Cybersecurity Trends

Edizione italiana, N. 4 / 2022

INTERVISTE VIP:

- LEONARDO TRICARICO
- PASQUALE STANZIONE
- MASSIMILIANO VALERII
- MICHELE MEZZA

Folder centrale: Cyberspazio, rischi e sicurezza

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

La frontiera elettronica.

Autore: Nicola Sotira

"Cyberspazio" è il "luogo" nel quale sembra accadere una conversazione telefonica. Non all'interno del vostro reale telefono, l'apparecchio in plastica o altro materiale che si trova sulla vostra scrivania. Non all'interno del telefono dell'altra persona, che si trova in qualche altra città.

Lo spazio tra i telefoni. ...negli ultimi venti anni trascorsi, questo "spazio" elettrico che un tempo era sottile e scuro e uni-dimensionale, poco più di uno stretto tubo parlante, che si allungava con un filo da telefono a telefono, si è praticamente espanso, schizzando fuori come un gigantesco joker dentro la scatola, la luce lo ha inglobato, sotto forma di luce tremolante dello schermo di un computer.

BIO

Nicola Sotira è 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.

Questo mondo scuro e nascosto rappresentato dal piccolo ricevitore telefonico connesso tramite un filo alla rete si è trasformato in un vasto e fiorente paesaggio elettronico. Dagli anni Sessanta, il mondo del telefono è divenuto ibrido con i computer e la televisione, e sebbene non vi sia ancora alcuna sostanza di ciberspazio, nulla che si possa maneggiare, esso ora ha uno strano tipo di fisicità. È buonsenso oggi parlare di ciberspazio come un "luogo a sé stante".

Così parla del Cyberspazio Bruce Sterling nel suo libro Hacker Crackdown che pur essendo pubblicato nel 1994 è ancora attualissimo. Questo termine, usato sempre di più, è ancora per molti oscuro, non riuscendo a percepire con chiarezza questo nuovo tipo di dimensione sospesa tra il reale ed il virtuale. Una dimensione che trova nel *metaverso* una specie di materializzazione e rende molto più simile questo spazio a qualcosa che ha una sua dimensione fisica che avrà come effetto la progressiva fusione proprio tra fisico e virtuale.

Uno spazio che l'industria considera come una delle prossime aree strategiche per la crescita del business, dove però vi sono alcuni problemi che ancora non sono stati del tutto risolti. Uno è il tema delle aziende che hanno un ritardo tecnologico che deve essere recuperato molto velocemente e l'altro tema è quella della sicurezza di questo ecosistema.

Lo sviluppo sostenibile di questo spazio richiede l'applicazione sinergica di tecnologie d'avanguardia anche per permettere una completa integrazione del mondo digitale e del mondo fisico. Una integrazione che si svilupperà anche nel settore economico, nella vita digitale e quella sociale dove avremo una completa integrazione di beni digitali e fisici e soprattutto una reale integrazione tra identità digitale e identità reale.

Chiaramente questo spazio ha delle implicazioni di sicurezza a livello nazionale e anche delle vulnerabilità sistemiche che richiederanno certamente degli interventi da parte del legislatore. Inoltre, data la sua natura che va al di là dei confini nazionali si porranno sicuramente nuove sfide di politica internazionale e tematiche relative al *nuovo ordine mondiale digitale*. Sarà fondamentale far sedere al tavolo la comunità internazionale per avviare l'attuazione di linee guida e politiche che regolino lo sviluppo del Cyberspazio in una direzione sana ed ordinata. Come giudicare questo sviluppo? Sarà positivo o negativo?

Qui utilizziamo la cinematografia per rispondere, in particolare un dialogo tratto dal film Blade Runner. Rachel, il replicante, chiede all'ispettore Rick Deckard una sua opinione sul lavoro della Tyrrel Corporation, come lui vede questo progresso fatto di macchine e replicanti, la risposta dell'ispettore che vigila su questo mondo arriva tagliente: *"I replicanti sono come tutte le altre macchine, possono essere un beneficio o un rischio e se sono un beneficio non sono un mio problema"*. Buona lettura. ■

Cyberspazio e sicurezza delle dorsali sottomarine in fibra ottica.

Autore: Calogero Vinciguerra

"Who rules East Europe commands the Heartland: who rules the Heartland commands the World-Island: who rules the World-Island commands the World". Secondo Sir Halford John Mackinder, esisterebbe nel mondo un'area geografica di rilevante valenza strategica, situata nella parte settentrionale dell'Eurasia. Il controllo di tale area, determinerebbe il dominio dell'intero pianeta.

Oggi l'Heartland del paradigma mackinderiano è il cyberspazio, il cui controllo condiziona l'egemonia di una potenza sulle altre

Nel corso degli anni, l'espansione del cyberspazio, oltre ad apportare vantaggi in termini di connettività e produttività, ha generato un sistema capillare di interconnessioni e interdipendenze, tale da divenire un fattore rilevante di vulnerabilità, in grado di condizionare la sicurezza delle infrastrutture critiche del Paese. In altri termini, stiamo assistendo a una sorta di spostamento del baricentro del rischio verso un nuovo dominio: il *cyber*spazio. L'analisi delle sue criticità richiede una metodologia olistica incentrata sul concetto multi spaziale di rappresentazione del *cyber*spazio, senza trascurarne la sua natura spiccatamente dicotomica (fisica e virtuale).

Rappresentazione del *Cyber*spazio

Il *cyber*spazio è un insieme di infrastrutture informatiche di interesse strategico, che raggruppa elementi di natura fisica *(hardware)*, virtuale *(software)* e umana (utenti), incluse le relazioni logiche tra di essi[1]. Questa *cyber*-architettura è raffigurabile come un insieme di livelli (fisico, logico, *software*/dispositivi utenti e cognitivo/semantico) interconnessi, interdipendenti e interagenti fra loro (Figura 1). Pertanto, un'anomalia riscontrata nel livello inferiore ha delle ripercussioni funzionali in tutti i livelli sovrastanti, pregiudicandone la normale operatività.

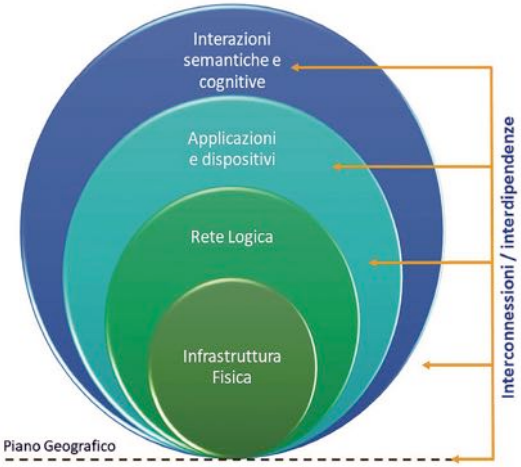


Figura 1: *Cyber*-Architettura - Elaborazione dell'Autore

Il primo livello, cioè quello fisico, è costituito da una immensa rete di collegamenti in fibra ottica (terrestre e sottomarina), di antenne per le comunicazioni *wireless* (spettro elettromagnetico), di apparati elettronici e sistemi digitali *(router, server, data center* ecc.), che insieme realizzano la *"backbone"* fisica di *internet*. Il secondo livello è rappresentato dalla rete logica e dai protocolli di comunicazione, che permettono di veicolare e instradare i dati dal mittente al destinatario e viceversa. Il terzo livello è formato dalle applicazioni *software* e dai dispositivi *hardware*, che permettono di utilizzare i servizi *internet*. Il quarto livello, infine, chiamato cognitivo o semantico, è quello rappresentato dalle interazioni e dalle interconnessioni sociali di natura virtuale degli utenti.

La prefata architettura raffigura il *cyber*spazio come uno "dominio sospeso" e fluttuante, fin quando non aggiungiamo un ulteriore livello, il piano statico, vale a dire il territorio geografico. Ogni elemento dell'architettura, traslato sul piano geografico, diviene soggetto ai vincoli della geografia fisica e politica,

alla geo-referenziazione e agli aspetti legali e normativi correlati al territorio.

Infrastruttura fisica: le dorsali sottomarine

L'elemento più rilevante e tangibile della *cyber*-architettura è il livello fisico, ampiamente raffigurato dalla rete di cavi sottomarini in fibra ottica, ossia la spina dorsale della rete telematica globale *(backbone)*.

Tale rete sfrutta la tecnologia della fibra ottica, la cui velocità di instradamento consentita è di gran lunga superiore rispetto a quella fornita dai collegamenti satellitari, in termini di larghezza di banda e latenza. Questo è il motivo per cui la stragrande maggioranza del traffico digitale, nello specifico circa il 96%, viene instradato attraverso i cavi sottomarini. Secondo i dati forniti dalla società TeleGeography[2], l'attuale estensione globale dell'infrastruttura sottomarina per telecomunicazioni è di circa 1,3 milioni di chilometri, connettendo più di 5 miliardi di utenti *internet* di tutto il globo (Figura 2).

Tuttavia, le dorsali sottomarine sono soggette ai vincoli della geografia fisica e politica, dello spazio di ubicazione e del Diritto Internazionale. Lo Stato che ospita sulle proprie acque territoriali i cavi può esercitare una forma di sovranità, nei termini stabiliti dalla *United Nations Convention on the Law of the Sea - UNCLOS*[3] (Figura 3).

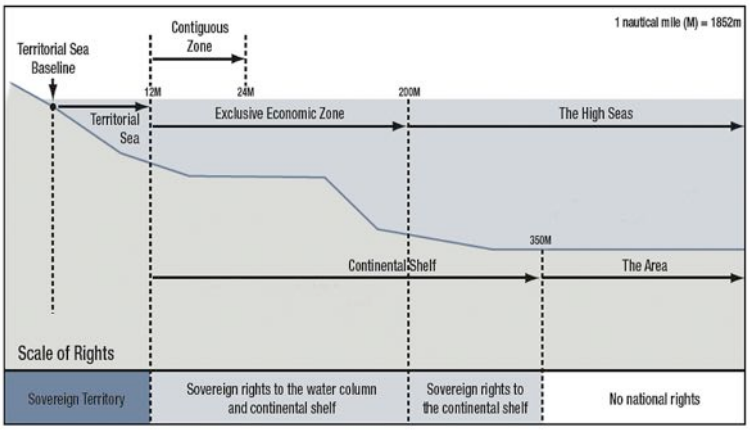


Figura 3: *Maritime Boundaries in the UNCLOS* (fonte: Arctic Council, Arctic Marine Shipping Assessment 2009 Report (Tromsø, Norway: 2009), p. 52).

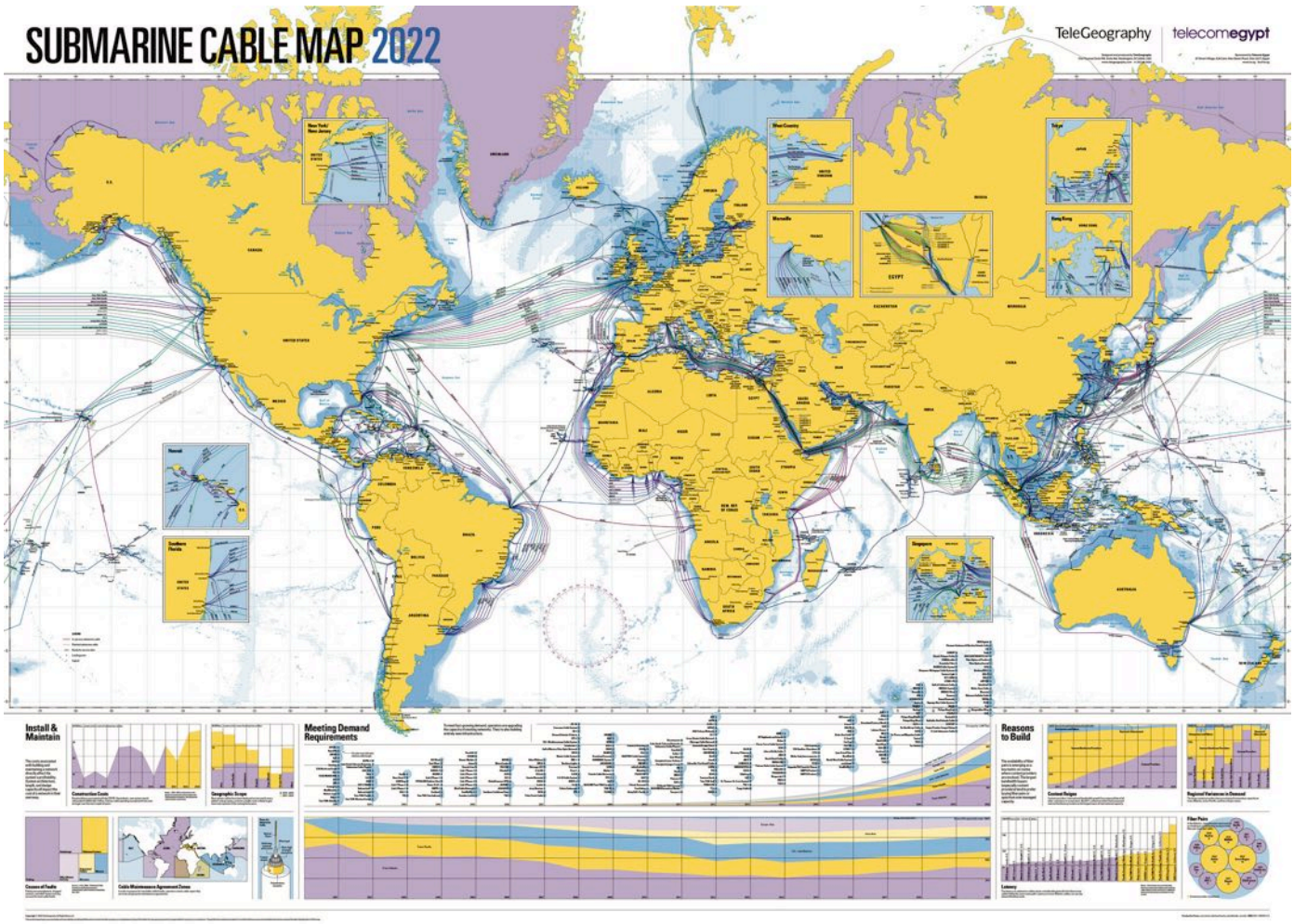
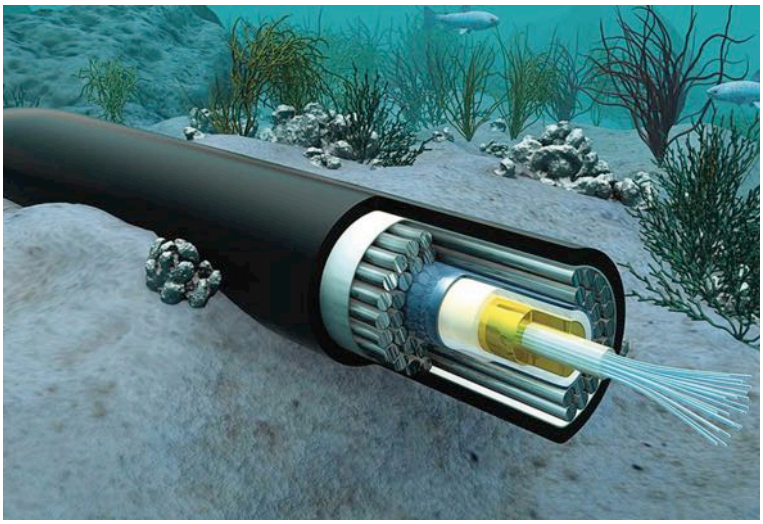


Figura 2: *Submarine Cable Map 2022 by TeleGeography - Copyright © 2022 PriMetrica, Inc* (fonte: https://submarine-cable-map-2022.telegeography.com).

I cavi sottomarini ripercorrono le rotte navali già tracciate e usate da tempo per lo scambio di merci e sono soggette, pertanto, alle normali costrizioni geografiche degli Stati che attraversano.

Vulnerabilità dei cavi sottomarini in fibra ottica

La vulnerabilità di questi cavi è rappresentata dalla loro esposizione a danni involontari, come i morsi di pescecane o dal transito di navi nelle zone di ancoraggio. Per questo motivo, le aziende produttrici realizzano una duplice protezione di acciaio e *kevlar*, per aumentarne la resilienza. Tra le minacce che inficiano la sicurezza fisica dei cavi sono incluse anche quelle generate da eventi naturali, come ad esempio gli *tsunami,* le eruzioni e i terremoti sottomarini. Le dorsali sottomarine sono facilmente individuabili e più esposte a potenziali atti di sabotaggio, perpetrati intenzionalmente per impedirne il normale funzionamento e l'instradamento dei dati. Il loro danneggiamento può causare l'interruzione delle comunicazioni tra nazioni o tra continenti, generando seri problemi di connettività e il rischio d'isolamento ove non si disponga di collegamenti alternativi, su cui dirottare il traffico dei dati compromessi.



Inoltre, se consideriamo la pervasività del *cyber*spazio, le interdipendenze e le interconnessioni delle infrastrutture critiche (inclusi i relativi settori vitali dell'energia, delle finanze, dei trasporti ecc.), l'eventuale interruzione intenzionale dei servizi di connettività *internet* potrebbe generare una sorta di "effetto domino", in grado di propagare la causa/effetto lungo tutta la catena operativa, causando l'interruzione dei servizi essenziali erogati dai settori compromessi, con severe ripercussioni sull'economia della nazione coinvolta e l'incolumità dei suoi cittadini.

Possiamo considerare, oggigiorno, l'infrastruttura fisica delle dorsali sottomarine ancora affidabile e sicura?

I recenti sabotaggi dei due gasdotti Nord Stream nel mar Baltico hanno sollevato varie preoccupazioni in merito alla sicurezza fisica dei cavi sottomarini che collegano il mondo a *internet*. Tale inquietudine è stata ulteriormente alimentata da un ulteriore incidente, che ha coinvolto alcuni cavi sottomarini dislocati nel sud della Francia, causando notevoli problemi di connettività *internet*. La sicurezza delle dorsali *internet* sottomarine sembra apparire fragile e inadeguata rispetto alla sempre più crescente minaccia ibrida globale.

Molto spesso associamo l'idea di *internet* in "a un'entità" astratta, in grado di fornire ogni tipologia di servizio *on-line*, trascurandone la sua "nativa" dipendenza dall'infrastruttura fisica, elemento cruciale e imprescindibile per il suo funzionamento. In caso di interruzione intenzionale dei servizi di connettività, una carente visione olistica del *cyber*spazio e delle sue peculiari stratificazioni, determina una grave sottostima del rischio reale, incluso il suo conseguente impatto negativo sulle attività che dipendono dai servizi *internet*.

In quale modo è possibile migliorarne il livello di resilienza e sicurezza?

La risposta al quesito scaturisce dal riesame del rischio globale, correlando le minacce emergenti, specie quelle di natura ibrida, con la probabilità che possano materializzarsi nel breve termine. Oggigiorno, purtroppo, tale livello di rischio sembra essere in continua ascesa. Data l'enorme mole di dati e informazioni che transitano nelle reti in fibra ottica sottomarine, al fine di garantire la *core business continuity*, occorre predisporre e all'occorrenza implementare una serie di misure di mitigazione del rischio. Tali misure potrebbero essere incentrate sulla ridondanza delle dorsali di instradamento del traffico *internet* su fibra ottica, senza trascurarne la complementarità dei collegamenti che sfruttano lo spettro elettromagnetico, in particolare quelle via satellite. Quest'ultime, infatti, possono rappresentare un'utile risorsa di *back-up* in particolari situazioni di contingenza.

Iniziative per l'espansione della copertura della rete

Nel settore privato, infatti, le società di telecomunicazioni sono sempre più orientate verso la realizzazione di percorsi alternativi, per creare varianti utili in caso di congestione o interruzioni del traffico.

BIO

Calogero Vinciguerra è Space Security Policy Officer e Space Threat Response Architecture Duty Officer presso la Divisione Spazio del Servizio europeo per l'azione esterna (SEAE) di Bruxelles. È laureato in Scienze Politiche e delle Relazioni Internazionali e ha conseguito il Master Universitario in "Sicurezza Informatica e Cybersecurity – Security Manager" presso la Link Campus University di Roma. Nel corso degli anni ha maturato molteplici esperienze sia nel campo addestrativo e operativo, sia in ambito nazionale e internazionale. Ha lavorato anche presso il NATO Headquarters di Bruxelles nel settore dell'Information Assurance. È autore di un libro intitolato "Intelligence e Sicurezza del Cyberspazio", pubblicato il 13 maggio 2022.

Da un punto di vista globale, ne è un esempio l'accordo stipulato tra Facebook, Microsoft e Telxius, per la realizzazione della moderna dorsale sottomarina trans-atlantiche in fibra ottica, denominata "Marea". Completata nell'aprile del 2018, la dorsale collega la Virginia (USA) con la Spagna, attraverso un cavo sottomarino di circa 6644 chilometri (realizzato con la tecnologia *Open Cable System*), che permette di raggiungere una velocità di trasmissione dati nell'ordine di 200 *Terabit* al secondo (circa 20 milioni di volte più veloce di una connessione *internet* domestica).

Un ulteriore caso che riflette tale tendenza è l'accordo stipulato tra China Mobile, Facebook, Mobile Telephone Networks, Orange, Saudi Telecom Company, Telecom Egypt, Vodafone e West Indian Ocean Cable Company, per la realizzazione del più grande progetto di connettività sottomarina al mondo, denominato 2Africa, che circoscriverà interamente il continente africano, fornendo collegamenti *internet* senza soluzione di continuità a 16 paesi dell'Africa. Entro il 2024, il colossale anello sottomarino collegherà l'Africa, il Medio Oriente e l'Europa, attraverso un cavo in fibra ottica di nuova generazione della lunghezza di circa 39.000 chilometri (costruzione a cura della Alcatel Submarine Networks), permettendo una capacità trasmissiva massima di 180 *Terabit* al secondo.

Il progetto si prefigge di incrementare il livello di connettività tra il continente africano e 23 paesi limitrofi, riducendone significatamene il *digital divide*, che ha storicamente contraddistinto questa area del globo (Figura 4).

Figura 4: 2Africa, l'infrastruttura sottomarina più grande al mondo (fonte: *2Africa Consortium*).

In ambito europeo, nel 2021 con la firma della dichiarazione *"European Data Gateways as a key element of the EU's Digital Decade"* gli Stati Membri si sono impegnati a rafforzare la connettività internet tra l'Europa e i suoi partner africani, asiatici, balcanici e dell'America Latina[4]. Tale iniziativa prevede la realizzazione di data center per l'immagazzinamento e l'elaborazione dei dati (in linea con la normativa EU sulla protezione dei dati), collegamenti satellitari sicuri e resilienti, ma soprattutto nuove dorsali sottomarine aggiuntive per instradare il crescente volume di traffico *internet*. Nell'arco di un decennio, attraverso la realizzazione di questi progetti, l'Europa intende diventare un *Global Data Hub,* consolidando la propria autonomia strategica e sovranità digitale.

Strategia di monitoraggio delle dorsali sottomarine

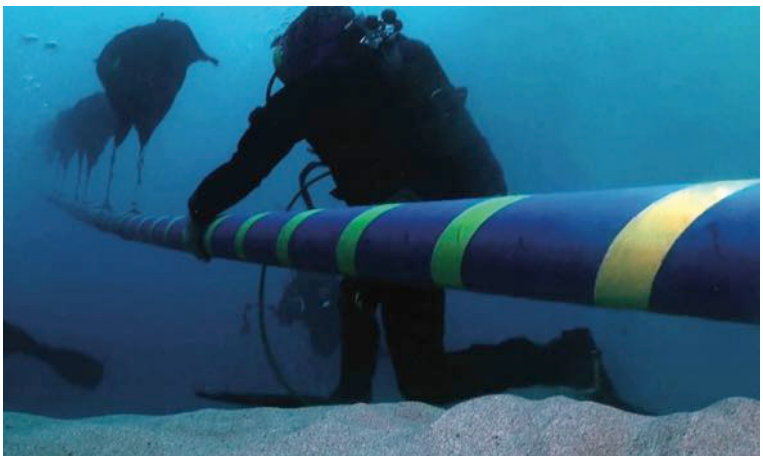
La sicurezza fisica dei cavi sottomarini e dell'infrastruttura di approdo è di competenza degli operatori privati, che ne assicurano la funzionalità operativa attraverso il monitoraggio e i servizi di intervento e manutenzione. Considerata l'ampia estensione dei cavi e il rischio crescente correlato alle minacce ibride, tuttavia, potrebbe risultare alquanto difficile individuare eventuali atti di sabotaggio in corso d'opera, specialmente nelle zone remote e profonde delle acque internazionali. Data l'importante valenza strategica, la sicurezza delle infrastrutture critiche sottomarine sta diventando una questione di sicurezza globale, che richiede un impegno collettivo e partecipato da parte di tutti gli *stakeholder* coinvolti.

Occorrono pertanto dei sistemi di sorveglianza ad ampio raggio d'azione, realizzati *ad hoc* per tale esigenza, capaci rilevare anticipatamente la materializzazione delle prefate minacce, allo scopo di salvaguardare non solo l'integrità fisica dei cavi, ma anche l'eventuale compromissione della confidenzialità delle informazioni in transito.

Il monitoraggio delle infrastrutture sottomarine, tuttavia, risulta particolarmente complesso e oneroso, in particolare per i tratti di dorsale che attraversano le acque internazionali, dove l'applicazione delle convenzioni non è del tutto chiara. Tali segmenti, quindi, risultano altamente vulnerabili e

più soggetti a potenziali attacchi o sabotaggi, dalle conseguenze disastrose sia sul piano economico sia su quello della sicurezza globale.

Una strategia globale di monitoraggio delle infrastrutture critiche sottomarine da sola non è sufficiente per arginare il problema. Occorre integrare e implementare anche dei meccanismi di segnalazione degli incidenti, incluse le procedure di gestione e *recovery*, per garantire la *core business continuity*. Quest'ultimo aspetto apre uno scenario inedito nella gestione e comunicazione degli incidenti relativi alle dorsali sottomarine, che trova riscontro anche nelle considerazioni introduttive della nuova direttiva NIS 2. Nel paragrafo n. 51 del preambolo della Direttiva viene enfatizzato, in particolare, la necessità di disporre di adeguate misure di *cybersecurity* e di segnalazione dei relativi incidenti sia per le dorsali *internet* sia per i cavi di comunicazione sottomarini, al fine di garantire l'erogazione dei servizi da parte degli operatori essenziali.



Tuttavia, l'attuazione della direttiva richiederà tempo, infatti, gli Stati Membri dovranno recepire le disposizioni nella loro legislazione nazionale.

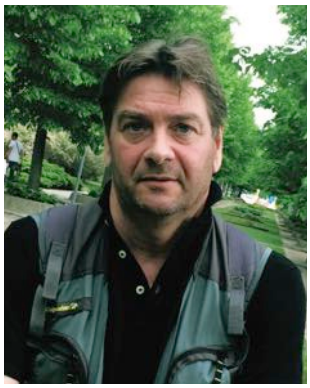
In conclusione, le dorsali sottomarine in fibra ottica rappresentano un elemento fondamentale del *cyber*spazio, la cui affidabilità e integrità gioca un ruolo vitale per la sicurezza e l'economia globale. L'analisi delle sue criticità richiede una metodologia olistica incentrata sul concetto multi spaziale di rappresentazione del cyberspazio, articolato per livelli (fisico, logico, *software*/dispositivi utenti e cognitivo/semantico). In sintesi, è necessario promuovere una nuova e più consapevole "cultura della sicurezza", unita a una cognizione sempre più profonda delle minacce, specie quelle di natura ibrida. La speranza è legata al fatto che la strada da seguire in materia di resilienza delle infrastrutture sottomarine, ancora lunga e irta di ostacoli, venga percorsa con determinazione al fine di raggiungere un livello comune di sicurezza tale da garantire le migliori condizioni di vita e di sviluppo. ■

DISCLAIMER

I contenuti di questo articolo riflettono esclusivamente la personale opinione del dott. Calogero Vinciguerra e non possono in alcun caso essere considerati come posizione ufficiale della Forza Armata e/o del Servizio europeo per l'azione esterna presso le quali presta la propria opera.

1 Presidenza del Consiglio dei Ministri, "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", dicembre 2013.
2 TeleGeography è una società di consulenza ed analisi del settore delle telecomunicazioni, specializzata nella produzione di mappe digitali interattive dell'infrastruttura ICT globale.
3 Legge 2 dicembre 1994, n.682 di ratifica ed esecuzione della Convenzione delle Nazioni Unite sul diritto del mare stipulata a Montego Bay il 10 dicembre 1982.
4 Digital Day 2021 – Dichiarazione Ministeriale europea del 19 Marzo 2021: "European Data Gatewaysas a keyelement of the EU's Digital Decade".

La sicurezza cyber nel segmento spaziale.



Autore: Francesco Corona

Generalità

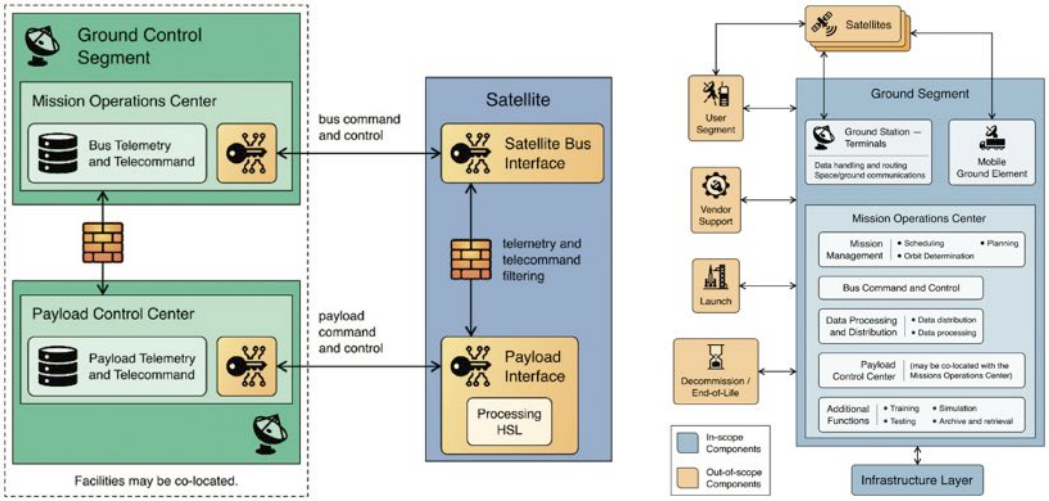
L'industria spaziale è vittima di numerosi attacchi sin dai suoi primordi da parte di una vasta gamma di avversari e per una moltitudine di motivazioni. Il comitato consultivo per i sistemi di dati spaziali (CCSDS) "Security Threats against Space Missioni" aggiorna costantemente una panoramica delle minacce alle missioni spaziali, incluse simulazioni di minacce contro diverse tipologie di missioni. Tuttavia, è di difficile rappresentazione un modello di minaccia dettagliato in quanto fortemente legato agli obiettivi e requisiti di sicurezza della specifica missione target. In generale attacchi specifici al segmento spaziale, inclusa la compromissione alla sicurezza fisica per ottenere ad esempio l'accesso non autorizzato a stazione di terra e ad altre risorse IT, sono fattibili con percentuali di riuscita molto elevate. Un successo nello sfruttamento di una vulnerabilità attraverso un attacco fisico potrebbe ad esempio disabilitare la stazione di terra e influenzare direttamente il funzionamento della missione e dei servizi forniti. Esso potrebbe anche mirare a sorpassare l'impianto di terra per prendere il controllo del veicolo spaziale senza attaccare tecnicamente i sistemi. Un rapporto della NASA, [B001], ha dettagliato il furto di un computer portatile non crittografato e la conseguente perdita dei software di comando e controllo della Stazione Spaziale Internazionale.

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR ed attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria.

Le pricipali componenti e le loro vulnerabilità

Parlando di sicurezza nel cosiddetto Segmento Spaziale, il profilo di base si concentra quindi su due componenti fondamentali del segmento: quello spaziale-terrestre attribuito alle cosiddette **Ground Station** (stazioni terrestri) e quello prettamente spaziale-satellitare attribuito al **Satellite in orbita**. Le due principali componenti della Ground Station, risultano essere Il **Mission Operations Center (MOC)** che impartisce comandi di controllo a uno o più satelliti e riceve la telemetria dai veicoli spaziali in orbita e il **Payload Control Center (PCC)** che invia comandi e ricevere risposte da un carico utile (payload) ospitato dal satellite (il payload può essere residente su un veicolo spaziale in cui le operazioni di autobus possono essere eseguite anche da un MOC indipendente e separato da quello di missione). Con la continua proliferazione di piccoli satelliti in orbita terrestre bassa, la sicurezza informatica è qualcosa che la comunità è costretta a prendere seriamente in considerazione.



Architettura generale di un Segmento Spaziale e sue componenti specifiche da proteggere

Con il basso costo dei piccoli satelliti controllati da hardware di tipo COTS (commercial off-the-shelf), software open source (prevalentemente Linux-based) e servizi di stazioni di terra basati sul web, aumenta chiaramente la probabilità di vulnerabilità.

Lo sfruttamento, inoltre, delle reti di computer (CNE) connesse all'architettura Ground Station può avvenire nel punto esatto dove l'attaccante è in grado di compromettere la rete a cui è collegata la stazione di terra. Allo stesso modo attacchi sulle reti IT aziendali potrebbero essere caratterizzati da exploitation di tecnologie mal configurate o vulnerabili per ottenere accessi non autorizzati alle stazioni di controllo a terra. L'infrastruttura cloud, alimenta la maggior parte del quadro di calcolo nella stazione di terra. Dai dati dall'archiviazione all'elaborazione dei dati, l'intera piattaforma di servizi risulta dipendente alle infrastrutture cloud. Il fallimento dell'infrastruttura cloud potrebbe avere effetti catastrofici sulla stazione di terra compreso il denial of service (DoS) per il ricevitore dei dati satellitari. Ad esempio, i principali fornitori di servizi cloud che includono Google Cloud Platform (GCP) sono noti per avere interruzioni delle loro infrastrutture a causa di attacchi interni ed esterni [B002]. Questi casi potrebbero ostacolare le operazioni dei sistemi satellitari in tempo reale. La corruzione/modifica dei dati che si riferisce all'intenzionale o non intenzionale compromissione dei dati può causare errori del software o bug, guasti hardware, uso di software non autorizzato o tentativi attivi di cambiare/modificare i dati con il loro mancato utilizzo. Un comando di un veicolo spaziale compromesso potrebbe causare catastrofici effetti a bordo di una navicella spaziale. Attacchi alla catena di approvvigionamento (Supply Chain) inclusa la perdita di software e strumentazione connessa e all'utilizzo di componenti condivise tra più attori, espone poi il sistema a vulnerabilità che risultano incorporate nella catena di approvvigionamento. Software COTS obsoleti e senza patch, precedentemente distribuiti, espongono il sistema a superfici di attacco molto pericolose. Per non parlare poi delle possibilità di attacco diretto allo spettro elettromagnetico attraverso Jammer. Le architetture di comunicazione tra Ground Station e Satelliti stanno tuttavia evolvendo verso sistemi ottici più sicuri basati su tecnologia laser e fibra ottica.

L'aggiunta di sistemi di propulsione desta ulteriore preoccupazione poiché esiste la possibilità che un attore malevolo prenda il controllo del veicolo spaziale e lo utilizzi per mirare e scontrarsi con altri veicoli spaziali. In risposta a questa minaccia, la NASA richiede a qualsiasi suo veicolo spaziale propulsivo entro 2 milioni di chilometri dalla Terra di proteggere il proprio collegamento di comando con una **crittografia conforme al Livello 1 del Federal Information Processing Standard (FIPS) 140-2**. La FCC ha anche preso in considerazione la richiesta di crittografia sulle comunicazioni di telemetria, tracciamento e comando per veicoli spaziali propulsivi, ma recentemente ha deciso di non incorporare un requisito specifico in questo momento. Le misure per la protezione dagli attacchi informatici dovrebbero essere prese in considerazione sia per i veicoli spaziali che per i sistemi di terra. Sebbene ulteriori regolamenti federali rimangano all'orizzonte, gli operatori di veicoli spaziali dovrebbero seguire le migliori pratiche.

Le 10 raccomandazioni MITRE, crittografia ed enti del settore

La MITRE Corporation ha offerto i seguenti dieci elementi da considerare per le migliori pratiche di sicurezza informatica dei piccoli satelliti:

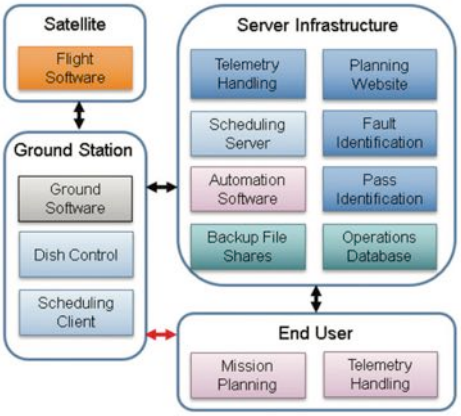
1. Comunicazione autenticata 2. Crittografia dei dati in trasmissione 3. Controllo degli accessi 4. Whie list e verifica/vincoli dell'input 5. Registrazione e controllo	6. Aggiornamenti sicuri 7. Processi di ingegneria sicuri 8. Funzionalità antivirus 9. Sicurezza del BIOS 10. Capacità di sicurezza in caso di guasto

Nuovi meccanismi crittografici stanno tuttavia emergendo nell'industria leggera satellitare. L'autenticazione del messaggio di navigazione (NMA) è un meccanismo di autenticazione per fornire autenticità e integrità dei dati di navigazione. NMA può utilizzare crittografie a chiave simmetrica/asimmetrica. **Chips Message Robust Authentication (CHIMERA)** è un NMA ibrido e l'autenticazione del codice di diffusione risulta un meccanismo proposto per segnali GPS che

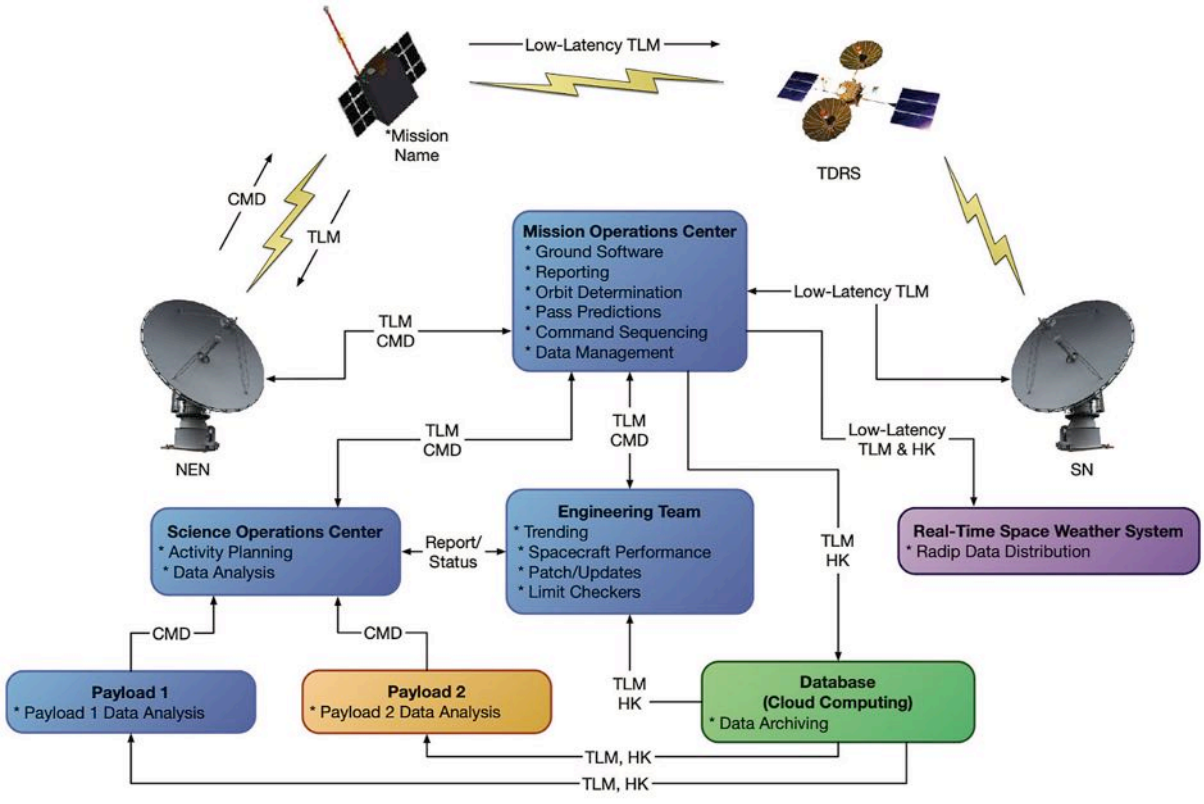
utilizza l'algoritmo di firma digitale a curva ellittica asimmetrica (ECDSA) P-224. Tuttavia, CHIMERA richiede che i ricevitori abbiano accesso occasionale, tramite canali non GPS, per fornire chiavi pubbliche GPS autenticate e un'infrastruttura a chiave pubblica (PKI) per verificare l'autenticità della chiave fornita. Il sistema Galileo GNSS, come parte dell'autenticazione dei suoi messaggi, incorpora un **Efficient Stream Loss-tolerant Authentication (TESLA) protocol** con una nuova singola catena unidirezionale di cripto-chiavi grafiche condivise da tutti i satelliti.

Le frequenze di comunicazione satellitare vengono pertanto intenzionalmente protette. I segnali dei satelliti nello spazio sono molto deboli e se c'è troppa interferenza non possono essere ascoltati. All'interno di ciascuna banda di frequenza ci sono designazioni governative e non governative. Alcune frequenze sono solo per uso governativo, altre sono non governative e alcune sono condivise. Tutti gli organismi nazionali devono coordinarsi con **l'Unione Internazionale delle Telecomunicazioni (ITU)**, che è l'organismo di governo a livello internazionale. In Italia ed Europa assisteremo tra qualche decennio a una maggiore liberalizzazione del settore che prenderà il via in ambiti universitari e di ricerca applicata per poi svilupparsi in un mercato sempre crescente che non sarà solo appannaggio delle grandi industrie.

I software da proteggere



La stazione di terra utilizza vari software per il controllo dell'antenna, il comando, la formattazione e la codifica del segnale, la programmazione dei passaggi e l'interfacciamento con il MOC, tutti software da proteggere a livello cyber. Un software calcola la direzione di puntamento utilizzando un **Set di elementi a due linee (TLE)** per definire il movimento del satellite, un modello accurato della montatura del sistema di puntamento e l'ora GPS, genera comandi motori in funzione del tempo. Il controller del motore utilizza questi comandi per tracciare attivamente il satellite durante un passaggio. Durante il passaggio, viene utilizzata un'altra suite software per monitorare il collegamento, elaborare e codificare i comandi per la trasmissione, gestire qualsiasi formattazione o crittografia del segnale e demodulare e decodificare le trasmissioni ricevute. Questo software gestisce anche la connessione di rete con il MOC su cui viene passato il TLE, nonché i dati per l'upload e le richieste di dati da scaricare. Quando il contatto è completo, i dati ricevuti dal satellite vengono ritrasferiti al MOC. La stazione di terra può anche avere la propria telemetria per



Architettura di un Ground Station per un piccolo satellite che utilizza la rete terrestre e la rete spaziale della NASA.

quel contatto. Questi dati vengono utilizzati per tracciare l'andamento delle prestazioni della missione. L'andamento delle prestazioni di ciascun contatto fornisce informazioni e avvisi di degrado sia per il satellite che per la stazione di terra. La stazione di terra può anche utilizzare un software di pianificazione durante la gestione di più missioni. Questo software utilizza la simulazione dell'orbita e le informazioni TLE correnti per determinare quando sono previsti i contatti. Per il MOC, il software di pianificazione della missione è necessario per missioni che richiedono un comportamento del satellite complesso come puntare un bersaglio durante la raccolta di dati scientifici da inviare al **SOC (Science Operations Center** distinto dal **MOC)** ad esempio nella fotogrammetria e telerilevamento in bande multi-spettrali. Il software includerà un modello di simulazione della dinamica del satellite e delle capacità dei suoi componenti. L'evento è pianificato definendo una serie di comandi/azioni che devono avvenire in un certo ordine e tempi precisi al passaggio del satellite. Il software simulerà la risposta del satellite e quindi i tempi e le azioni verranno regolate in modo reiterato secondo necessità per ottimizzare il piano e non causare una condizione di guasto. L'output del piano è costituito da tutti i comandi e i database richiesti dal satellite al suo passaggio. Nei satelliti geostazionari le operazioni risultano avere profili di complessità inferiori.

Le vulnerabilità di un MOC sono da ricercare soprattutto nei software di terze parti come quelli che gestiscono l'invio di comandi oppure lo spostamento dell'antenne per il corretto tracciamento dei satelliti oppure software per analizzare automaticamente la telemetria. Il SOC utilizza software specifici per gestire la ricezione, il disassemblaggio, la ricostruzione e la post-elaborazione dei dati scientifici della missione che verranno poi memorizzati nel cloud.

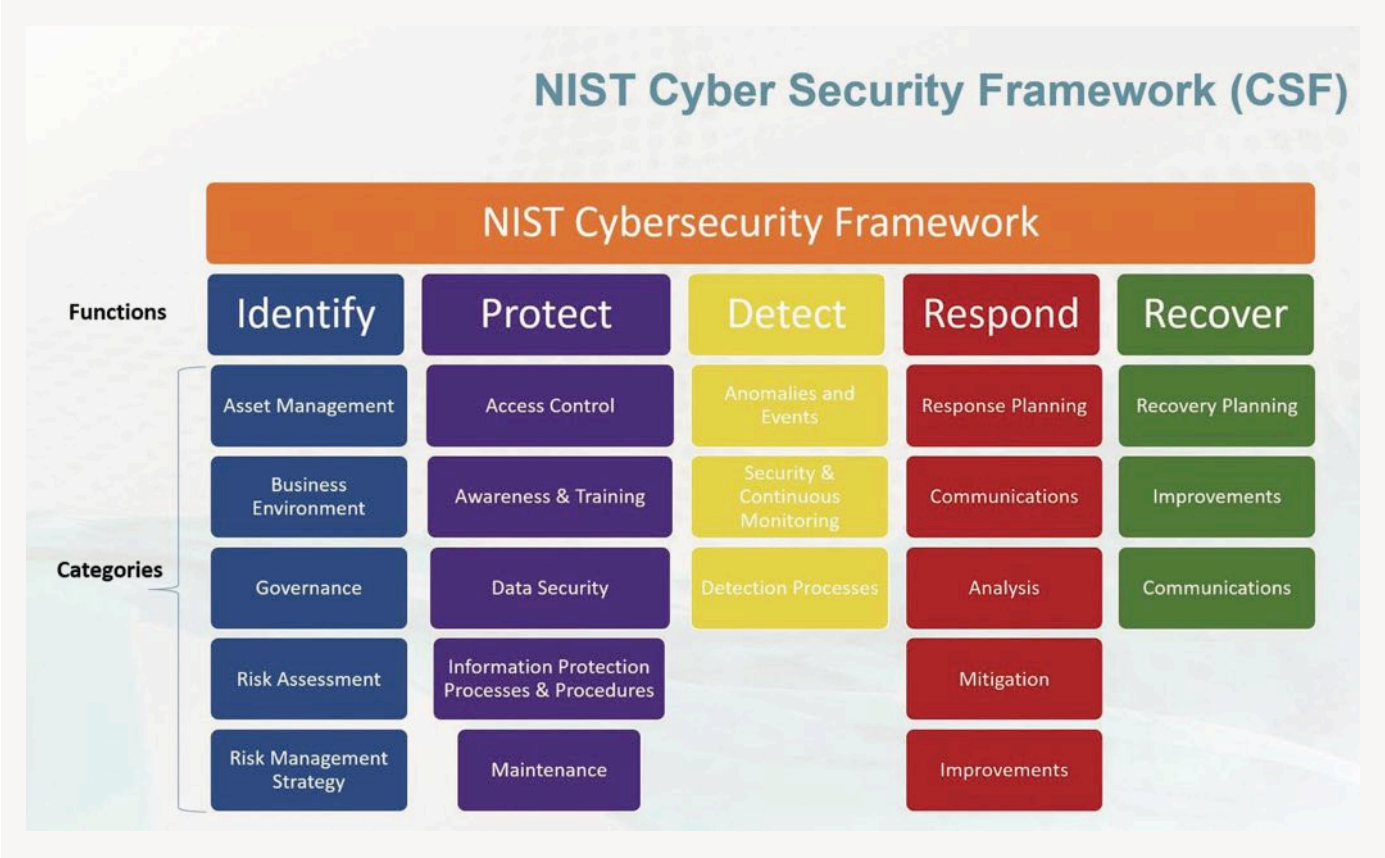
NIST e la gestione dei rischi connessi al segmento spaziale

La direttiva **NIST (National Institute of Standard and Technology) IR 8401 IPD SATELLITE GROUND SEGMENT: APPLYING THE CYBERSECURITY FRAMEWORK TO ASSURE SATELLITE COMMAND AND CONTROL [B003]**, fornisce un adeguato profilo di sicurezza cyber per il segmento spaziale delle Ground Station basandolo sul noto framework NIST a cinque funzioni come riportato in figura e oggetto di precedenti pubblicazioni specificatamente. Tale framework è stato specificatamente adattato alle infrastrutture satellitari di terra.

Il profilo di sicurezza cyber del segmento è progettato per essere utilizzato come parte di un programma di gestione del rischio per aiutare le organizzazioni a gestire rischi di sicurezza informatica per sistemi, reti e asset che costituiscono appunto il segmento satellite terrestre. Il profilo fornisce indicazioni specifiche per:

1 Classificare sistemi, processi e componenti di comando, controllo e comunicazione via satellite nonché sistemi di payload al fine di determinare la posizione esatta del rischio cyber e affrontare il rischio residuo nel modo più adeguato;

2 Definire una postura di sicurezza cyber per sistemi, processi e componenti di sistemi di comando e controllo e payload nel segmento specifico;



3 Stabilire approcci di gestione del rischio definiti e ripetibili per raggiungere uno stato di sicurezza informatica desiderato.

Si rimanda pertanto alla bibliografia specifica [B003] per ulteriori approfondimenti.

Scenari evolutivi: comunicazioni ottiche e utilizzo di laser

La crescente domanda di dati dalle missioni della NASA ha portato negli ultimi decenni a una migrazione verso bande di radiofrequenza (RF) sempre più elevate (X, K e Ka) e, infine, al regime ottico e del vicino infrarosso (near infrared). Si prevede che le comunicazioni ottiche aumenteranno la velocità dei dati di due ordini di grandezza (o più) rispetto ai tradizionali collegamenti RF. I sistemi di prossima generazione incorporeranno comunicazioni ottiche e si prevede che una serie di prime dimostrazioni di volo e usi delle comunicazioni ottiche nel prossimo decennio saranno trasformative per la NASA e altre organizzazioni spaziali. Mentre le frequenze in banda Ka arrivano fino a 40 GHz, il segnale ottico non supera la soglia dei 200.000 GHz. Frequenze più alte offrono il potenziale per enormi aumenti della velocità dei dati, teoricamente proporzionali alla frequenza al quadrato se tutti gli altri fattori sono uguali. In aggiunta alle lunghezze d'onda ottiche, devono essere considerati anche altri fattori, come disturbi atmosferici, sensibilità del ricevitore, apertura e potenza, ma ciononostante, le comunicazioni ottiche offrono il potenziale per un miglioramento di ulteriori ordini di grandezza nel throughput dei dati. Il termine «comunicazione ottica» si riferisce all'uso della luce come mezzo per la trasmissione dei dati. Per le applicazioni spaziali, i laser vengono utilizzati come sorgente luminosa. I sistemi laser con sistemi dinamici come gli specchi a guida rapida vengono utilizzati per puntare con precisione il laser sul veicolo spaziale verso il terminale di terra. Sono in fase di sviluppo anche altri metodi che utilizzano array laser per il puntamento del raggio al fine di ridurre la necessità di sistemi dinamici complessi. I dati vengono trasmessi sotto forma di centinaia di milioni di brevi impulsi di luce laser ogni secondo. La luce è costituita da fotoni e i terminali ottici di terra impostati per raccogliere la luce a livello di fotoni. Infatti, i terminali di terra sono progettati per un ambiente in cui possono essere ricevuti relativamente pochi fotoni dal veicolo spaziale trasmettitore, specialmente dallo spazio profondo. Il rilevamento diretto dei fotoni con Pulse Position Modulation (PPM) viene utilizzato al posto della comune tecnica RF della modulazione coerente della portante diretta per trasmettere informazioni. La modulazione PPM utilizza un intervallo di tempo suddiviso in un numero di possibili posizioni dell'impulso, ma solo un singolo impulso viene collocato in una delle possibili posizioni, determinate dalle informazioni trasmesse. Per rilevare segnali ottici estremamente deboli con relativamente pochi fotoni attraverso l'atmosfera, le stazioni di terra ottiche possono utilizzare un rivelatore di fotoni a nanofilo superconduttore (SNSPD), che, per aumentare la sensibilità dei nanofili, utilizza un criorefrigeratore a 1 Kelvin. Un ricevitore di elaborazione del segnale in tempo reale utilizza arrivi di fotoni con timestamp per sincronizzare, demodulare, decodificare e deinterlacciare i segnali per estrarre le parole in codice delle informazioni. Pertanto, mentre le tecnologie specifiche impiegate differiscono per alcuni aspetti da quelle utilizzate nei terminali di terra a radiofrequenza, le funzioni di livello superiore svolte dal terminale di terra per comunicazioni ottiche sono simili. La comunicazione ottica rappresenterà il nuovo orizzonte degli eventi in termini di cybersicurezza perché aprirà la strada a sistemi di crittografia quantistica e canali dati quantistici molto veloci ed efficienti inseriti dei futuri progetti di Space Management e missioni spaziali.

Bibliografia utile

[B001] Martin, P.K.: NASA Cybersecurity: An Examination of theAgency's Information Security. Testimony before the Subcommittee on Investigations and Oversight (Feb 2012). https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf. Accessed 23 May 2019

[B002] Google cloud networking incident #19020. https://status.cloud.google.com//incident/cloud-networking/19020, Accessed 24 Feb2020

[B003]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiO69em_uH7AhUCif0HHRuRCQsQFnoECC8QAQ&url=https%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2Fir%2F2022%2FNIST.IR.8401.ipd.pdf&usg=AOvVaw3uY5S4qAEyr0nH_kmA7z2i ■

Processi di attribuzione, sicurezza del cyberspazio ed equità: aspetti interrelati nell'era del web.

Intervista a Marco Ramilli.

Autore: Massimiliano Cannata

"Per attribuzione si intende un processo, molto complesso e, a volte, persistente nel tempo, assolutamente reale e percorribile, adatto a ricercare e dimostrare il coinvolgimento di un'infrastruttura, di una persona e/o di un gruppo nell'architettura e realizzazione di un evento di cybersicurezza che genera un impatto su una o più vittime".

BIO

Esperto di sicurezza Informatica, specializzato in Malware Analysis e sistemi di evasione, Marco Ramilli ha ottenuto un PhD presso l'Università degli studi di Bologna in collaborazione con l'Università della California, Davis, dove ha realizzato alcune delle principali tecniche per individuare nuove famiglie di Malware ed alla messa in sicurezza di noti sistemi di voto elettronico. Ha lavorato per il Governo degli Stati Uniti d' America, dove ha contribuito alla realizzazione dell OEVT. CyberSecurity blogger dal 2007, autore di due libri sulla sicurezza informatica e sulle metodologie di penetrazione di sistemi informatici, autore di innumerevoli articoli scientifici pubblicati su note riviste quali IEEE ed ACM. CEO e fondatore di Yoroi, una delle aziende più innovative di Cybersecurity, appartenente al Gruppo Tinexta S.p.A. dal 2020.

***Marco Ramilli**, Founder & CEO di Yoroi* ci aiuta a comprendere, nell'intervista che segue il perimetro entro cui bisogna collocare il processo di attribuzione che risulta decisivo per focalizzare la responsabilità di atti criminali che nella società del web hanno come mira le infrastrutture digitali e il cyber spazio.

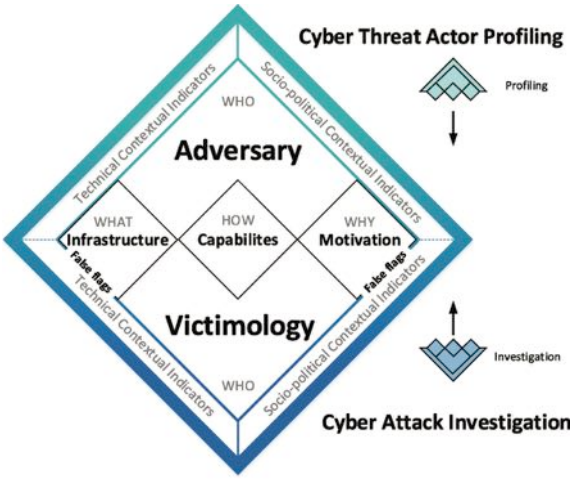
Ingegnere da dove vogliamo partire?

Un ricordo dell'infanzia credo possa aiutarci. Il classico pallone che rompe la finestra di casa, almeno una volta siamo stati nelle scarpe di chi quel pallone lo ha calciato, oppure di chi quel pallone lo ha "subito". Quante volte ci siamo trovati a giocare con amici al parco, se ripensiamo a quei momenti belli, spensierati e irripetibili possiamo avere un esempio ben chiaro di cosa significhi attribuzione.

La domanda è sempre la stessa: "chi è stato?". In altre parole, con chi posso esercitare il diritto di rivalsa (chi rimborsa il vetro rotto? per rimanere nell'immagine iniziale). Nello spazio digitale l'impatto che un attacco informatico può avere, non è mai da sottovalutare, l'esempio del pallone fa sorridere al confronto. Immaginiamo quello che può accadere nelle sale operatorie, alle pompe di insulina, alle automobili in movimento, ai sistemi di comunicazioni satellitari, ai processi che regolano i pagamenti internazionali. L'orizzonte diventa complesso e delicato, qualsiasi ironia evapora immediatamente. L'equivalente del pallone che rompe un vetro nel cyber spazio si identifica con un attacco informatico spesso dalle gravi conseguenze.

Quali strategie vanno messe in campo per individuare con ragionevole probabilità di successo gli "attentatori" della sicurezza nel cyber spazio?

Partiamo da una considerazione a mio giudizio chiave: riuscire a individuare i responsabili di un attacco o un crimine informatico è un passo fondamentale per garantire la giusta protezione secondo un criterio di giustizia in ambito digitale. Ne discende che l'impegno da dedicare a questa attività deve essere massimo. Un processo di attribuzione è un processo deduttivo che porta l'analista, sulla base di prove digitali più o meno stringenti, a dichiarare una probabilità di coinvolgimento di un sistema, di una persona o di un gruppo. Sono pertanto tre i principali livelli di attribuzione. Il primo è il livello di sistema, che vuol dire lavorare all'identificazione del sistema avversario coinvolto.



Questo livello di attribuzione è fondamentale per la corretta difesa, perché consente, per esempio, di bloccare connessioni provenienti da specifici indirizzi, oppure comunicazioni rivolte a servizi speciali o di effettuare controlli puntuali su protocolli sospetti. Il secondo livello di attribuzione riguarda il soggetto fisico che ha operativamente effettuato l'attacco. Tale livello di attribuzione è utilizzato soprattutto per mettere in atto le azioni legali contro la persona fisica a cui viene attribuita l'azione criminale. Infine, arriva l'ultimo livello che è dedicato alla comprensione del gruppo di affiliazione.

Lei parla molto di gruppi e sistemi. Non c'è mai nessuna iniziativa individuale a monte degli attacchi che sconvolgono il cyber spazio?

Difficile che il singolo abbia la motivazione e capacità tecnologica di effettuare attacchi o azioni criminali di un certo rilievo. La storia digitale ci insegna che c'è spesso la regia dei gruppi criminali, se non delle organizzazioni governative, dietro attacchi sofisticati e a grande impatto che hanno come obiettivo organizzazioni complesse.

Identificare i colpevoli certo. Un grande pensatore francese del Novecento come Michel Foucault parlava

di "Sorvegliare e punire" cosa sempre molto difficile, perché risulta sotto scacco la definizione stessa di civiltà e di progresso cui ci aggrappiamo. Il digitale amplia la sfera delle implicazioni, tanto che i nostri sistemi giuridici andranno "aumentati" come sostiene, il giurista e membro dell'Authority Guido Scorza. È d'accordo con questa visione?

Stiamo parlando di un problema di grande attualità che ha una vasta portata. Individuare uno o più attori coinvolti in un attacco ha implicazioni molto ampie. Basti pensare che i rapporti diplomatici tra vari stati subiscono influenze dal perimetro cibernetico, soprattutto dopo che il "cyber spazio" è diventato ufficialmente il quinto ambiente in cui è possibile dichiarare guerra, che va ad aggiungersi a terra, cielo, mare e spazio. Anche nella vita di tutti i giorni l'attribuzione gioca un ruolo molto importante, la deterrenza alla criminalità dimostra ampiamente in che contesto viviamo.

Ci sono sempre meno "borseggiatori" e sempre più criminali informatici come phishers, malware writers, affiliati alle *gang ransomware* che traggono maggiore beneficio in termini economici e rischiano meno di essere individuati. Favorire l'attribuzione significa fare da deterrente perché aumenta il rischio per il criminale informatico di essere individuato rendendo, in questo modo, meno vantaggiosa la sua attività. Ma gli aspetti interessanti non finiscono qui.

Prego vada avanti…

Il processo di attribuzione favorisce la nascita di nuove tecnologie, stimolando la creazione di un ecosistema e di know-how adatti a cooperare a livello internazionale per sviluppare un'azione concertata di contrasto dei cybercriminali che operano a livello globale. Questo serve a farci comprendere che pur trattandosi di un tema tecnico, non si può considerare di esclusivo appannaggio dei tecnologi di professione. In letteratura vi sono alcuni casi molto eloquenti come, per esempio, la scoperta e relativa attribuzione di APT10 (attribuito da Mandiant al governo cinese) oppure il più recente attacco all'Albania attribuito dagli USA ad un gruppo affiliato

all'Iran, che mostrano come le attività effettuate abbiano un profilo tecnico, ma esclusivamente tecnologico. I tecnici chiamati a effettuare tale attività non sono esclusivamente *malware analysts, gli incident responders e forensic investigators* ma sono anche avvocati, esperti di geo-politica, criminologi e psicologi. Le modalità di collaborazione, gli artefatti dedicati al raggiungimento di un obiettivo comune, gli strumenti utilizzati e il modo con cui si raggiunge un comune accordo sono tutti aspetti in costante evoluzione oggetto di approfondimento e di studio.

Esistono *delle best practices* di riferimento

Non esistono attualmente dei framework di riferimento, piuttosto esistono best practices che possono fare da modello. Una di queste è la cosiddetta "Malware-Infrastructure-Control server-Telemetry-Intelligence-Cui bono", un metodo spesso riferito come MICTIC.

	Aspect	Example Evidence
_M	Malware	e.g., language settings, timestamps, strings
_I	Infrastructure	e.g., WHOIS data, links to private websites
_C	Control Server	e.g., source code or logs on seized hard drives
_T	Telemetry	e.g., working hours, source IPs, malware generation
_I	Intelligence	e.g., intercepted communication
_C	Cui bono	Geopolitical analysis of strategic motivation

Il nome stesso fa capire quanto sia complesso e lungo l'intero processo di attribuzione che prevede cinque step: analisi degli artefatti coinvolti, analisi delle infrastrutture oggetto dell'attacco, analisi dei sistemi di controllo remoto, telemetria, intelligence e attività di contesto. L'analisi del Malware è molto utile per due aspetti essenziali.

Quali, possiamo esplicitarli?

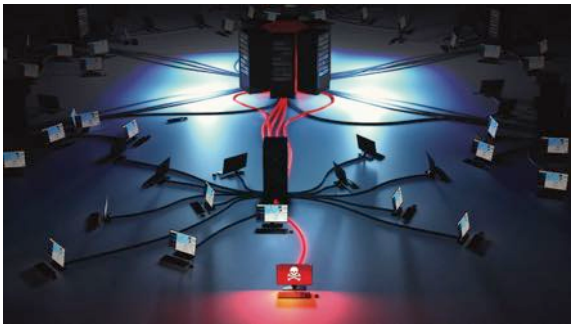
Il primo riguarda l'individuazione di possibili somiglianze con Malware già attribuiti, favorendo così un'accelerazione delle attività di investigazione; il secondo si concentra sulla raccolta delle evidenze finalizzate a tracciare i comportamenti del software malevolo, al fine di effettuare, sviluppando un percorso a ritroso, una corretta attribuzione di responsabilità.

Il processo di attribuzione può anche aiutare a individuare le fragilità e i livelli di vulnerabilità di reti e sistemi digitali?

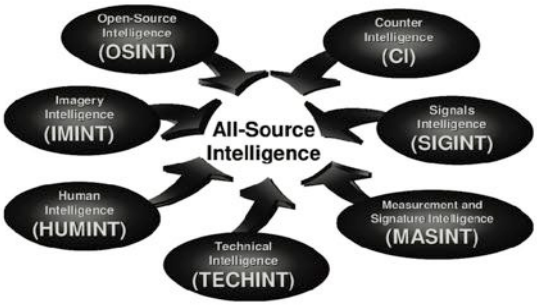
Certamente sì. Dobbiamo ricordare che l'analisi dell'infrastruttura compromessa è una attività propedeutica da un lato per avviare un'azione di *incident response*, da un altro per analizzare quali sono i movimenti favoriti da parte dell'attaccante come per esempio: quali sistemi operativi sono spesso attaccati rispetto ad altri, quali sono i servizi preferiti dell'attaccante e con quali eventuali vulnerabilità il soggetto criminale tenta la compromissione, valendosi di strumenti di *post-exploitation* e di una *"cassetta degli attrezzi"* che deve essere neutralizzata nella maniera più efficace possibile. Gli attaccanti, pur con motivazioni differenti, tendono sempre a riutilizzare la struttura di controllo e, in alcuni casi, anche quella di delivery. Pertanto, analizzare i server di comando e di controllo C2 è una attività di primaria importanza in ogni processo di attribuzione e per questo motivo tale attività è spesso inserita nei report di analisi.

La telemetria come entra in gioco, in questa dinamica volta all'accertamento dei punti deboli del cyberspazio?

La telemetria è spesso utilizzata come conferma oppure come "cartina tornasole" nei casi sempre più frequenti di "false flag", in cui l'attaccante finge di essere un altro attore malevolo. Per telemetria si intende la successione di eventi, le date di accadimento e la quantità di elementi (oggetti) presenti in un processo di attacco informatico. Molto importanti sono le attività di



intelligence che danno un maggiore valore aggiunto nel caso in cui l'attore sia totalmente sconosciuto. In questo contesto le attività di intelligence sviluppate da esperti (human int) piuttosto che provenienti da network internazionali oppure da fonti OSINT offrono un'importante direzione di analisi, ma difficilmente se non accompagnate da ulteriori evidenze riescono a concludere la probabilità di attribuzione.



Pertanto, tali informazioni sono da un lato molto rilevanti per l'orientamento di una analisi sconosciuta ma, va anche detto, sono anche molto deboli. Vi è poi un ultimo caso che vale la pena considerare.

A cosa si riferisce?

Parlo del *"Cui bono"*, che rappresenta le attività fondate sulla conoscenza politica, geo-politica, alimentare, energetica, sociale e legale utile a contestualizzare una scelta di attribuzione. In alcuni casi il contesto è il primo elemento che sentenzia una prima traccia di probabilità per definire una corretta attribuzione che in alcuni casi particolari, sebbene per molti aspetti il processo si può considerare parziale, può essere considerato sufficiente per determinare azioni di risposta che hanno una rilevanza politica, se non addirittura geostrategica. In questi giorni, durante i quali assistiamo al nefasto attacco da parte della Russia nei confronti dell'Ucraina, ci rendiamo conto delle responsabilità che una guerra comporta proprio riguardo alle questioni oggetto di questa conversazione. Se l'Ucraina, nel corso del conflitto, subisse un attacco informatico, ci sarebbe un'elevata probabilità che il mandante sia lo stato occupante. Siamo a una situazione limite, ma tremendamente reale che rende bene l'idea di cosa significa attribuzione di responsabilità nell'orizzonte della storia contemporanea. ■

I rischi del Cyber Spazio.

Autore: Giancarlo Butti

Affronteremo in questo articolo il tema del rischio nel cyber spazio e lo faremo da diversi punti di vista.

Quando si parla di come affrontare tali rischi si pensa subito alla cyber security quale disciplina per affrontarli, ma è davvero corretto?

Iniziamo con una considerazione; la definizione di cybersecurity è tutt'altro che univoca e condivisa.

Secondo l'**European Council - Council of the European Union** la cybersecurity *"includes the activities necessary to protect network and information systems, the users ofsuch systems, and other persons affected by cyber threats"*, ma differenti definizioni si ritrovano ad esempio nelle normative emesse dal resto del mondo.

FSB FINANCIAL STABILITY BOARD

Al riguardo il **Financial Stability Board**, nell'ottobre del 2017 ha pubblicato il **Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices**, nel quale sono riportate le definizioni citate nella seguente tabella:

Argentina.
"A cycle composed by 5 related and integrated information security processes: awareness, access control, integrity and register, control and monitoring, incident management".

China.
"Using of technology and management to ensure the usability, confidentiality, intactness and non-repudiation of information during collection, transit, exchange and storage. Cybersecurity includes internet security, system security and content security, which covers all levels of security, i.e. physical circumstances, internet, mainframe system, desktop system, data, application, storage, disaster back-up, security management and personnel".

Hong Kong.
"The ability to protect or defend against cyber attacks, which refer to attacks that target an institution's IT systems and networks with an aim to disrupt, disable, destroy or maliciously control an IT system/network, to destroy the integrity of the institution's data, or to steal information from it".

India.
"Measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber attack and to continue operation during, and recover from, a cyber attack".

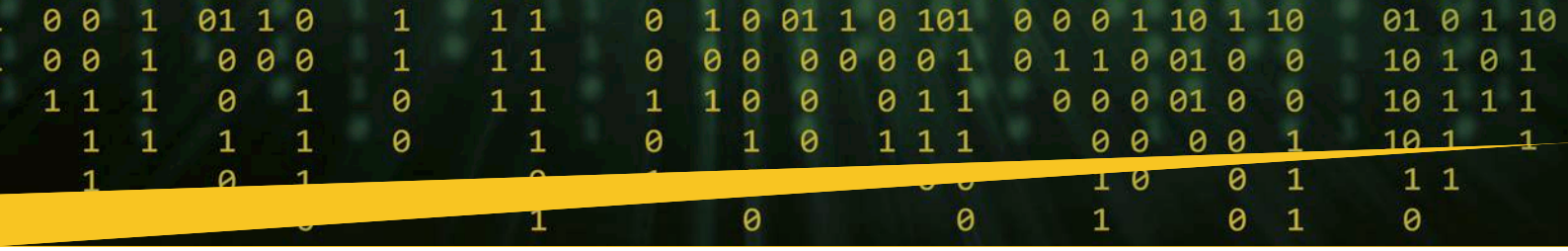
Italy.
"The set of controls and organizational measures and means (human, technical, etc.) used to protect information systems assets and communication networks against all non-physical attacks, irrespectively of the attack being initiated through a physical or logical security breach".

Saudi Arabia.
"The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats".

I rischi del cyber spazio sono primariamente quelli legati alle architetture ed alle applicazioni ICT che costituiscono l'infrastruttura su cui lo stesso si basa.

EBA | EUROPEAN BANKING AUTHORITY

Al riguardo va considerato che i rischi legati al mondo ICT non sono solo quelli legati alla sicurezza (e alcune delle precedenti definizioni vanno in questa direzione) e di questo ne dà un buon esempio **EBA**, nella sua



pubblicazione: **Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP)) (EBA/GL/2017/05)**.

Il documento riporta, ad esempio, le seguenti categorie di rischi legati all'ICT:

Rischio di disponibilità e continuità ICT

Il rischio che le prestazioni e la disponibilità dei sistemi e dei dati ICT siano influenzati negativamente, incluso il rischio di incapacità di ripristinare tempestivamente i servizi dell'ente a causa di un guasto delle componenti ICT hardware o software; debolezze nella gestione dei sistemi ICT; o qualsiasi altro evento:

- Inadeguata gestione della capacità
- Guasti dei sistemi ICT
- Inadeguatezza dei piani di ripristino in caso di disastro e della continuità dei sistemi ICT
- Attacchi informatici dirompenti e distruttivi

Rischio di sicurezza ICT

Il rischio di accesso non autorizzato ai sistemi e ai dati dei sistemi ICT dell'ente, dall'interno o dall'esterno (ad esempio nel caso di attacchi informatici):

- Attacchi informatici e altri attacchi esterni ICT
- Insufficiente sicurezza interna delle ICT
- Insufficiente sicurezza fisica ICT
- Rischio relativo ai cambiamenti ICT

Rischi relativi ai cambiamenti ICT

Il rischio derivante dall'incapacità dell'ente di gestire i cambiamenti dei sistemi ICT in modo tempestivo e controllato, in particolare per quanto concerne programmi di modifica complessi e di grandi dimensioni:

- Controlli inadeguati rispetto a cambiamenti dei sistemi ICT e sviluppo di ICT
- Architettura ICT inadeguata
- Gestione inadeguata del ciclo di vita e delle patch
- Rischio di integrità dei dati ICT

Rischi di integrità dei dati ICT

Il rischio che i dati archiviati ed elaborati dai sistemi ICT siano incompleti, inesatti o incoerenti nei vari sistemi, in seguito, ad esempio, a controlli ICT carenti o assenti durante le varie fasi del ciclo di vita dei dati ICT (vale a dire, progettazione dell'architettura dei dati, costruzione del modello e/o dei dizionari di dati, verifica degli inserimenti dei dati, controllo delle estrazioni, dei trasferimenti e delle elaborazioni dei dati, inclusi i risultati forniti), tali da compromettere la capacità di un ente di fornire servizi e di produrre le informazioni finanziarie e relative alla gestione (del rischio) in modo corretto e tempestivo:

- Trattamento o gestione inadeguati dei dati ICT
- Controlli di validazione dei dati progettati in modo inadeguato per i sistemi ICT
- Modifiche dei dati non adeguatamente controllate nei sistemi ICT in produzione

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 e 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.

- Architettura di dati, flussi di dati, modelli di dati o dizionari di dati progettati e/o gestiti in modo inadeguato

Rischio di esternalizzazione ICT

Il rischio che il ricorso a una terza parte o a un'altra entità del gruppo (esternalizzazione intra-gruppo), per la fornitura di sistemi ICT o servizi connessi incida negativamente sulle prestazioni e sulla gestione del rischio dell'ente:

- Resilienza insufficiente di servizi di terzi o di altri enti del gruppo
- Organizzazione inadeguata dell'esternalizzazione
- Insufficiente sicurezza di terzi o altri enti del gruppo

Che i rischi ICT non siano solo quelli legati alla sicurezza appare chiaro anche in base alle definizioni degli incidenti in ambito ICT; ad esempio, sempre **EBA**, nel suo documento **Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza** ne dà la seguente definizione:

▸ ***Incidente operativo o di sicurezza***

"Singolo evento o serie di eventi collegati, non pianificati dall'istituto finanziario, che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi."

La definizione evidenzia chiaramente che gli incidenti ICT possono essere sia operativi sia di sicurezza.

Ancor più incisiva è inoltre la definizione di **ITIL 3** che definisce un incidente come:

"Un'interruzione non pianificata di un servizio IT o una riduzione della qualità di un servizio IT. Anche il malfunzionamento di un elemento della configurazione che non ha ancora impattato un servizio viene considerato un incident. Per esempio il malfunzionamento di un disco in un set di dischi mirrorati" che ben evidenzia come anche la riduzione della qualità di un servizio debba essere considerata un incidente ICT. Al riguardo, ad esempio, è sufficiente considerare come l'allungamento dei tempi di risposta di un portale di e-commerce possa renderlo non fruibile e portare un utente/cliente ad abbandonare il sito.

Ulteriori considerazioni possono essere fatte in merito al fatto che l'immaterialità del cyber space è basata su strutture fisiche; di fatto qualunque asset immateriale necessità per la sua esistenza di un asset materiale che lo supporti, fosse anche la mente di una persona fisica.

Ecco quindi che fra i rischi che interessano l'immateriale cyber space troviamo tutti quelli che possono impattare fisicamente l'infrastruttura che lo supportano.

È importante avere una chiara visione di tutti gli aspetti sopra citati in quanto una esaustiva valutazione dei rischi non può ignorarli; una classica analisi dei rischi che prenda in considerazione solo aspetti quali l'integrità, la disponibilità e la riservatezza è fortemente deficitaria.

Prendiamo ora in considerazione un ulteriore punto di vista; quali sono gli ambiti che possono subire conseguenze da un incidente al cyber spazio secondo quanto fin qui illustrato?

Il primo e più intuitivo è sicuramente quello che interessa gli asset aziendali ed i servizi dell'azienda ad esso collegati.

Ma ci sono anche altri ambiti da considerare; ad esempio i rischi di soggetti terzi rispetto all'azienda, in particolare i rischi per i diritti e le libertà delle persone

fisiche e dei soggetti di cui l'azienda tratta i dati ai sensi della normativa privacy.

In termini aziendali, tali rischi si possono tradurre in rischio risarcitorio e rischio sanzionatorio nel caso che un incidente comporti ad esempio una violazione dei dati personali. Per questo specifico ambito quindi è possibile considerare due diversi tipi di approccio: uno dal punto di vista del soggetto che può subire un danno e un altro dal punto di vista delle conseguenze per l'azienda derivate dal precedente.

Un ulteriore ambito da considerare riguarda i rischi, sempre più rilevanti, così detti di terza e quarta parte, cioè quelli derivanti dal ricorso a fornitori terzi (fornitori o sub fornitori), molto spesso tramite soluzioni cloud.

La valutazione del rischio aziendale complessivo deve quindi prendere in considerazione tutti questi ambiti perché solo una valutazione esaustiva potrà consentire una corretta valutazione dei costi/benefici delle misure tecniche ed organizzative messe in atto per fronteggiare il rischio.

In sintesi quindi, quando si parla di rischi del cyber spazio è necessario avere una visione molto più ampia di quanto si è soliti affrontare in termini di cyber security. ■

La Cyber Threat Intelligence e l'Information Sharing quale "game changer" nei conflitti e nelle offensive cibernetiche.

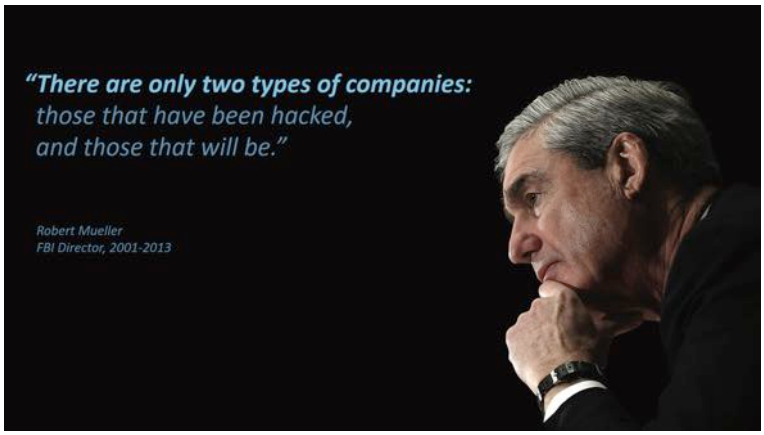
Autore: Emanuele Gentili

La romantica immagine del "fortino" circondato da un fossato con coccodrilli ed un ponte levatoio quale unica strategia difensiva è un qualcosa di non molto lontano da quello che diverse organizzazioni applicano come propria strategia di sicurezza cibernetica. Un approccio sicuramente "low budget", ma decisamente rischioso e poco efficace.

BIO

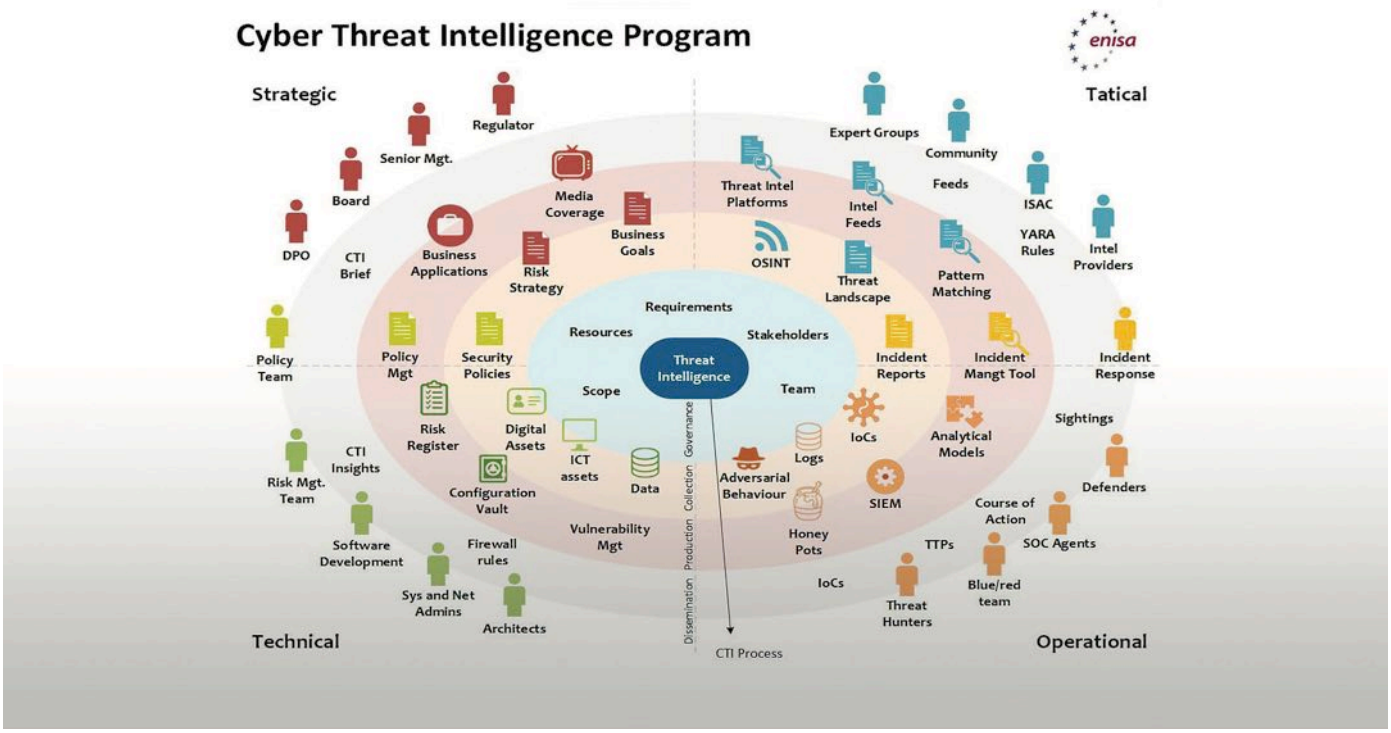
Fondatore e SVP of Threat Intelligence in TS-WAY, ha maturato una lunga esperienza nell'analisi e nell'identificazione di minacce cibernetiche complesse. Advisor di realtà pubbliche e private, è Co-Direttore delle Iniziative di Cyber Security della Fondazione ICSA, membro del consiglio direttivo della 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.

Le offensive cibernetiche, se opportunamente finanziate e progettate, sono in grado di paralizzare servizi digitali, organizzazioni ed in alcuni casi anche intere nazioni. Tra gli addetti ai lavori nel campo della sicurezza cibernetica, esiste un aneddoto che recita più o meno così: "esistono due tipi di organizzazioni: quelle che sono state compromesse e quelle che ancora non lo sanno".



La sfida reale per le aziende e gli enti pubblici è quella di porre in campo le migliori soluzioni e processi di prevenzione per rendere il costo dell'attacco cibernetico particolarmente alto a chi lo effettua da un lato e dall'altro svolgere attività di monitoraggio dei propri sistemi ed infrastrutture tecnologiche per identificare, nel minor tempo possibile, di essere diventate target e di aver avuto un problema di sicurezza a cui dover immediatamente rispondere.

In questo contesto la Cyber Threat Intelligence (CTI) e la condivisione di informazioni provenienti da questa disciplina giocano un ruolo chiave. Non è un caso che colossi come Google, Microsoft ed Amazon abbiano investito pesantemente negli ultimi anni in questi settori sia per finalità di protezione

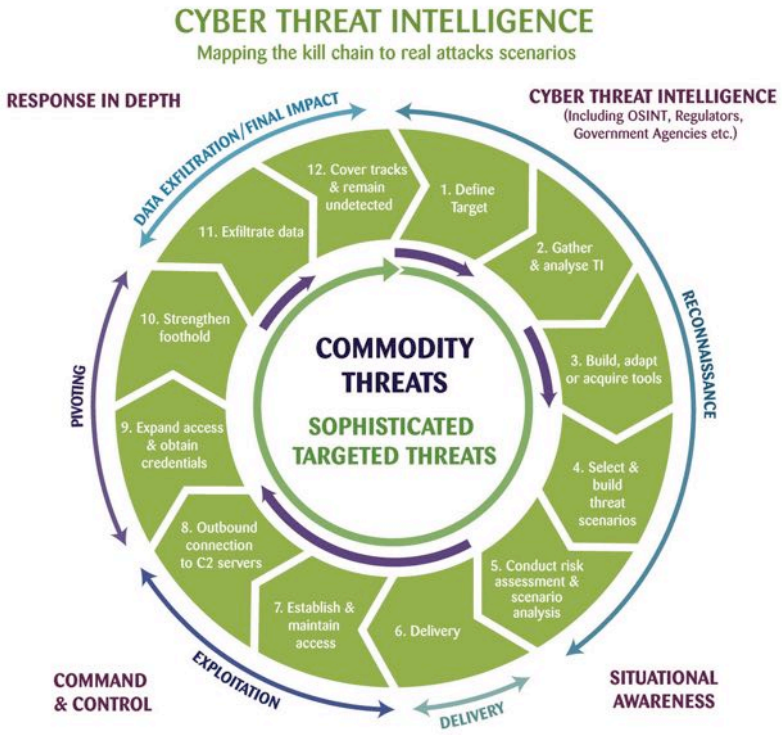


interna ma anche per sviluppare modelli di protezione per i propri clienti finali.

La CTI è una disciplina molto complessa ed articolata che si occupa di analizzare dati provenienti da molteplici fonti per produrre informazioni strutturate di intelligence che possono essere di tipo Strategico, Tattico ed Operativo. Tali informazioni, dipendentemente dalla loro natura, concorrono nel rendere gli strumenti difensivi capaci di riconoscere minacce cibernetiche che possono avere impatto sul proprio perimetro digitale e nel supportare le decisioni degli stakeholder, rappresentando un vero e proprio "game changer".

Lo ha sostenuto pubblicamente anche il Segretario Generale della NATO, Jens Stoltenberg, nel suo discorso alla NATO Cyber Defence Pledge Conference 2022 che si è tenuto recentemente alla Farnesina, comunicando che: "l'Ucraina ha accesso alla piattaforma di condivisione delle minacce cibernetiche della NATO dove esperti condividono informazioni sulle minacce in tempo reale".

Grazie alla Cyber Threat Intelligence e alle azioni di information sharing il Computer Emergency Response Team (CERT) del governo ucraino è riuscito a disinnescare il sabotaggio per mano cibernetica di alcune sub-centrali elettriche in Ucraina, perpetrato dall'unità dei servizi di intelligence militare di Mosca conosciuta come Sandworm, spingendo la Russia a cambiare strategia ed utilizzare i tradizionali armamenti cinetici per mettere fuori uso le infrastrutture energetiche e di approvvigionamento idrico, non essendoci spazio per agevoli incursioni digitali.



La compagine istituzionale italiana sul tema dell'information sharing è particolarmente proiettata in avanti, da diversi anni questo tipo di azione viene svolta dal CNAIPIC della Polizia Postale e delle Comunicazioni che ha fatto di questo tema uno dei suoi punti fermi a supporto delle attività di prevenzione. Strada poi intrapresa più recentemente anche dal CERT di AGID ed in modo più strutturato dallo CSIRT Italia, della neonata Agenzia per la Cybersicurezza Nazionale.

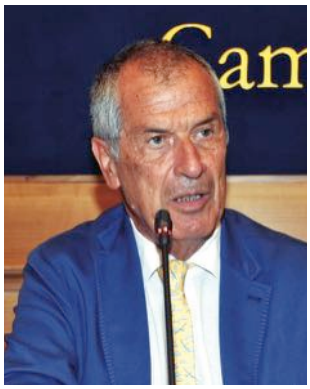
Le informazioni di intelligence sulle minacce, se prodotte in modo puntuale e condivise in tempo reale permettono di prevenire compromissioni, individuarle quando già presenti ed attribuire le offensive. Tutto questo a patto che il ricevente abbia una infrastruttura tecnologica di sicurezza moderna in grado di utilizzare il dato e renderlo operativo nel minor tempo possibile.

Il processo di evoluzione nazionale sui temi della Cybersicurezza, trainato dal Perimetro di Sicurezza Cibernetica ma anche dal GDPR e dalle ulteriori normative di carattere europeo che l'Italia si sta apprestando a ratificare, mostra un'importante rincorsa all'ammodernamento tecnologico ed un fondamentale inserimento di risorse umane specializzate da parte delle così dette "infrastrutture critiche" e dei grandi player privati. Un processo ormai vitale da cui non si può più tornare indietro che vedrà progressivamente, nei prossimi cinque anni, un aumento del livello di sicurezza delle infrastrutture informatiche nazionali da un lato e una crescita esponenziale del costo, in termini di skills e strumenti, per chi invece effettua attacchi informatici.

Fenomeno non ancora presente e/o visibile nel tessuto delle Piccole e Medie Imprese. Tuttavia, considerando anche il recente progetto di creazione dei CERT regionali e l'impegno dei grandi gruppi industriali nel far evolvere la postura di sicurezza della propria supply chain, è plausibile ed auspicabile pensare che quanto osservato sulle primarie aziende ed istituzioni nazionali possa "rimbalzare", se pur con le dovute proporzioni, anche su questo importante segmento solo apparentemente periferico e secondario. ■

Finito il tempo delle deleghe: l'Europa deve riprendere in mano la *governance* della sua sicurezza.

Intervista VIP al Generale Leonardo Tricarico.



Autore: Massimiliano Cannata

Il Generale Leonardo Tricarico, Presidente della Fondazione ICSA, nell'intervista che ha concesso al nostro periodico affronta il delicato binomio: guerra e tecnologie, nel contesto della crisi geopolitica generata dal conflitto in Ucraina, che sembra aver riportato l'orologio della storia indietro nel tempo, quando l'Europa era il campo di battaglia attraversato da spinte egemoniche e dalla sete di conquista.

Generale Tricarico, "la Rete - scrive Michele Mezza (cfr. recensioni di questo numero n.d.r) - rientra nella logistica dei conflitti moderni". In che misura le tecnologie digitali stanno cambiando il modo di fare la guerra?

Lo strumento militare è sempre accompagnato, passo dopo passo, dalla tecnologia. Se guardiamo all'attualità quella digitale, un esempio su tutti il caccia di 5a generazione F35, non si tratta più di un velivolo ma di un sistema net centrico volante. I pur moderni caccia che lo hanno preceduto, *Eurofighter* e simili hanno 8/900 mila linee di software, il caccia F35 dieci volte tanto e più. L'integrazione del software è stata l'impresa più ardua nello sviluppo del sistema. Il suo utilizzo odierno è legato alla capacità di sfruttare le potenzialità praticamente illimitate di inserirsi negli scenari bellici. La sua superiorità, si potrebbe dire il suo dominio degli spazi aerei, è fuori discussione.

Reale e virtuale si mescolano, lo stesso campo di battaglia è un campo ibrido, come si sta vedendo nel conflitto in Ucraina, che rende difficile una lettura di fatti ed eventi. L'azione militare non deve presidiare solo un fronte fisico, ma anche il cyber spazio. Quali scenari si aprono dal

punto di vista della sicurezza globale e degli esiti militari del conflitto in Ucraina?

Anche in questo caso può aiutarci un esempio illuminante. La Russia, forse in seguito a un mutamento di dottrina, ha posto tra gli obiettivi primari quello delle fonti di energia elettrica. Già in tempi non sospetti aveva lasciato al buio l'Ucraina sferrando un attacco informatico senza eccessive difficoltà. Oggi questo non gli è possibile grazie all'intervento dei big del web statunitensi che hanno accolto le richieste di aiuto ucraine e si sono mobilitate per presidiare l'infrastruttura critica dagli attacchi russi. Con il risultato che questi ultimi debbono fare con i missili e le bombe quello che non sono riusciti a fare con il web. Per quanto riguarda le possibili capacità risolutive del cyber, pare di assistere, come da sempre avviene nell'orizzonte convenzionale, a un sostanziale inceppamento della macchina bellica.

La Comunicazione sta cambiando la guerra. Si combatte anche sul fronte dell'informazione, dei contenuti, dei saperi, delle conoscenze. Dobbiamo concludere che oggi vince chi possiede il know-how ed è capace di presidiare le fonti dell'informazione e di regolare il flusso delle notizie?

La guerra non si vince solo con le informazioni, anche se sono d'accordo sul fatto che va presidiato un ambito che si è certamente evoluto negli ultimi anni, ma che da solo non può essere considerato risolutivo. Il dominio delle informazioni va presidiato più di quanto non si facesse in passato e questa è una delle principali lezioni che il conflitto russo-ucraino ha fornito alla dottrina militare.

BIO

Presidente della Fondazione ICSA (Intelligence Culture and Strategic Analysis). Generale di Squadra Aerea (r), già Capo di Stato Maggiore dell'Aeronautica Militare (2004-2006), già Consigliere Militare dei Presidenti del Consiglio D'Alema II (1999-2000), Amato II (2000-2001) e Berlusconi II (2001-2004), Comandante della 5^ Forza Aerea Tattica Alleata della NATO e Vice Comandante della Forza Multinazionale nel conflitto dei Balcani (1999). Durante il governo Berlusconi, è stato presidente del Nucleo Politico Militare (Unità di Crisi), presidente del Comitato di Coordinamento Interministeriale per la Sicurezza dei Trasporti e delle Infrastrutture (COCIST) e presidente del Gruppo di Lavoro Interministeriale per il Coordinamento delle Esportazioni dei Materiali per la Difesa (GLICED).In carriera ha svolto numerosi incarichi e missioni in Italia e all'estero, maturando la propria esperienza di pilota esclusivamente su velivoli monoposto da caccia e da addestramento e totalizzando complessivamente oltre 3000 ore di volo.

Sul fronte ucraino si combattono più conflitti: uno di stile ottocentesco che mira alla conquista dei territori; un altro fondato sull'uso di droni, smartphone, Google, sistemi satellitari per la georeferenziazione, che risponde a una logica di alta sofisticazione tecnologica. Per quale ragione nell'era della disintermediazione e della "fine dei territori", per usare una celebre definizione di Bertand Badie, si può condurre una guerra di conquista come quella innescata da Putin?

In Ucraina tutte le regole sono saltate, comprese quelle su cui si fonda il nostro stare insieme militarmente, col termine nostro mi riferisco alla cultura occidentale. Questo è il più preoccupante cruccio che non sembra affliggere più di tanto i decisori dell'una e dell'altra parte, mentre invece è il vero centro di gravità della vicenda. Tutto questo è preoccupante perché in assenza di regole tutto può succedere. Scendendo in concreto: la Russia, più che una guerra ottocentesca sta conducendo una guerra primordiale per la quale dovrà rispondere alla giustizia, ancora una volta quella contemplata dalle regole che ci siamo dati e non certo da tribunali da istituire ad hoc. Il lavoro da fare oggi quindi, più che contemperare due anime, due diverse interpretazioni dell'uso della forza, è quello di una riflessione generale sul come fermare la valanga che si sta ingigantendo e sulle strategie da mettere in atto per fermarla. Creare le

condizioni per evitare il ripetersi di scenari fuori controllo risulterà decisivo. Si tratta di un compito arduo anche per la multipolarità della governance internazionale e l'inadeguatezza dei "fori" che dovrebbero fare da punto di riferimento del confronto. Penso prima di tutto all'ONU.

Emergenza è divenuta la parola chiave di questo tempo di crisi, come osserva Alessandro Colombo nel saggio:* Il governo mondiale dell'emergenza *(ed. Raffaello Cortina). Si è passati, sostiene lo studioso, dall'apoteosi della sicurezza alla epidemia dell'insicurezza generata da una molteplicità di fattori di instabilità che segnano la contemporaneità, in un generale pericoloso declino della democrazia liberale. Come se non bastasse la "rivoluzione digitale" sta modificando la geografia dei poteri, per cui la geopolitica ha mutato il suo profilo di disciplina scientifica. Quali strategie bisognerà adottare per riaffermare la sicurezza come valore condiviso in un orizzonte che garantisca i diritti e le libertà fondamentali dell'individuo?

La sicurezza continuerà a essere uno strumento nelle mani del più forte. Chi ha l'egemonia manipola, ieri come oggi, interventi e azioni di contrasto, reinterpretando persino il campo dei diritti, delle regole e la definizione dei trattati secondo le convenienze del momento.

Credo sia venuto il momento di "riprendere la delega" dagli Stati Uniti e riprendere in mano la gestione della nostra sicurezza. Il destino dei nostri paesi, e dei nostri interessi, non può più essere affidato ad altri. Purtroppo, ho l'impressione che neppure la tragedia in Ucraina sia uno stimolo sufficiente per intraprendere con sollecitudine un percorso di edificazione per un sistema di sicurezza autenticamente europeo, abbandonando definitivamente pretesti, ipocrisie e alibi di qualsiasi tipo. ■

Diritto e tecnica nella difesa del Cyber spazio.

Intervista VIP con Pasquale Stanzione, Presidente dell'Autorità Garante per la Protezione dei Dati Personali.

Autore: Massimiliano Cannata

"Nel rapporto tra diritto e tecnica, il vero rischio per il primo è quello dell'anacronismo, tutte le volte in cui pretende di rincorrere un'evoluzione troppo incessante, preferendo le regole ai principi. Mai come nella normazione della tecnica è, invece, necessario restituire al diritto la sua dimensione assiologica cui troppo spesso tende a rinunciare, governando l'innovazione secondo la gerarchia di valori che si riflette nelle Costituzioni e nei principi supremi di ogni ordinamento. Soltanto essi, infatti, garantiscono alla norma la duttilità e lungimiranza necessarie a disciplinare una realtà, quale quella attuale, in costante evoluzione. Di qui l'importanza di quelle clausole generali non a caso valorizzate da Stefano Rodotà, quali elementi di flessibilità e di "apertura" di un sistema normativo che deve essere capace di "dialogare" con l'evoluzione della società".

Pasquale Stanzione, insigne giurista e Presidente dell'Autorità Garante per la protezione dei dati personali, affronta il tema della sicurezza del Cyber Spazio tratteggiando gli scenari evolutivi della scienza giuridica in materia di governo della tecnologia, in una società che ormai "vive" la rete in una dimensione omeopatica.

Presidente, la rivoluzione tecnologica ha modificato i concetti di vulnerabilità e rischio. Con quali conseguenze sul piano di una corretta governance della sicurezza?

L'affermarsi della rivoluzione tecnologica conferisce alla privacy una grande forza che risiede nella duttilità e neutralità tecnologica. La sua disciplina è stata pensata e costruita in modo da essere "future-proof", resistente all'usura del tempo, potendo adeguarsi con la flessibilità dei

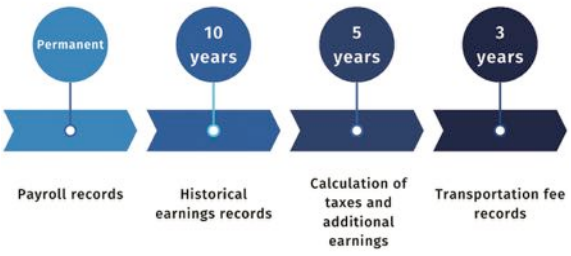
BIO

Pasquale Stanzione, Presidente Autorità Garante per la protezione dei dati personali, Cavaliere di Gran Croce all'Ordine "Al merito" della Repubblica Italiana, è stato professore ordinario di Istituzioni di Diritto Privato presso la facoltà di Giurisprudenza dell'Università degli Studi di Salerno dal 1984 ad oggi. Consigliere della Banca d'Italia a Salerno e Giudice tributario presso la Commissione tributaria provinciale.

principi a contesti diversi. Grazie a questa sinergia, la disciplina della *privacy* sarà in grado di governare il passaggio verso le nuove frontiere della società digitale e i rischi, anche in termini di sicurezza, che ne derivano.

Il Cyber spazio è la nuova frontiera da difendere. Con quelli che vengono definiti "processi di attribuzione" si sta cercando di mappare gli autori dei reati e i cyber criminali. Sul piano della sicurezza delle informazioni questa metodologia quali conseguenze comporta?

L'individuazione degli autori di un reato *on line* è un processo che comporta indagini e tecniche investigative mediamente più complesse di quelle proprie della criminalità comune, se non altro per le possibilità di dissimulazione consentite dalla dimensione virtuale. A queste difficoltà deve perciò corrispondere una (almeno potenziale) maggiore invasività delle tecniche investigative, oltre che una necessità, spesso, di collaborazione delle piattaforme la cui complessità è stata ben evidenziata nel corso dell'esame della disciplina europea sulle prove elettroniche. La tensione che può derivarne sotto il profilo della protezione dati va governata secondo il canone di proporzionalità che deve regolare, secondo la Carta di Nizza, ogni limitazione dei diritti fondamentali. Su questo criterio si fonda, per altro, una giurisprudenza particolarmente lungimirante della Corte di giustizia, in tema proprio di *data retention*.



Nella sua relazione annuale ha sottolineato il delicato rapporto che si deve instaurare per temperare* rule of technology *e* rule of law *mentre si fa sempre più evidente il processo di "datificazione della vita individuale e collettiva". Le organizzazioni produttive sono pronte a recepire questo suo messaggio, che va certamente oltre la mera logica dell'adempimento?

Vi è una vulnerabilità che caratterizza ciascuno di noi nel rapporto con la tecnica e che è imputabile al rischio di esserne dominati, anziché di dominarla, per effetto di meccanismi che non comprendiamo fino in fondo o della facilità con cui cediamo frammenti di noi (e quindi anche della nostra libertà) in cambio di servizi on line o poco più. Dobbiamo superare questo rischio con una vera e propria *paideia*: una formazione complessiva di tutti, nativi digitali o meno, singoli ed enti, soggetti privati e pubblici, tale da fornire a ciascuno le coordinate essenziali per orientarsi consapevolmente in una dimensione, quale quella virtuale, che ormai ci assorbe sempre più. Per questo la logica del mero adempimento non basta più: serve un investimento culturale sul digitale che renda ciascuno attore consapevole del proprio essere "on-life" (per riprendere la definizione di Floridi).

Anche sotto questo profilo, la disciplina di protezione dati è stata particolarmente lungimirante, valorizzando il criterio della responsabilizzazione proprio per sganciare l'osservanza della norma dalla logica del mero assolvimento dell'obbligo, in favore di una prospettiva più costruttiva quale quella *dell'accountability*.

Come governare il potere delle piattaforme

Il recente Rapporto sull'Internet Society ha denunciato lo strapotere delle piattaforme digitali coniando la definizione di* total service envinonments. *Lei ha curato una interessante raccolta di saggi: "I poteri privati delle piattaforme e le nuove frontiere della privacy" (ed. Giappichelli). Questa nuova forma di capitalismo centrato proprio sulle piattaforme è un rischio per la libertà democratica?

Il controllo della rete garantisce alle piattaforme un potere di condizionamento che nessun mezzo di comunicazione di massa poteva avere prima, che si risolve nella capacità di orientare l'opinione pubblica agendo con la formidabile leva della profilazione, così da proporre non solo pubblicità ma persino informazione mirata e, quindi, più persuasiva. Questa capacità di condizionamento può avere effetti determinanti non solo sulle scelte individuali ma anche su quelle più determinanti per la democrazia quali quelle politico-elettorali. Come ha dimostrato il caso Cambridge Analytica, infatti, con il microtargeting si modella il messaggio politico da promuovere, orientando il consenso elettorale verso il risultato voluto. Si eludono così le garanzie previste da decenni per il pluralismo informativo e politico, come pure per l'autodeterminazione individuale, con il rischio di una manipolazione del consenso, tale da alterare dalla radice i più rilevanti processi democratici.

Che tipo di* compliance *giuridica va adottata per limitare il potere dei "gigacapitalisti" che questi strumenti controllano?

Bisogna pensare che la diffusione pervasiva delle tecnologie digitali che controllano e condizionano i comportamenti della collettività può persino pregiudicare l'altrimenti intangibile sovranità statuale, ogniqualvolta la manipolazione del consenso sia organizzata da governi stranieri, così da orientare il risultato elettorale verso la soluzione a loro più favorevole. La prospettiva, sottesa al Digital Services Act, della responsabilizzazione delle piattaforme e dell'imposizione di obblighi di trasparenza verso gli utenti è certamente la strada giusta da percorrere nella direzione di un governo sostenibile della rete.

La via europea al digitale

La via europea al digitale è l'orizzonte di riferimento imprescindibile per attuare una sicurezza che non si può più misurare su un recinto fisico - spaziale definito. L'Artificial Intelligence act, nel cui ambito il GDPR svolge un ruolo centrale, e il Digital Service Act ritiene che possano aprire una nuova dimensione della compliance?

Dal GDPR in poi, passando per il Data Governance Act, l'Artificial Intelligence Act e, appunto, il Digital Services (e Markets) Act, l'Europa ha investito sulla governance del digitale quale tema centrale e prioritario nell'agenda politica, dalla valenza fortemente identitaria. Nella competizione sino-americana per la primazia sul digitale, l'Europa ha infatti progressivamente affermato, anche attraverso queste discipline, una propria egemonia "culturale" volta a promuovere un governo antropocentrico e democraticamente sostenibile dell'innovazione.

È sbagliato sostenere che ci stiamo avvicinando a definire quella Costituzione per Internet, per cui tanto si era speso in passato Stefano Rodotà?

Questo, pur articolato, tessuto normativo non ha certamente la portata (e la stessa vocazione universalistica) di quella Costituzione per Internet invocata, con la consueta lungimiranza, di Stefano Rodotà, ma ne condivide certamente i valori di fondo. Proprio i principi di trasparenza e responsabilizzazione sono i cardini attorno ai quali si sviluppano tanto l'AIA quanto il DSA, rilevanti in termini non solo regolatori ma anche e soprattutto valoriali. Essi esprimono, infatti, l'esigenza di rimodulare il perimetro del tecnicamente possibile sulla base di ciò che si ritiene giuridicamente ed eticamente accettabile, temperando - come è stato detto- l'algocrazia con l'algoretica e responsabilizzando gli attori principali del capitalismo della sorveglianza.

La protezione dei dati ha delle ricadute sugli equilibri geopolitici. Cina, Stati Uniti e Europa stanno discutendo della possibile definizione di una "sovranità digitale". Di che cosa si tratta in concreto e quale apporto dovranno dare i Garanti a livello europeo in questa difficile e complessa partita?

Della sovranità digitale si possono, ovviamente, dare varie letture. Ve n'è una più minimalista, ma anche pragmatica, che enfatizza l'esigenza di indipendenza nazionale nella fornitura, gestione e finanche negli stessi assetti proprietari delle infrastrutture tecnologiche. È il tema che ricorre spesso a fronte dei casi di acquisizione, da parte di aziende straniere, del controllo societario rispetto ad asset strategici. Questa declinazione "materialistica" della sovranità nazionale coglie, senza dubbio, la rilevanza del rapporto tra **l'assetto dominicale delle tecnologie e la loro funzionalità** anche in termini democratici, sottolineando l'esigenza di una *governance* non soltanto interna (non straniera) ma, soprattutto, pubblica delle principali infrastrutture digitali. Vi è poi è una **diversa accezione di sovranità digitale, declinata in chiave valoriale**, intesa come **governo della tecnica secondo la gerarchia assiologica espressa da ciascun ordinamento**, conformemente alla sua identità e tradizione costituzionale. È significativo che l'UE abbia ritrovato, in particolare sul terreno del governo antropocentrico della tecnica, un'unità smarrita da tempo in molti altri settori, riaffermando la propria identità come ordinamento fondato su alcuni, irrinunciabili, valori.

La protezione dei dati fattore determinante della geopolitica

"L'algoritmo d'oro" per usare la definizione del presidente emerito della Corte Costituzionale Giovanni Maria Flick è divenuto il nuovo vitello d'oro, il cui uso distorto rischia di attuare una "colonizzazione del pensiero", incidendo sulla libertà cognitiva, non solo sulla circolazione di dati e informazioni sensibili. Abbiamo strumenti efficaci per contrastare questa deriva?

Il capitalismo delle piattaforme è stato definito, anche, il capitalismo della sorveglianza, proprio perché fondato sul pedinamento digitale dell'attività in rete degli utenti e sulla modulazione dell'offerta resa possibile dalla profilazione predittiva. Ne risulta insidiata, sotto molti profili, la libertà di autodeterminazione, in un contesto che è stato significativamente definito "società dell'"anticipazione", per il pervasivo ricorso ad algoritmi capaci di prevedere il comportamento di ciascuno, ridotto a mero elemento di un cluster. La strategia di contrasto degli effetti più negativi, anche sotto il profilo antropologico e sociale, di questo fenomeno, non può che essere articolata. Da un lato è necessario temperare lo stra-potere delle piattaforme con obblighi di trasparenza e una complessiva responsabilizzazione, come prevedono il Digital Services e il Digital Markets Act.

Dall'altro lato, è necessaria una strategia di autotutela individuale, fondata sulla gestione consapevole dei propri dati, sul rilascio ponderato dei consensi al trattamento e sulla massima attenzione all'atto della diffusione in rete (e soprattutto sui social) di informazioni relative a sé stessi o, a più forte ragione, a terzi.

Culture giuridiche profondamente diverse, come quella americana ed europea, specie in fatto di privacy, riusciranno a dialogare per definire delle linee di governo e di sviluppo della trasformazione tecnologica, condivise e soprattutto rispettose delle libertà civili e dei diritti fondamentali conquistati dopo secoli di lotte?

Il GDPR ha rappresentato la prima effettiva, organica regolazione del digitale, che non a caso viene assunta a paradigma in molti altri Paesi (effetto Bruxelles) tra i quali, da ultimo, la Cina.

La disciplina europea appare infatti, sempre più, un modello equo di bilanciamento tra le esigenze di tutela della persona e di libera circolazione dei dati. Del resto, la temperata extraterritorialità della sua disciplina (che si applica anche a titolari esteri) comporta, di fatto, un'uniformazione delle garanzie a livello globale, come dimostra la vicenda delle sentenze Schrems e dei successivi accordi con gli Usa. Ecco anche perché la protezione dei dati assurge sempre più a fattore determinante della geopolitica, in un contesto di progressiva omogeneizzazione non soltanto delle norme sulla protezione dei dati personali, ma anche della "cultura" che ne costituisce il fondamento. ■

Una società "senza", quasta è l'Italia post populista.

Intervista VIP a Massimiliano Valerii, Direttore Generale CENSIS.

Autore: Massimiliano Cannata

Il 56° Rapporto Censis* sulla situazione sociale del Paese *ha tratteggiato un'Italia malinconica, che vive "imprigionata" - ha commentato il Segretario Generale Giorgio De Rita – in un "tempo di latenza". Direttore quali scenari si aprono in una situazione sociale segnata da incertezza e paure?

L'elemento di discontinuità rispetto al recente passato è la sensazione, che si è sedimentata nell'immaginario collettivo, di essere esposti a rischi globali fuori dal nostro controllo. Il 61% degli italiani teme un terzo conflitto mondiale, il 59% ha paura che si possa fare ricorso alla bomba atomica, il 58% teme che l'Italia possa entrare in guerra. Siamo, in effetti, al termine di un triennio segnato da emergenze globali, i cui effetti si sono sovrapposti alle nostre vulnerabilità economiche e sociali strutturali, di lungo periodo: la pandemia perdurante, benché in forma attenuata, la guerra cruenta scoppiata alle porte dell'Europa, l'inflazione a due cifre (come non si registrava nel nostro Paese da quattro decenni) e la morsa energetica, con il paventato rischio di un razionamento delle forniture.

L'irruzione dei grandi eventi della storia, che si è rimessa in moto, sulle microstorie delle nostre vite individuali ci fa riscoprire più fragili e, almeno in questo momento, poco disposti a fare ulteriori sacrifici per essere migliori.

I gravi fattori di contesto che Lei ha richiamato nel corso della presentazione del Rapporto, dalla guerra in Ucraina, alla pandemia, dall'ottovolante dell'inflazione al caro energia, hanno determinato il crepuscolo dell'antropocentrismo come modus vivendi. Con quali conseguenze?

Oggi si sta affermando un riconosciuto primato della sostenibilità ambientale e l'ecologismo diventa il nuovo paradigma della cultura collettiva. Sono cambiamenti che possiamo definire epocali: l'individuo

BIO

Massimiliano Valerii si laurea in Filosofia all'Università degli studi La Sapienza di Roma. Lavora al Centro studi investimenti sociali (CENSIS) dal 2001, prima come direttore di ricerca e poi come responsabile della comunicazione, dove cura i rapporti con i media, la produzione editoriale, i contenuti web. Oggi è Direttore Generale del Centro studi investimenti sociali (CENSIS) e il curatore dell'annuale «Rapporto sulla situazione sociale del paese», che dal 1967 è considerato uno dei più qualificati e completi strumenti di interpretazione della realtà socio-economica italiana.

comincia ad avvertire di non poter più esprimere un dominio onnipotente e incontrastato sul mondo e sugli eventi. È finita l'era dell'abbondanza, ha affermato recentemente il presidente francese Macron. Direi che tutto ciò fa sì che, al momento, il carattere degli italiani sembra malinconico. Un sentimento che riflette la fine del vecchio ordine delle cose, in attesa che se ne definisca uno nuovo, anche attraverso la riscoperta dei propri limiti quando si tratta di governare il destino.

Un nuovo fenomeno: il friend-shoring

Dopo la lettura apologetica la globalizzazione si sta sgonfiando. Il* friend-shoring *è il fenomeno emergente che apre la strada a una sorta di guerra fredda. Possiamo spiegare di che si tratta?

Dopo l'aggressione russa all'Ucraina, Janet Yellen, segretario al Tesoro degli Stati Uniti, ha usato questo neologismo, friend-shoring, per dire che in prospettiva i Paesi occidentali dovranno limitare le catene globali del valore e confinare gli scambi internazionali entro un perimetro definito unicamente da quegli Stati che condividono con noi i nostri stessi valori di democrazia e libertà. Certo, suona come un modo edulcorato di parlare di una «seconda guerra fredda». Probabilmente una de-globalizzazione non conviene a nessuno. Ma è indubbio che le frizioni geopolitiche di quest'ultimo scorcio di storia sembrano ridisegnare due poli nel mondo: uno intorno agli USA, l'altro gravitante della Cina. In gioco c'è la supremazia a livello economico, tecnologico e militare sul mondo.


ECONOMY

Yellen says the U.S. and its allies should use 'friend-shoring' to give supply chains a boost

PUBLISHED TUE, JUL 19 2022-7:06 AM EDT

Su-Lin Tan
@SULIN_TAN

La domanda di prospettiva di benessere e di maggiore equità fa parte dell'agenda collettiva del Paese post-populista. Verso quali equilibri stiamo andando?

Negli ultimi anni, tutte le élite politiche occidentali stanno integrando misure di protezione dei ceti popolari e della classe media, dopo che, come affermano ormai molti analisti, la globalizzazione accelerata degli ultimi trent'anni è colpevole di aver impoverito ampie fasce di lavoratori a vantaggio delle classi medie dell'Asia. A prescindere dalle culture politiche di provenienza e di appartenenza, è questa la tendenza attuale. C'è, ad esempio, una perfetta continuità tra l'amministrazione Biden e il predecessore Trump, (che avevamo indicato come il "populista" per eccellenza) nell'attuare forme di protezionismo verso la Cina attraverso i dazi e vincoli alla vendita di prodotti strategici per la competizione tecnologica, quali i microchip e i semiconduttori. Con Biden, gli Usa hanno registrato il massimo storico di debito pubblico. Mi chiedo allora: chi è il populista?

Si registra una progressiva diminuzione dei reati, aumentano però il senso di insicurezza come si vede molto bene da una lettura attenta dei dati Censis. Come si spiega questa palese contraddizione?

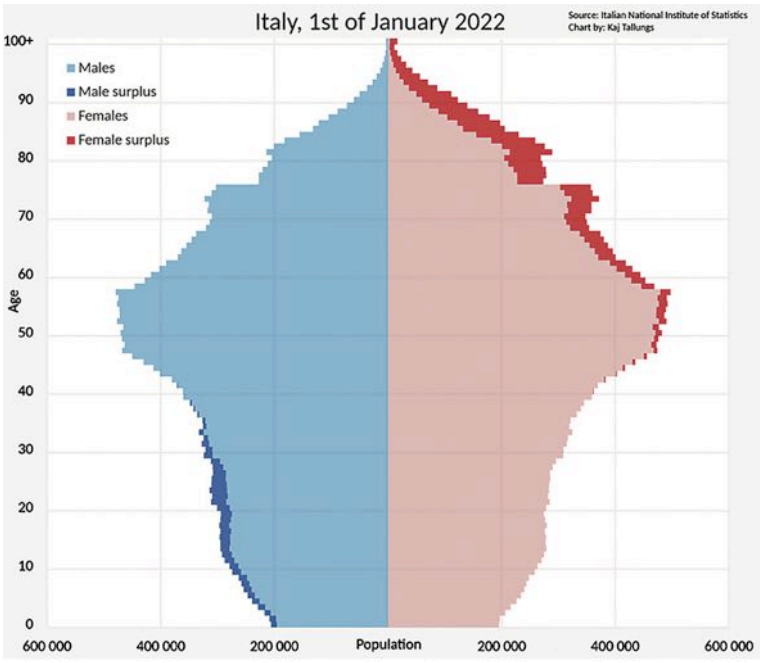
In Italia negli ultimi dieci anni i reati complessivi si sono ridotti di oltre il 25%, ma oggi più della metà della popolazione ha paura di rimanere vittima di reati. Siamo il Paese statisticamente più sicuro di sempre, con il

minimo storico di omicidi e di fenomeni di criminalità predatoria, come furti e rapine. In realtà ci sentiamo particolarmente vulnerabili e insicuri a causa di prospettive economiche e sociali incerte.

Un paese senza: l'inverno demografico

Spesso viene sottovalutato il dato demografico. Nel Rapporto si parla di un "Paese senza": senza giovani, senza infermieri, di fatto senza un motore produttivo. Siamo destinati al declino?

La transizione demografica, con una pesante denatalità e un forte invecchiamento della popolazione, è la questione numero uno a cui è appeso il nostro futuro. Va affrontata con uno sguardo lungo, perché il



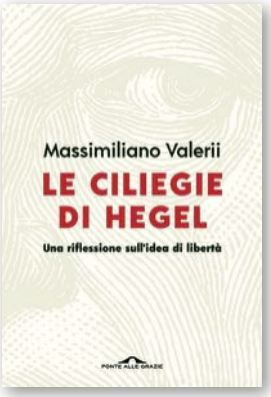
rischio è che si restringa la base lavorativa e produttiva del Paese, cioè la popolazione in attività, che rappresenta il motore produttivo di una nazione.

"I cittadini perduti della Repubblica", colpisce questa definizione che si trova nel rapporto, perché fotografa un altro fenomeno grave che mette in evidenza le responsabilità della politica. Cosa bisogna fare per ridare ossigeno alla democrazia e vitalità alla partecipazione in un Paese che sembra aver messo in soffitta lo spirito costruttivo e che vede l'infiacchimento di ogni schema proiettivo?

Le ultime elezioni hanno segnato un record di astensionismo si tratta di una vera e propria ferita nella storia della Repubblica: ha vinto il partito del non voto, astenuti, schede bianche e nulle la hanno fatta da

padrone. Parliamo di quasi 18 milioni di persone, pari al 39% degli aventi diritto. In 12 province italiane i non votanti hanno superato il 50%. Tra le politiche del 2006 e quelle del 2022 i non votanti sono raddoppiati: +102,6%.

Quando non funziona più l'intreccio virtuoso tra lavoro e acquisizione del benessere, le democrazie vacillano. L'assalto a Capitol Hill - il tempio inviolabile delle moderne democrazie liberali - dello scorso anno – credo vada letto come un segnale da non sottovalutare.



La libertà è un tema forte di cui lei si è occupato nel suo ultimo saggio* "Le ciliegie di Hegel" *(ed. Ponte alle grazie). Ritiene che la perdurante condizione di crisi economica e geopolitica stia mettendo a repentaglio i diritti fondamentali generando un oggettivo stato di sofferenza delle democrazie?

Credo che questo sarà un tema con cui le società occidentali si dovranno confrontare negli anni a venire. Anche perché dall'altra parte del mondo è avvenuto qualcosa che mette in crisi le nostre convinzioni più radicate. Negli ultimi trent'anni in Cina non c'è stata solo una crescita economica impetuosa, ma anche enormi progressi sociali. Fino a trent'anni fa, due terzi dei cinesi vivevano in povertà, oggi solo lo 0,5%. Mentre da quest'altra parte del mondo le classi medie temono il declassamento sociale. Il dilemma che ne consegue è molto chiaro: a che serve la libertà, se una società può stare meglio anche senza essere libera? ■

La mediamorfosi: informazione e guerra sono ormai inscindibili.

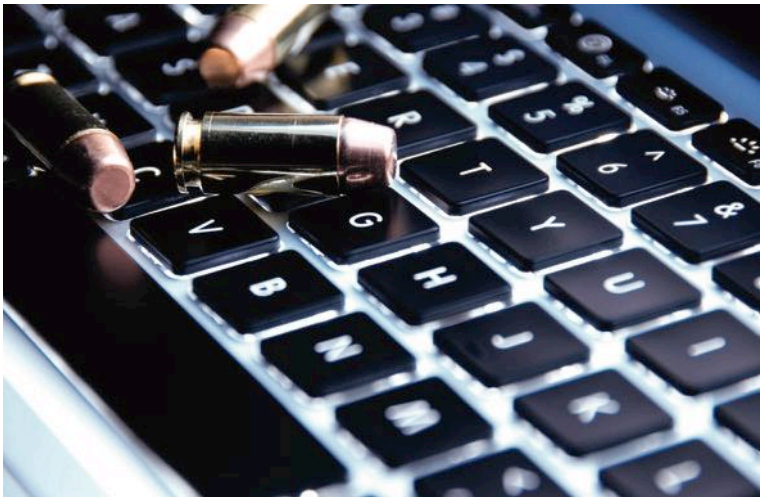
Intervista VIP a Michele Mezza.

Autore: Massimiliano Cannata

"È in atto una mediamorfosi, particolarmente visibile sul campo di battaglia ucraino, in cui appare evidente come la professione giornalistica sia a una svolta. Le informazioni sono divenute alluvionali e gratuite, mentre un tempo erano costose, rare e riservate. Sono parallelamente cambiati gli assetti di mercato, in una generale modificazione del rapporto tra conflitto e comunicazione. La rete ha oggi assunto l'informazione come «logistica militare», mentre si combatte utilizzando i contenuti come strumento di offesa, contenuti che agiscono sulla psicologia dell'avversario". Michele Mezza ex giornalista Rai, ideatore del progetto RaiNews24 e attento osservatore dei fenomeni di trasformazione della società globale, nel saggio "Net-war" (ed. Donzelli) fa vedere con efficacia e lucidità di analisi come il giornalismo stia cambiando la guerra e come tutta la macchina produttiva, a cominciare dai giornali, abbia mutato i suoi asset produttivi e organizzativi.

Il binomio Net - War svela la modalità di una guerra che non ha più nulla di convenzionale. Il campo di battaglia si è spostato su un terreno ibrido, in cui il conflitto è ininterrotto. Siamo di fronte a una dinamica che conosciamo poco. A cosa stiamo andando incontro?

Nel mio lavoro ho cercato di ricostruire il complesso processo di elaborazione maturata nel cuore degli apparati militare, che stanno sperimentando anche al loro interno l'espansione progressiva della rete e delle relazioni sociali che questo strumento comporta. In particolare, il



vero "salto di paradigma - va individuato nell'ultima guerra in Libano fra il 2006/2008 in cui i più avvertiti analisti americani si chiesero come mai durante l'attacco degli Hezbollah, Israele non riuscisse a far valere la propria superiorità tecnologica. In quell'occasione è stato messo a fuoco come i

BIO

Michele Mezza, giornalista, è stato inviato del Giornale radio Rai in Urss e in Cina. Nel 1993 ha collaborato al piano di unificazione del Gr. Nel 1998 ha elaborato il progetto di Rai News 24. Attualmente dirige il centro di ricerca sul mobile PollicinAcademy e la comunità web www.mediasenzamediatori.org, e cura un blog per l'«Huffington Post». Michele è docente di Epidemiologia sociale all'Università Federico II di Napoli. Tra i suoi vari libri ha pubblicato: Sono le news, bellezza! Vincitori e vinti nella guerra della velocità digitale (2011), Avevamo la luna. L'Italia del miracolo sfiorato, vista cinquant'anni dopo (2013), Giornalismi nella rete. Per non essere sudditi di Facebook e Google (2015), e recentemente Algoritmi di Libertà, Il Contagio dell'algoritmo e, in collaborazione con Andrea Crisanti, Caccia al virus.

sistemi digitali decentrassero il sapere costringendo gli apparati militari ad intrecciarsi con la società civile.

A seguito si è fatto strada il pensiero russo, che nel 2013 con un famoso saggio di Valery Gerasimov, il capo di stato maggiore attuale delle forze del Cremlino teorizzò come la guerra procedesse ormai "mediante la capacità di interferire nelle psicologie dell'avversario ". Poco dopo nasce Cambridge Analytica che pratica questa teoria con il massiccio intervento molecolare sull'elettorato americano. Le rivoluzioni arancioni innestate dai servizi americani sia in Oriente che nei paesi arabi mostrano, infine, l'ulteriore potenziale di queste nuove procedure che con la guerra in Ucraina sono diventate logistica militare, rispetto a cui la società civile diventa, con le sue abilità e relazioni, prima linea.

"La rete, un luogo ma anche uno strumento della logistica militare". Cosa vuol dire in concreto e quali sviluppi comporta una dinamica del confronto tra le parti che non ha una natura solo strategico militare presentando un fitto intreccio di tecnologia e informazione?

Chi ha osservato attentamente soprattutto la prima fase del conflitto, diciamo i primi cento giorni, avrà notato come si siano confrontati da una parte un modello che qualcuno ha definito ottocentesco di azione militare, simboleggiato dall'ormai famosa sequenza video della poderosa colonna di blindati russi lunga 65 km.

Dall'altra parte un sistema articolato e distribuito che combinava le risorse più ordinarie della rete, dai droni agli *smartphone*, da Telegram a Google Street per localizzare e colpire il nemico mediante la combinazione di informazioni che affluivano dalla popolazione e i sistemi di guerriglia territoriale. L'emblema di questa seconda strategia è l'altrettanto famoso appello del ministro dell'innovazione digitale Fiodorov ad Elon Musk di un paio di giorni dopo l'invasione in cui si chiede di mettere a disposizione della resistenza la sua flotta satellitare, cosa che avviene dopo qualche ora, con una spettacolare capacità di georeferenziare ogni singolo soldato russo che si muoveva sul territorio.

La Rete come logistica della guerra

Nei conflitti l'informazione ha sempre avuto un ruolo, pensiamo alla propaganda ai tempi del primo e soprattutto del secondo conflitto mondiale. Oggi siamo però di fronte a un fenomeno diverso. L'informazione cambia la guerra. Con quali conseguenze?

Non sarebbe certo una novità rilevare come anche questa guerra si combatta con le armi della propaganda. La novità semmai che va sottolineata è che questa sia la prima guerra che si conduce con gli strumenti del giornalismo: esattamente le infrastrutture digitali, dai cloud, ai data base, dai filmati a Twitter, insieme al linguaggio della narrazione in diretta, con le riprese dei combattimenti realizzate mentre si spara. La guerra è diventata innanzitutto un fenomeno di mediamorfosi, in cui appunto l'abbondanza di materiali ha affiancato e a volte anche sostituito lo scontro a fuoco. Pensiamo a cosa è accaduto a Bucha, con una contrapposizione

di documenti, fonti, reportage, che hanno poi modificato la visuale della guerra. Questo gorgo ha separato i fatti dalle fonti. Per la prima volta abbiamo constatato un'abbondanza di fonti, tutte robustamente documentate da immagini e testimonianze, che contestavano e alteravano i fatti. Lo sosteneva cinquanta anni fa Hanna Arendt, che scriveva: *"La libertà di opinione è una farsa a meno che l'informazione fattuale non venga garantita e i fatti siano sottoposti alla disputa".*

La conoscenza ai tempi della rete e dell'IA, il sapere che si tramuta in giornalismo. In questo processo che vede le redazioni ormai alla stregua di* software Hours *i professionisti che ruolo rivestono?

Il tema che, a mio parere si pone con urgenza, riguarda la ricomposizione della frattura fra informazione e informatica. Oggi la padronanza della programmazione del software e della gestione del *machine learning* sono

funzioni essenziali del bagaglio di un giornalista che si trovi a giostrare fra flussi di dati e supporti di intelligenza artificiale. Come non è concepibile che in una redazione si appaltino conoscenze e saperi in materia di economia e politica, tanto meno è accettabile che si affidino ai fornitori di soluzioni digitali la filosofia e l'etica con cui funzionano questi sistemi e la capacità di decifrare in *real time* documenti e filmati.

Oggi all'ordine del giorno c'è da una parte l'integrazione di queste capacità nella struttura di base del giornalismo e dall'altra la combinazione di professionalità e pratiche giornalistiche in ogni tipo di attività che sempre più sono proiettate sullo scenario della comunicazione come la guerra sta ampiamente facendo vedere.

L'intelligence è un termine critico. Solo Machiavelli aveva saputo usare questo termine nella triplice natura che comprende sapere informazione sicurezza. Viviamo di intelligence in una dimensione che è quella che Luciano Floridi ha definito "infosfera". Quali scenari si aprono per il prossimo futuro?

Due sono gli asset rispetto a cui si sta evolvendo lo scenario antropologico: da una parte quello che Vittorio Foa, un grande vecchio del sindacalismo italiano, definiva lo scontro fra orizzontale e verticale, che vuol dire la geometria dei poteri e la qualità della partecipazione alle decisioni; dall'altra il nodo della trasparenza. Io ho dedicato il mio libro ad Assange e alla Politoskajia, due figure che a livello diverso, e su scacchieri diversi, sono vittime di poteri oscuri e riservati. Oggi cresce una pretesa sociale di trasparenza e condivisione di ogni tipo di informazione.

L'*intelligence* diventa democratica in ogni sua accezione e questo crea problemi al potere e alle istituzioni che sono invece il portato di secoli di riservatezza e segretezza. Pensiamo ad esempio che in Ucraina, proprio per quello che è accaduto nel coinvolgimento diretto della società civile nei combattimenti sarà più complesso procedere a trattative di pace. Non decide solo Zelenskij ma anche tutta la filiera sociale, dai sindaci alle comunità, che ha partecipato alla resistenza che vuole condividere e partecipare alle decisioni. In questa chiave il giornalismo diventa sempre più un linguaggio civile e non più una professione retribuita.

Algoritmi e opinione pubblica disintermediata

Nel saggio si parla di opinione pubblica disintermediata in un universo mediatico che non ha nulla in comune con i sistemi tradizionali di controllo e di governo dell'informazione. È cambiato il flusso e il rapporto tra informazione e potere, lo stato non è il monolite del leviatano ma una struttura porosa innervata da poteri diversi e da una rete di informazioni che lo attraversano. Neanche la guerra ha nulla in comune con le guerre del passato. Viene da chiedersi se gli eserciti servono ancora e chi sono i vincitori di questo modo diverso di fare e condurre la guerra?

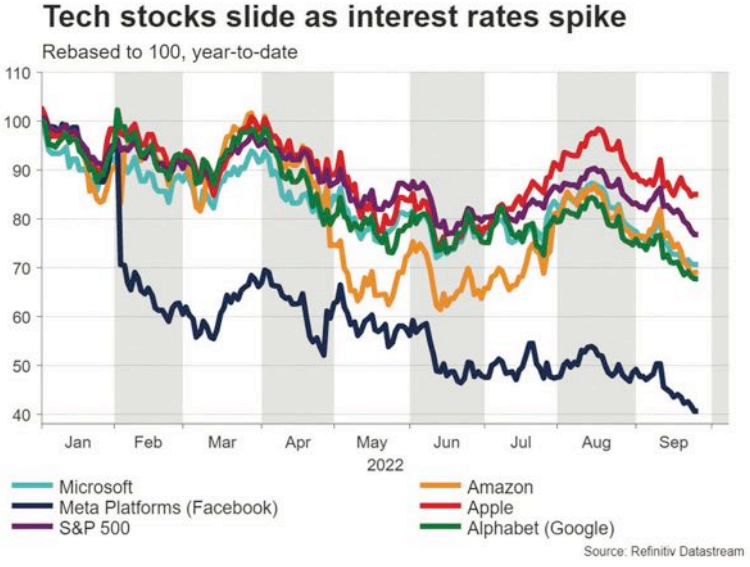
Dipende cosa si intende per eserciti. In Ucraina abbiamo visto che i mezzi blindati sono ormai un bersaglio fin troppo facile per satelliti e droni, così come le navi. Mentre diventano insidiosi i missili teleguidati e georeferenziati. Dall'altra parte lo scontro si sposta sul terreno dell'intelligence e ogni paese deve avere strumenti e saperi per reggere la competizione. Da questo punto di vista trovo illuminante il saggio del generale cinese Quiao Liang, *"L'Arco dell'Impero"* che spiega come ormai il processo di decentramento delle decisioni indotto dalla rete abbia investito anche gli apparati militari.

La geopolitica come disciplina scientifica risponde ormai a dinamiche nuove. Quale Europa verrà fuori dal conflitto russo - ucraino?

Mi ritengo un semplice cronista che cerca di capire quello che vede. Al momento mi pare si sta configurando un'Europa molto americana. Dovremo vedere come Germania e Francia si assestano. Ma il vero "buco nero" credo sia rappresentato dall'America dove è in corso un processo di scollamento fra comunità locali e interessi che mette in discussione lo stesso patto federativo. Il futuro degli Usa è il vero interrogativo.

Si automatizza il pensiero, ma anche il conflitto. Saranno gli algoritmi a sedare le controversie nella prospettiva che molti studiosi collocano nell'era del post umano?

Indiscutibilmente questo tema è entrato nel novero delle variabili plausibili. Gli algoritmi già sono oggi arbitri della nostra vita e lo saranno anche dei nostri conflitti. La crisi che vive in questi mesi il *Big Tech* con la caduta dei valori di borsa ci annuncia un prossimo tornante che muterà forma e ruolo delle tecnologie con l'avvento del calcolo quantico. Per questo avremo sempre maggior bisogno di maggiori competenze e conoscenze per negoziare la potenza di calcolo. ■

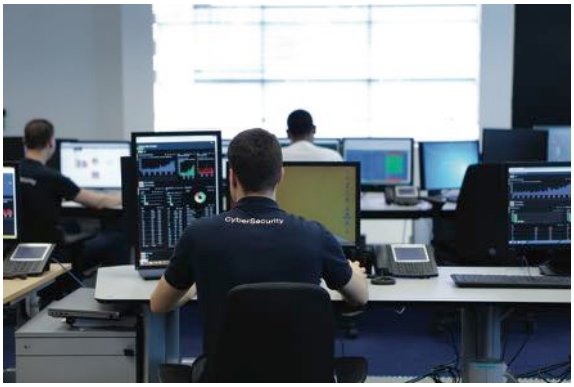


Le nuove fondamenta della sicurezza moderna: workload, identità e dati.

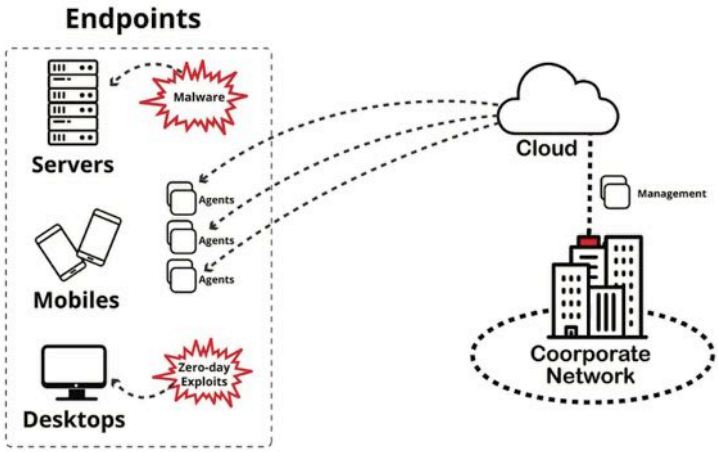
CROWDSTRIKE

Autore: Luca Nilo Livrieri

Persone, processi e tecnologia sono da tempo i pilastri fondamentali che dettano il modo in cui vengono gestiti i programmi di cybersecurity, e in effetti un motivo c'è: le aziende necessitano di personale esperto, di processi affidabili per prevenire violazioni e per reagire nel caso in queste si verifichino, oltre alle ultime tecnologie di sicurezza per rilevare e bloccare attività malevole. Questo approccio stratificato alla sicurezza ha protetto le aziende per diversi anni, ma oggi non è più sufficiente a garantire la sicurezza delle imprese. Gli avversari informatici odierni sono infatti sempre più capaci a riadattare le proprie tecniche e a renderle sempre più sofisticate.



Sebbene il principio *"persone, processi e tecnologia"* rimanga comunque valido e un presupposto fondamentale della cybersecurity, gli esperti in IT e sicurezza devono pensare a come questi tre pilastri abbraccino tre importanti domini a cui le aziende dovrebbero dare maggiore priorità nelle loro strategie di difesa. I team di sicurezza devono considerare i workload (endpoint e cloud), le identità (utente e macchina) e i dati come l'epicentro del rischio di sicurezza aziendale, nonché il cosiddetto "sgabello a tre gambe" su cui basare il loro approccio.



L'unico modo per essere sempre un passo avanti rispetto agli avversari è adattarsi. Se si guarda all'attività delle minacce, tutti gli indicatori confermano che gli aggressori stanno seguendo la tendenza all'adozione del cloud aziendale e stanno sviluppando le loro capacità di navigare e sfruttare i workload in cloud. Il compromesso dell'identità è diventato una componente importante delle minacce alla sicurezza e sta aumentando il valore delle credenziali dei dipendenti per i criminali informatici. Una serie di credenziali valide, o una singola misconfigurazione, possono essere tutto ciò di cui un autore delle minacce ha bisogno per ottenere accesso a un pool crescente di dati e di risorse critiche nel cloud.

Workload: endpoint e cloud

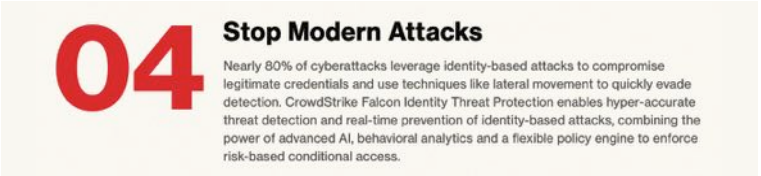
I nemici informatici vedono il cloud come un'opportunità per perseguire, tra gli altri obiettivi, il furto di proprietà intellettuale, l'estorsione di dati e le campagne ransomware. I vettori comuni di attacco al cloud includono lo sfruttamento delle vulnerabilità, il furto delle credenziali, l'abuso dei provider di servizi cloud, l'uso di servizi cloud per l'hosting del malware e il command-and-control (C2) e lo sfruttamento di container d'immagini con configurazioni errate.

Ovviamente, i workload in cloud non sono gli unici a dover essere protetti. Gli esperti in sicurezza devono proteggere anche gli endpoint, che hanno profili di rischio ed esposizione alle minacce differenti. Quando gli avversari puntano lo sguardo sugli endpoint, continuano a dimostrare di essere andati oltre il cloud. Piuttosto, sono stati osservati mentre utilizzavano credenziali legittime e strumenti integrati - un approccio noto come «living off the land» - per eludere il rilevamento da parte degli antivirus tradizionali.

Man mano che le aziende crescono e integrano più endpoint, workload in cloud e container, oltre a nuovi strumenti di protezione, la sicurezza può diventare sempre più complicata. Gli esperti in sicurezza informatica dovrebbero attivare la protezione runtime, ottenere visibilità in tempo reale ed eliminare gli errori di configurazione come parte delle loro best pratices per garantire una maggiore sicurezza delle loro risorse.

Identità: utente e macchina

Gli avversari odierni usano milioni di credenziali rubate per eludere i sistemi di difesa legacy e agire come utenti legittimi. La maggior parte delle violazioni è, per queste ragioni, legata al furto delle identità (l'80% per la precisione), un dato che dovrebbe motivare gli esperti in sicurezza a ripensare attentamente le proprie strategie di protezione dell'identità.



Le intrusioni basate sulle credenziali che prendono di mira gli ambienti cloud sono tra i più comuni vettori usati sia nel cybercrimine sia negli attacchi targettizzati. I criminali informatici ospitano spesso pagine di autenticazione false per raccogliere credenziali legittime per i servizi cloud più diffusi, successivamente usate per tentare di accedere agli account delle vittime. Essi hanno solo bisogno di un set di credenziali valide per accedere in qualità di dipendenti, supponendo che le misure di sicurezza aggiuntive non li ostacolino.

Nell'ambito della loro strategia di difesa, le aziende devono assicurare la piena adozione dell'autenticazione multi-fattore (MFA), specialmente per gli account privilegiati, disabilitare i protocolli di autenticazione legacy che non supportano la MFA, monitorare e controllare i privilegi e le credenziali sia per gli utenti che per gli amministratori di servizi cloud.

Dati: l'importanza della protezione dei dati

In ultimo luogo, gli avversari prendono di mira i dati. Le aziende pensano al futuro della protezione dei dati, ma dovrebbero considerare come i workload (endpoint e cloud), le identità (utente e macchina) e i dati siano interconnessi; e come i dati cambino in base a come questi asset interagiscono tra di loro. Le identità sono autenticate attraverso gli endpoint, mentre i repository di codici, i workload in cloud e le applicazioni sono accessibili tramite endpoint. I dati fluiscono da un asset all'altro ed esistono tra i dispositivi e gli ambienti cloud.

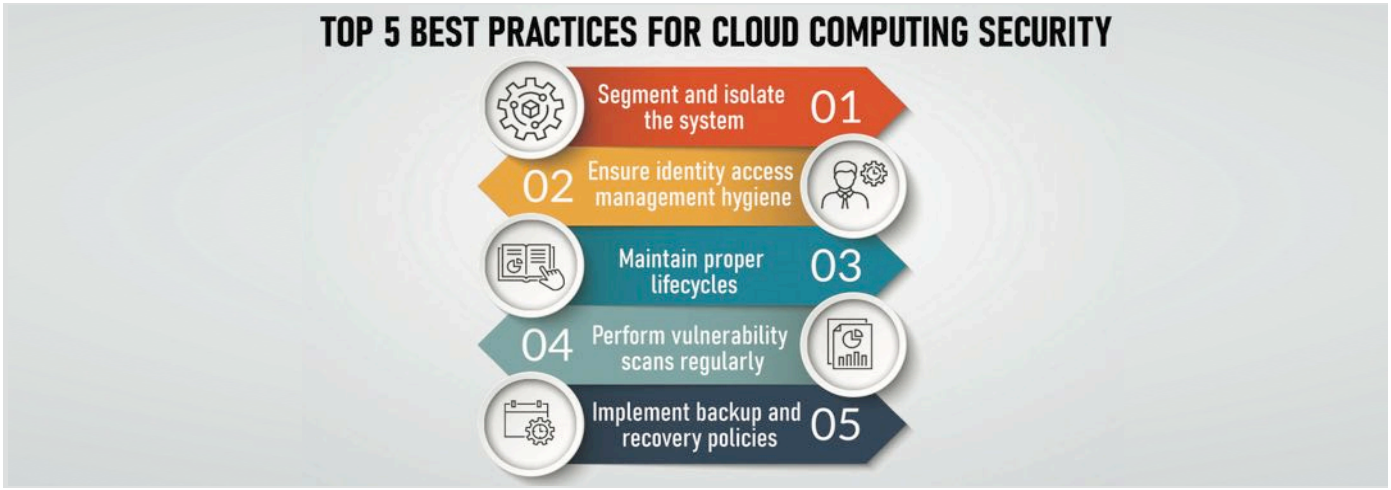
Proteggere tutti questi dati è un lavoro consistente e avviene in modo leggermente diverso per ogni azienda. Ci sono diverse fasi che gli esperti in cybersecurity devono eseguire al fine di proteggere i dati che garantiscono l'operatività aziendale:

- **Abilitare la protezione dei workload in cloud:** proteggere i workload richiede la visibilità e l'individuazione di ogni workload e degli eventi di container, proteggendo l'intero stack cloud-native su qualsiasi cloud tra workload, container e applicazioni prive di server.
- **Proteggere tutte le identità:** i nemici informatici usano credenziali rubate per eludere i sistemi di difesa legacy e camuffarsi in utenti legittimi. I team di sicurezza devono concentrarsi fortemente sull'identità per proteggere l'azienda dalle minacce moderne.
- **Sapere cosa è bene proteggere:** le aziende devono avere una comprensione a livello aziendale dei loro asset di dati. La visibilità unificata di asset, configurazioni e attività può aiutare a rilevare configurazioni errate, vulnerabilità e minacce alla sicurezza dei dati, fornendo al contempo approfondimenti e soluzioni guidate.

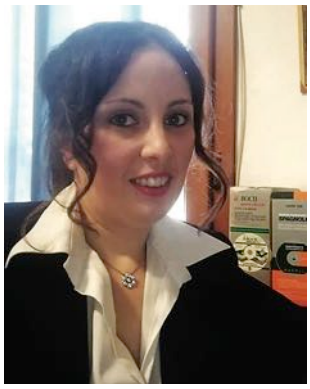
Oggi più che mai le aziende devono pensare alla loro sicurezza in ogni parte del business: la superficie di attacco continua a espandersi, specialmente in un contesto in cui l'adozione del cloud computing e del lavoro da remoto sono sempre più diffusi. È necessario, pertanto, che la sicurezza aziendale si basi su tutti i workload, le identità e i dati e faccia di questi tre elementi le fondamenta della propria strategia di difesa. ■

BIO

Luca Nilo Livrieri è l'SE Manager di Crowdstrike per il Sud Europa. L'ingresso in Crowdstrike avviene nel maggio 2021, con la responsabilità di seguire lo sviluppo e la crescita della struttura di prevendita nel Sud Europa. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, sicurezza, cloud e digital transformation fra cui Security Summit, ISMS forum, IDC e Cybertech. Prima di Crowdstrike, Livrieri è stato manager per l'Italia, la Spagna e il Portogallo della struttura prevendita di Forcepoint. Ha maturato esperienze come membro dell'"Office of the CSO" e Senior SE per il mercato enterprise, e la formazione e affiancamento del canale di rivendita in Websense e Surfcontrol. Prima di svolgere il ruolo di SE ha lavorato come consulente Gfi-Ois per la programmazione web presso alcune importanti aziende italiane. Precedentemente ha conseguito la Laurea magistrale in Comunicazione nella Società dell'Informazione, con tesi specialistica presso il dipartimento di informatica dell'Università Degli Studi Di Torino.



La security awareness nell'uso del cloud nella pubblica amministrazione italiana.



Autore: Valentina Domenica Cuzzocrea

Introduzione

Il Rapporto Clusit di marzo 2022 evidenzia che nell'anno precedente gli attacchi cibernetici sono aumentati di quasi un decimo rispetto al 2020 e che il guadagno economico che scaturisce da queste azioni criminose è tale da spingere gli attaccanti a migliorare le modalità con cui agiscono, divenendo sempre più precisi e adattandosi alle situazioni specifiche.

La Pubblica Amministrazione italiana, assieme al settore finanziario, rappresenta quasi la metà degli obiettivi preferiti. Questo rappresenta un vulnus per il nostro Stato, tanto che, come evidenziato da Aldo di Mattia nel rapporto Clusit: *"chi si occupa delle strategie di difesa informatica dovrà pianificare in anticipo le azioni da mettere in campo sfruttando la potenza dell'AI per accelerare la prevenzione, il rilevamento e la risposta alle minacce"*(1).

Per questa motivazione, si ritiene fondamentale la preparazione dei dipendenti, funzionari e dirigenti pubblici sulle materie riguardanti la cybersecurity. Nello specifico, non si dovrà tentare di trasmettere le nozioni prettamente informatico-ingegneristiche, bensì quei comportamenti e quelle accortezze da adottare per fare in modo da diminuire il rischio di perdita o di manomissione delle informazioni.

Infatti, la Pubblica Amministrazione è detentrice di un incommensurabile patrimonio di dati dei cittadini. Per questo motivo, un buon piano di security awareness nella Pubblica Amministrazione rappresenta la scelta vincente, poiché la consapevolezza dei dipendenti permette di fronteggiare un problema in rapida ascesa, derivante dall'evoluzione tecnologica da un lato, e dall'altro da comportamenti scorretti che, involontariamente o meno, ci si ritrova ad attuare.

La trasformazione digitale nella PA

Poniamo delle riflessioni di carattere normativo in Italia. La Legge sul procedimento amministrativo (L. 241/902) (2), prettamente riferita al mondo analogico, adesso è accompagnata dal CAD (D. Lgs. 82/20053) (3)

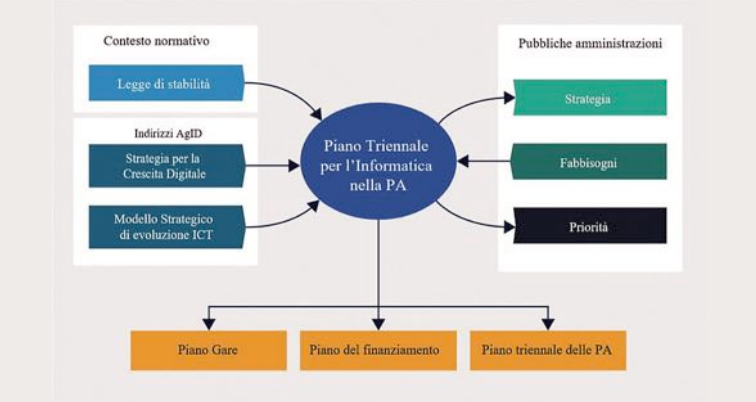
BIO

Valentina Domenica Cuzzocrea (1990), Funzionario Amministrativo presso Inail, membro del Comitato Tecnico Operativo del Laboratorio sull'Intelligence dell'Università della Calabria e ricercatrice presso lo stesso ente. Laureata col massimo dei voti in lingue e letterature moderne con una tesi sperimentale dal titolo 'Personaggi alla deriva nella letteratura francese del XX secolo: Lafcadio, Roquentin, Meurault', ha conseguito il Master in Intelligence con una tesi sul riconoscimento delle origini dei migranti.

che non prevede più il solo "documento amministrativo", ma si sofferma sui formati e sulle tipologie di documento amministrativo digitale, nonché sul valore probatorio degli stessi, stabilendone processi e caratteristiche che mantengano inalterata la validità del documento.

Accanto a questo, trova spazio anche il concetto di privacy, previsto dal Codice in materia di protezione dei dati personali (D. Lgs 196/20034) (4) accanto al quale troviamo il GDPR (Reg. UE 2016/6785) (5), il quale si concentra sul data breach, cioè la violazione dei dati personali.

Si tratta di una falla nella sicurezza del trattamento dei dati conservati dal titolare e che, se non opportunamente controllata, conduce all'accesso non autorizzato ai dati personali e, in seguito, alla perdita, modifica, o divulgazione non autorizzata degli stessi. Possiamo citare un altro caso in cui il digitale si intreccia con la vita delle persone, la Legge 81/20176 (6) recante *"Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato"*, nella quale l'intero capo II è dedicato al lavoro agile.



La legge anticipa di almeno tre anni quelle che saranno le necessità del periodo pandemico. Un ulteriore cenno normativo che testimonia la sempre crescente attenzione che lo Stato e i suoi organi rivolgono al mondo digitale è il DPCM 17 luglio 2020 (7), con il quale è stato approvato il Piano Triennale per l'Informatica nella PA 2020-2022 (8). Quest'ultimo mira a realizzare una strategia volta:

- a favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della pubblica amministrazione (…)
- a promuovere lo sviluppo sostenibile, etico e inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale (…)
- e a contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici (9).

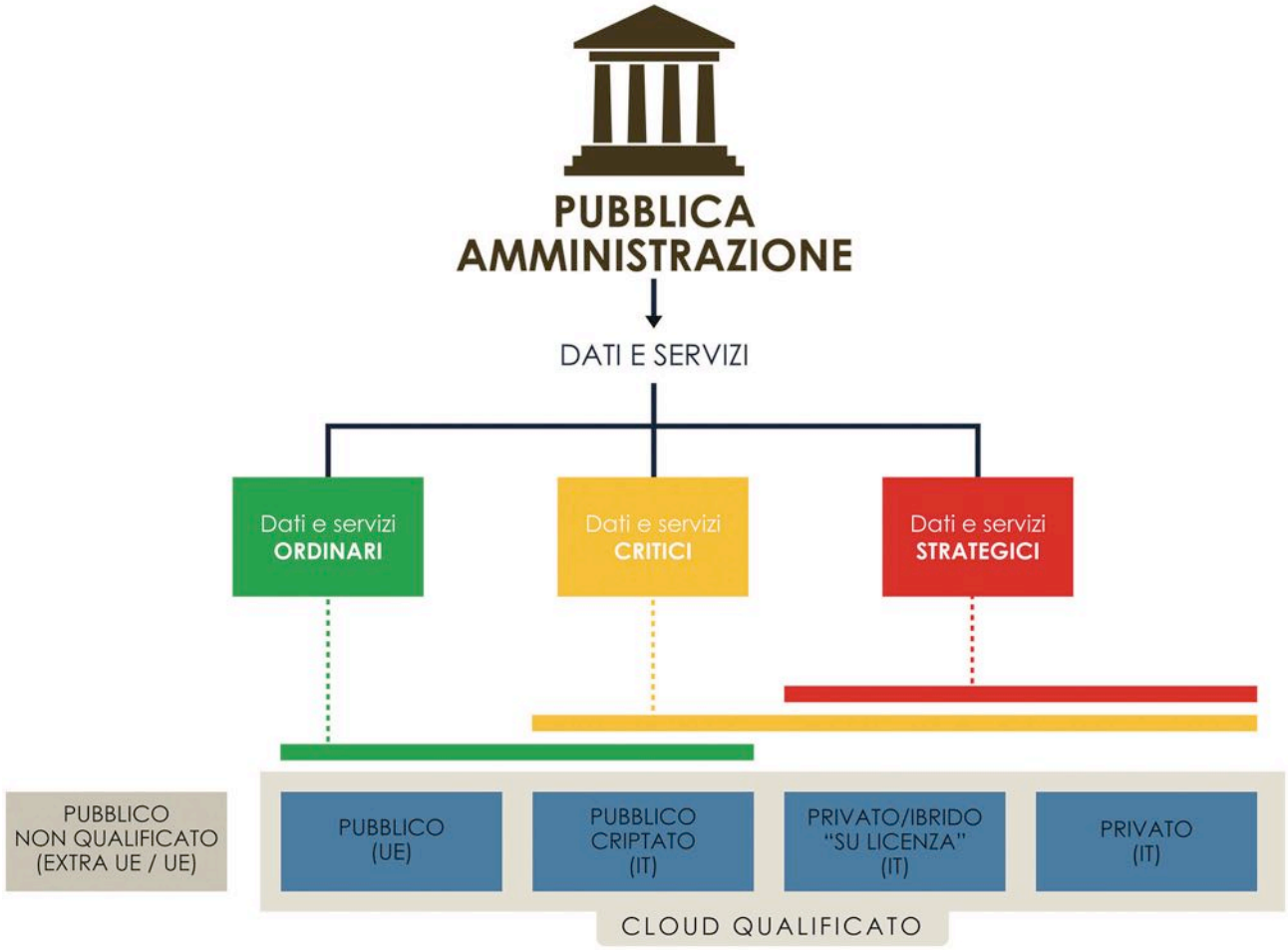
Ad inizio 2021, il Ministro per l'innovazione tecnologica e la transizione digitale, Colao, ha tenuto una relazione nella quale ha rivisto le priorità del Governo in tale ambito, anche in conformità a quanto previsto dell'EU Digital Compass 2030. In questo contesto, tra le proposte è stato introdotto il Cloud PA (10).

A tal riguardo, non possiamo dimenticare che le informazioni che scaturiscono da dati online hanno acquisito nel tempo maggiore importanza poiché permettono di conoscere usi, consumi, abitudini o, nei casi più delicati, orientamenti sessuali e problematiche sanitarie dei cittadini. Per questo motivo, l'art. 4 del GDPR distingue diverse tipologie di dati: personali, genetici e biometrici. I primi sono identificabili come: *"qualsiasi informazione riguardante persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica o sulla salute di detta persona fisica, genetica, psichica, economica, culturale o sociale."*

I dati genetici, invece, sono "relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione", mentre per dati biometrici si intendono "quelli ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

La Pubblica Amministrazione va a toccare tutti questi dati poiché copre l'intera vita dei cittadini, dall'anagrafe all'istruzione fino ad arrivare alla sanità, perciò impiegati, funzionari e dirigenti dello Stato dovranno essere a conoscenza di queste nozioni giuridiche e riuscire ad avere la consapevolezza che da un loro errore o disattenzione potrebbe derivare una lesione di diritti della persona fisica, quindi anche del cittadino.

A tal riguardo, introduciamo un altro concetto: l'accountability, cioè la responsabilità. In un articolo di poco più di tre anni fa, Ottaviani (11) presenta la configurabilità di un *"responsabile interno nella Pubblica Amministrazione"* (12). La sua riflessione parte dagli artt. 4 e 28 GDPR poiché definiscono il Responsabile del trattamento come quella persona fisica, giuridica, pubblica amministrazione, servizio o altro organismo che tratta dati personali per conto del titolare e che deve essere in grado di fornire garanzie per il rispetto delle norme e per la tutela dei diritti dell'interessato. Tale figura dovrà adottare misure di sicurezza adeguate al rischio, vincolandone i dipendenti e chiarendone i rischi che derivano da un mancato o scorretto trattamento dei dati.



Infatti, anche la Pubblica Amministrazione è soggetta a rischi quali quelli reputazionali, poiché i cittadini perderebbero fiducia nello Stato con conseguente disordine sociale e, nello stesso tempo, si verrebbe a creare diffidenza da parte degli Stati esteri che vedrebbero l'Italia come un paese instabile e facilmente penetrabile. Tuttavia, vi è la possibilità che si manifestino anche rischi economici, poiché una violazione dei diritti della persona fisica agevolerebbe un contenzioso da parte del cittadino per risarcimento dei danni subiti per

mancato rispetto della normativa europea. Si possono venire a creare anche rischi operativi, dal momento che il *data breach* di un cloud contenente dati anagrafici e/o sanitari crittografati dagli hacker bloccherebbero tutto un settore della PA, portando all'interruzione del servizio.

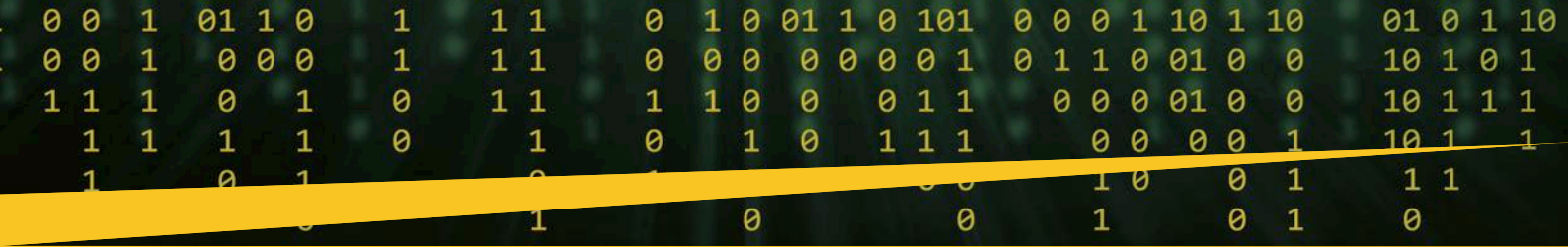
È chiaro che ci saranno delle soluzioni tecnologiche per ovviare al problema, ma è pur vero che il fattore umano rimane uno dei più alti fattori di rischio.

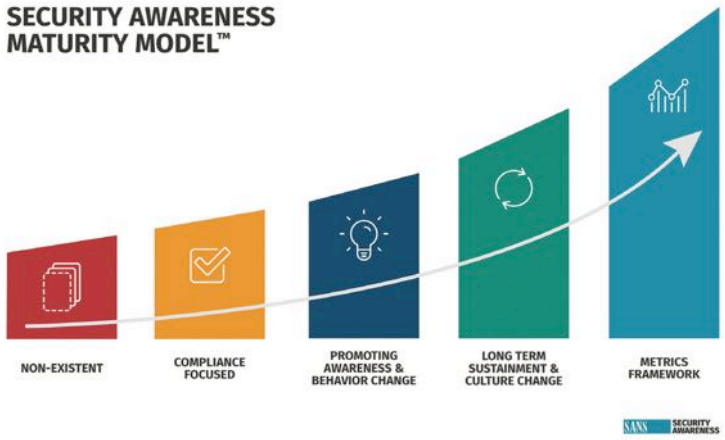
È per questo motivo che una buona formazione dei dipendenti pubblici e l'aumento della consapevolezza delle tematiche cyber da una parte, e la conoscenza dei possibili danni che un loro atteggiamento scorretto può causare dall'altra, può rappresentare un'ottima prevenzione per la limitazione del problema. Qui entra in gioco la security awareness.

Security awareness nella PA

La Security Awareness si inserisce come crocevia tra il campo della Cyber Counterintelligence e quello della Humint. Gli attacchi cyber, infatti, sfruttano le debolezze tecnologiche e umane al fine di poter ottenere dati, o ancora meglio, informazioni, per trarne benefici, siano essi politici o economici. Il Dizionario dei termini militari del DOD statunitense, definisce la Cyber Counterintelligence come *"le misure per identificare, penetrare o netraulizzare operazioni straniere che usano mezzi cyber come tecnica metodologica primaria"* (13).

La Humint è definita come *"una categoria di intelligence derivante dalle informazioni raccolte e fornite da fonti umane"* (14). La security awareness, infatti, parte dallo studio del fattore umano per carpirne le fragilità e le debolezze al fine di elaborare strategie che mirino all'ideazione di tecniche per contrastare eventuali attacchi cyber ad un determinato sistema social-informatico.





Non si deve sottovalutare che i dipendenti della PA devono essere prima di tutto consapevoli di fare parte del sistema Stato sotto una duplice veste, quella di pubblici ufficiali e quella di cittadini. Questa dualità fa sì che essi possano e debbano comprendere che da una loro disattenzione o mancato rispetto delle norme prestabilite e dalle regole definite dal contesto lavorativo possano derivare danni ai cittadini. Il primo passo di un piano di security awareness nella PA è, dunque, proprio quello di evidenziare questo aspetto.

È possibile farlo attraverso dei video di breve durata, pochi minuti dove passi il messaggio che tutti possono essere facilmente colpiti da un attacco informatico, ma che attraverso delle strategie comportamentali è possibile limitarne gli effetti negativi. Una volta innescato il processo motivazionale è necessario passare a concetti utili a non essere vittime ultime di attacchi di mind hacking, cioè di quei *"fattori che possono compromettere le capacità del processo decisionale in quanto diminuiscono la lucidità dell'utente, confondendolo"*(15).

Tra le componenti idonee a mitigare le abilità razionali dell'uomo possiamo enucleare l'urgenza e, di conseguenza, la velocità, la paura, la competizione (collegata anche all'importanza data dall'introduzione della performance con la L. 150/2009) o anche l'altruismo (una persona viene a chiedere informazioni personali su un terzo). È in questo contesto che si inseriscono le e-mail di phishing, cioè:

una frode informatica, realizzata attraverso l'invio di e-mail contraffatte, finalizzata all'acquisizione, per scopi illegali, di dati riservati oppure a far compiere alla vittima determinate operazioni/azioni. I malintenzionati che si avvalgono delle tecniche di phishing non utilizzano virus, spyware, malware o altre tipologie di software malevolo, ma si limitano, piuttosto, ad usare tecniche di social engineering, attraverso le quali vengono studiate e analizzate le abitudini (…) delle potenziali vittime, al fine di carpirne potenziali informazioni utili (16).

Si tratta del metodo più utilizzato per dare avvio a un attacco informatico e il suo successo risiede proprio nella fragilità e/o bontà psicologica dell'attaccato, il quale per disattenzione, paura o anche altruismo, rischia di abboccare all'amo (dal verbo *to fish*: pescare) gettato dal furfante. Si concretizza attraverso l'utilizzo di link/allegati malevoli o richieste di informazioni e gli attacchi possono essere sia senza un destinatario preciso (in quel caso, solitamente, ha uno scopo economico) oppure rivolgersi a un soggetto o ente preciso (questa volta l'obiettivo è quello di destabilizzare una determinata cerchia di persone o servizi).

Per la PA è molto importante conoscerne le modalità, poiché è attraverso l'acquisizione delle credenziali dei dipendenti che un estraneo può riuscire ad acquisire

informazioni sensibili. Sicuramente, la *Multifactor Authentication* ha mitigato il rischio, ma è altrettanto vero che venire a conoscenza di come venga formato uno username della PA rende più facilmente attaccabile l'intero sistema. La pericolosità aumenta nel momento in cui un attaccante viene a conoscere, oltre lo username, anche solo la password di un dipendente.

Per questa motivazione, è fondamentale creare dei corsi ad hoc che contengano, ad esempio, brevi video illustrativi o anche documenti formativi più articolati nel caso in cui qualcuno volesse approfondire l'argomento. Si può sfruttare anche la cosiddetta *gamification*, cioè l'utilizzo di videogiochi creati appositamente dall'ente con schermate che possano riprendere le abitudini tipiche dei propri dipendenti o gli applicativi utilizzati per lo svolgimento del proprio lavoro al fine di una maggiore sensibilizzazione dei propri dipendenti.

Maggiore è la verosimiglianza tra l'ambiente ricreato nel gioco e la realtà, maggiori saranno i risultati che si potranno ottenere nel lungo periodo perché, come abbiamo detto a più riprese, l'awareness non è una semplice forma di apprendimento, ma è l'acquisizione di un comportamento che deve aver luogo nel quotidiano.

Per rendere il tutto più stimolante e avvincente, è possibile impostare un gioco a punti dove per ogni

risposta corretta, vi sia un riscontro positivo che invogli a continuare col gioco e, in caso di risposta negativa, un messaggio che avvisi dell'errore senza svilire il giocatore, il quale, temendo un giudizio negativo, andrebbe a chiedere la soluzione a un collega solo per portare a termine il gioco senza farne esperienza diretta, rendendo il gioco inutile dal punto di vista formativo.

Utili possono essere anche i poster informativi situati lungo i corridoi dell'ente o anche l'utilizzo dei social media. Riteniamo, invece, l'utilizzo di e-mail informative un po' meno efficiente, poiché durante la giornata lavorativa ci si può cimentare in diverse procedure e non sempre è possibile prestare attenzione a ciò che vi è scritto nelle mail ricevute.

Diverso è, tuttavia, l'utilizzo di finte e-mail di phishing, le quali permetterebbero ai dipendenti di concretizzare l'importanza dell'attenzione al momento dell'apertura di e-mail o allegati potenzialmente pericolosi. In quest'ultimo caso, potrebbe essere utile capire la struttura di una e-mail-tipo che si scambia tra colleghi e provare a ricrearla con qualche errore per far prestare attenzione a quei dettagli che possono favorire il riconoscimento di un tentativo di intrusione. In tal frangente, è importante dare delle istruzioni che permettano di individuare l'azione criminosa, come, per esempio, passare sopra un link per verificare la provenienza e, qualora fosse diverso da come ci si poteva aspettare, decidere di non aprirlo e segnalarlo alla direzione IT del proprio ente.

Accanto all'aspetto delle responsabilità, ritroviamo quello della motivazione che può essere introdotta attraverso l'aggiunta di badge di completamento di unità didattica. Sarà necessario, al termine del processo di security awareness, la misurazione delle nozioni apprese dai dipendenti per avere un riscontro delle tematiche realmente apprese, per esempio rendendo il gioco a punti o verificando se, attraverso dei quiz saltuari o dei finti attacchi, il dipendente sia capace di riconoscere e segnalare un attacco.

Conclusioni

La security awareness si rivela una mossa vincente per una Pubblica Amministrazione al passo coi tempi. Uno Stato che trasmette ai propri dipendenti e quindi ai propri

cittadini, una conoscenza normativa e informatica (seppur basilare) andrà a creare una società più attenta ai bisogni propri e altrui, aumentando il livello di sicurezza. Questo non sostituisce la sicurezza tecnologia, ma permette una riflessione sulla tematica e una minore esposizione ai rischi. D'altronde, è inutile installare un costosissimo impianto di videosorveglianza se non si è chiusa il portone di casa a chiave. Non renderà invulnerabili, ma sicuramente più protetti.

Riferimenti

1 https://clusit.it/rapporto-clusit/
2 LEGGE 7 agosto 1990, n. 241 - https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1990;241 [visitato il 10/09/2022]
3 DECRETO LEGISLATIVO 7 marzo 2005, n. 82 - https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig= [10/09/2022]
4 DECRETO LEGISLATIVO 30 giugno 2003, n. 196 - https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196 [10/09/2022]
5 EUR-Lex - 32016R0679 - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679 [10/09/2022]
6 LEGGE 22 maggio 2017, n. 81 - https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017; 81 [10/09/2022]
7 https://pianotriennale-ict.italia.it/assets/pdf/2020-2022/DPCM_17_luglio_2020_pdf_testo.pdf
8 https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf
9 Ibidem.
10 https://www.camera.it/temiap/documentazione/temi/pdf/1104999.pdf?_1661095662148 [visitato il 21/08/2022]
11 Gilberto Ottaviani, GDPR nella P.A., responsabile interno od esterno?, Altalex.com. https://www.altalex.com/documents/news/2019/03/26/gdpr-nella-pa-responsabile-interno-od-esterno [visitato il 05/09/2022]
12 Ibidem.
13 "Cyber Counterintelligence", Department of Defense Dictionary of Military and Associated Terms, p. 139. "https://dcsg9.army.mil/assets/docs/dod-terms.pdf" [visitato il 23/08/2022].
14 "Humint", Department of Defense Dictionary of Military and Associated Terms, p. 247. "https://dcsg9.army.mil/assets/docs/dod-terms.pdf" [visitato il 23/08/2022].
15 Alessandra Rose, «Aspetti psicologici e cognitivi: il valore dell'individuo per la cybersecurity», in N. Sotira (ed.), Il fattore umano nella cyber security. Valori e strategie da costruire insieme, 2020 (Franco Angeli ed.), p. 19.
16 https://cert-agid.gov.it/glossario/phishing/ [visitato il 05/09/2022] ■

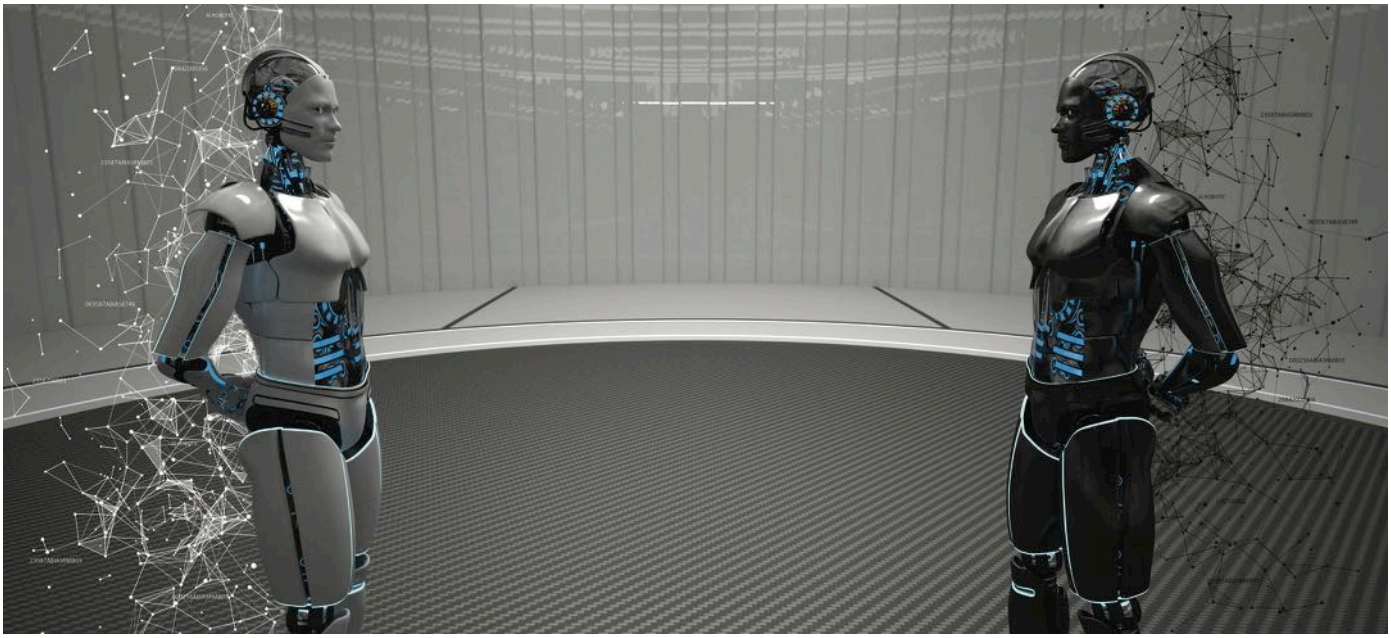
Intelligenza Artificiale "Cattiva" vs Intelligenza Artificiale "Buona". Chi vincerà?

Autore: Rachele Genise

L'Intelligenza Artificiale è una disciplina dell'informatica che studia i fondamenti teorici, i metodi e le tecniche che consentono la progettazione di sistemi hardware e sistemi di programmi software in grado di simulare la capacità e il comportamento del pensiero umano. Questa disciplina negli ultimi anni sta giocando un ruolo sempre più importante nella Cybersecurity. Gli attacchi informatici stanno diventando sempre più complessi e pertanto è sempre più necessario sviluppare nuove tecnologie per gestire tale complessità. Ogni giorno le aziende elaborano grandi volumi di dati sugli eventi, record errati o duplicati e numerosi modelli di malware in migliaia di registri; quindi, il lavoro dell'analista della sicurezza è sempre più complesso e richiede l'aiuto dell'AI. Tuttavia, l'Intelligenza Artificiale può aiutare anche i cybercriminali a condurre attacchi molto più veloci ed efficienti.

L'Intelligenza Artificiale come scudo

L'Intelligenza Artificiale applicata alla Cybersecurity, quindi, entra in gioco per individuare anomalie in tutti i dati raccolti ed esaminati. Le aziende di tutto il mondo sono impegnate nella ricerca di soluzioni per combattere e ridurre il cybercrimine. L'AI si sta rivelando la tecnologia migliore e più adatta a risolvere alcuni dei principali problemi nell'area della Cybersecurity. L'utilizzo dell'Intelligenza Artificiale e del Machine Learning per automatizzare



BIO

Laureata in Informatica e Tecnologie per la Produzione del Software presso l'Università degli Studi di Bari "Aldo Moro", ricopre in SCAI LAB il ruolo di Junior Full-Stack Developer. I suoi studi si sono incentrati principalmente sugli aspetti della programmazione (sia frontend che backend) e nell'utilizzo dell'intelligenza artificiale e dei Big Data, ma nell'ultimo periodo si è dedicata anche allo studio della cyber security e della sicurezza delle informazioni. Rachele crede che con il processo tecnologico sarebbe utile soffermarsi anche sull'uso sicuro e responsabile della tecnologia.

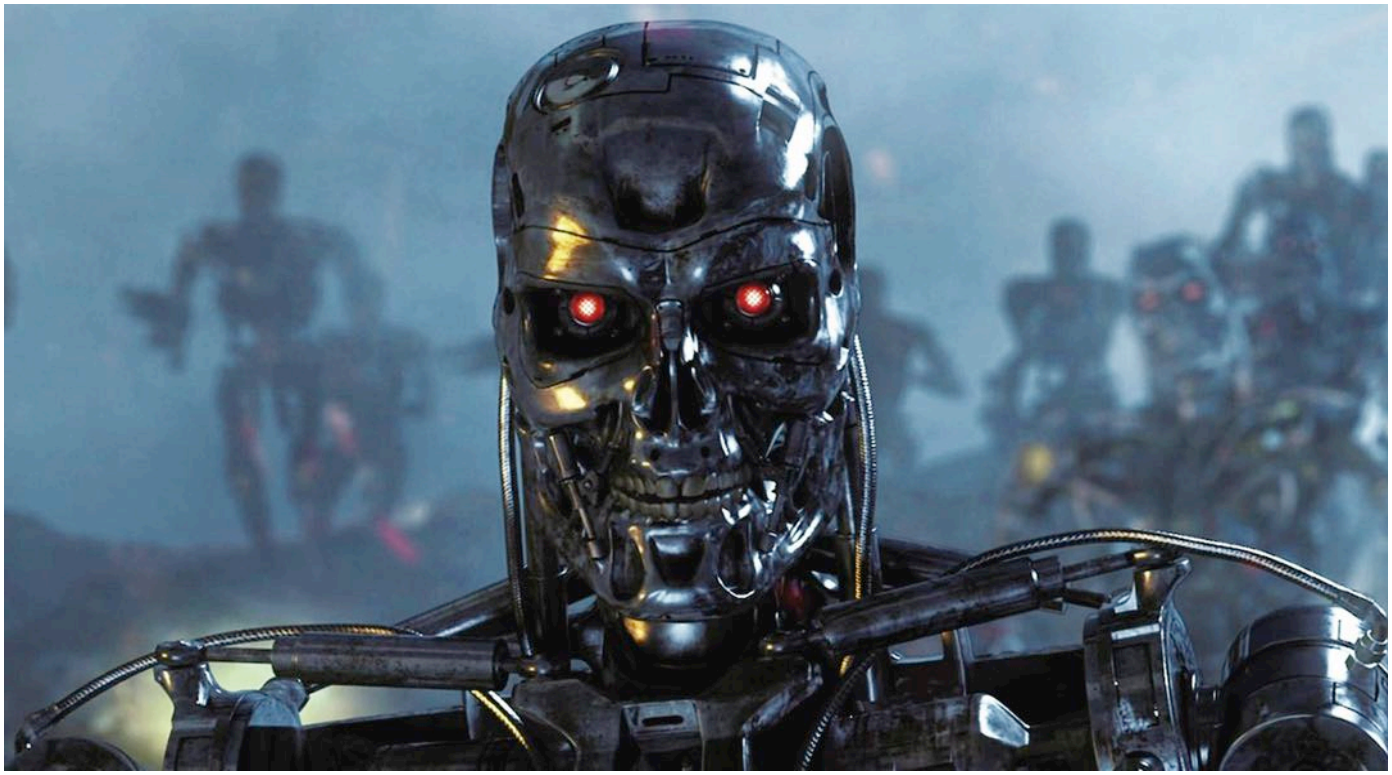
l'individuazione delle minacce, consente di rispondere in maniera più efficace agli attacchi informatici di quanto non avvenga con i tradizionali approcci basati su software. Nello specifico, l'AI aiuta le aziende durante le operazioni di Prevention e Detection degli incidenti di sicurezza. L'automazione consente alle aziende di distinguere tra comportamenti "benigni" e "criminali" attraverso modelli predittivi e utilizzo di dati storici. Questi modelli sono abbastanza intelligenti da rilevare e prevenire una moltitudine di minacce informatiche in tempo reale. Eliminando la necessità di un intervento manuale, le aziende possono focalizzarsi su altri processi che potrebbero richiedere maggiore attenzione. L'AI può anche utilizzare i dati degli attacchi informatici provenienti da più domini e settori in tutto il mondo per migliorare continuamente l'efficacia e i tassi di rilevamento.

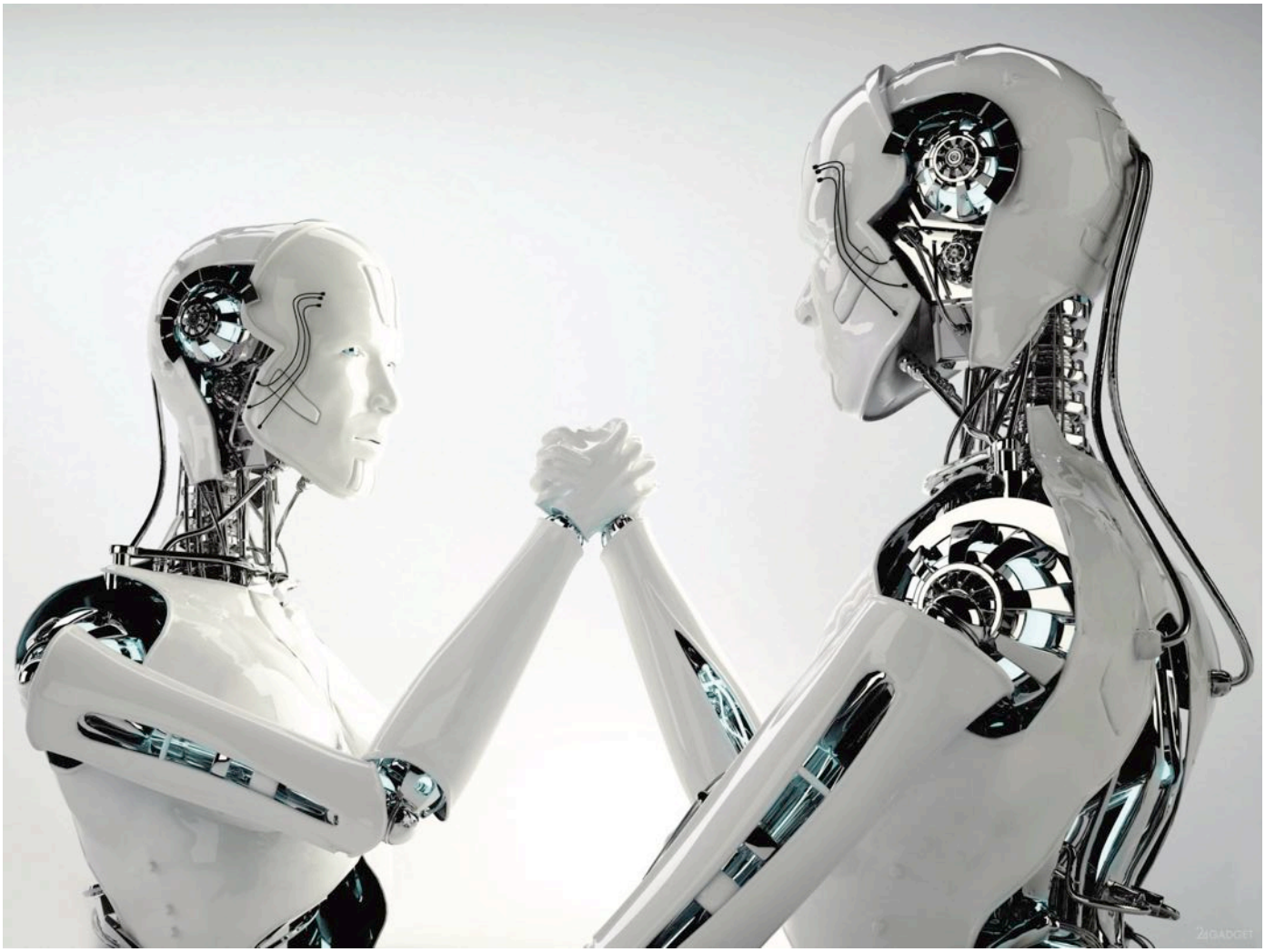
L'Intelligenza Artificiale come arma d'attacco

L'Intelligenza Artificiale può essere vista anche come un'arma, il cui effetto dipende da chi la tiene in mano ed a chi essa è rivolta. Grazie all'utilizzo di tecniche di penetrazione e analisi comportamentali, l'AI può aiutare anche i cybercriminali a effettuare e migliorare i loro attacchi. Nello specifico, l'AI può essere utilizzata dagli attaccanti per la ricerca di vulnerabilità informatiche, ovvero, esegue la scansione di più interfacce all'interno del sistema IT della vittima. Quando si verifica un "hit", l'AI può distinguere se un attacco alla vulnerabilità è in grado d'impattare il sistema o se può semplicemente fungere da mezzo per inserire malware o codice dannoso nella rete. Può indovinare automaticamente le password attraverso l'apprendimento automatico. I criminali informatici possono utilizzano l'AI in connessione con il malware inviato tramite e-mail. Il malware può utilizzare l'AI per imitare il comportamento degli utenti. Gli assistenti d'intelligenza virtuale possono creare testi di qualità semantica così elevata che i destinatari trovano molto difficile distinguerli dalle e-mail reali. Infine, con l'aiuto dei sistemi d'Intelligenza Artificiale, le informazioni disponibili online possono essere estratte in modo più specifico per adattare siti web, collegamenti o e-mail, obiettivo di un attacco.

Artificial Intelligent wars

Come detto in precedenza, l'AI è un'arma e ha i suoi pro e contro in base a chi la utilizza. I cybercriminali la utilizzano per attaccare le aziende, mentre le aziende la utilizzano per difendersi, una specie di guerra tra AI.





Uno dei metodi che usa l'Intelligenza Artificiale attaccante per manipolare l'Intelligenza Artificiale che difende le aziende è il "data poisoning", ovvero, "inquinamento dei dati". Questa minaccia può avvenire in due modi:

- manipolando il set di dati utilizzato dall'Intelligenza Artificiale delle aziende;
- utilizzando tecniche di evasion, ovvero, manomettendo i dati di input forzando gli errori.

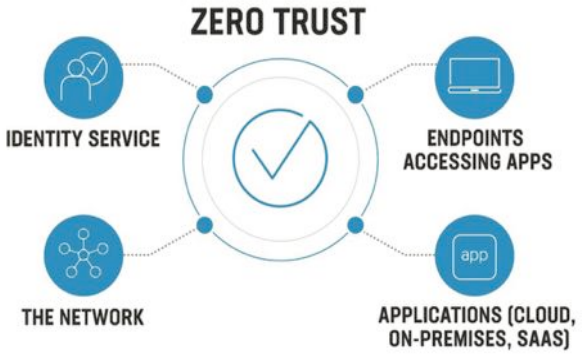
In entrambi i casi, con l'avvelenamento il set di dati è compromesso e quindi non sarebbe affidabile. Una soluzione sarebbe quella di controllare accuratamente i dati già presenti e in input, verificando che le fonti siano affidabili.

Un altro metodo è l'"inferenza", ossia, che gli attaccanti riescano a decodificare i sistemi d'Intelligenza Artificiale da poter capire quali dati utilizza l'AI per l'apprendimento. Questa minaccia consente:

- l'accesso ai dati sensibili;
- spianare la strada al data poisoning;
- riprodurre il sistema d'Intelligenza Artificiale.

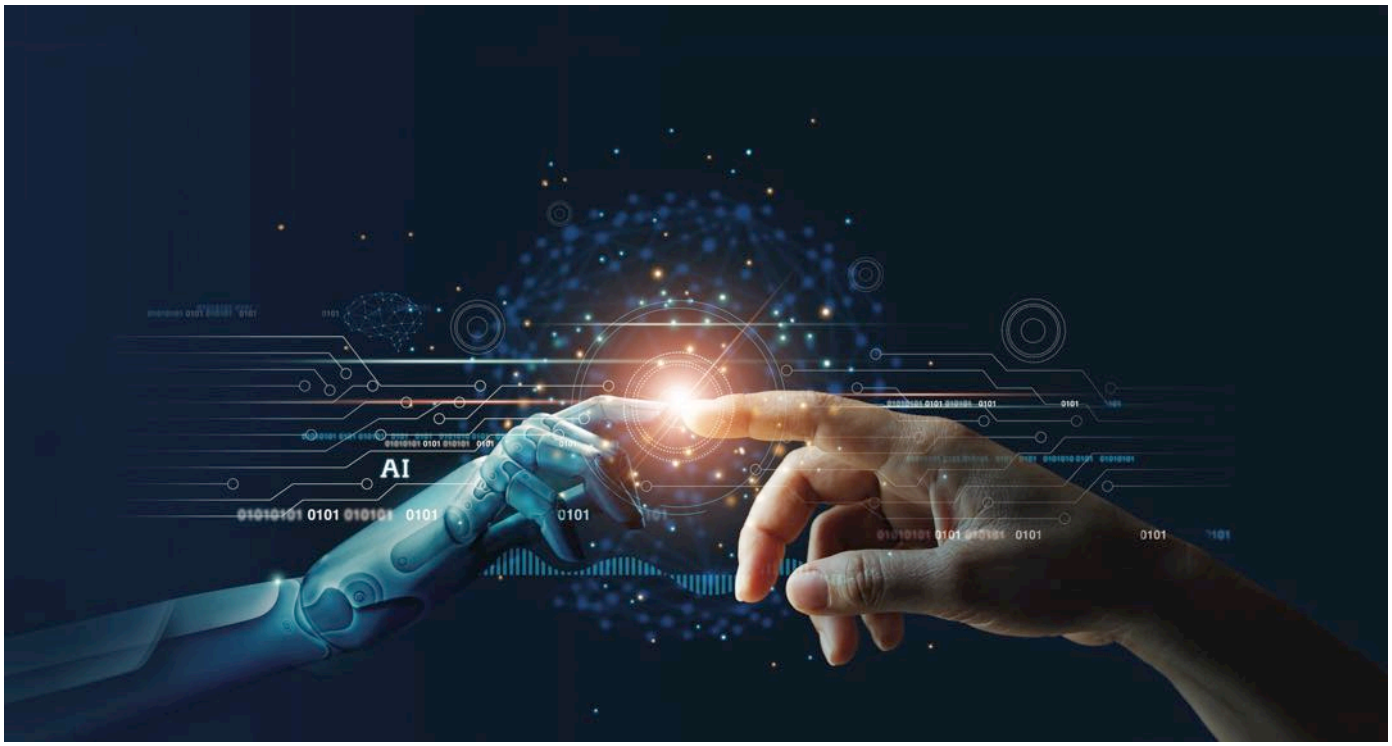
E questo è uno dei problemi più difficili da risolvere.

Le aziende per difendersi da questi attacchi stanno iniziando a combinare algoritmi di machine learning e la politica Zero Trust (considerando tutto dannoso tranne ciò che è esplicitamente considerato "buono") garantendo la sola esecuzione di software autorizzati in precedenza. Questi algoritmi



sono in grado di utilizzare pattern appresi per rilevare quando un processo in esecuzione cambia la sua modalità d'interazione con il sistema operativo e la rete, e sono in grado di prevenire e ripristinare lo stato normale del sistema. Questo approccio, quindi, blocca tutti i tipi di attacchi, anche gli attacchi zero-day, senza introdurre costi operativi eccessivi per le aziende.

I criminali informatici possono utilizzare l'Intelligenza Artificiale per supportare gli attacchi di ingegneria sociale. L'Intelligenza Artificiale può imparare a



riconoscere i modelli comportamentali per convincere le persone via e-mail a intraprendere azioni rischiose o addirittura a consegnare informazioni sensibili. Una contromisura che potrebbe essere utilizzata per mitigare questo rischio include programmi di miglioramento continuo per addestrare il personale a difendersi dagli attacchi di ingegneria sociale attraverso simulazioni e sessioni di brainstorming.

Conclusioni

In un mondo in cui gli strumenti intelligenti sono sempre più utilizzati per scopi vitali e delicati, anche la possibilità teorica che gli hacker possano interromperne la funzionalità solleva molte preoccupazioni. L'AI rileva i rischi e automatizza le procedure di Cybersecurity, ma in realtà offre solo le basi per i processi decisionali umani. A un certo punto deve entrare in gioco l'intelligenza umana, che deve tenere conto anche delle implicazioni sociali ed economiche. In altre parole, l'AI aiuta a costruire conoscenze basate su regole e analisi rigorose, ma non copre aspetti altrettanto importanti come l'intuizione, la creatività, l'empatia o l'intelligenza umana. Non ci dobbiamo solo chiedere se siamo fiduciosi nel compiere un'azione al posto di un'altra, ma anche se ne vale la pena. I dati non possono essere protetti al 100% dall'Intelligenza Artificiale.

Come abbiamo visto, in un modo o in un altro, i cybercriminali potrebbero "prenderla in giro". Infatti, la tutela dei dati personali e la sicurezza sono gli argomenti più discussi in questo ambito. L'AI può esaminare tutti i dati e proteggere il sistema dalle minacce o riparare il sistema se è stato danneggiato. Ma la sicurezza informatica deve essere realizzata con la collaborazione di uomini e macchine. In questa moderna guerra tra AI in ogni caso anche l'intelligenza umana deve arruolarsi! Solo insieme possono combattere gli attacchi informatici. Ci sono così tante possibilità che un sistema completamente AI non può gestire: nuovi attacchi, nuove vulnerabilità e persone che commettono errori.

L'intelligenza Artificiale è utile nella Cybersecurity se c'è un'attenta supervisione umana. Inoltre, visto che i Big Data e l'Intelligenza Artificiale avranno un ruolo sempre più centrale nella sicurezza informatica negli anni a venire, è necessario essere sempre aggiornati e all'avanguardia per poter mettere in atto una risposta adeguata alle minacce. L'Intelligenza Artificiale deve svilupparsi anche mettendo al centro l'etica, per garantire i nostri valori di giustizia, equità e sostenibilità. Concludendo, l'AI è costruita dall'uomo e di conseguenza deve essere l'uomo a porsi le domande per costruirla correttamente sotto il profilo dell'etica, della sicurezza e della privacy. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Cyber Spazio e Psicologia

Negli ultimi anni con l'evoluzione di nuove teconologie abbiamo assistito anche ad una trasformazione dei processi di comunicazione, arrivando a parlare di comunicazione digitalizzata e new media.

Ed è proprio i new media che hanno creato un nuovo spazio comunicativo definito cyberspazio, nel quale sono assenti gli aspetti di metacomunicazione, come la mimica facciale, il tono, la postura, che caratterizzano le conversazioni nello spazio fisico e che indicano quale significato attribuire all'atto comunicativo.

Ma perché quando ci troviamo in un contesto digitale abbassiamo la nostra percezione del rischio?

Sono i nostri 5 sensi che ci aiutano a convivere nel mondo fisico e ci proteggono.

Quando entriamo in un contesto digitale lo scenario cambia, vengono a mancare i sensori per muoversi con sicurezza.

Per esempio durante una rapina c'è l'interazione fisica con il rapinatore, mentre in una frode informatica, la vittima non entrando in contatto fisico con l'autore del reato ha una diversa percezione del rischio.

La distanza psicologica tra aggressori e vittime, generata dall'uso della tecnologica, ha determinato una differente percezione del rischio tra il mondo virtuale e quello reale.

I new media hanno creato nuove tipologie di comunicazione, arrivando a superare le barriere fisiche che causano una limitazione nell'interazione faccia a faccia, ma allo stesso tempo è necessario adottare nuove competenze e comprendere in che modo i cyber criminali stanno riuscendo a trarre vantaggio da questa nuova tipolgia comunicativa, influenzando i comportamenti degli individui rendendoli vulnerabili nel cyber spazio.

Alcuni dei fattori su cui fanno leva le tecniche di manipolazione in ambiente cyber sono:

ANONIMATO
Porta a ridurre l'inibizione e favorisce la messa in atto di comportamenti che offline sarebbero ritenuti negativi o sconvenienti.

VELOCITA'
In internet basta un click, un tempo molto breve affinchè le aree del cervello che permettono un'analisi precisa delle azioni, vengano attivate.

IMPULSIVITA'
Fornire una risposta rapida influenza la capacità di valutare una possibile minaccia.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud.cloud

Michele Mezza
Net-war
Donzelli ed.

Autore: Massimiliano Cannata

La "mediamorfosi", come la tecnologia sta cambiando la guerra

La battaglia in Ucraina ha mostrato nella massima evidenza come la professione giornalistica sia a una svolta. Michele Mezza, ex giornalista e inviato della RAI nel saggio Net-war definisce il fenomeno *mediamorfosi*. "Le informazioni – scrive - sono divenute alluvionali e gratuite, un tempo erano costose, rare e riservate. Questo ha cambiato gli assetti del mercato, causando una modificazione radicale della macchina produttiva. La rete ha oggi assunto l'informazione come "logistica militare", mentre si combatte utilizzando i contenuti come strumento di offesa, agendo sulla psicologia dell'avversario".

Il generale cinese Quiao Liang, ne *"L'Arco dell'Impero"* (ed. LEG) offre una spiegazione ben documentata di quel processo di decentramento delle decisioni indotto dal web, che ha tracciato una diversa geografia dei poteri, rimodellando gli equilibri degli apparati militari. La prima fase del conflitto ha messo a confronto da una parte un modello "ottocentesco" di azione militare, simboleggiato dalla sequenza video della poderosa colonna di blindati russi lunga 65 km; dall'altra parte un sistema articolato e distribuito che combinava le risorse più ordinarie della rete, dai droni agli *smartphone*, da Telegram a Google Street, per localizzare e colpire il nemico mediante la combinazione di informazioni che affluivano dalla popolazione con i sistemi di guerriglia territoriale. L'emblema di questa seconda strategia si può individuare nel celebre appello del ministro dell'innovazione digitale Fiodorov ad Elon Musk di un paio di giorni dopo l'invasione in cui si chiede di mettere a disposizione della resistenza la sua flotta satellitare.

La cosa avviene subito, con una spettacolare capacità di georeferenziare ogni singolo soldato russo che si muoveva sul territorio. Significativo quanto accaduto a Bucha, con la contrapposizione di documenti, fonti, reportage, che hanno poi modificato la visuale stessa del conflitto. Ci si è trovati di fronte a un proliferare di fonti separate dai fatti, sovrabbondanti e parimenti verosimili, perché robustamente documentate da immagini e testimonianze. Arrivare alla conoscenza, per un cronista per raccontare quello che avviene ai tempi della rete e dell'Intelligenza artificiale, in un percorso evolutivo che vede le redazioni trasformate in *software Hours* richiede grande perizia, una lotta estrema contro il tempo, e un estenuante lavoro di formazione.

Risulterà decisivo per ricomporre la frattura tra informazione e informatica, affinare la padronanza della programmazione del software e della gestione del *machine learning* che appaiono oggi funzioni essenziali del bagaglio di un giornalista che si trovi a verificare flussi di dati e a maneggiare supporti di intelligenza artificiale. Come non è concepibile che in una redazione si appaltino conoscenze in materia di economia e politica, tanto meno è accettabile che si possa affidare ai fornitori di soluzioni digitali il compito di decifrare in tempo reale documenti e filmati, senza alcun intervento dell'intelligenza umana. Si automatizza il pensiero, ma anche il conflitto e la geopolitica assumerà un diverso profilo disciplinare, saranno dunque gli algoritmi a sedare le controversie nella prospettiva che molti studiosi collocano nell'era del post umano?

E' lecito chiederselo mentre il disorientamento diventa ancora più forte se si considera che in un universo mediatico sconvolto dall'innovazione tecnologica, il delicato rapporto tra informazione e potere subirà forti contraccolpi. In questa prospettiva lo stato non assumerà più le sembianze del "Leviatano" di Hobbes, ma avrà una struttura porosa costituita dalle reti di informazioni che lo attraversano. Il governo dell'informazione potrà costituire il "respiro" della democrazia, solo a condizione che il diritto di cronaca e la libertà nell'esercizio della professione giornalistica vengano difese, senza cedere di un millimetro a tutte le latitudini. ■

Luca Feliciani, Pierpaolo Rovero
Viaggio nella Rete
Ed. Il battello a Vapore

Autore: Massimiliano Cannata

La storia di Matteo nel "mare aperto" di Internet

La storia di Matteo è quella di tanti bimbi affascinati dal mare periglioso di Internet, ma inevitabilmente ignari dei pericoli che corrono nel loro viaggio in rete. Luca Feliciani è, come si legge nel profilo curato dall'editore, un papà che ama giocare, un creativo che passa molto del suo tempo con i bambini. Il coautore Pierpaolo Rovero, insegnante presso l'Accademia delle Belle Arti di Torino, è un apprezzato disegnatore (molte gallerie d'Europa hanno ospitato i suoi lavori) che fa lavorare la fantasia costruendo mondi, orizzonti, trame che rispecchiano con originalità il fluttuante universo entro

cui viviamo immersi. Quella che hanno intessuta, pubblicata nel libro *Il battello a vapore*, è una trama agile, impreziosita da gustose illustrazioni, che ha la "leggerezza" del racconto calviniano (una rarità va detto se guardiamo ai tanti testi che ingolfano le librerie, ma soprattutto le menti dei lettori oggi) capace di trasmettere significati forti, in maniera facilmente comprensibile, senza orpelli retorici, con il linguaggio che i bambini amano: diretto, privo di ambiguità, immaginifico.

Nel racconto accade che Matteo affascinato dall'*iPhone* del papà lasciato incustodito, cosa che tutto noi facciamo molto spesso con colpevole superficialità, entra nel mondo di Internet, trova un portale meraviglioso dove ci sono oggetti, figure, giocattoli, tutto straordinariamente a portata di mano. Una "pacchia", senza alcuna fatica fisica percorre strade illuminate, lo chiamano anche gli sconosciuti per giocare e divertirsi. Un "paese dei balocchi" di collodiana memoria, ambientato però nell'era virtuale. La morale è sempre la stessa: bisogna essere pronti a resistere alle tentazioni che la società propone, stare lontani dagli sconosciuti, non farsi abbagliare dalle apparenze. La corazza dell'educazione, della formazione, la conoscenza di strumenti e apparati certo aiuta, ma impossibile pretenderle da un bambino, soprattutto quando noi stessi genitori dimostriamo di non essere all'altezza. Il richiamo a un'etica della responsabilità diffusa nell'uso di Internet non è solo il *fil rouge* delle avventure di Matteo, ma l'imperativo categorico che gli autori rivolgono a noi tutti.

Il nostro protagonista si accorge, fortunatamente in fretta, che sta sperimentando una strana realtà, soprattutto una condizione esistenziale non facilmente definibile. Lo "straniamento" che grandi e piccoli dovremmo provare è il primo alert che dovrebbe imporre un freno, alla curiosità legittima quando si sviluppa dentro le regole, altrimenti da sentimento positivo diventa una pericolosa malattia. La ricerca del portale originario ha anche il significato simbolico di chi vuole riappropriarsi della sua vera identità, la porta e il "rito di passaggio" ci dicono gli antropologi, che segna l'attraversamento. La crescita è un attraversamento che dobbiamo compiere insieme ai figli, affrontando l'universo fisico replicato con i materiali della comunicazione, che è il web appunto, ambiente che frequentiamo per molte ore della giornata. Smarrito dalla condizione di inappartenenza, oscillante tra reale e virtuale, Matteo è salvato da papà che lo chiama, usando un epiteto che solo lui può conoscere. C'è dunque, fortunatamente non viene minacciata, un'autenticità segreta che appartiene all'intimità delle nostre relazioni, che non dobbiamo mettere a nudo. Insegnamento prezioso in un'era in cui la "privacy" è ormai esposta nelle piazze virtuali. Matteo aveva pensato di essere un "zombi", di aver cambiato identità. Un'esperienza scioccante per molti aspetti, che bambini e ragazzi vivono continuamente avendo in mano strumenti digitali piccoli ma estremamente potenti.

Feliciani e Rovero chiamano in causa Alessandro Curioni, giornalista e docente molto esperto di sicurezza informatica, che la nostra rivista ha in passato più volte interpellato. *"Siamo come pesci nella rete – ci aveva detto lo studioso - dobbiamo per questo maturare la consapevolezza che le nuove tecnologie presentano dei vantaggi e che i rischi sono direttamente proporzionali a questi vantaggi. Se le tecnologie penetrano il mondo reale e ne gestiscono in modo autonomo i mezzi e gli strumenti dobbiamo comprendere che tutte le minacce che abbiamo sempre pensato fossero confinate al di là di uno schermo, da domani saranno "applicabili" al mondo reale, con tutto quello che ne consegue. Chi opera nella sicurezza a tutti i livelli dovrà tenere conto che la logica del "controllo" legata alla vecchia concezione dei perimetri fisici da presidiare ha ceduto il passo alla governance del rischio. Il risultato è che avremo bisogno di aggiornare conoscenze e competenze per reggere la sfida portata da livelli crescenti di complessità".*

Riportando il ragionamento all'educazione dei più piccoli, Curioni suggerisce di adottare comportamenti coerenti, rispettosi della logica che può apparire elementare, che sovente trasgrediamo. Lasceremmo da solo nostro figlio di 4 anni ai giardinetti? Eppure lo lasciamo con lo smartphone, gli consentiamo di navigare e di soffermarsi su immagini pericolose. Facciamo postare ai figli foto delle loro feste private, senza tenere conto della platea che può andare a vederle. Esiste insomma quella che Curioni definisce "insostenibile leggerezza" che diversamente da quella calviniana che ricordavamo all'inizio, tradisce una scarsa cultura del digitale, che non possiamo più permetterci.

Il libro contiene un'appendice dedicata ad alcune interessanti istruzioni per viaggiare in rete in sicurezza che vale la pena ripercorrere. Chiedere sempre ai genitori il permesso di usare dispositivi elettronici che si trovano in casa, fare attenzione alle app che sono utilizzabili, osservare il massimo rigore nel far circolare informazioni personali, ragionare sempre nel doppio binario reale virtuale per cercare di adottare comportamenti meno esposti al rischio. I dubbi sono legittimi, probabilmente mamma e papà ne sanno di più, consultiamoli con fiducia e meno scetticismo. Una cosa è certa: disconnettersi non è un reato quando si è stanchi o a disagio, giova anche non dimenticare mai che in rete molte cose non sono reali, le identità possono essere camuffate; quindi, ogni cosa va "presa con le molle". Si potrebbe obiettare che non sempre i genitori e nemmeno gli adulti sono vicino a noi, un motivo in più per aspettare prima di addentrarsi in pratiche e iniziative di navigazione potenzialmente pericolose. Come si vede bastano anche pochi accorgimenti per riuscire a far emergere tutto il potenziale della tecnologia, minimizzando quel "lato oscuro della rete" che pure esiste, e da cui dobbiamo tenere il più possibile lontano noi e i nostri figli, se vogliamo guardare con fiducia alla positività del progresso. ■

Gian Luca Comandini
L'uomo più ricco del mondo
Ed. Rizzoli

Autore: Massimiliano Cannata

Satoshi Nakatomo ha ideato i bitcoin?

Sono sempre le persone normali che cambiano il mondo. L'importante è crederci, senza stancarsi mai di sfidare l'esistente. "L'uomo più ricco del mondo" è un libro su una di queste persone, Satoshi Nakamoto, ideatore dei *bitcoin* (forse), non vogliamo infatti togliere al lettore il gusto di scoprire la composizione del puzzle fino allo svelamento del mistero. Si capisce subito che il problema non è l'identità del singolo, perché non fa la differenza, l'attenzione dell'autore si concentra sull'entità e le conseguenze della rivoluzione tecnologica. "Nakamoto potrebbe essere una delle tante icone, reali o virtuali, della digital society, una delle nuove divinità della nostra epoca. Da sempre gli uomini hanno bisogno di trovare guide e quando le guide terrene falliscono, cerchiamo risposte e responsabilità in modelli che hanno matrici ideologiche, spirituali, invisibili e intoccabili. Il protagonista del mio racconto è frutto di questa esigenza. Chi si cela dietro di lui ha cercato disperatamente di sparire dai radar e facendoci capire che bisognava concentrarsi sui fenomeni di trasformazione che stanno modificando equilibri sociali ed economici che credevamo consolidati".

L'argomentare di Comandini si conferma sempre brillante, la nostra rivista si era già occupata dell'ultimo suo scritto *Da zero alla luna* (Ed. Dario Flaccovio), coniugato com'è al futuro, che è la cifra di questo brillante imprenditore e manager inserito dalla rivista "Forbes" tra gli under 30 più influenti del Pianeta, considerato da *Millionaire* tra i quindici giovani in grado di cambiare il volto del nostro Paese. In questo scritto è la ricchezza il tema centrale, concetto difficile da declinare nella società del web segnata dagli extra profitti dei giganti di internet e dal prepotente sviluppo del "capitalismo delle piattaforme" fenomeno complesso da disciplinare. "Nulla di diverso rispetto a quanto siamo sempre stati abituati – commenta l'autore - il turbocapitalismo ci aveva, infatti, condotti molto prima dell'era dei colossi web a percorrere itinerari non facili da decifrare.

Gli extra profitti in passato erano generati da altre industrie ed altri "giganti", refrattari al disciplinare, che in seguito sono stati inquadrati in un tessuto normativo, attraverso un processo che ha comunque portato alla nascita di una nuova era e all'emergere di nuovi colossi. Ritengo che in breve tempo dovrà farsi strada una regolamentazione più stringente, soprattutto a livello fiscale, dei colossi web e questo porterà verso un diverso mercato, magari proprio inerente a quello che possiamo definire come web3.

Serviranno teorie economiche aggiornate per spiegare quello che sta già accadendo, inutile cercare o praticare conoscenze obsolete, che hanno fatto il loro tempo. Persino termini chiave come "privacy" e "dato", andranno sintonizzati e riscritti, lo richiede la rivoluzione in corso".

Blockchain è oggi la parola *passe-partout*, sulla bocca di tutti anche se pochi ne conoscono realmente il significato. "Si tratta di una tecnologia rivoluzionaria che si pensa potrà cambiare la nostra quotidianità da dieci a quindi volte più di quanto abbia fatto Internet" - spiega l'imprenditore - non è altro che un registro di informazioni immutabile e basato su crittografia, simultaneamente condiviso in maniera decentralizzata tra più utenti, che hanno tutti lo stesso potere in virtù del quale possono tutti consultarlo, ma le decisioni spettano alla maggioranza di loro, come nel caso di un unico grande controllore.

Se tutti si possono controllare, viene disincentivato il ladro o il delinquente tra loro. I *Bitcoin* e le *criptovalute* sono solo alcune delle applicazioni che la blockchain rende possibili e che cambieranno il nostro mondo, come di fatto sta già accadendo". La fascinazione per il futuro e la trazione anteriore che ne consegue non deve far dimenticare il valore della memoria. "Essere stati è la condizione per essere" come ricorda il grande storico degli Annales, Fernand Braudel, la riflessione rispecchia molti passaggi interessanti del saggio a partire dal delicato rapporto che si sta instaurando tra la moneta virtuale, esaltata da molti analisti e osservatori, e la moneta reale, che sta riprendendosi il suo spazio, basti prendere in esame progetti come quello che sta portando avanti Paolo Pampaloni che sta coinvolgendo un fitto tessuto di PMI.

Non bisogna pensare che siano fenomeni in controtendenza, perché esprimono la necessità di ritrovare un appiglio etico nella pratica degli scambi, ridando valore delle relazioni interpersonali, al rispetto delle persone che vengono prima di qualsiasi oggetto, fosse anche in assoluto il più prezioso. Relazione, per usare il linguaggio hegeliano, che deve farsi prassi inverandosi nella storia per assumere le sembianze dell'innovazione dirompente.

Su questo fronte, teoretico e pratico insieme, il nostro interlocutore mostra di avere le idee chiare, sollevando inquietanti interrogativi: "L'uomo è molto più vecchio della moneta e oltre 10.000 anni fa non ne avevamo neanche bisogno, ci basavamo sull'Economia del dono e poi sul baratto, anche civiltà evolute come gli Antichi Egizi non avevano bisogno della moneta e questo va sottolineato. Abbiamo dovuto creare la moneta per comodità ma anche perché non ci fidavamo più delle persone, ed è lì che abbiamo fallito.

Se smettiamo di fidarci delle persone, subiremo il potere degli strumenti. Il mondo che stiamo costruendo dovrà seguire nuove regole, se non siamo in grado di scriverle allora creeremo nuovi ricchi senza regole che finiranno per non riconoscere nessun orizzonte regolatorio, con le conseguenze del caso.

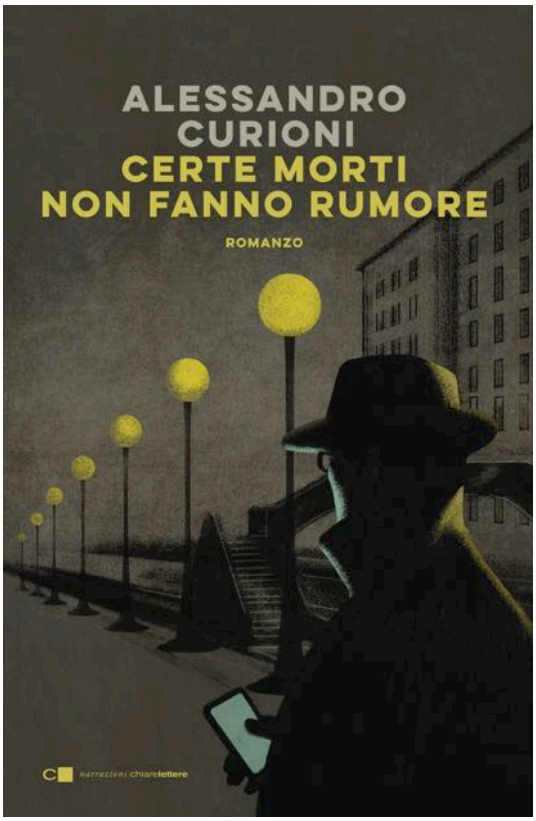
Facciamo l'esempio di Elon Musk: se arrivasse su Marte e decidesse di costruire la sua civiltà? Chi potrebbe contrastarlo? Si arriverebbe a una guerra interplanetaria tra un governo mondiale riconosciuto e un ricco privato che si auto-proclama proprietario di un nuovo mondo? La massa chi seguirà?". Trovare risposte appare impossibile mentre siamo nel guado di una trasformazione che investe la mentalità e la cultura; quindi, il tessuto antropologico e la struttura profonda della civiltà cui apparteniamo.

Una cosa appare evidente: la rivoluzione digitale imporrà un aggiornamento continuo delle competenze. Nel saggio Comandini sottolinea a più riprese la necessità di aggiornare i saperi per far crescere nella collettività la giusta sensibilità per affrontare le fenomenologie del cambiamento, nei diversi ambiti in cui si manifestano. Servirà anche l'intervento dello Stato, altro aspetto importante sostenuto nella trattazione. I fondi pubblici andranno finalizzati a formare e alfabetizzare vecchie e nuove generazioni, in modo da colmare la domanda di figure professionali emergenti. La tv, la scuola, la politica devono affrontare i grandi temi della trasformazione epocale entro cui tutti siamo immersi.

"Dovremmo mettere – conclude Comandini - la stessa attenzione e premura che riserviamo all'effettivo raggiungimento della parità di genere, al rispetto di tutte le religioni, alla libertà di espressione, alla salvaguardia dell'ambiente. Educare al futuro si configura come un imperativo categorico, che richiederà determinazione, consapevolezza, competenza, perché l'alternativa vuol dire estinzione della specie umana, riflettiamoci seriamente una volta per tutte…". ■

Alessandro Curioni
Certe morti non fanno rumore
Chiarelettere Ed.

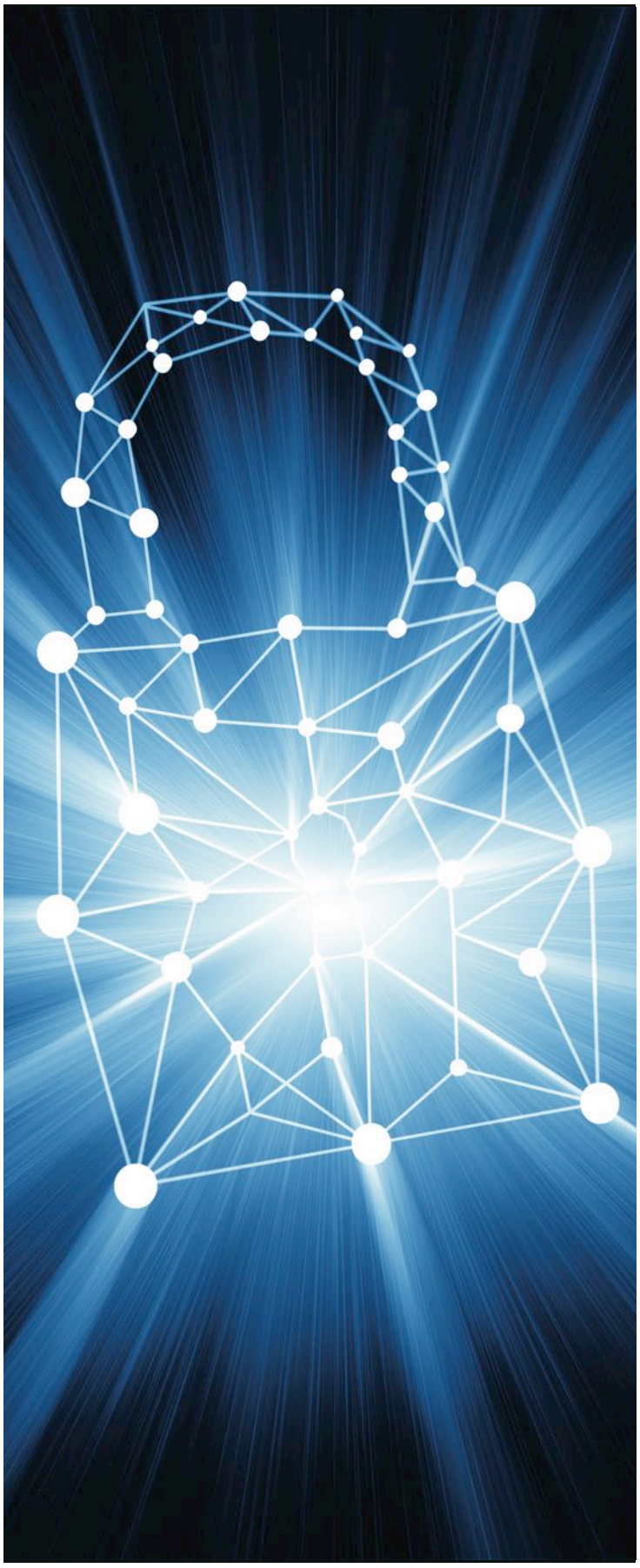
Alessandro Curioni (1967) nasce giornalista e nel 2003, dopo un biennio di studio, pubblica per Jackson Libri il volume Hacker@ tack dedicato alla sicurezza informatica. Da questa esperienza, e dopo sette anni nel settore, fonda nel 2008 Di.Gi. Academy, azienda specializzata nella formazione e nella consulenza nell'ambito della cybersecurity, della quale è azionista e presidente. È autore di saggi di successo, divulgatore, docente universitario e commentatore presso organi d'informazione come Rai, "Il Sole 24 Ore" e Class Cnbc. Certe morti non fanno rumore è il secondo romanzo della serie che vede protagonista l'esperto di cybersecurity Leonardo Artico.



Dopo aver messo a soqquadro il Dark Web, debellando la più pericolosa rete di criminali informatici in circolazione, l'esperto di cybersecurity Leonardo Artico finisce di nuovo nel mirino. Dal suo passato riemerge un'amante, nel frattempo diventata la potentissima manager di una big tech, e con lei si materializza un'eminenza grigia a capo di un nucleo dei servizi segreti. Entrambi con un'offerta che non si può rifiutare. Artico - con i suoi compagni di avventura Roberto Gelmi, hacker geniale, e Teresa Aprili, brillante giornalista – si ritrova così coinvolto nel segretissimo Progetto Da Vinci, che attraverso l'uso dell'intelligenza artificiale punta a rivoluzionare il mondo della cybersecurity.

Ma con quali conseguenze? Leonardo giocherà la sua personalissima partita con obiettivi molto diversi da quelli degli altri due giocatori. Il doppio e il triplo gioco saranno la regola, la manipolazione d'informazioni e persone la normalità. In un mondo oscuro sul quale aleggia l'ombra di un nemico sconfitto, ma non abbattuto, Leonardo, Teresa e Roberto scopriranno che per smascherarlo devono rischiare molto più della loro vita digitale.

Certe morti non fanno rumore è un romanzo che ci pone di fronte a temi di stringente attualità e ci fa riflettere sul ruolo dell'umanità nel momento in cui la tecnologia, con l'avvento delle intelligenze artificiali, sembra pronta a un nuovo grande balzo. ■



Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

Co-Lead Sponsor **Strategic Partner** **Media Partner**

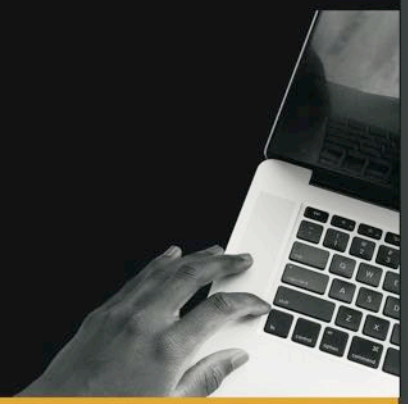
KEKST CNC

AMERICAN CHAMBER OF COMMERCE IN ITALY
Est. 1915

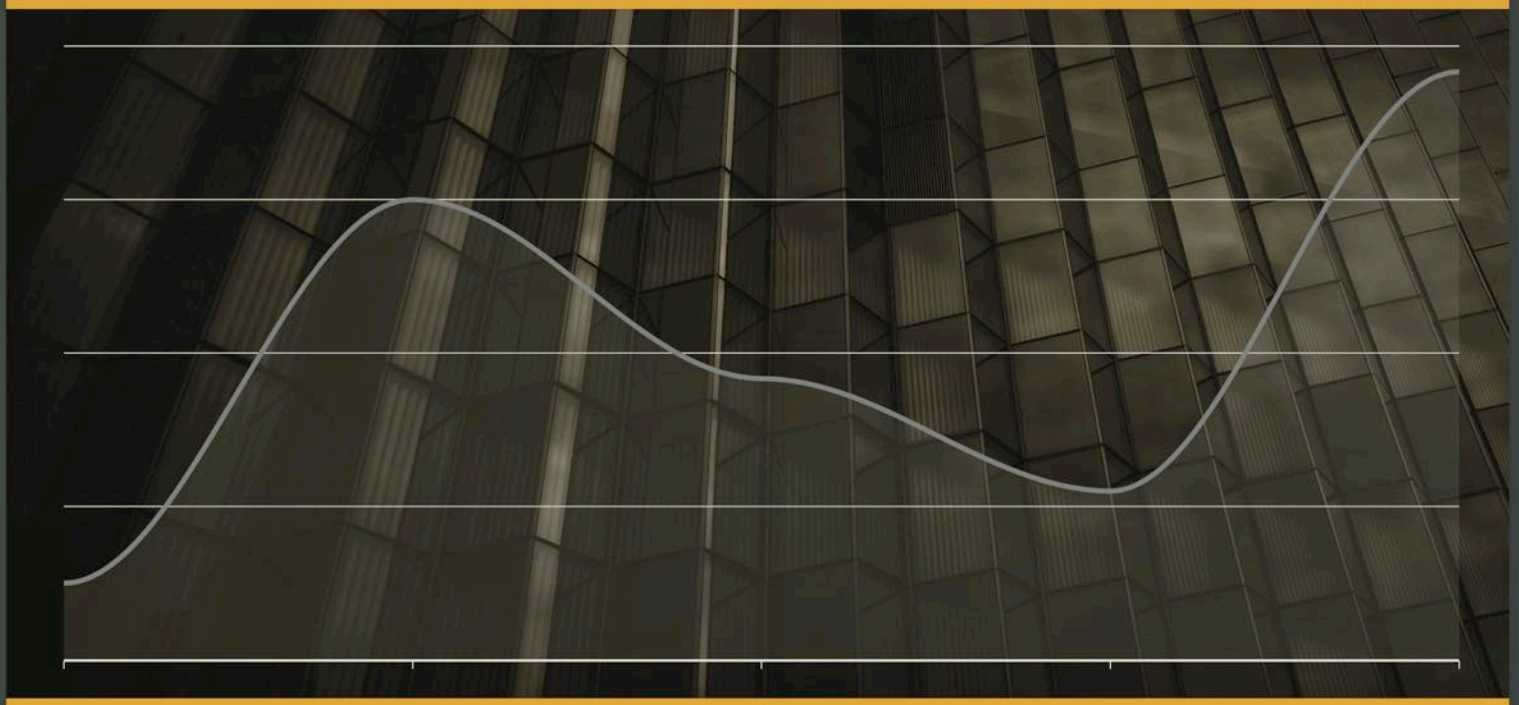
Cybersecurity Trends

IT Security Ranking

Conosci il livello di sicurezza IT della tua azienda?



Misuralo con la nostra piattaforma di valutazione



PRESTO DISPONIBILE SU cybertrends.it

Cybersecurity Trends