordare, per capire il grado di complessità cui si è ormai arrivati che esistono diverse tipologie di IA: un primo livello limitato (ANI, *Artificial Narrow Intelligence*), generale (AGI, *Artificial General Intelligence*) e super (ASI, *Artificial Super Intelligence*). Interagiamo già quotidianamente con l'ANI, rispetto a cui abbiamo ormai maturato una certa dimestichezza, il secondo livello rappresentato dall'AGI si caratterizza a stessa capacità degli esseri umani ed è in grado di risolvere compiti che vanno al di là di ciò per cui è stata originariamente programmata. Si tratta di un campo che seppur emergente è stato già "superato" dal livello più alto dell'IA, l'ASI che supera

BIO

Fabio Sammartino, appassionato di innovazione tecnologica ha sviluppato negli anni una forte esperienza nel settore della vendita di software di sicurezza oltre ad un'eccellente capacità di supporto tecnico e diagnosi attraverso una metodologia sistematica di analisi dei problemi tecnici. Da settembre 2017, in qualità di Head of Pre-Sales per Kaspersky Lab Italia, è responsabile del team italiano che si occupa di gestire tutte le operazioni di prevendita e le attività di training per partner e clienti. Da gennaio 2013 ad agosto 2017 ha ricoperto il ruolo di Pre-Sales Manager e Technical Trainer per Kaspersky Lab Italia occupandosi nello specifico di gestire tutte le operazioni di prevendita e le attività di training per partner e clienti tra cui dimostrazioni, presentazioni ai clienti, realizzazione di proof-of-concept, report e analisi delle infrastrutture dei clienti. Dal 2009 al 2013, sempre in Kaspersky Lab, ha ricoperto il ruolo di Technical Trainer & Pre-sales Engineer, occupandosi delle attività di supporto post-vendita, analisi dei prodotti e formazione manageriale.



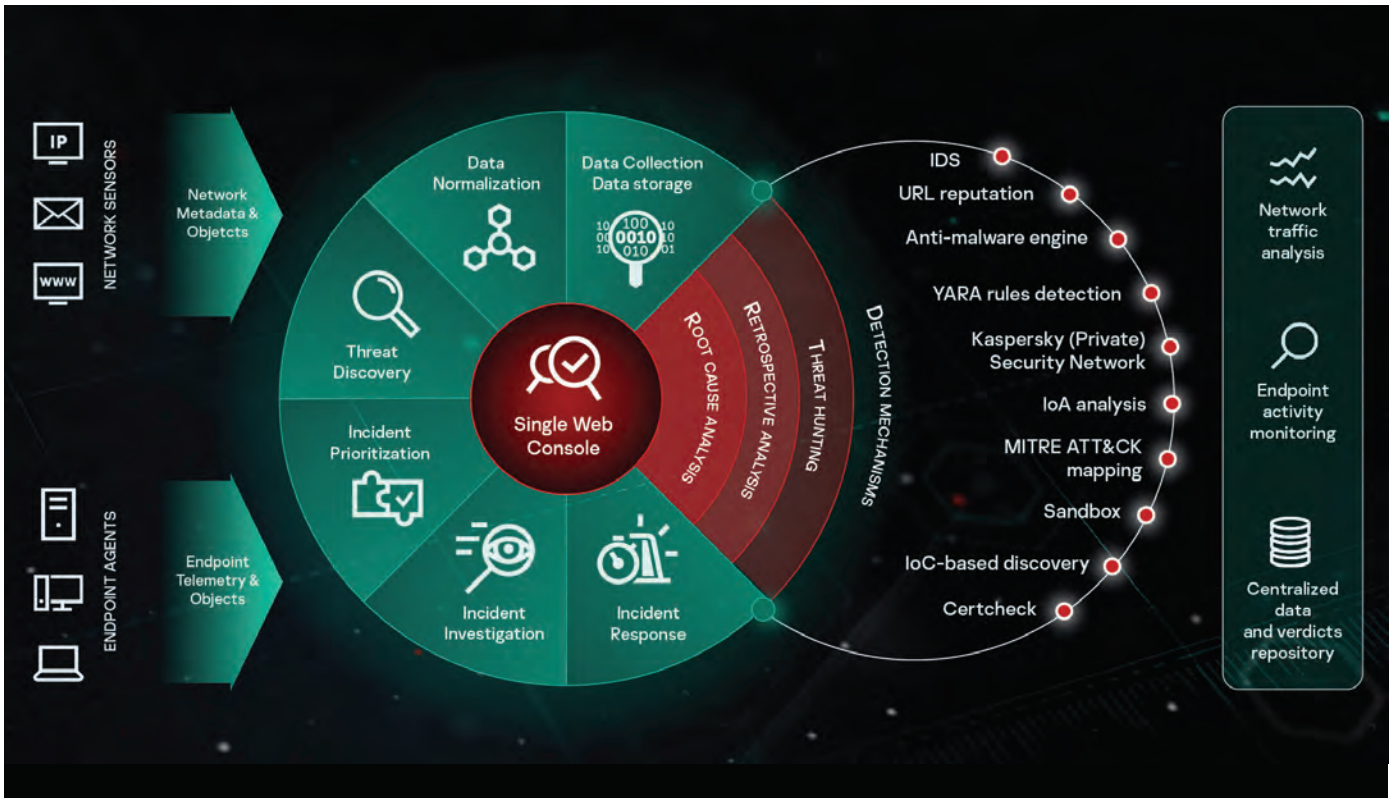
le possibilità degli esseri umani in stile Terminator o Matrix. Siamo su un terreno ancora sperimentale, che richiederà ancora molta ricerca e attività di testing prima di approdare sul mercato.

Il contraltare all'eccezionale progresso dell'IA, colta nelle diverse sfaccettature, che abbiamo provato ad accennare fin qui, va individuato nella crescita del fenomeno di quella criminalità informatica, che ha imparato in fretta a padroneggiare le nuove tecnologie, piegandole ai propri scopi. Appare infatti superfluo ricordare come L'IA non venga utilizzata esclusivamente per fare del bene. Un report di Forrester "Using AI for Evil, 2018" lo sottolinea molto bene: *"Ignorare i rischi legati ai possibili impieghi dell'intelligenza artificiale può determinare una serie di fallimenti, dettato dallo sfruttamento sbagliato delle reti e delle infrastrutture future. È arrivato il momento di prepararsi e comprendere la natura di questo tipologia di minacce".*

Un esempio può far comprendere molto bene la portata del fenomeno. Così come nelle varie divisioni marketing delle aziende si utilizza l'intelligenza artificiale per un targeting di precisione su larga scala, lo stesso vale per i truffatori che sfruttano tecniche di *social engineering*. L'uso improprio dell'intelligenza artificiale include anche la creazione e il *targeting* di campagne di disinformazione e di "contraffazione" degli individui attraverso l'uso del *deepfake*. Gli insight basati sull'IA possono, come si è visto in molti casi, aiutare a sviluppare *malware* pericolosi o mostrare insight importanti su sistemi vulnerabili.

Il *Machine Learning* può sconfiggere la criminalità informatica

Oggi, sia le enterprise che le organizzazioni di medie dimensioni hanno bisogno di strumenti avanzati per ridurre al minimo il rischio di attacchi complessi e avanzati. Secondo l'indagine condotta da Kaspersky IT Security Risks[1], circa il 40% delle aziende di medie dimensioni e delle enterprise non è dotata di intelligence e insight sufficienti sulle minacce affrontate dalla propria organizzazione[2]. Questo dipende principalmente dalle risorse limitate di cui dispongono per affrontare minacce



complesse. *"La tecnologia e la sicurezza informatica si stanno evolvendo rapidamente e questo, significa per le aziende, dover affrontare un numero maggiore di sfide, senza risorse aggiuntive. Dotarsi di soluzioni avanzate di rilevamento e di risposta automatica diventa di importanza vitale per le organizzazioni"* spiega ***Morten Lehn, General Manager Italy di Kaspersky***. *"Per raggiungere questo obiettivo il fattore tempo e la qualità del capitale umano sono aspetti fondamentali. Kaspersky è impegnata su questo delicato terreno, il suo sforzo in tecnologia e presidio del know-how è infatti finalizzato a fornire soluzioni avanzate per effettuare indagini approfondite delle vulnerabilità, per attuare un'azione di controllo e di ripristino delle attività, messe a rischio da incidenti informativi sempre più gravi e diffusi".*

Per analizzare una quantità sempre crescente di incidenti occorre mettere in campo un maggior numero di dipendenti tra cui analisti di sicurezza specializzati, threat hunter e incident responder. Per rispondere a questa esigenza, è stata testata e adottata la soluzione *Endpoint Detection and Response* (EDR), che sfrutta tecnologie di Machine Learning. Automatizzare l'identificazione e la risposta alle minacce, senza interruzioni per l'attività, migliorando la visibilità degli endpoint tramite tecnologie avanzate, come ML (Machine Learning), Sandbox, IoC scan e Threat Intelligence sono le caratteristiche essenziali di questo dispositivo, che costituisce un supporto importante per i Security Team e i SOC, impegnati nella difesa dai cyber-attacchi. Altro aspetto importante, che cerchiamo con il nostro impegno e la nostra ricerca di garantire è la capacità di sviluppare una visione d'insieme sugli incidenti di sicurezza e sulla capacità dell'azienda di reagire agli attacchi, senza però sovraccaricare ulteriormente il proprio team e le proprie risorse. Le soluzioni che Kaspersky propone nelle varie articolazioni danno la possibilità alle organizzazioni di avere una visibilità immediata delle minacce e di collocarle nello scenario completo costituito da tutte le attività potenzialmente pericolose per le persone e dannose per il business. Elaborare in dettaglio la tipologia degli alert, focalizzando il percorso di diffusione degli attacchi è la strada maestra di una strategia che deve evolversi in coerenza con lo sviluppo prepotente degli strumenti high tech.

Infine sul delicato fronte della *threat remediation*, si sta rilevando come siano di importanza capitale la tempestività delle azioni di risposta e l'isolamento di un endpoint nel quale è stato rilevato un potenziale malware o di un file sospetto. Per limitare il più possibile la diffusione degli attacchi informatici ad altri strumenti, gli specialisti di sicurezza possono creare indicatori di compromissione (IoC ovvero artefatti che indicano la violazione di un sistema) con diversi clic e quindi pianificare una scansione automatica degli endpoint volti a neutralizzare l'agente potenzialmente pericoloso. Tutte le funzioni, che abbiamo sinteticamente riassunto, presentano il vantaggio di consentire una gestione centralizzata degli incidenti di sicurezza e quindi all'organizzazione di reagire rapidamente alle minacce critiche, prevenendole. Solo un'efficace strategia di prevenzione rende possibile la riduzione del potenziale impatto negativo che gli attacchi informatici esercitano sulle attività di business. ■

1 L'indagineKaspersky Global Corporate IT Security RisksSurvey (ITSRS) è un sondaggio condotto nel 2019 a livello globale tra idecision makerITaziendali. In totale sono state condotte 4.958 interviste in 23 Paesi.
2 Il 39% delle imprese con 250 - 999 dipendenti e il 40% delle imprese con più di 1000 dipendenti.

ITALIANO ENGLISH

CyberSecQuiz
BROWSE SAFELY?

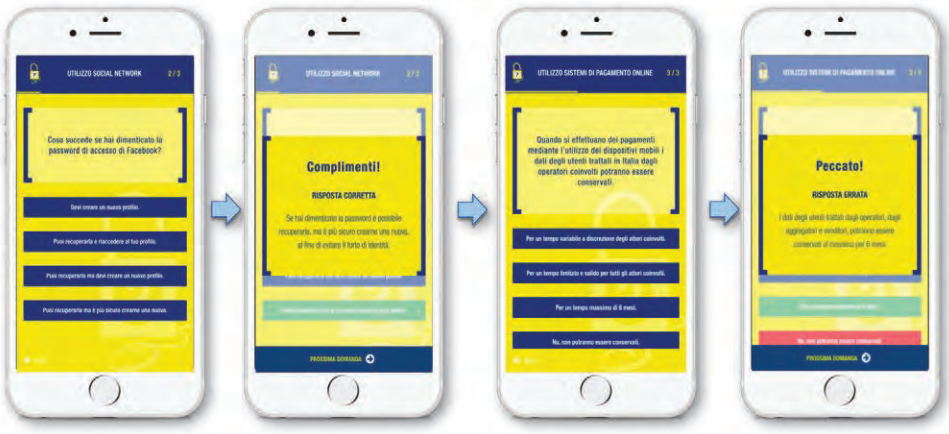
VALUTA SUBITO IL TUO LIVELLO DI CONOSCENZA SULLA SICUREZZA INFORMATICA SU INTERNET

INIZIA IL TEST

CyberSecQuiz

CyberSecQuiz è la piattaforma di Poste Italiane che testa il livello di conoscenza sulla sicurezza informatica e consente di aumentare e "alimentare" regolarmente la consapevolezza della sicurezza delle informazioni su internet attraverso dei test.
La piattaforma è stata ideata come uno strumento ludico che presenta all'utente un test quiz a risposta multipla, di difficoltà variabile, riguardante operazioni comunemente effettuate online, raggruppate nelle seguenti categorie: Internet, Posta Elettronica, Sistemi di Pagamento Online, Social Network e Smartphone.
CyberSecQuiz può essere utilizzato da qualunque dispositivo (mobile o fisso) ed è dedicato a studenti, lavoratori, aziende, associazioni e Istituzioni. Il quiz è composto da domande a risposta multipla selezionate in ordine casuale. Ogni domanda presenta 4 risposte di cui due sbagliate, una corretta ed una perfetta.

Un algoritmo intelligente assegna le domande in funzione delle risposte dell'utente, in base a tre livelli di difficoltà basso, intermedio e alto. Il grado di difficoltà delle domande varia in base alle risposte; aumenta se l'utente risponde perfettamente, rimane uguale se risponde correttamente, diminuisce in caso di errore.
Alla fine del quiz, l'utente viene inserito in un ranking generale in cui può comprendere il proprio livello di conoscenza sia comparandolo agli altri, sia comparandolo al quiz effettuato precedentemente.
L'utente può accedere a CyberSecQuiz in maniera del tutto anonima, oppure tramite login (Email e Password), o, in alternativa, compilando il form di registrazione per ottenere delle credenziali di accesso.
Cimentati con CyberSecQuiz di Poste Italiane per valutare quanto navighi sicuro perché la sicurezza online inizia dalla consapevolezza dei rischi!



Quanto ne sai di Sicurezza Informatica?
Fai un test su www.distrettocybersecurity.it/cybersecquiz/

IA e sicurezza: le fonti dati per gli incidenti operativi

Autore: Giancarlo Butti

L'IA può dare un rilevante supporto nella prevenzione e nella gestione degli incidenti di sicurezza, ma le aziende nella visione degli eventi che possono avere impatti sul business e sugli asset aziendali (o di terzi), devono estendere la loro visione, individuando correttamente le fonti informative utili a tale attività.

Come ampiamente presentato negli altri articoli presenti su questo numero della rivista, con il termine Intelligenza artificiale[1] si intendono un insieme di tecnologie quali cognitive computing, machine learning, deep learning, natural language processing (NLP), riconoscimento delle forme…, che negli ultimi anni sono in costante e rapida evoluzione anche grazie alla disponibilità di risorse elaborative sempre più potenti ed economiche e alla disponibilità di un rilevante quantità di informazioni fruibili con facilità, in particolare on line.

Dal punto di vista della sicurezza le implicazioni della IA possono essere affrontate almeno secondo tre direttrici:

a) l'uso dell'IA quale strumento di ausilio nel contrasto degli attacchi cyber, o più in generale quale strumento per attività di intelligenze e difesa; in questo caso le capacità di effettuare analisi automatizzata di grandissime quantità di dati e parimenti le capacità predittive di questa tecnologia vengono utilizzate per aumentare le possibilità di contrastare minacce in continua evoluzione e ormai impossibili da ostacolare con tecniche di analisi tradizionali

b) l'uso dell'IA quale strumento di ausilio nel condurre attacchi. L'IA può essere infatti essere utilizzata per automatizzare:

- le attività coinvolte nell'esecuzione degli attacchi informatici (spam "intelligente", analisi automatizzata di vulnerabilità di sistemi, siti web…)
- l'uso di droni o altri dispositivi per attacchi fisici
- la creazione di fake news di varia natura
- …

c) le vulnerabilità in ambito sicurezza intrinseche nei sistemi di IA:

- legate al software, analogamente a qualunque altra applicazione
- legate agli algoritmi
- legate ai dati utilizzati per l'addestramento delle applicazioni di IA ed alla possibilità della loro manipolazione al fine di pilotare i risultati elaborati dagli algoritmi
- …

Le applicazioni per la sicurezza

Limitandoci ad una breve e non esaustiva carrellata dell'utilizzo dell'IA quale ausilio alla sicurezza troviamo numerosi ambiti applicativi; ad esempio:

- relativamente alla cybersecurity soluzione basate sull'IA trovano applicazione per:
  - la detection
  - l'analisi
  - la predisposizione di difese contro cyber attacchi
  - …
- nell'ambito delle analisi dei dati nelle attività di intelligence le applicazioni di IA sono utilizzate per:
  - l'analisi semantica profonda del testo al fine di comprenderne significato e tono

- la ricerca di correlazioni fra informazioni provenienti da diversi fonti e da diversi media
- l'individuazione dei soggetti influenti, ad esempio nei social network
- l'individuazione della rete di collegamenti di un soggetto
- l'individuazione degli spostamenti di un soggetto
- l'individuazione di suoni impulsivi in file audio
- l'individuazione di oggetti pericolosi in immagini e video

al fine, ad esempio di potere individuare, segnali di possibili azioni criminali e terroristiche, i loro potenziali obiettivi, i relativi autori.

In tale ambito nel passato sono state proposte anche diverse soluzioni per:

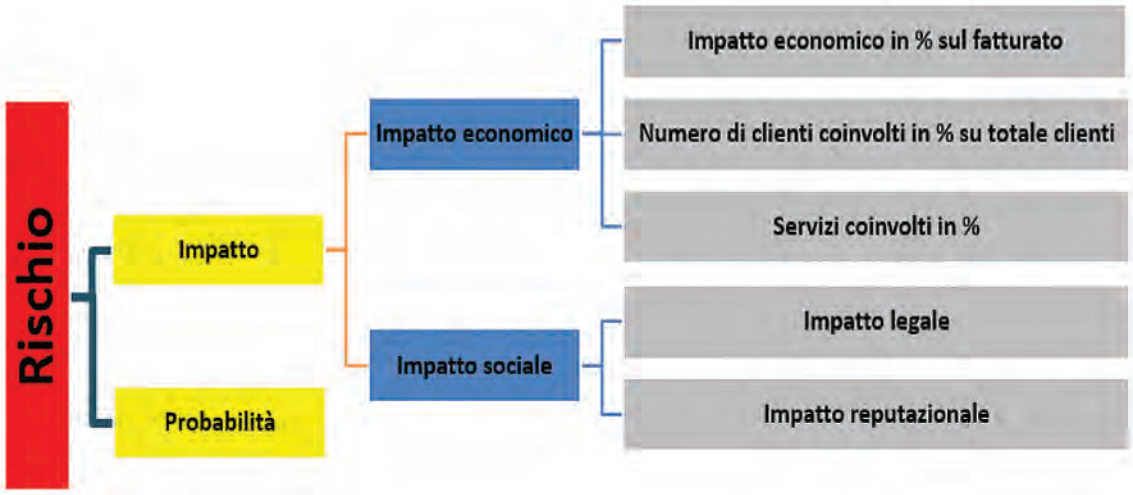
- la prevenzione di azioni terroristiche
- la classificazione di eventi legati al terrorismo
- l'analisi del testo presente nelle pagine web, nei messaggi di posta elettronica, nei messaggi online.

In tale contesto l'attività di intelligence si basa su diverse tipologie di dati, fra le quali:

- fonti dati aperte
  - web site e blog
  - social network
  - forum, chat
- fonti dati parzialmente accessibili
  - deep web
  - dark nets
  - eventuali altri
- data base proprietari
  - database storico cyber attacchi
  - database storico attacchi terroristici
  - database su vulnerabilità, minacce di sicurezza informatica
  - ecc.
- altre fonti dati[2]
  - messaggi di posta elettronica
  - sistemi di messaggistica istantanea
  - sms, mms
  - messaggi vocali
  - telecamere e webcam
  - IOT
  - …
- L'analisi dei rischi[3] in ambito aziendale, come descritto nella pubblicazione **Intelligenza artificiale e soft computing** (L. Schiavina, G.Butti, FrancoAngeli 2017):

BIO

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, whitepaper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security,
Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR…
È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/ IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.



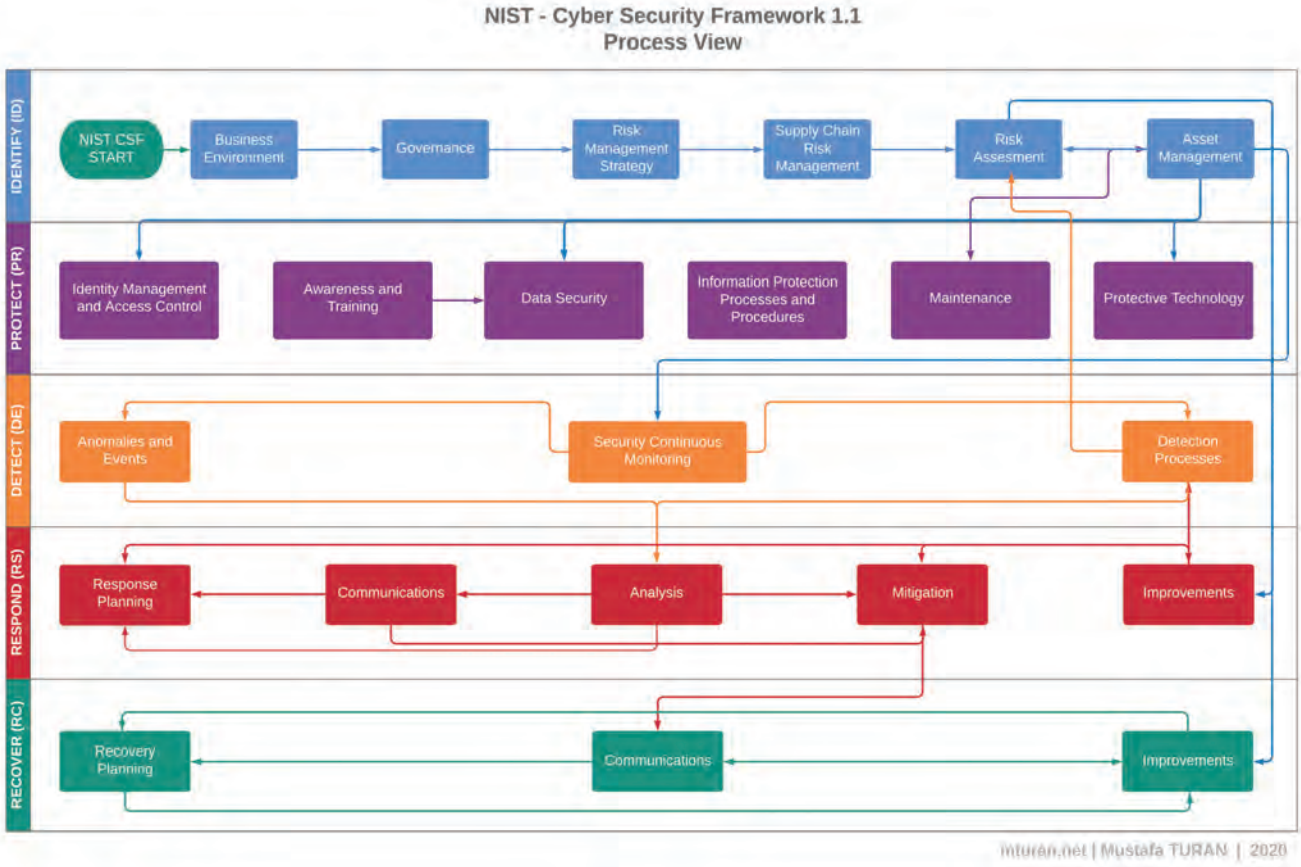
Gli ambiti applicativi della IA nella sicurezza sono quindi veramente molteplici e coprono aree fra loro molto diverse, accomunate dal fatto che l'obiettivo finale è quello di prevenire o ridurre l'impatto che eventi dannosi possono avere sul business aziendale e/o il danneggiamento diretto o indiretto degli asset aziendali o di terzi (ad esempio i diritti e le libertà fondamentali delle persone fisiche).

Ciò che accomuna questi ambiti è comunque la presenza di:

- un'applicazione di IA il cui compito è elaborare le informazioni raccolte
- le informazioni che costituiscono l'input per l'elaborazione.

Gli incidenti e le informazioni

Gli impatti negativi citati nel paragrafo precedente derivano dal verificarsi di un evento dannoso (un incidente), che nella letteratura del rischio per le informazioni (o più in generale della gestione del rischio) trova una elencazione dei possibili casi all'interno di diversi cataloghi facilmente reperibile on line, quali ad esempio:



- IT-Grundschutz catalogues (BSI)
- Threat taxonomy (ENISA)
- NIST.

Un incidente è di fatto quell'evento che le misure di sicurezza e le azioni di prevenzione, comprese quelle di intelligence, dovrebbero anticipare o quantomeno aiutare nel limitarne gli effetti negativi.

Per comprendere cosa sia un incidente può essere di aiuto, come in precedenti articoli, la definizione che dello stesso danno alcune normative del mondo finanziario.

Ad esempio Banca d'Italia riporta nella Circolare 285 la seguente definizione:

"incidente di sicurezza informatica": ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi);

EBA, in modo più estensivo e corretto, nel suo documento Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2), riporta invece la seguente definizione:

Incidente operativo o di sicurezza

Singolo evento o serie di eventi collegati non pianificati dal prestatore di servizi di pagamento che ha o probabilmente avrà un impatto negativo su integrità, disponibilità, riservatezza, autenticità e/o continuità dei servizi connessi ai pagamenti.

Come si noterà, mentre la normativa di Banca d'Italia limita la propria definizione ed attenzione agli incidenti di sicurezza veri e propri ed alle informazioni quali asset interessati dall'evento, più correttamente EBA estende il concetto di incidente sia ad altri ambiti, sia ad altre circostanze.

Se infatti gli obiettivi di chi effettua un'attività di prevenzione e contrasto degli incidenti è quella di limitare i potenziali impatti su un'organizzazione, i suoi dati, i suoi servizi, i soggetti di cui tratta i dati, non dovrebbe essere così importante distinguere, per garantire la corretta operatività dell'organizzazione, se un "incidente" derivi da un attacco informatico, dalla rottura di un disco o dal malfunzionamento di un applicativo, o ancora da un allagamento o da una pandemia.

Il risultato per l'organizzazione infatti potrebbe essere il medesimo; ad esempio il non poter continuare ad operare per un certo periodo o l'impossibilità di accedere ai dati…

Di fatto la normativa di EBA considera che la conseguenza di un incidente, sia questo operativo o di sicurezza abbia un impatto negativo su:

- integrità
- disponibilità
- riservatezza
- autenticità
- continuità,

parametri tipici della sicurezza, quasi ad enfatizzare che non è l'origine dell'incidente che è importante, ma quali sono le sue conseguenze.

La visione di EBA è quindi particolarmente interessante: conseguenze sulla sicurezza possono derivare anche dai così detti incidenti operativi.

Purtroppo però le aziende nella maggior parte dei casi concentrano la propria attività di prevenzione degli incidenti sugli aspetti strettamente connessi alla sicurezza, quali la presenza di nuove vulnerabilità, anomalie nel funzionamento nella rete, tentativi di accesso…, dimenticando che anche un semplice malfunzionamento applicativo può portare allo stesso disservizio di un attacco informatico.

Questa visione si riflette anche nella organizzazione interna delle aziende: sono di norma diverse le strutture che si occupano delle due tipologie di eventi e manca un'unica regia ed una condivisione delle informazioni fra i vari attori coinvolti.

Chi si occupa prettamente di sicurezza è concentrato sulle proprie fonti informative e sulla prevenzione di una sola tipologia di incidente, mentre le varie strutture aziendali dovrebbero operare con un unico obiettivo, indipendentemente dalla tipologia di incidente occorso, coordinandosi, là dove esista, con la struttura che coordina la continuità operativa.

Le fonti informative per gli incidenti operativi [4]

Diamo per scontato che le aziende nella predisposizione degli incidenti di sicurezza propriamente detti abbiamo adeguatamente censito le loro fonti informative.

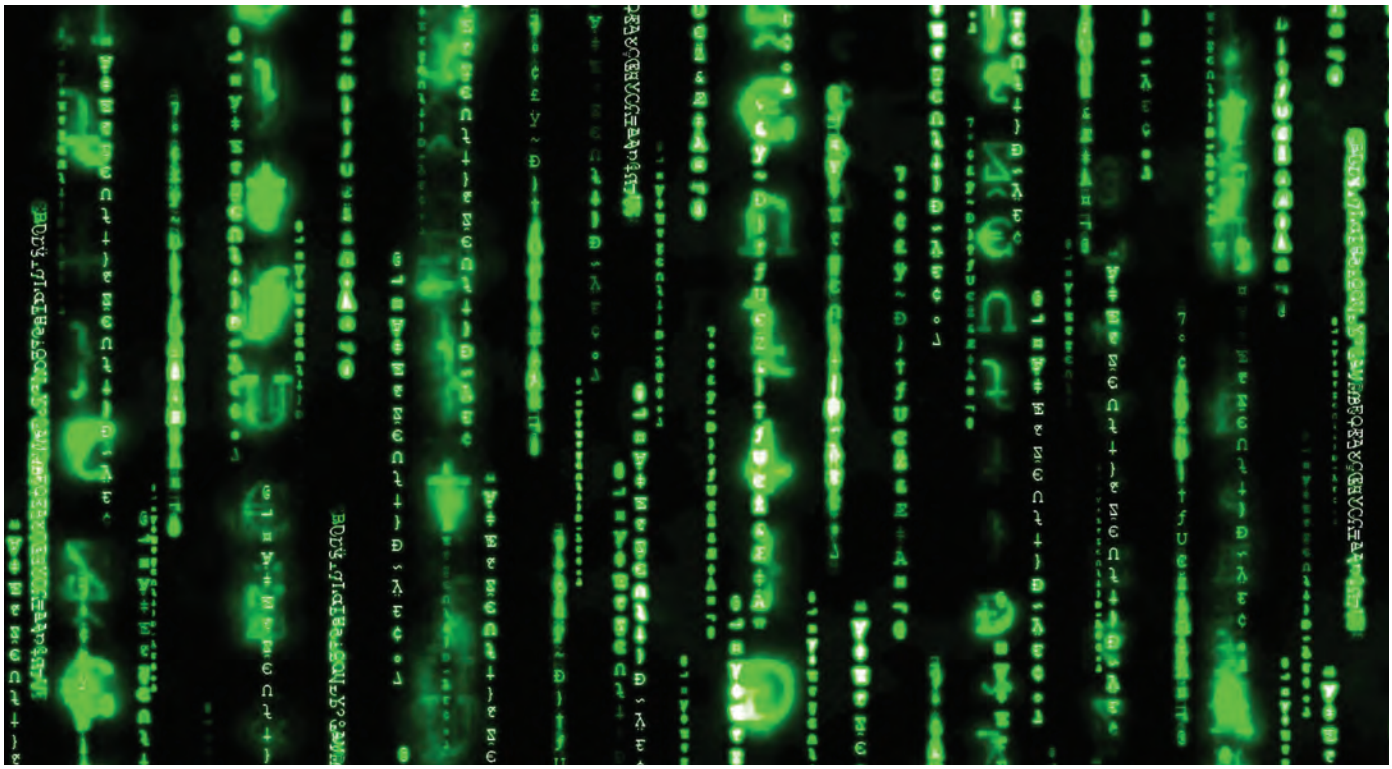
Tuttavia le organizzazioni dispongono anche di molteplici fonti dati dalle quale possono ricavare informazioni utili a valutare la probabilità che accada un incidente operativo e a monitorare i relativi eventi.

Il problema è che tali informazioni sono solitamente ignorate, non raccolte e non classificate.

È quindi opportuno identificare tali fonti ed iniziare a raccogliere e collezionare tali informazioni.

Fra queste troviamo:

- quelle certamente riconducibili direttamente al sistema informativo, quali ad esempio:
  - la segnalazione di anomalie e malfunzionamenti da parte di utenti sia interni che esterni
  - le richieste di interventi da parte degli utenti per risolvere tali situazioni (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdita ed alterazione di dati, rotture hw…)



- quelle che possono in qualche modo derivare da problemi legati al sistema informativo, quali ad esempio:
  - reclami, in particolare dei clienti (ad esempio ritardi nelle consegne, errate evasione di un ordine…)
  - reclami dei fornitori (ad esempio ritardi nei pagamenti).

Per poter fornire informazioni utili tali eventi vanno adeguatamente censiti in appositi database.

Per le segnalazioni direttamente riconducibili al sistema informativo le aziende più grandi dispongono di processi formalizzati e di apposite procedure per la gestione dei ticket di assistenza.

Tuttavia spesso il livello di dettaglio con cui sono segnalati i problemi o meglio ancora il livello di dettaglio con cui viene censita l'identificazione della causa e la descrizione della soluzione non è sufficiente.

Si perde in questo modo la possibilità di effettuare un'analisi a posteriori di quali siano le aree del sistema informativo più esposte, piuttosto che le applicazioni più carenti.

Spesso chi analizza e risolve il problema è concentrato unicamente a fornire supporto nei tempi più rapidi possibili e non dedica adeguato tempo per procedere alla fase, altrettanto importante, di corretta classificazione delle cause.

Tale mancanza è determinata in larga parte dalla scarsa formazione del personale e dalla scarsa sensibilità del management aziendale che privilegia la soluzione immediata e "tattica" di problemi, piuttosto che affrontarne alla radice le possibili cause.

Anche nel caso della gestione dei reclami provenienti dall'esterno, in particolare dai clienti, sono rari i casi in cui vi è una gestione informatizzata del processo di risoluzione.

Solo in aziende come le banche, che hanno specifici obblighi normativi, si procede di solito ad una gestione mediante un processo formalizzato che tiene traccia dell'iter seguito.

Anche in questo caso però è raro trovare un'idonea classificazione dei problemi e delle cause scatenanti, tali da poter determinare un'analisi a posteriori delle aree più a rischio del sistema informativo.

I problemi in questo caso si pongono a diversi livelli; innanzi tutto ricondurre un reclamo esterno ad un malfunzionamento del sistema informativo non è immediato.

È necessario analizzare nel dettaglio il contenuto stesso del reclamo, interagendo da un lato con un cliente "ostile" e dall'altro con un insieme di strutture aziendali che partecipano al processo che non ha correttamente funzionato.

Restando in ambito bancario un reclamo derivante da una errato calcolo della rata di un mutuo può derivare da diverse cause, una delle quali può essere un malfunzionamento dell'applicazione che effettua il conteggio delle rate, o di una qualunque delle applicazioni a monte e a valle della stessa.

Per verificare se si tratta effettivamente di un problema applicativo e non di un malfunzionamento isolato sarebbe necessario disporre di un sufficiente numero di segnalazioni opportunamente classificate; in particolare censite con modalità omogenee.

Le premesse per poter effettuare queste analisi sono comunque:

- una corretta segnalazione da parte dei clienti direttamente al call center o all'ufficio reclami della banca
- una corretta segnalazione da parte della filiale nel caso in cui il cliente si rechi direttamente allo sportello.

Ulteriori fonti dati sono costituiti dai sistemi di monitoraggio; questi possono fornire dati in tempo reale o a scadenze prefissate, con diversi livelli di dettaglio ed aggregazione.

I sistemi di monitoraggio possono ad esempio verificare:

- la raggiungibilità di un sistema
- l'esistenza in vita di un sistema
- il corretto funzionamento di un sito web mediante robot di navigazione automatica che simulano un utente reale
- la misurazione delle prestazioni della LAN
- la misurazione delle prestazioni della WAN
- …

Ulteriori fonti informative sono costituiti da una serie di indicatori, quali ad esempio il numero di righe di codice modificate in un certo periodo, distinguendo fra quelle effettuate per attività di manutenzione risolutiva da quelle effettuate per attività evolutiva.

Nel primo caso gli interventi evidenziano la presenza di situazioni anomale che sono state o sono in fase di risoluzione.

Il secondo caso introduce invece una possibile instabilità futura nei sistemi, a causa delle novità introdotte.

Il livello di obsolescenza di un sistema potrebbero renderlo inefficace rispetto ad una evoluzione delle esigenze introducendo elementi di rischio, quali ad esempio una caduta delle prestazioni in termini di capacità elaborativa, risorse disponibili, tempi di risposta…

Si pensi ad esempio ad elaborazioni batch notturne che si allungano sempre di più e non rendono disponibile il sistema informativo in tempo per l'orario di apertura delle filiali di una banca.

Anche il sistema dei controlli interni (di linea e di secondo livello) e l'audit costituiscono, oltre che strumenti di controllo e di indagine anche una fonte di informazioni per rilevare situazioni anomale, legate direttamente ai sistemi informativi ovvero potenzialmente derivanti da questi.

In realtà le attività di audit dovrebbero essere pianificate sulla base delle analisi delle informazioni precedentemente censite, le quali dovrebbero consentire l'individuazione delle aree del sistema informativo più a rischio, sulle quali è quindi maggiormente utile effettuare indagini.

Gli esempi riportati evidenziano tutti una serie di elementi comuni:

- la necessità di specifiche regole di rilevazione e classificazione (non interpretabili) degli eventi, ad esempio mediante strumenti che prevedano un'adeguata alberatura che guidino nella compilazione coloro che effettuano la segnalazione e successivamente la risoluzione del problema (in questo ambito l'implementazione di adeguati Sistemi esperti potrebbe agevolare non poco la classificazione e risoluzione di problemi)
- una corretta identificazione e classificazione delle cause
- una analisi a posteriori dei dati raccolti, al fine di individuare la presenza di problemi endemici e non legati a fattori casuali, al fine di individuare le aree di rischio e predisporre opportuni interventi sia di controllo, sia correttivi; si evidenzia che tale attività può essere notevolmente agevolata da applicazioni di IA
- la necessità di adeguata formazione e sensibilizzazione di tutto il personale su questi temi
- la necessità che il management aziendale dia adeguata importanza alla gestione di questi aspetti, affiancando alle soluzioni tattiche quelle strategiche.

Conclusioni

È opportuno che le aziende (intendendo con tale termine in realtà qualunque tipo di organizzazione) nella prevenzione gestione degli incidenti di sicurezza abbiamo una visione e gestione olistica di tutti quelli che possono essere gli eventi scatenanti.

Al riguardo è auspicabile che definiscano adeguate modalità per la raccolta delle informazioni e delle segnalazioni utili anche alla loro prevenzione mediante adeguate correlazioni. ■

1 Cosa possa essere considerato IA non è univocamente determinato ed accettato; anche questo aspetto è in continua evoluzione.
2 L'accesso a tali dati è diversamente regolamentato.
3 Una sintetica descrizione del modello è disponibile on line negli articoli dell'autore:
- Misurare la physical cyber security http://www.isticom.it/documenti/rivista/rivista2016/6_85-118_misurare_la_sicurezzaiscom.pdf
- Intelligenza artificiale e soft computing nella lotta al terrorismo https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligenza-artificiale-e-soft-computing-nella-lotta-al-terrorismo.html

4 Adattamento dal libro Governance del rischio - Dall'analisi al reporting e la sintesi per la Direzione, di Giancarlo Butti e Alberto Piamonte- ITER 2020.

Luciano Floridi,
"La quarta rivoluzione"
"Pensare l'infosfera"
"Il verde e il blu",
Raffaello Cortina Editore

Una trilogia per una società matura dell'informazione

Autore: Massimiliano Cannata

"Il verde e il blu" (ed. Raffaello Cortina) di Luciano Floridi è un saggio ispirato da una precisa finalità: offrire idee "ingenue" (la precisazione dell'autore ha l'apprezzabile sapore della "dotta ignoranza" socratica) per migliorare la politica, al fine di rivedere i fondamenti della democrazia, nella prospettiva di creare presupposti credibili per la costruzione di una società matura dell'informazione. Per comprendere meglio la trattazione è sicuramente utile prendere in considerazione due scritti precedenti dello stesso autore: *"La quarta rivoluzione"* e *"Pensare l'infosfera"* pubblicati sempre da Raffaello Cortina. Il primo affronta le implicazioni economiche sociali e culturali determinate dal cambio di paradigma dall'analogico al digitale (cfr. CST N. 1 2018). Reale e virtuale, questa la tesi di fondo del libro, sono categorie dell'essere che non è più possibile separare, il mondo in cui viviamo è il risultato della densa contaminazione tra questi due ambiti.

Un "salto" in avanti così netto ha bisogno di una filosofia per essere spiegato. Filosofia, intesa come elaborazione di un pensiero sistematico per comprendere la natura stessa dell'informazione, per prevedere e gestire l'impatto etico dell'ICT su di noi e sul nostro ambiente, per migliorare le dinamiche di sviluppo della *web society* e, non ultimo, per individuare un percorso di senso, nel solco di una globalizzazione contrassegnata da molte contraddizioni. *"Pensare l'infosfera"* è lo scritto che dà forza e dignità alla speculazione "utile", libera dagli inutili orpelli dell'erudizione, capace per questo di tornare a rivestire la funzione di disciplina orientata alla lettura del presente e all'individuazione di soluzioni praticabili dall'umanità. Quando l'esercizio del pensiero segue questi canoni assume i contorni innovativi del *design concettuale*. Su questa visione del mondo e delle cose si innesta l'ultima opera: "Il verde e il blu", attraverso questi colori-concetti si snoda, infatti, un itinerario di trasformazione della società.

Il libro è costruito su una fiducia di fondo: esiste la "politica buona". La prova storica, afferma con nettezza disarmante Floridi sfidando ogni scetticismo di maniera, ci è data dalla nostra Costituzione, testo mirabile per sintesi di visioni, esigenze e posizioni ideologiche diverse. Ma la fiducia non basta. I guasti del presente impongono un cambio di marcia, un rinnovamento autentico dei partiti, e del modo di esercitare la democrazia. "L'errore – spiega l'autore – è quello di pensare di agire dall'interno di un meccanismo che si è rotto. Non si deve migliorare la politica *nella* politica, ma lavorando *per* la politica, obiettivo realizzabile a patto di alzare le aspettative dei cittadini. Non accontentiamoci del menu a prezzo fisso pensando che ci sia un unico ristorante del paese, ma obblighiamo chi sta al potere ad arricchire la propria offerta, con trasparenza, qualità e impegno".

Perché dobbiamo saperci prendere cura del mondo

Il progetto umano che ha in mente Floridi è di vaste proporzioni, per questo dedica un intero capitolo del libro (il diciannovesimo n.d.r.) in cui enuncia ben cento tesi, che rimettono in discussione tutto l'intero vocabolario della scienza e della filosofia della politica: democrazia, stato, pubblica amministrazione, sovranità, ambiente, giustizia, solidarietà, cittadinanza, sono tanti i concetti che finiscono sotto la "lente" dello studioso. Il prerequisito per quella che si presenta come un'opera di trasformazione "ciclopica", soprattutto se affrontata senza i giusti strumenti culturali e professionali, risiede nella capacità/volontà di tornare a elaborare strategie di lungo termine, capacità che sembra da troppo tempo smarrita da parte delle élites. Detto in estrema sintesi: la miopia non può essere ammessa quando c'è da mettere mano ai fondamenti del contratto sociale in tutte le sue articolazioni. L'autore si serve sovente di metafore semplici per far passare messaggi complessi. In questo caso ricorre alla musica: "Occorre dare il la ai nostri governanti – proprio come si fa con un'orchestra – perché cominci a suonare con la giusta armonia. Vuol dire in concreto cominciare sul serio a prendersi cura dell'ambiente sociale, politico, fisico geografico, tecnologico che ci circonda. La mia idea di verde ha un'accezione molto vasta, quando parlo, invece di *blu*, intendo volgere l'attenzione a quegli strumenti della tecnologia che stanno cambiando le nostre vite: Rete, 5G, intelligenza artificiale, piattaforme social, *smartphone* sempre più sofisticati…".

Un buon punto di partenza per voltare pagina risiede nel cambio radicale di prospettiva che dobbiamo adottare. "La festa non è più per noi, il mondo non è a nostra disposizione,

dobbiamo adottare – questa una delle tesi forti del libro - una decentralizzazione dell'io, per ritrovare la dimensione dell'altro". Non si tratta solo di un'impegnativa svolta epistemologica, e come tale di un bel tema magari per un convegno tra filosofi, quanto piuttosto di una cambiamento strutturale che investe il lavoro e il settore produttivo fin dalle fondamenta. La potremmo chiamare "economia dell'esperienza", centrata sui servizi, la qualità di quello che facciamo più che la quantità, qualità che va negoziata in dialogo costante con il cittadino – fruitore – consumatore. È evidente che per allinearsi a queste diverse dinamiche occorrerà modificare gli assetti organizzativi e il modo stesso di fare impresa. "Per me stare nel XXI secolo vuol dire adottare un punto di vista diverso da un passato fondato sullo sfruttamento dell'ecosistema, sull'avidità e sull'ignoranza. Chi non ha capito dove stiamo andando – afferma senza mezzi termini Floridi - non è capace di vivere il presente, né tanto meno può essere adatto a governarlo".

Esperienza e design, saranno dunque i codici di un capitalismo etico, orientato alla soddisfazione dei bisogni, aperto e inclusivo, che non ha nulla a che fare con quello che abbiamo alimentato nel tempo della "modernità industriale" che ha portato, la terra e chi la abita, allo stremo. Due immagini della storia recente possono riassumere la sofferenza di questi difficili anni. La prima: il terribile ritrovamento di Aylan il bambino curdo-siriano rinvenuto su una spiaggia, fotografia terribile di un mondo che ha smarrito il senso di umanità e di una civiltà come quella occidentale che sembra aver smarrito secoli di progresso, negati nel sonno della morte di quel bimbo innocente. La seconda diventata l'icona di una nuova centralità dei giovani, è stata come è noto espressa dalla denuncia di *Greta Thumberg* che ai grandi della terra rivolse il famoso monito: "non vi perdoneremo mai perché ci avete rubato i sogni". Quasi fosse una riedizione dell'*Urlo di Munch* la giovane svedese è riuscita così a dare voce a un dolore profondo e indicibile, espressione di sgomento, terrore, paura, facendo con il suo gesto cadere definitivamente "il velo di maya" della finzione.

La scrittura "figlia" di un pianeta che soffre

Il saggio di Floridi risente della stessa sofferenza. La scrittura è "figlia" di un pianeta ferito nella coscienza, e oggi ancor più sfiancato nel corpo dalla pandemia. La malattia che non ha risparmiato nessun angolo del globo è, infatti, l'ultimo *allarme* che dovrebbe portarci a capire che dobbiamo cambiare strada. "Aziende e istituzioni dovrebbero comprendere che il digitale non è la ciliegina sulla torta ma l'intera torta, così come il verde non è un costo ma un investimento necessario senza il quale sarà impossibile reggere i ritmi di trasformazione della contemporaneità".

Su questo terreno prende corpo il "progetto umano", la proposta che è il cuore pulsante attorno a cui ruota il libro. Per dare effetto concreto all'idea servirà coniugare "individuo e totalità", rispettare i soggetti senza dimenticare la società di cui fanno parte. Una sintesi difficile per stessa ammissione dell'autore ma assolutamente necessaria. Gli "ismi" hanno fatto il loro tempo. L'individualismo che ha dominato la seconda parte del novecento come reazione ai totalitarismi non è più sufficiente. Alla gamba dei diritti individuali va associata la seconda importante gamba dei diritti sociali, che permettono di riscoprire l'altro e la dimensione comunitaria, dopo mesi di difficile isolamento fisico e psicologico. "Se nessuno si salva da solo", come ha ricordato a più riprese Papa Francesco nella Roma "spettrale" della scorsa quaresima, risulterà decisivo ridare linfa a organismi comunitari e sovranazionali che purtroppo non appaiono molto in salute. La crisi dell'Onu e le difficoltà dell'Europa sono indici negativi, che non devono però allentare la forza del progetto, perché senza un alto livello di coordinamento (altra tesi importante del saggio) non usciremo mai dalla depressione in cui siamo caduti. "La politica non ha *logout*" (cfr. tesi 77 pag. 243) non è solo un modo originale escogitato dal filosofo Floridi per affermare un convinto europeismo, perché problemi epocali come giustizia sociale, povertà crescenti, diseguaglianza, diritti delle minoranze, *global warming*, inquinamento atmosferico, regolazione dei flussi migratori non ammettono soluzioni limitate e parziali. La "cinquecento" si è fermata, bisogna spingerla insieme, non basta uno che gira la chiave (altra metafora gustosa…) In quest'ottica anche la sovranità deve essere aperta e interdipendente, in contrapposizione a chi alimenta rigurgiti di un tardo nazionalismo che non può avere prospettiva. "Quando si cominciano a usare parole come popolo, nazione, razza, l'individuo rimane schiacciato, con buona pace dei diritti di libertà costati anni di lotta e di sacrifici". Rendiamoci conto che si è ormai esaurito tutto il quadro mentale che ha dominato il secolo breve, bisogna uscire da una concezione economicistica della politica per comprendere che non esiste solo il contratto sociale, quale pavimento solido su cui abbiamo poggiato la civile convivenza. È venuta l'ora di passare dal "contratto sociale al trust universale". Questo che si configura come un "salto quantico" può aiutarci a percepire il pianeta come un'eredità ricevuta, che va curata e lasciata alle future generazioni in condizioni di salute e di vivibilità alte. La rigida certezza che tutto si risolva in un contratto è legata a una mitologia e a una narrazione che non ha riscontri nella quotidianità Ciascuno di noi nasce in circostanze particolari, è "gettato" nel mondo, (in questo le riflessioni di Floridi ripercorrono alcune posizione che richiamano l'esistenzialismo di Heidegger) deve perciò sentire con responsabilità il sentimento etico del rispetto dell'ecosistema. Su questo si innesta un altro termine importante (cfr. tesi 84 pag. 245) *"il capitale di cittadinanza"*, definizione che nulla ha in comune con il più noto reddito che tante polemiche ha generato alle nostre latitudini. Siamo sempre dentro il perimetro dell'eredità (il trust) che abbiamo ricevuto in dono, nascendo nella parte più ricca del mondo. Non dobbiamo dilapidarla, piuttosto dimostrando talento e intelligenza, dobbiamo cercare di meritare un "prestito d'onore" che lo stato deve assegnare ai giovani, sapendo che potrà recuperare con gli interessi tutto quello che viene speso per promuovere il capitale dell'ingegno. Qui il rovesciamento rispetto al trend corrente, non potrebbe essere più netto. La cittadinanza oltre a configurarsi come diritto fondamentale è un patrimonio da far fruttare, che può tornare utile al fatturato in deficit dell'"azienda Italia".

Quando la speranza supera l'interesse

Relazione è il termine chiave di un vocabolario della politica che per la prima volta deve prendere in esame il rapporto che lega *res publica* e *ratio publica (cfr. tesi 66 e segg. Pag. 240).* Alt dunque alla politica che guarda alla mera gestione delle cose, che pensa solo a occupare spazi di potere. Nell'economia dell'esperienza, dei servizi immateriali e del *design,* è la relazione, la cura dei rapporti sociali, la rete da implementare, in quanto volano di energia e di valori. "Non preoccupiamoci di proteggere solo ed esclusivamente Romeo e Giulietta (questa volta la metafora fa riflettere) nella loro singolare ed esclusiva individualità, impegniamoci a far crescere il loro amore, che è il cemento che li tiene insieme e li fa andare avanti". Siamo di fronte a un vocabolario diverso che in passato, che proietta la politica oltre lo stretto recinto dei partiti. Il dibattito pubblico deve tornare a occuparsi del destino delle classi sociali (torna inaspettatamente la classe, termine sembrava sepolto nell'armamentario ideologico post marxista n.d.r) e della qualità dei rapporti che intercorrono tra gli individui. Fa capolino (cfr. tesi 23, pag. 232) un neologismo *"infraetica", di cui l'autore si serve per disegnare* quelle reti relazionali di fondo che, protette da una buona politica finalmente alleata alle parti sociali e da una PA efficiente, sono il vero catalizzatore dei comportamenti virtuosi.

Perché la "speranza possa diventare più forte dell'interesse" tutti gli attori della sfera pubblica devono essere coinvolti, cominciando dallo stato da molti anni in crisi di fiducia. Il *Leviatano* di Hobbes, è innegabilmente da molti anni in crisi di "sufficienza" (cfr. tesi 88 pag. 247), in quanto l'impatto di problemi globali rende sempre più necessario l'apporto di un apparato pubblico che risulta palesemente insufficiente quando non del tutto inadeguato. Vanno riformati i gangli della macchina pubblica insieme alla struttura della burocrazia, che presiede i meccanismi di funzionamento dello stato. La PA rimane il fulcro di un concreto e finalmente realizzabile progetto di cambiamento radicale, perché la politica buona, (concetto da cui siamo partiti) possa tradursi finalmente in buon governo, generando esternalità positive per le comunità di riferimento.

Lo stato non può (questo è uno dei passaggi delicati della trattazione, anche perché si contrappone in maniera netta alle recenti posizione neo-stataliste sostenute da molti autori non solo nel nostro paese) sostituirsi alla libera intrapresa, non deve in una parola "svuotare" il mercato, ma lavorare per farlo funzionare meglio, in quanto agente relazionale che si muove nel teatro di tra altri agenti relazionali, nell'ottica di una *gradualità della sovranità*. Nella dinamica di una *governance multilivello*, ritroviamo la funzione di una PA rinnovata che, nell'orizzonte della democrazia "partecipativa" e "cosmopolita", non potrà limitarsi a difendere i diritti dei cittadini, perché è parimenti importante rendere facile l'esplicazione dei doveri, per migliorare l'efficienza e la produttività di tutto il sistema-Paese. Solo a queste condizioni, "la politica (cfr. tesi n. 80 pag. 244) potrà tornare con i piedi per terra, ritrovando lo spirito di missione e di servizio, evitando di gestire la *velocità* dei cambiamenti, piuttosto impegnandosi a determinare la bontà della loro *direzione"*. Un aspetto quest'ultimo, che dovrebbero tenere a mente le nostre classi dirigenti, per assumere quelle decisioni rapide, efficaci e coerenti, da cui dipende il destino di intere comunità e in larga parte il nostro stesso futuro. ■

Luca Toselli,
La Didattica a Distanza. Funziona, se sai come farla
Edizioni Sonda

Si può stare bene anche nella scuola «ribaltata» dal *lockdown*

Autore: Luca Toselli

Luca Toselli *è un insegnante impegnato nella didattica a distanza di ogni giorno, ma anche uno studioso e ricercatore dei nuovi media, sin dalle prime esperienze teledidattiche degli anni Novanta. Ha pubblicato Il progettista multimediale (Bollati Boringhieri), Creatività multimediale (Lattes), Didattica dell'Editoria Multimediale. Ipotesi e progetti (Cuem), oltre a numerosi saggi e articoli. Vive tra Torino e Milano. Con questo interessante manuale d'uso (La didattica a distanza: funziona se sai come farla (edizioni Sonda) l'autore apre un fronte interessante di analisi, ma soprattutto di sperimentazione, destinato a diventare il fulcro di un rinnovato metodo pedagogico. "Durante la pandemia da*

covid-19 – si legge nella nota stampa curata dall'editore- la Didattica a Distanza è stata un'imposizione faticosa e difficile da accettare per il mondo della scuola. Grazie a questa guida, potrà diventare un prezioso strumento di potenziamento nel processo di apprendimento, senza sostituirsi del tutto alla relazione umana. Il virtuale è parte integrante delle vite di ragazzi e adulti e la DaD può essere una grande opportunità: stabilisce un patto tra docenti, studenti e genitori, che si regge su regole semplici, ma indispensabili, valide per tutti i mezzi a disposizione: libro, chiamate, chat di gruppo, email e video-lezioni. Toselli viene in soccorso di insegnanti e genitori, raccontando ogni aspetto della DaD, sciogliendone i nodi, e proponendo le migliori pratiche alla luce delle linee pedagogiche più recenti: dal decalogo per la gestione di una buona chat, fino agli strumenti per formulare una buona valutazione con nuovi criteri a distanza, passando per le istruzioni per usare al meglio il canale mail. Il segreto è la ricerca della giusta mediazione tra leggerezza ed efficienza. La DaD può essere una buona occasione per avvicinarsi – seppur lontani – e coltivare il rapporto umano anche attraverso lo schermo. Un'ottima occasione per gli insegnanti di gestire i programmi e progettare in modo funzionale ed empatico; e per i genitori, di capire che è un'ottima opportunità per i figli, per sviluppare nuove forme di comunicazione e partecipazione, obiettivo scolastico numero uno".

Pubblichiamo un estratto della introduzione, particolarmente efficace, che fa comprendere molto bene l'importanza dell'applicazione corretta delle nuove tecnologie all'insegnamento, in un contesto come quello scolastico da cui dipende il futuro del Paese.

"Mi occupo di Didattica a distanza (DaD) da parecchio tempo. Giovane laureato in Lettere, approdo a metà degli anni Novanta in un mondo fatto solo di ingegneri, informatici, a volte fisici: l'universo dei nuovi media. La fascinazione è immediata: mi piace molto interfacciarmi con studiosi e ricercatori che si pongono il problema di gestire la «transizione» verso il nuovo. Sono stati anni di entusiasmo e di nuove prospettive.

Intuisco un'inedita figura professionale, quella del progettista multimediale, ponte tra il sapere umanistico e tecnico-scientifico, e mi butto a capofitto in quel lavoro e nella ricerca. A un certo punto vengo a sapere di un finanziamento abbastanza cospicuo del Miur sul capitolo della DaD che non interessava ai colleghi, ma a me sì.

Inizio così a coordinare un progetto di teledidattica per l'Università degli Studi di Milano con la sede distaccata di Varese e a intravedere le grandi possibilità di questo strumento, che non è solo tecnologico ma anche metodologico. Poi passo ai programmi sperimentali Rai per la scuola trasmessi sui nuovi canali satellitari e tematici, stringo contatti a distanza con università americane e australiane già più avanti di noi.

Alla DaD riconosco un potenziale enorme: colmare il divario di conoscenze tra il Nord e il Sud del mondo; l'aggiornamento continuo e permanente anche in età adulta; una didattica diversa, più spettacolare e interattiva; la contaminazione tra i saperi ecc. L'interesse verso questo campo è alto, ma gli interlocutori sono ancora molto circoscritti.

A metà del primo decennio del Duemila entro nella scuola come docente di Lettere in un istituto superiore. Ormai la DaD ha un'accezione soprattutto commerciale (università a distanza private, corsi obbligatori di aggiornamento professionale ecc.) mentre quella più globale, un nuovo paradigma anche estetico-comunicativo, credo si imporrà nel lungo termine.

L'importanza delle buone pratiche pedagogiche

La pandemia di Covid-19 all'improvviso ha portato alla ribalta la DaD per la prima volta in assoluto. Di colpo tutti sapevano che cos'era, tutti ne parlavano. Un balzo in avanti che non mi aspettavo più. L'isolamento totale e necessario in cui si è chiuso il Paese per l'emergenza ha trovato nella DaD una sponda amica, alleata nell'irrinunciabile bisogno di relazione umana, certo non fisica ma capace comunque di dare senso al nostro quotidiano, diventato triste e pesante. Lo schermo di un computer o di uno smartphone ci ha tenuto uniti, ci ha permesso di continuare a parlarci, a volte di salutarci per l'ultima volta. […]Ed è appunto questa «pratica» che affronto nel libro. Sono convinto che le modalità della tecnologia vadano prima di tutto praticate, e poi da quella esperienza discusse e anche eventualmente aspramente criticate. […]

Proprio negli ultimi mesi in modo evidente, ma anche prima per chi la conosceva e praticava, la DaD ha dato la possibilità di implementare buone pratiche pedagogiche e didattiche, che non devono andare sprecate per un approccio nostalgico al liceo classico «vecchia maniera» o a stili di insegnamento che noi adulti abbiamo patito e contestato da studenti e che ora, per una forma di coazione a ripetere, vogliamo riproporre per i nostri figli e allievi, quasi come risarcimento della fatica fatta allora.

Al contrario, queste nuove pratiche e una nuova didattica devono affiancarsi al normale andamento scolastico di tipo più tradizionale che si svolge in aula. Se invece decidiamo di rifiutarle accantonandole, perderemo anche quel poco di buono che la crisi del Coronavirus ci ha lasciato.

Ecco perché in questo libro mi sono sempre sforzato di non contrapporre mai la didattica a distanza a quella in presenza, ma di far intravedere i punti di contatto e le interazioni tra i due momenti, nonché gli auspicabili travasi dall'una all'altra.

Per la stessa ragione non ho mai usato il termine «virtuale» per la lezione in collegamento e «reale» per quella nell'edificio scolastico: oggi più che mai ciò che prima ci sembrava «virtuale» (cioè, «in potenza») fa parte della nostra quotidianità.

L'innovazione non deve spaventarci

Certamente, quando durante l'emergenza Covid-19 il mondo dei docenti si è diviso tra «lamentosi» e «volenterosi» (a volte si può essere anche entrambi!), ho subito deciso di far parte dei secondi. Il mio impegno di docente giorno per giorno è stato: «Cosa posso fare io a distanza per far sentire la mia vicinanza agli studenti?».

E così ho cercato di stabilire un rapporto con i miei studenti di scuola superiore con ogni mezzo: telefonate, messaggi, chat, video, videolezioni, videoconferenze. È stato bello, spesso emozionante.

Ci siamo incoraggiati a vicenda. I ragazzi hanno apprezzato molto - così poi mi hanno detto - il fatto che tutte le volte iniziavo la lezione domandando: «Come state? Ognuno di voi mi dica come sta». Mi domandavo: «Che ne sarà di noi?», un modo per sentirci vicini nella sventura e prenderci cura gli uni degli altri. Alla fine anche i ragazzi, vinta una certa ritrosia e il solito riserbo verso il mondo adulto, soprattutto docente, mi domandavano ogni volta: «E lei, professore, come sta?».

Posso dirlo? Nella scuola «ribaltata» dal lockdown noi siamo stati bene: liberi finalmente di progettarci, di parlarci e di ascoltarci. Le «distese praterie» didattiche che ogni giorno si prospettavano davanti a noi docenti - con i film, i repertori visivi e audio e le discussioni tra noi - erano invitanti. Nella scuola che aboliva di colpo molte prassi inutili perché nessuno sapeva ben dirti cosa dovevi davvero fare, noi siamo stati bene. E ci siamo anche divertiti. Mai così distanti, mai così vicini. ■

Bernard-Henry Lévy
Il Virus che rende folli
La Nave di Teseo Editore

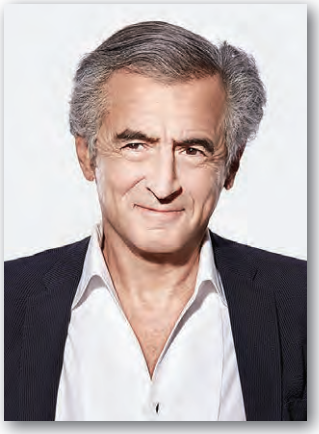
Per superare le "malattie" del nostro tempo bisogna gettare lo "sguardo oltre" il pensiero unico

Autore: Massimiliano Cannata

"Il male sta nelle parole" su questa celebre affermazione di Luigi Pirandello, si troverebbe probabilmente d'accordo il filosofo francese Bernard - Henri Lévy il cui saggio *"Il virus che rende folli,* ed. *La Nave di Teseo*)" prende le mosse dall'analisi del termine "confinamento", parola trappola, che ha generato una girandola

di equivoci, a cominciare dall'abusato esercizio del "distanziamento sociale", che forse faremmo tutti bene a definire distanziamento fisico, facendo almeno uno sforzo lecito di neutralizzare implicazioni discriminatoria.

La questione non è certo solo linguistica, perché il bel libro di BHL ha il pregio, sempre più raro ormai, di offrire uno sguardo originale sulla contemporaneità. La sua è da sempre una *"voce fuori dal coro",* da intellettuale impegnato in prima linea, non gli è mai mancata la capacità di fare notizia. Assumendo posizioni controcorrente, ha spezzato e continua a spezzare la monotonia di un *mainstream,* ossessivamente ripetitivo, prigioniero di ritualità senza contenuti. Il nostro non corre mai questo rischio, che potremmo definire come un *maitre a penser* (categoria in estinzione), che mostra di non amare le prediche ex cathedra, preferendo agire sulla delicata frontiera delle crisi umanitarie, dove la sofferenza ha un volto oltre che una ragione molto precisa. È stata, infatti, Lesbo (icona del dramma migranti del nostro tempo in cui in questi giorni si sta consumando un vero e proprio disastro umanitario) la meta del suo ultimo viaggio, come ha spiegato ad Anais Ginori in una interessante intervista apparsa sul *Venerdì di Repubblica*, isola martoriata dove è andato ad ascoltare la voce degli ultimi. Stessa cosa aveva fatto in Blangadesh, e in Libia, nel tentativo di denunciare i disegni neo imperialisti di Putin e Erdogan. In piena emergenza COVID il filosofo non potendo lasciare la sua residenza, è sceso "idealmente" in campo alzando ugualmente i toni della protesta. "Siamo reduci della prima paura mondiale" - denuncia nel *pamphlet* – il punto è che non credo debba esistere solo una sicurezza sanitaria di cui dobbiamo occuparci, perché esistono altre minacce all'orizzonte che non possiamo trascurare".



Il tragico abita il nostro tempo

Preparazione mentale, ecco il vaccino che andrebbe testato e posto in essere nella costruzione di un percorso esistenziale che ha bisogno, per ciascuno di noi, di poter contare su garanzie plurime. "Abbiamo creduto per molti anni di espellere il tragico. Prima della pandemia tutto ci sembrava curabile". La pia illusione è purtroppo svanita, aprendo il baratro della paura. Ora dovremmo imparare a essere più umili, dimostrando almeno di aver capito la lezione. Non esiste,

infatti, alcuna ricetta, che possa risolvere i drammi della vita che sono tanti e tutti diversi. Posti di fronte a questa spiacevole evidenza l'unica cosa che possiamo augurarci che questa paura universale, sia l'ultima.

BHL nel corso della trattazione non discute la misura del lockdown che si è resa inevitabile in relazione alla drammaticità della situazione verificatasi in molti paesi del mondo, l'aspetto inaccettabile risiede nell'accettazione acritica delle imposizioni decise da chi gestisce a vari livelli il potere. "Tracciare", "testare", "isolare" il mantra obbligato in questi difficili mesi ha "oscurato" il celebre trinomio che ha ispirato i valori della Rivoluzione francese "Liberté, egalité, fraternité". Il parallelismo utilizzato dall'autore potrebbe sembrare forzato, ma rende molto bene, per contrasto, il senso della posta in palio, in questa delicata fase in cui la pandemia ha sconvolto il nostro "essere nel mondo", costringendoci a rivedere abitudini e stili di vita, nel contesto di città che hanno cambiato profilo.

Non si può scambiare – questo il passaggio probabilmente più forte del libro – la libertà con la sicurezza sanitaria, contravvenendo ai principi di quel patto sociale costato anni di lotte e rivendicazioni: "Salvare la vita è bene, ma salvare la vita libera è ancora meglio", al di là del gusto per la provocazione, fa riflettere la irriducibile dicotomia tra libertà e sicurezza, diritti individuali e garanzie collettive che continuerà a mettere a dura prova i governi a tutte le latitudini. Il dilemma ha una precisa formulazione: "Esiste un modo per combattere una pandemia senza cadere nella trappola dello stato di sorveglianza sanitaria?". L'interrogativo posto dal filosofo è destinato a rimbalzare a lungo senza risposta, a giudicare dalle tante incertezze che stanno accompagnando il difficile autunno che si sta aprendo.

Il paradosso di un mondo incerto

Sullo sfondo della trattazione i dati di contesto che hanno ispirato questo scritto non sono certo confortanti. Il pericolo delle diseguaglianze crescenti a livello planetario in uno scenario geopolitico che ha perso i punti di riferimenti che hanno segnato il secolo breve, non trovandone di nuovi, sono forse l'aspetto più inquietante che nasconde dietro l'angolo il pericolo di gravi rivolgimenti sociali. Il progressivo disimpegno degli USA riguardo alle vicende di un'Europa troppo debole e divisa, le spinte neo imperialiste di nuovi dittatori, la crisi degli organismi internazionali, di cui l'ONU è l'emblema, il dramma della fame con 25 mila persone che continuano a morire ogni giorno in molte aree del mondo sono tutti aspetti che fanno ben comprendere come la "malattia" del pianeta non sia una sola. Il Covid - 19 non è l'unica patologia con cui dobbiamo fare i conti, perché il quadro clinico della democrazia nel mondo e lo stato di salute dei diritti dell'uomo stanno attraversando un momento non certo facile. "Siamo entrati nell'epoca dell'imprevedibilità permanente. Viviamo dentro un ossimoro" ha commentato lo scrittore argentino Martin Caparros in questi giorni a Mantova per il festival della letteratura. Dentro questo ossimoro Bernard - Henri Lévy non si trova a proprio agio, per questo invita il lettore a mantenere il grandangolo, nell'osservazione delle principali fenomenologie del cambiamento. Solo alla condizione di esercitare il pensiero critico con apertura e libertà di giudizio potremo venire fuori dal buio della notte dentro cui ci siamo cacciati. ■

Una pubblicazione

web for business
swiss webacademy

A cura del

Global Cyber Security Center

Redazione:
Laurent Chrzanovski e Romulus Maier (†)
(tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org
Şcoala de Înot nr.18, 550005,
Sibiu, Romania

www.gcsec.org
www.cybersecuritytrends.ro
www.swissacademy.eu
www.cybertrends.it

TREND MICRO | THE ART OF CYBERSECURITY

"ZEROLOGON": LA VULNERABILITÀ CHE DIMOSTRA ANCORA UNA VOLTA L'IMPORTANZA DEL VIRTUAL PATCHING

A cura di Gastone Nencini, Country Manager Trend Micro Italia

Recentemente è stata scoperta una nuova vulnerabilità che ha guadagnato molto spazio sui media: Zerologon. Questa vulnerabilità può consentire a un malintenzionato di sfruttare l'algoritmo crittografico utilizzato nel processo Netlogon di Microsoft e di impersonare l'identità di qualsiasi computer, al momento di autenticarsi con il controller di dominio. In parole più semplici, questa vulnerabilità nel protocollo Netlogon Remote Protocol (MS-NRPC) potrebbe consentire agli aggressori di eseguire le proprie applicazioni su un dispositivo in rete. Un utente malintenzionato non autenticato utilizzerebbe il protocollo MS-NRPC per connettersi a un controller di dominio (DC) e ottenere l'accesso amministrativo. La criticità risiede nella mancanza di una soluzione completa. La patch attualmente disponibile consente ai controller di dominio di proteggere i dispositivi, ma una seconda patch, prevista al momento per il primo trimestre del 2021, rafforzerà il Remote Procedure Call (RPC) di Netlogon per risolvere completamente questo bug. Dopo aver applicato la patch, si dovranno comunque apportare modifiche al controller di dominio. Microsoft ha pubblicato delle linee guida per aiutare gli amministratori a scegliere le impostazioni di sicurezza corrette.

Se esiste una patch, qual è il problema?

Si potrebbe pensare che nel momento in cui esiste una patch questo non sia un problema reale, ma l'idea di risolvere tutto con una patch non è così semplice come sembra. Il tempo medio per creare una patch è compreso tra 60 e 150 giorni. Questa vulnerabilità è stata pubblicata all'inizio di agosto, quindi il tempo medio per l'implementazione della patch è compreso tra ottobre 2020 e gennaio 2021. Nel mercato della security si scherza sul fatto che dopo il Patch Tuesday arrivi l'Exploit Wednesday. Questo perché dopo che le patch relative alle ultime vulnerabilità vengono rilasciate il primo martedì di ogni mese, da Microsoft e Adobe, i cybercriminali si mettono al lavoro per invertirle e per scrivere exploit che sfruttino il bug prima che le patch vengano applicate. Considerando Il tempo medio per creare una patch, le aziende rimangono esposte a una minaccia conosciuta fino a 5 mesi.

Come proteggere la propria organizzazione?

Trend Micro ha messo a punto nel corso degli anni la soluzione perfetta per le criticità date dalle vulnerabilità e dal ritardo o mancata applicazione delle patch: il virtual patching. Questo sistema fornisce un ulteriore livello di sicurezza per proteggersi dalle vulnerabilità prima di applicare la patch ufficiale del vendor. Come suggerisce il nome è come una patch, perché protegge in modo specifico l'ambiente nel caso in cui qualcuno tenti di sfruttare una vulnerabilità. Le patch virtuali sono un paracadute fondamentale, che consente poi di applicare le patch nel modo più adatto per ogni azienda. Trend Micro protegge da Zerologon e da migliaia di altre vulnerabilità attraverso patch virtuali, come parte del processo di patch management. Lo sfruttamento delle vulnerabilità è un fenomeno in crescita. Considerando anche che nella prima metà del 2020 la Trend Micro Zero Day Initiative (ZDI) ha pubblicato un totale di 786 avvisi di vulnerabilità, ovvero il 74% in più rispetto alla seconda metà del 2019, e con un particolare focus sui sistemi di controllo industriali. Ecco perché proteggersi è fondamentale. Grazie alla Trend Micro Zero Day Initiative (ZDI), le organizzazioni che utilizzano Trend Micro TippingPoint sono protette fino a 81 giorni prima che una patch venga rilasciata dal vendor proprietario del software vulnerabile (dato 2019). Ci si potrebbe chiedere come è possibile. È molto semplice: quando una vulnerabilità viene scoperta dalla ZDI, Trend Micro si mette subito al lavoro per mettere al sicuro i propri clienti da quella vulnerabilità ancora senza soluzione. I clienti Trend Micro possono beneficiare della tecnologia di virtual patching sugli ambienti protetti dalle soluzioni di Trend Micro ApexOne, Deep Security, Cloud One – Workload Security e Tipping Point.

Ulteriori informazioni sono disponiblil su :
https://www.trendmicro.com/it_it/what-is/zerologon.html

www.trendmicro.com

CERTrating
Maturity Evaluation Tool

Il primo Tool per valutare il livello di maturità del tuo CERT e dei suoi Servizi

Available Now

www.certrating.it

GLOBAL CYBER SECURITY CENTER

Per maggiori dettagli
Info@gcsec.org

Il fattore umano nella cyber security

Valori e strategie da costruire insieme

A cura di Nicola Sotira

MANAGEMENT

TOOLS

GLOBAL CYBER SECURITY CENTER

FrancoAngeli