Cybersecurity Trends

Edizione italiana, N. 2 / 2019

INTERVISTE VIP:

Paolo BENANTI
Luciano FLORIDI

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Central Folder: Etica e Intelligenza Artificiale

Global Cyber Security

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

Information Sharing
Creazione di modelli di information sharing pubblico - privato

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

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione e corsi di specializzazione e master

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

GLOBAL CYBER SECURITY CENTER

Indice

Intelligenza aumentata ed etica la nuova sfida

Autore: Nicola Sotira

Sempre più presente in workshop, eventi, articoli il tema dell'Intelligenza artificiale (AI) o intelligenza aumentata, tema che promette una nuova rivoluzione, un cambiamento radicale che coinvolgerà tutti i settori industriali e la pubblica amministrazione introducendo innumerevoli cambiamenti nei modelli di business e migliorando l'efficienza dei processi. Come sempre l'innovazione digitale introduce nuove opportunità e scenari da terra promessa, occorre però valutare, in questo caso, che il tema potrebbe nascondere anche alcuni rischi come la limitazione delle libertà personali, la discriminazione e la manipolazione dell'opinione pubblica. Sul tema dell'informazione, per esempio, la nuova frontiera del giornalismo si chiama **Knowhere News**, una startup americana che promette informazioni neutrali; in questa piattaforma una sapiente combinazione di l'intelligenza artificiale e machine learning promettono ai lettori solamente fatti. Chi pensava solo alle auto intelligenti e alla guida autonoma, forse dovrebbe considerare anche le informazioni automatizzate dalle macchine come già succede nel settore musicale.

Gli algoritmi regoleranno: notizie, automobili, fabbriche, reti e la medicina. Ma quali sono i lati oscuri, i rischi di tutta questa innovazione? Sicuramente i temi di sicurezza e fiducia saranno sempre più centrali nella mitigazione del rischio e nel garantire la tutela dei nostri dati; la trasparenza e la corretta gestione di questi aspetti saranno fattori determinanti per il successo aziendale.

Nick Bostrom, nel suo controverso libro "La superintelligenza", sottolinea come sia necessario sviluppare, fin dall'inizio, tattiche e strategie per evitare che la superintelligenza arrechi minacce all'umanità. Bostrom propone alcune soluzioni, e in particolare una di queste consisterebbe nell'assegnare a questi agenti artificiali non solo compiti, ma anche valori reali, insistendo su come i governi debbano avviare una vera riflessione etica sugli usi e la governance di questa tecnologia. Uno dei temi centrali ad esempio sono i dati, sappiamo che tutti questi sistemi di AI per poter apprendere hanno bisogno di enormi quantità di dati e sarà quindi necessario valutare l'impatto su privacy e sicurezza.

Le tecnologie AI potrebbero essere soggette a gravi violazioni di dati e furto di identità. Dobbiamo coinvolgere i data scientist a sviluppare modelli che tengano conto degli utenti e della sicurezza e riservatezza dei loro dati. Il GDPR ha già indirizzato il tema, creando un quadro normativo che garantisce la protezione dei dati personali insistendo su modelli di security by design che devono trovare applicazione e diventare processi consolidati nel software e nello sviluppo hardware.

In questo contesto, la Commissione Europea ha pubblicato delle Linee Guida con riferimento alla progettazione di sistemi affidabili di intelligenza artificiale ma che al momento non sono requisiti obbligatori.

Le linee guida includono una check-list che consente di verificare, già in fase di progettazione, la conformità alle raccomandazioni, una sorta di *etica-by-design*. Un nuovo concetto che deve essere coniugato insieme al quasi consolidato tema della *sicurezza by design*.

Il documento della Comunità Europea non raccomanda solo la robustezza e la sicurezza dei sistemi, ma si focalizza sul ruolo centrale dell'essere umano nella relazione con l'intelligenza artificiale. I principi che devono essere combinati sono la dignità e la libertà, specialmente quando entrano in gioco gli algoritmi. Il documento evidenzia come l'autonomia delle persone deve prevalere sull'autonomia delle macchine e deve essere garantito un potere di supervisione da parte degli uomini. L'evoluzione di questi sistemi deve andare verso forme di AI trasparenti e chiaramente tracciabili, garantendo in questo modo uno sviluppo sostenibile di cui la nuova industria potrà beneficiare portando innovazione e benessere per l'uomo. ■

BIO

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

Autore: **Marco Obiso,**
Coordinatore per la cyber security, International Telecommunications Union, Ginevra

L'etica ovvero la più grande sfida nel campo dell'ICT

L'etica è certamente uno degli aspetti più dibattuti della rivoluzione digitale, che raggiungerà il suo apice con l'implementazione della tecnologia 5G, permettendo alla maggior parte degli abitanti del pianeta di avere un accesso a internet a piena velocità.

L'etica dipende in larga misura dal contesto sociale, politico e religioso, e ogni paese e organizzazione dovrà definire quale codice etico applicare.

Per rendere significativo il "viaggio etico", il punto di partenza è come di consueto la sensibilizzazione e la condivisione della conoscenza, consentendo a tutti gli stakeholder e al pubblico in generale di comprendere meglio il concetto nel contesto della trasformazione digitale.

Un'ampia sezione del presente numero è dedicata a tali riflessioni, al fine di facilitare una migliore comprensione del rapporto tra comportamenti etici e le immense opportunità che le tecnologie digitali attuali ed emergenti possono portare alla comunità globale. ■

Buona lettura!

L'evoluzione normativa tra privacy e Intelligenza Artificiale

Autore: Giancarlo Butti

Ritorniamo[1] dopo oltre un anno ad affrontare il tema di privacy ed IA (si veda in proposito il n. 2/2017 di Cybersecurity trends). L'occasione è la recente pubblicazione (25 gennaio 2019 a Strasburgo) da parte del **Comitato consultivo (cd. t-pd) della convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (convenzione 108) delle Linee-guida in materia di intelligenza artificiale[2] e protezione dei dati.**

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9096716

Si tratta di un passo importante che si colloca in un percorso che aveva visto a ottobre 2018 le Autorità Garanti privacy mondiali emettere un documento dal titolo molto significativo: **Declaration on ethics and data protection in artificial intelligence.**

Tale documento[3] è stato adeguatamente sintetizzato dall'Autorità Garante italiana[4] nei seguenti punti:

- sviluppare le applicazioni di IA secondo un principio di correttezza, garantendo che vengano utilizzate soltanto per facilitare lo sviluppo umano senza ostacolarlo o minarlo
- responsabilizzare tutti i soggetti coinvolti, attivando forme di vigilanza continua e definendo processi verificabili di governance dell'IA
- migliorare la trasparenza e l'intelligibilità dei sistemi di IA
- permettere un effettivo "controllo umano"
- sviluppare le applicazioni di IA secondo principi di privacy-by-design e di privacy-by-default.

Già in precedenza specifiche Autorità Garanti avevano emesso pubblicazioni su questo tema.

In particolare **ICO** (Autorità garante inglese) ha pubblicato: **Big data, artificial intelligence, machine learning and data** ed il **CNIL** (Autorità garante francese): **Comment permettre à l'homme de garder la man?**

Le pubblicazioni esprimono preoccupazioni in merito all'uso dell'IA, in particolare riguardo alla scarsa trasparenza degli algoritmi e alla loro possibile manipolazione, e propongono dei suggerimenti su come realizzare applicazioni che garantiscano una maggior trasparenza e un maggior coinvolgimento degli utenti.

Al riguardo le **Linee guida** recitano:

11.Gli interessati dovrebbero essere informati se interagiscono con un'applicazione IA e hanno il diritto di ottenere informazioni sulla logica alla base dei trattamenti di dati che li coinvolgono. Le informazioni da fornire dovrebbero comprendere le conseguenze derivanti dall'applicazione di tale logica.

Anche nel caso in cui siano fornite adeguate informazioni, si pone il problema di capire se le stesse siano veritiere, e quindi uno dei temi evidenziati dai documenti di cui sopra è la possibilità di poter effettivamente verificare il comportamento di tali applicazioni, tramite un'attività di audit.

Attività questa tutt'altro che semplice e che richiede la disponibilità di competenze molto specializzate.

Anche il governo delle soluzioni di IA pone diversi problemi.

Come già espresso nel precedente articolo, il GDPR, nel suo articolo 22 **"Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione",** cerca di porre un freno quantomeno all'uso di profilazioni completamente automatizzate che abbiano conseguenze significative sugli individui.

Anche in questo caso ci sono tuttavia delle limitazioni. Da un lato, tale pratica è comunque consentita con il consenso del soggetto interessato o nell'ambito di un contratto (entrambe situazione dove la reale libertà di scelta dell'interessato è dubbia), dall'altra tale tutela riguarda unicamente le persone fisiche. Il GDPR introduce comunque delle misure correttive al possibile uso distorto dell'IA allorquando si presentino i casi prima citati (consenso dell'interessato o adempimenti contrattuali, autorizzazione di legge):

il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Il limite della reale tutela di questo articolo sta nella sua interpretabile applicabilità, che si limita a considerare i casi in cui la profilazione: *produca effetti giuridici che lo riguardano o che incida in modo analogo* ***significativamente*** *sulla sua persona.*

Sicuramente in tale fattispecie non si sarebbe portati a considerare l'inoltro mirato di semplici messaggi pubblicitari ad esempio ad una futura mamma, salvo poi essere contraddetti dalla missiva che Gillian Brockell ha indirizzato alle aziende che le inondavano di messaggi mirati per prodotti per bambini: *"se siete abbastanza intelligenti da rendervi conto che sono incinta siete sicuramente abbastanza intelligenti da rendervi conto che il mio bambino è morto".*

Appare evidente come la futura mamma fosse stata profilata in funzione della consultazione di siti dedicati a prodotti per neonati e in conseguenza di questo ricevesse pubblicità mirata.

Purtroppo i sistemi che hanno raccolto ed elaborato tali informazioni non hanno saputo cogliere un'altra importante informazione: l'assenza improvvisa di quelle ricerche cha hanno portato alla sua profilazione.

Certamente dopo la perdita del figlio, quella che poteva essere considerata una innocua e anche utile comunicazione, è diventata talmente spiacevole da spingerla alla comunicazione sopra riportata.

BIO

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

Questo sposta notevolmente la valutazione di cosa possa essere considerato *significativo*, e come, in casi analoghi a quello considerato, tale valutazione possa variare nel tempo, o meglio come non ci si possa limitare all'uso di sistemi di profilazione automatizzata, ma debba esistere un sistema complessivo di governo degli stessi, capace di gestire rapidamente casi come quello citato.

Anche la limitazione alle persone fisiche della tutela offerta dalla normativa suscita qualche perplessità; concedere o meno un fido ad un'azienda in base a scelte totalmente automatizzate non trova una mitigazione nel GDPR, che non si applica a tali soggetti, ma presenta gli stessi limiti e rischi che si hanno con le persone fisiche.

Non va inoltre dimenticato che un'azienda è comunque composta da persone fisiche e quindi, una decisione che può influenzare il futuro di un'azienda, impatta sicuramente su tali soggetti.

Anche in questo caso l'uso di sistemi automatizzati rende sicuramente più oggettiva la valutazione, (ovviamente se non sono stati introdotti ad arte criteri

discriminatori) e questo è sicuramente un grosso vantaggio per tutti; il problema può risiedere nella incapacità del sistema di cogliere aspetti nuovi o diversi rispetto a quelli che rappresentano il suo patrimonio di conoscenze. È lì che l'uomo prevale sui sistemi automatizzati e suggerisce che l'ottimo per creare un sistema che possa essere oggettivo, ma anche flessibile, richieda necessariamente la combinazione di uomo e macchina.

Anche nel caso della concessionaria di auto, che si è vista rifiutare la pubblicità da parte di un social network, (perché il suo nome è stato considerato offensivo dall'algoritmo che controlla i testi da pubblicare), il problema non è certo dell'algoritmo utilizzato (che ha fatto il suo dovere), quanto sul governo del processo. Sarebbe sufficiente la presenza di un operatore che possa raccogliere le osservazioni di soggetti coinvolti per migliorare la capacità di analisi del sistema e offrire un servizio di qualità.

Ma c'è un altro articolo del GDPR che impone l'uso di misure tutelanti per gli interessati; l'art. *Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, richiede*, più comunemente noto come privacy by design e by default.

È interessante notare che le **Linee guida** citate all'inizio si spingono oltre tale formulazione, e introducono il concetto di *"human rights by design"*, riferendosi alle cautele che gli sviluppatori di applicazioni di IA devono mettere in atto onde *evitare qualsiasi potenziale pregiudizio (bias), anche involontario o occulto, il rischio di discriminazione o altri effetti negativi sui diritti umani e le libertà fondamentali degli interessati.*

Tali rischi possono derivare, fra gli altri, dalle vulnerabilità intrinseche di qualunque applicazione software, alle quali però si aggiunge un ulteriore strato di vulnerabilità, costituito dagli algoritmi che già in fase di addestramento o successivamente possono essere a loro volta manipolati e indotti nell'errore. Da ultimo un cenno al problema della qualità dei dati utilizzati (molto spesso provenienti da fonti aperte) ad esempio per elaborare profili o per concedere un prestito.

Al riguardo la pubblicazione **Big data and privacy – Making ends meet della FPF (Future of Privacy Forum)** riporta il caso della signora Judy Thomas e dalla signora Judith Upton i cui profili creditizi sono stati scambiati in conseguenza della quasi perfetta coincidenza dei loro SSN, con le relative conseguenze. La pubblicazione indica che ben il 26% dei credit report analizzati contenevano errori. ■

1 Coautore con il prof. Lorenzo Schiavina di "Intelligenza artificiale esoftcomputing", FrancoAngeli, 2017
2 Il Consiglio d'Europa definisce l'IA come „Un insieme di scienze, teorie e tecniche il cui scopo è quello di riprodurre, attraverso la macchina, le capacità cognitive di un essere umano. Gli sviluppi attuali mirano, ad esempio, ad affidare a una macchina compiti complessi precedentemente delegati a un essere umano."
3 https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
4 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9059156#4

Siamo di fronte a un'altra specie di sapiens che abita il pianeta

Intervista VIP a Paolo Benanti

Autore: Massimiliano Cannata

Lo sviluppo e la diffusione delle intelligenze artificiali ha cambiato il nostro modo di essere nel mondo, oltre ai nostri processi conoscitivi. La svolta non è solo di natura tecnica, ma spirituale e filosofica. Tornano di attualità grandi interrogativi che hanno segnato l'evoluzione del pensiero occidentale. Quella di Benanti è una delle voci più lucide della contemporaneità. Aperto in maniera autentica all'innovazione, segue con passione e senso della trascendenza lo spostamento della frontiera della conoscenza verso traguardi sempre più ambiziosi, senza mai perdere di vista la centralità dei valori e dell'uomo. "Solo se sapremo includere – spiega nell'introduzione del suo stimolante saggio – le *humanities* nella creazione delle macchine sapienti potremo sperare di non produrre, in un futuro più o meno vicino, società disumane". Un monito importante che le classi dirigenti a qualunque livello dovrebbero tenere ben presente.

BIO

Frate francescano del Terzo Ordine Regolare - TOR - sono nato il 20 luglio del 1973. Docente alla Pontificia Università Gregoriana, mi occupo di etica, bioetica ed etica delle tecnologie. In particolare i miei studi si focalizzano sulla gestione dell'innovazione: internet e l'impatto del Digital Age, le biotecnologie per il miglioramento umano e la biosicurezza, le neuroscienze e le neurotecnologie. Cerco di mettere a fuoco il significato etico e antropologico della tecnologia per l'Homo sapiens: siamo una specie che da 70.000 anni abita il mondo trasformandolo, la condizione umana è una condizione tecno-umana. Autore di una quindicina di libri ed un centinaio di articoli scientifici. (www.paolobenanti.com)

L'intervista

Prof Benanti che cosa dobbiamo ancora capire dell'intelligenza artificiale per superare l'atteggiamento di paura e di sbigottimento che sembra oggi prevalere in diversi contesti sociali?

Girerei la questione in un'altra direzione. Quello che vediamo nella società non è tanto un atteggiamento di paura quanto piuttosto un senso di disagio che è generato dalla scoperta di un nuovo "utensile". Sembra strano che un semplice strumento possa provocare questo sbigottimento, non è però la prima volta che accade. Quando nel XVI secolo è stata creata la lente convessa, sono nati due potentissimi strumenti: il telescopio e il microscopio. Il primo ci ha permesso di indagare l'infinitamente grande, il secondo di studiare l'infinitamente piccolo. Da quel momento è cambiata per sempre la conoscenza dell'universo, abbiamo infatti compreso che la

terra non era più al centro del sistema solare e che noi siamo fatti di un numero sterminato di cellule.

In questa fase della storia sta avvenendo qualcosa che può rievocare la rivoluzione della modernità?

Vi sono molte analogie. Disponiamo del pc che lavora i dati, generando un nuovo strumento, che definiamo macroscopio per intenderci, che ci consente di studiare l'infinitamente complesso. L'intelligenza artificiale che opera su grandi masse di dati che è un presidio fondamentale in grado di allargare l'ambito delle nostre conoscenze. Quello che sta avvenendo in molti ambiti disciplinari può dare molto bene l'idea di questo continuo spostamento in avanti della frontiera dei saperi.

Possiamo fare qualche esempio?

Le neuroscienze, le cui teorie più avanzate hanno dimostrato come viviamo immersi in un ecosistema di relazioni complesse sostanziate di neuroni, ma anche le scienze economiche e ingegneristiche si ormai fondano le loro indagini sulla realtà sull'analisi di una mole enorme di dati. Dobbiamo, insomma renderci conto, che siamo a un cambio d'epoca e questo, come avevo accennato prima, crea un disagio analogo a quello che abbiamo sperimentato con l'avvento della modernità.

Come va affrontata una svolta così radicale?

Le trasformazioni in atto non sono arrestabili, come tali non sono né da temere né da accogliere in maniera acritica. Non si può, infatti, nutrire la vana pretesa di fermare il vento con le mani. Quello che possiamo esercitare da esseri dotati di intelligenza e ragione è una forma di equilibrato discernimento che ci consenta di afferrare tutte le opportunità che possono aprirsi in un universo in divenire.

I robot ne sanno più di noi?

Quando si parla di macchine sapienti dobbiamo pensare a dei "mostri" che ne sapranno più di noi e che ci domineranno?

Bisogna capirsi bene su questo che è certamente un aspetto delicato. Quando settantamila anni fa ci siamo spostati dall'Africa e abbiamo abitato diverse latitudini della terra, il nostro comportamento è stato molto diverso da quello di molti animali. Se un mammut si fosse spostato dalle steppe siberiane per andare in Africa e in Asia, prima di affrontare questa nuova avventura della sua storia evolutiva, avrebbe dovuto aspettare i tempi evolutivi di una discendenza che avrebbe portato alla nascita di esemplari privi della folta pelliccia. L'uomo non ha osservato nessuna attesa, perché fin dall'inizio si è attrezzato di strumenti adeguati per preparare il suo lungo viaggio verso il progresso. Detto in altri termini: quello che per altri esseri viventi è rigidamente confinato nel DNA per noi è qualche cosa di aperto che ha a che fare con l'uso sapiente di artefatti tecnologici. L'artefatto tecnologico è la nostra "traccia" che serve ad abitare il mondo, o se preferisce è una modalità importante per manifestare la nostra umanità.

Non crede che gli "'utensili" che ci mette a disposizione la telematica sono, però, bel altra cosa rispetto agli strumenti del passato?

E' vero. C'è stata una stagione in cui l'artefatto è stato un utensile legato alla mano poi è arrivata la rivoluzione industriale ed è arrivata la macchina, che programmata e guidata dall'uomo è in grado di fare delle operazioni senza stancarsi mai. Mentre per la mano che agita il martello non era, evidentemente, possibile, raggiungere una performance paragonabile.

Con l'IA siamo un passo ancora oltre rispetto alla civiltà delle macchine?

Sicuramente sì, perché la macchina, cui lei si riferisce, è diventata non più qualcosa che programmiamo, ma che addestriamo a fare delle operazioni. Mi riferisco all'IA e al machine learning. La rivoluzione di cui tanto si parla sta nel fatto che prima d'ora pensavamo che questo ambito fosse esclusiva prerogativa umana. Siamo, invece, di fronte a un'altra specie di "sapiens" che abita il pianeta, ecco perché la comprensione di questa macchina diventa qualche cosa di particolarmente impegnativo.

Nasce così il problema di comprendere la fisionomia di questa nuova specie. A che punto siamo su questo fonte?

E' la scommessa con cui dobbiamo fare i conti. Quando parliamo di macchina sapiens parliamo di quella particolare sensazione dell'uomo di non essere l'unico in grado di fare cose intelligenti sulla terra. Dobbiamo abituarci a questo salto epistemologico, che in maniera così forte e netta non si era probabilmente mai verificato. Sta di fatto cambiando il nostro modo di capire e di conoscere il mondo. La correlazione di quantità impressionante di informazioni unita alla potenza dei PC che danno un significato ai dati ha aperto orizzonti inimmaginabili.

La hanno avuto dunque vinta ingegneri e informatici, che si muovono a loro agio in questa "selva" fittissima di codici e informazioni?

Il paradigma di cui stiamo parlando sembra effettivamente fondato su saperi di

stampo ingegneristico, questo è vero solo parzialmente. Penso a un vecchio detto di Eraclito, che sosteneva che l'oracolo di Delfi non parlava, né taceva, semplicemente significava.

Può spiegarlo, a chi non ha molta dimestichezza, con il mito e la storia delle religioni?

Tradotto nella contemporaneità vuol dire che noi possiamo accedere a questi computer che si nutrono di dati lavorando sugli algoritmi. Per restare nell'analogia dobbiamo vedere la macchina come se fosse una divinità in grado di "pronunciare delle profezie oracolari" sulla realtà.

La capacità ermeneutica rimane, però, una prerogativa umana, non dimentichiamolo. E' la più certa ancora di salvezza cui possiamo agganciarci?

Certamente. La macchina sapiente non deve, infatti, entrare in competizione darwiniana con l'uomo, ma diventare una sua alleata.

Quale Governance per la IA

Una parte molto interessante del saggio parla di Governance dell'IA. A chi va affidata e come andrà strutturata questa delicata attività?

La Governance è la traduzione contemporanea di un processo molto antico. Noi veniamo da una tradizione occidentale che risale alla polis, che esprime un modo di essere della società. La piazza è il punto focale, il luogo dove diverse componenti sociali si ritrovano per confrontarsi sul bene comune. Sulla scia di questo ragionamento occorre dire che una buona governance dell'IA non la si ottiene applicando direttive che dall'alto vengono calate verso il basso. Lo sforzo che dobbiamo compiere sarà quello di creare degli spazi dove persone competenti cercano di coniugare il progresso tecnologico con lo sviluppo effettivo della comunità amministrata. L'immagine che dobbiamo avere in mente è insomma quella di un'agorà aperta dentro cui l'intelligenza collettiva potrà agire per orientare al bene comune il prepotente sviluppo tecnologico che sta segnando questa fase della nostra storia.

Humanities dentro le tecnologie. Un progetto o più semplicemente un auspicio?

Quando si parla di RenAissance scritto all'inglese con la "A" maiuscola si vuole evidenziare il tentativo di togliere i dati dal centro della società digitale per raffermare l'uomo quale protagonista, proprio come era avvenuto durante la grande stagione dell'umanesimo.

Torna sempre con prepotenza la partita delle competenze e della conoscenza. Una ricerca condotta dalla Fondazione GCSEC e dall'Università di Oxford (di cui hanno riferito Elena Agresti e Marco Fiore nel numero scorso della nostra rivista n.d.r) pone l'accento sul fenomeno dello skill shortage. Di quali profili bisognerà dotarsi per riuscire ad agire nel mondo complesso?

Esiste un problema di formazione e di educazione. Bisogna ridare all'uomo la capacità di decodificare quello che accade. C'è bisogno di un nuovo curriculum di scienze umanistiche che sappiano dare alle persone la capacità leggere questa svolta epistemologica e di utilizzare le competenze tecniche che sappiano dire cosa accade all'interno di queste "scatole" che sono gli algoritmi. Fino a quando trattiamo gli algoritmi come delle scatole nere, delle black box, saranno loro a decidere per noi. Le nuove competenze devono insomma permetterci di rendere trasparenti queste black box.

Le imprese di fronte alla quarta rivoluzione

Altra cosa che bisognerà cercare di capire è fino a che punto il mondo del lavoro potrà essere pronto a reggere l'impatto della "Quarta rivoluzione". Mentre sindacati e imprese si stanno interrogando sulle trasformazioni in atto, la dottrina sociale ha preso posizione in maniera netta sul tema della difesa dei diritti dell'uomo e del lavoratore. Papa Francesco sta forse svolgendo un ruolo di "supplenza"?

Esiste una cultura ecclesiale che cerca di diventare fermento per tutta la società. C'è una domanda di senso su queste questioni cruciali che richiedono una riflessione sociale e teologica. Mi pare legittimo, oltre che necessario, che l'impegno del Papa vada in questa direzione.

Etica e sviluppo tecnologico. Vengono in mente le preoccupazioni espresse negli ultimi scritti di Emanuele Severino. Si tratta di timori infondati?

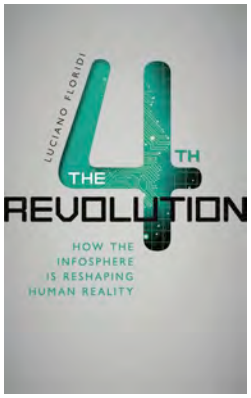
Severino forse è troppo tranchant nelle sue posizioni. In realtà sappiamo che la tecnologia non è solo cieca volontà di potenza ma anche un insieme di risposte rispetto a una domanda che l'uomo si fa sulla realtà che ci circonda. L'uomo che nel passato si è sentito minacciato dalla realtà, ha fatto uno strumento che si chiama fucile. Quel fucile non è solo uno strumento di offesa, ma è anche uno strumento ermeneutico, che mi fa vedere il mondo diviso tra amici e nemici. Ecco che entra in gioco l'artefatto tecnologico, come risposta a una domanda sulla realtà. Solo se vedo la domanda che sta dietro l'artefatto potrò avere un rapporto etico con l'artefatto. Definire un codice etico vuol dire questo: far risuonare la domanda dal produttore al consumatore in ogni istante, perché quella domanda sia soffocata con indifferenza e superficialità. ■

Benvenuti robot! Però nessuna paura: l'uomo è un'altra cosa

Intervista VIP a Luciano Floridi, Università di Oxford

Autore: Massimiliano Cannata

Viviamo la dimensione dell'infosfera, in cui reale e virtuale sono categorie che si mescolano in maniera inscindibile. Per questa ragione nessuna riflessione sull'etica applicata allo sviluppo delle tecnologie può essere adeguata se non ci si sforza di recuperare uno sguardo di sistema, che deve abbracciare tutto l'esistente, l'ambiente naturale, come l'universo digitale. "Non ci sono – spiega Luciano Floridi direttore di ricerca e docente di filosofia ed etica dell'informazione presso l'Università di Oxford - tante etiche parallele a secondo della convenienza piuttosto, ce lo hanno insegnato i grandi pensatori dell'antichità da Platone ad Aristotele a San Tommaso, esiste l'etica, disciplina cui spetta di enucleare principi e valori universali. In relazione alle paure e false convinzioni che accompagnano da sempre l'innovazione precisa lo studioso: "Non dobbiamo temere il diffondersi dell'IA e di strumenti sofisticati come i robot, che rimangono al servizio dell'uomo e non viceversa. Il mondo della significazione, del linguaggio articolato, come la capacità di risolvere i problemi in modo creativo, sono prerogative dell'intelligenza umana, che a differenza di quanto avviene alle macchine, non crolla verticalmente quando si trova di fronte a una situazione mai sperimentata prima. Gli individui sono, infatti, in grado di fare il "passo di lato", quella mossa del cavallo resa possibile dalla plasticità del nostro cervello, non replicabile in nessun laboratorio". A dimostrazione dell'urgenza del tema una ***Commissione interdisciplinare*** a livello europeo è impegnata a fornire un quadro etico su disegno, sviluppo, utilizzo dell'IA e a definire le linee guida che possono servire al mondo industriale per indirizzare lo sviluppo del business digitale.



BIO

Professore di Filosofia ed Etica dell'informazione all'Università di Oxford, dirige il Digital Ethics Lab dell'Oxford Internet Institute, il Data Ethics Research Group dell'Istituto Alan Turing e il comitato consultivo sull'etica dell'European Medical Information Framework. Esperto di filosofia dell'informazione – disciplina di cui è considerato il fondatore -, di computer ethics, data ethics, di etica dell'informazione e di filosofia della tecnologia, è anche membro del comitato consultivo di Google sul "diritto all'oblio". Con la Oxford University Press ha pubblicato, tra gli altri, *The Fourth Revolution* (2014), *The Ethics of Information* (2013), *The Philosophy of Information* (2011). La sua ultima pubblicazione in italiano: La rivoluzione dell'informazione (Codice 2012). È in corso di stampa presso Raffaello Cortina, *La Quarta Rivoluzione. Come l'infosfera sta trasformando il mondo (2017).*

L'intervista

Professore il messaggio che viene da molti suoi scritti è improntato un ottimismo razionale che fa ben sperare: l'uomo deve rapportarsi con equilibrio e misura agli apparati tecnologici, la sua sovranità moralità e intellettuale non è in discussione. Partendo da questo assunto per comprenderlo meglio il rapporto tra etica e* digital society *vorrei che si soffermasse preliminarmente sulla definizione di* infosfera, *termine da lei

introdotto negli anni novanta e ampiamente discusso nel Suo saggio* La Quarta rivoluzione*, (ed. Raffaello Cortina). Possiamo spiegare di che cosa si tratta?

Mi pare un giusto punto di partenza. Il concetto di *infosfera* implica, infatti, considerazioni di carattere ambientale, imprescindibili se vogliamo parlare di etica nella contemporaneità. Le nuove generazioni passano sempre più tempo collegate in uno spazio ibrido tra on line e off line, tra analogico e digitale. Si è scritto molto su questo, ma la definizione *"infosfera"* ha suscitato interesse perché coglie un "salto" in avanti. Faccio un esempio concreto. Le nostre cucine moderne non sono più come quella della nonna, sono infatti popolate di oggetti tradizionali dal forno elettrico alle pentole, ma anche da oggetti elettronici e digitali. Noi abitiamo un "ibrido", abbiamo le pentole, ma anche l'orologio elettronico, il micro onde insieme alla griglia per fare gli arrosti, il forno elettrico e la spugnetta per lavare i piatti insieme a Alexa. Il mondo è fatto da questo mix, fondato sull'interazione di oggetti diversi. La vecchia idea per cui si andava nel *cyber spazio* per collegarsi e poi ci si disconnetteva per tornare "sulla terra" è ormai superata, questa è appunto l'*infosfera*.

L'ambiente digitale sta generando possibilità di relazione nel passato impensabili, aprendo un nuovo capitolo nel rapporto uomo macchina. Cosa dobbiamo aspettarci per l'immediato futuro?

In passato non esistevano processi di interazione e di simbiosi con gli oggetti, come quelli che stiamo sperimentando. Il disorientamento da parte di molti è dunque molto comprensibile. Bisogna però ricordarsi che gli strumenti tecnologici di cui disponiamo sono programmati per risolvere problemi specifici, non sono particolarmente intelligenti come si crede. Disponiamo di oggetti che sono in grado di apprendere, elaborare dati, migliorare la loro performance e, novità importante, sono parzialmente autonomi. Ricorro sempre a un esempio per farmi capire: il termostato di casa è un po' *"smart"*, cioè intelligente nel senso che una volta impostato mi fa trovare gli ambienti che abito alla temperatura che preferisco e al momento giusto, ed è anche uno strumento "autonomo" nel senso che sa ottimizzare i consumi, regolando l'alternanza accensione - spegnimento. L'uomo aveva nel passato avuto esperienza di interazioni con artefatti che non erano per nulla autonomi, né tanto meno interattivi. Questo può aiutare a far capire molto bene la natura del cambiamento epocale che stiamo vivendo.

Questi ecosistemi "ibridati", che Lei ha descritto molto bene, comportano dei rischi?

Porrei l'accento su poche famiglie di problemi, che racchiudono una molteplicità di questioni. Il primo versante di analisi riguarda l'enorme produzione di dati legati al funzionamento di questi sofisticati strumenti digitali, dati che impattano sulla nostra privacy. Altro aspetto molto importante riguarda la capacità di agire con relativa autonomia che caratterizza i robot e le macchine cosiddette intelligenti. La capacità di scegliere, agire, ponderare, prendere decisioni, ma anche cambiare idea o risolvere un problema mai incontrato prima è prerogativa dell'individuo come essere pensante. È evidente che immettendo sul mercato questa categoria di oggetti interattivi e autonomi si possono creare dei contrasti che hanno a che fare con le nostre preferenze e scelte. Entriamo, così, nel campo dei valori, il discorso si fa dunque molto delicato. Non si tratta solo di un termostato che magari per risparmiare mi fa trovare la casa fredda, ma di scelte ben più impegnative e gravi, in cui la macchina si può interpolare condizionando la libera volontà del singolo, ad esempio negandomi un muto in banca.

La sorprendente attualità dei pensatori classici

Autonomia, criteri di scelta, valori, sono le categorie che l'etica classica, da Platone ad Aristotele, per citare solo i più grandi, avevano preso in esame. Questioni antiche che ritornano attuali, come dimostra il lavoro che una commissione interdisciplinare di esperti sta portando avanti per conto dell'UE. Su quali versanti state lavorando?

Il gruppo di cui faccio parte insieme ad altri 51 esperti (oltre a Floridi, vi sono altri tre italiani Andrea Renda, ricercatore del Centre for European Policy Studies di

Bruxelles, Giuseppe Stefano Quintarelli presidente dell'Agenzia per l'Italia digitale e Francesca Rossi, Università di Padova n.d.r.) ha tre macro obiettivi molto precisi: fornire un quadro etico su disegno, sviluppo e utilizzo dell'IA, definire una piattaforma di valutazione per i prodotti dell'IA che rispondono a dei requisiti etici, elaborare delle linee guida che possono servire al mondo industriale per indirizzare lo sviluppo del business digitale e dell'IA. Sono tutte questioni cruciali perché mettere in campo investimenti correttamente orientati e finalizzati, oltre a far crescere la salute delle imprese, può avere delle ricadute molto importanti sulla progettazione delle politiche sociali.

Una macchina per rispondere a dei requisiti etici cosa deve avere?

Un primo requisito riguarda gli standard di sicurezza, che non rispondono più alla logica del vecchio sistema industriale. Pensiamo *all'air bag*, oggi tutte le macchine devono montarlo, rispondendo a dei criteri molto precisi. Vale lo stesso per la progettazione dei robot che devono essere coerenti rispetto a criteri di utilizzazione che siano socialmente validi. Interviene infine la valutazione di processi e prodotti che a valle del processo di produzione dovrà testare la congruenza tra la definizione delle scelte strategiche, lo sviluppo del business e il rispetto dei codici etici.

Le trasformazioni in atto stanno sempre più incidendo sulle competenze e gli assetti organizzativi. In Italia e più in generale in Europa il contesto socio - economico è pronto a sfruttare al meglio le opportunità generate della "quarta rivoluzione"?

Non si può rispondere in maniera univoca alla sua domanda. Vi sono a macchia di leopardo zone dinamiche

e molto avanzate, nel Sud come nel Nord dell'Europa, talvolta collocate in aree insospettabili, che si stanno attrezzando molto bene. Altre realtà mantengono un atteggiamento tra il timoroso e il riottoso, capiscono l'utilità dell'innovazione, ma hanno paura ad affrontare il cambiamento. Tale atteggiamento è molto diffuso nelle PMI, che spesso non dispongono di quelle risorse necessarie per alimentare gli investimenti in ricerca e innovazione. Si tratta di un errore che spesso anche molti governi fanno. Il "falso risparmio" di oggi, obbligherà a una spesa ancora più alta di adeguamento domani, con tutte le conseguenze del caso.

Individui e macchine sapienti

Questo per quanto riguarda il soggetto - impresa, ma gli individui come dovranno comportarsi di fronte a macchine sapienti (cfr. intervista a padre Benanti pubblicata in questo stesso numero di CST) che presto ne sapranno più di noi?

Sgombriamo il campo da false convinzioni. Proprio perché sono delle macchine, parliamo di dispositivi altamente focalizzati, come dicevo prima, sulla risoluzione di problemi specifici. La lavatrice lava i panni non può fare anche i piatti, il robottino che taglia l'erba non batte i tappeti. Non alimentiamo la fantascienza. L'elasticità, la capacità di fissare le priorità, di modificare un percorso in maniera originale è solo dell'essere umano. La nostra intelligenza non crolla verticalmente quando si trova di fronte a una situazione mai sperimentata nel passato. La mia caffettiera elettrica se manca l'energia si ferma, l'uomo non si ferma trova un'altra soluzione e va avanti. Questa flessibilità che non ha limiti è un connotato della plasticità del nostro cervello, impossibile da replicare in laboratorio. Per dirla in termini filosofici, è perché siamo scollati dal mondo che riusciamo a essere intelligenti, mentre il digitale ha successo solo se è ben incollato ai problemi specifici che deve risolvere.

Tanti timori dunque infondati?

Direi di sì, perché il mondo dell'intelligenza e della significazione, così come la ricchezza del linguaggio articolato dell'uomo, fino alle vibrazioni più intime legate alla sua emotività non saranno mai scalfiti da nessuna macchina.

A proposito di emozioni. Molti studiosi sostengono che anche i sentimenti e l'affettività sono fatti di algoritmi. Vorrà dire che ci innamoreremo di un robot se ci farà gli occhi "dolci"?

Almeno dai tempi più remoti del mito greco gli uomini si sono innamorati degli artefatti. Pigmalione si innamora di una statua che diventa reale, da bambini abbiamo giocato con dei soldatini, credendo che fossero veri, abbiamo innescate battaglie autentiche molto sofferte e partecipate.

L'essere umano è portato alla proiezione. Pensiamo ad Apollo e Dafne, alla metamorfosi della ninfa trasformata in alloro. L'uomo innamorato crea con la sua fantasia scenari da sogno che si dissolvono per ricrearsi subito dopo. Però attenzione a non confondere la realtà con l'immaginazione, l'essere con le proiezioni che continuamente siamo portati a generare, l'uomo con il robot.

Nel saggio sulla* "quarta rivoluzione digitale" *il capitolo dedicato all'etica arriva verso la fine del libro, legato al concetto di ambientalismo digitale. Per quale ragione?

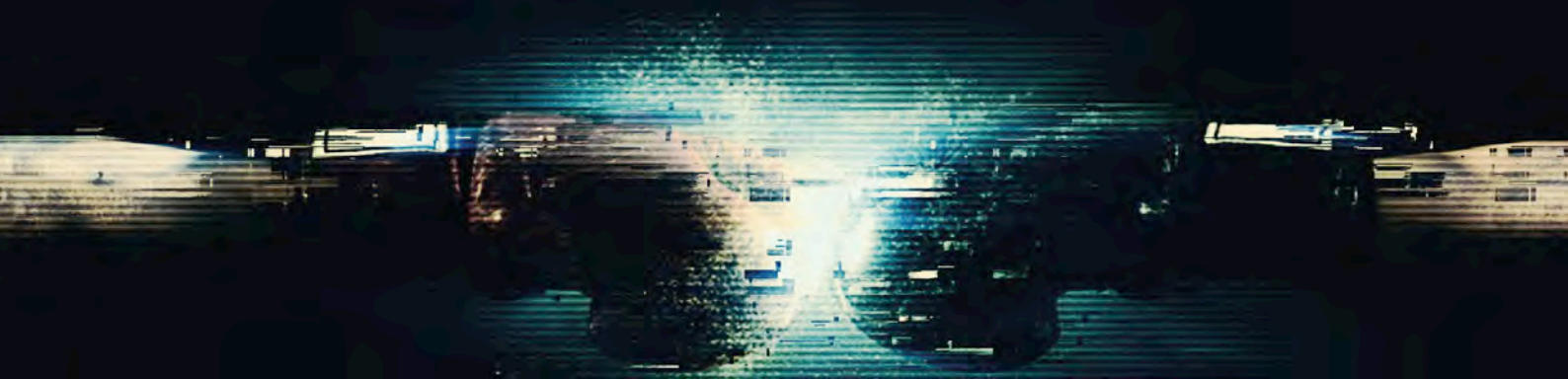
Perché è essenziale considerare gli aspetti di sistema per affrontare un tema così vasto e complesso. Spesso si parla di etica degli oggetti, dell'IA, della sanità, dell'impresa, si tratta di una frammentazione arbitraria. L'etica è un concetto onnicomprensivo, vorrei, perciò, che si prendesse in esame tutto quello che riguarda l'universo digitale, sfera troppo importante per relegarla nei circoli chiusi per super esperti. Torna ancora di attualità la cultura greca che applicava i principi dell'etica a tutto l'essere, senza parcellizzazioni.

Nella nostra conversazione è stata chiamata più volte in causa l'attualità della filosofia. Giuseppe Cambiano ha scritto un brillante saggio (*Sette ragioni per amare la filosofia, ed. Il Mulino *n.d.r.) elencando le ragioni per amare una disciplina che sembrava in crisi fino a qualche anno fa. "Fare domande, usare parole, cercare risposte, apprezzare i dissensi, aprire confini, capire gli altri tempi e gli altri mondi" sono queste le ragioni per cui bisogna tornare a esercitare la speculazione filosofica. Condivide la visione di Cambiano?

I motivi ben esplicitati dal grande storico della filosofia sono senz'altro condivisibili, ma aggiungerei una definizione per me decisiva: la filosofia è soprattutto *design concettuale*, questo è un aspetto della sua eternità. Crea, articola e manipola idee e teorie, interpretazioni e punti di vista, per dare senso al mondo che ci circonda, e alle nostre vite individuali e sociali. Diceva Popper: tutta la vita è risolvere problemi, direi anzi che tutta la vita è identificare nuovi versanti di indagine per andare oltre, per spostare la frontiera della conoscenza in territori inesplorati. Questo intendo per *design concettuale*, questo è l'uomo, che pirandellianamente agita "l'arrovello dell'arcolaio" sollecitando la sua intelligenza a trovare risposte di senso agli eterni dilemmi che dai tempi più remoti agitano a tutte le latitudini la coscienza dei viventi. ■

CYBER CORPORATE FIGHT CLUB

Powered by: CTF365



October 11 2019

The first rule of Fight Club is: you do not talk about Fight Club.

http://cybercorporatefightclub.com

Etica e Intelligenza Artificiale. L'approccio "Trustworthy" dell'Unione Europea all'innovazione tecnologica.

Autore: Marco Fiore

L'intelligenza Artificiale rappresenta sicuramente la nuova frontiera con la quale bisognerà confrontarsi. Lo ha capito bene anche l'UE che nel corso dell'ultimo anno, più precisamente dall'aprile del 2018, ha iniziato un percorso di assimilazione, armonizzazione e coordinamento nel sistema giuridico, in quello socio-economico, e in quello etico e tecnologico di una Intelligenza Artificiale sicura, responsabile ed inclusiva.

Come riportato dal sito istituzionale della Commissione[1], l'UE ha riconosciuto l'Intelligenza Artificiale come un **obiettivo strategico chiave dell'evoluzione tecnologica**, tanto da decidere di istituire una commissione ad-hoc per poter studiare i possibili approcci alla nuova tecnologia, impegno coronato nella stesura di un documento: **Ethics guidelines for trustworthy AI.**

La parola *"Trustworthy AI"* assume in tale ottica una dimensione decisamente rilevante, una intelligenza artificiale affidabile e fondata su tre principi cardine: quello della (1) **liceità** nel rispetto delle leggi, direttive e regolamenti applicabili, quello dell'(2) **etica** nel rispetto dei principi e valori etici che da sempre contraddistinguono il panorama europeo e quello della (3) **robustezza e affidabilità** intesa sia dal punto di vista tecnico che di inserimento nel tessuto sociale poiché, nonostante le buone intenzioni, una scarsa padronanza della tecnologia potrebbe involontariamente causare potenziali danni.

La connotazione ovviamente socio-economica, che da sempre caratterizza il mercato europeo, ha fatto si che tale *Trusthworthy AI* sia accompagnata dalle oramai granitiche garanzie di competitività che il mercato esige e da condizioni generali a salvaguardia dello sviluppo e utilizzo di tali tecnologie. Garantire un quadro etico e giuridico appropriato, basato sui valori dell'Unione e in linea con la Carta dei diritti fondamentali dell'UE, esige una rilevante valutazione delle norme esistenti in materia di responsabilità del prodotto, un'analisi dettagliata

delle sfide emergenti e la necessaria cooperazione con le parti interessate, attraverso un'alleanza europea per l'intelligenza artificiale fondata su linee guida etiche.

Il Progetto, oramai completato[2], è stato preceduto da una dichiarazione di intenti comune tra i vari stati membri dell'UE[3] e partito nell'Aprile del 2018 con una Comunicazione ufficiale della Commissione Europea al Parlamento al Consiglio, al Comitato Economico e Sociale (CESE), e al Comitato europeo delle regioni (CdR). L'iniziativa ha avuto come fine ultimo quello di pubblicare delle **Linee Guida europee con un approccio etico all'intelligenza artificiale.**

Dallo studio preliminare, che ha preceduto il testo definitivo, già si evinceva il ruolo che l'AI avrebbe avuto nelle dinamiche dell'evoluzione tecnologia: *"L'AI ci sta aiutando a risolvere alcuni dei più grandi del mondo sfide: dal trattamento delle malattie croniche o alla riduzione dei tassi di mortalità negli incidenti stradali combattere il cambiamento climatico o anticipare minacce alla cybersicurezza."* [4] Addirittura il documento sottolinea l'importanza dell'intelligenza artificiale alla stregua dei decisivi cambiamenti occorsi durante la prima rivoluzione industriale del '700 che hanno portato il motore a vapore ad essere l'innovazione che cambiò l'intera società.

Gli obiettivi investimento e cambiamento socio-economico dell'Unione:

Oltre a sottolineare la consapevolezza dell'importanza dell'AI, la prima Comunicazione dell'UE offre numerosi spunti di riflessione sulle potenzialità e sul fine ultimo che la tecnologia potrebbe offrire:

- Nel campo della ricerca con la formazione di ricercatori e creazione di laboratori e startup di livello mondiale ma anche nel mondo della robotica[5] e dell'industria per settori come trasporti, sanità e manifatturiero; l'UE ad oggi infatti è leader in molti settori tecnologici[6] tanto da rappresentare una eccellenza a livello mondiale.

- Per il progresso del mercato unico digitale, progetto nel quale si inseriscono proprio le Linee Guida, con regole comuni, ad esempio sulla protezione dei dati e la portabilità dei dati nell'UE, la sicurezza informatica e la connettività che aiutano le aziende a creare valore e investimenti;

- per creare, elaborare, condividere dati industriali, del mondo della ricerca, sanità e del settore pubblico che possono sfruttare i sistemi di l'intelligenza artificiale per essere valore aggiunto al progresso (ad esempio i processi di ***deep learning e machine learning e le nuove frontiere del deep reinforcement learning un apprendimento per rinforzo che ha come obiettivo non solo l'apprendimento ma il compimento del sistema di vere e proprie azioni***)[7 8].

"No one is left behind in the digital transformation. *AI is changing the nature of work: jobs will be created, others will disappear, most will be transformed.* ***Modernisation of education****, at all levels, should be a* ***priority for governments****. All Europeans should have every opportunity to acquire the skills they need. Talent should be nurtured, gender balance and diversity encouraged.". "It is necessary to modernise Europe's education and training systems, including* ***upskilling and reskilling European citizens.****"* [9]

Il progetto Horizon 2020 sicuramente deve essere considerato il progetto cardine nel quale le Linee Guida europee si inseriscono. Tale progetto prevede tra i tanti obiettivi quello di connettere e rafforzare i centri di ricerca in Europa, supportare lo sviluppo di una piattaforma di AI-on-demand[10] che dia accesso a risorse rilevanti a tutti gli utenti, supportare lo sviluppo di applicazioni AI nei settori ritenuti chiave e strategici.

La prima Comunicazione dell'UE non tralascia quello che è stato il lavoro iniziato pochi mesi dell'inizio del progetto europeo e condotto da una task force di esperti riuniti sotto il nome di AI4People che ha esaminato quello che poi sono stati definiti gli *"EGE Principles"*. Il documento infatti delinea ben 36 principi etici suddivisi in quattro **"Imperativi Etici": rispetto e autonomia dell'essere umano, beneficenza (fare del bene) ovvero di non maleficenza (non nuocere), equità e giustizia, autonomia ed esplicabilità**[11], principi integralmente poi sposati dalle linee Guida dell'Unione Europea[12].

BIO

Marco è un research fellow della Fondazione Global Cyber Security Center di Poste Italiane. Laureato in Giurisprudenza presso La Sapienza di Roma in Procedura Penale. Ha svolto una tesi in "Intercettazioni di messaggistica istantanea Blackberry e utilizzazione probatoria nel processo penale". Dopo gli studi ha svolto la pratica forense e contestualmente portava a termine il Master di II livello "Homeland Security" presso il Campus Bio Medico di Roma dove trasversalmente ha approfondito le tematiche in Security e Privacy e Social Communication. Continua a svolgere ricerche per la Fondazione GCSEC. Tra le varie iniziative rilevanti ha contribuito allo studio del 2019 sul Cyber Security Skill Shortage internazionale Mind the Gap e quello Italiano "Il fenomeno del Cyber Security Skill Shortage italiano nel contesto internazionale". Contribuisce alla gestione e pubblicazione di diverse pubblicazioni sul sito ufficiale della Rivista Cybertrends.it.

La *Roadmap* delle Linee Guida sull'etica dell'IA:

L'obiettivo primario dell'Unione era quello di creare un framework che coinvolgesse interlocutori in materia di AI ed esperti - *l'Alleanza europea di Intelligenza Artificiale HLEG* ***High-Level Expert Group***[13] *in collaborazione con il Gruppo europeo di Etica delle Scienze e delle Nuove Tecnologie* - per lo sviluppo di linee guida sull'etica dell'IA, nel doveroso rispetto dei diritti fondamentali, entro la fine del 2019.

Riassumendo l'infografica possiamo scandire esattamente quelli che sono stati i passaggi per la creazione delle Linee Guida etiche della *"Trustworty AI"*. Successivamente alla formazione e nomina degli esperti e una prima Comunicazione è stato pubblicato un primo Draft iniziale[14] (il 18 dicembre 2018) e ufficialmente avviato un processo di consultazione con l'obiettivo di raccogliere feedback, commenti e proposte.

La consultazione si è conclusa il 1° febbraio 2019 con oltre 500 feedback ricevuti. Tali feedback analizzati e valutati dall'**AI HLEG** hanno prodotto una versione rivisitata e finale delle Linee guida sulla *"Trustworthy AI"* consegnata e pubblicata dalla Commissione Europea il **8 aprile 2019**[15].

Lo scheletro delle linee guida:

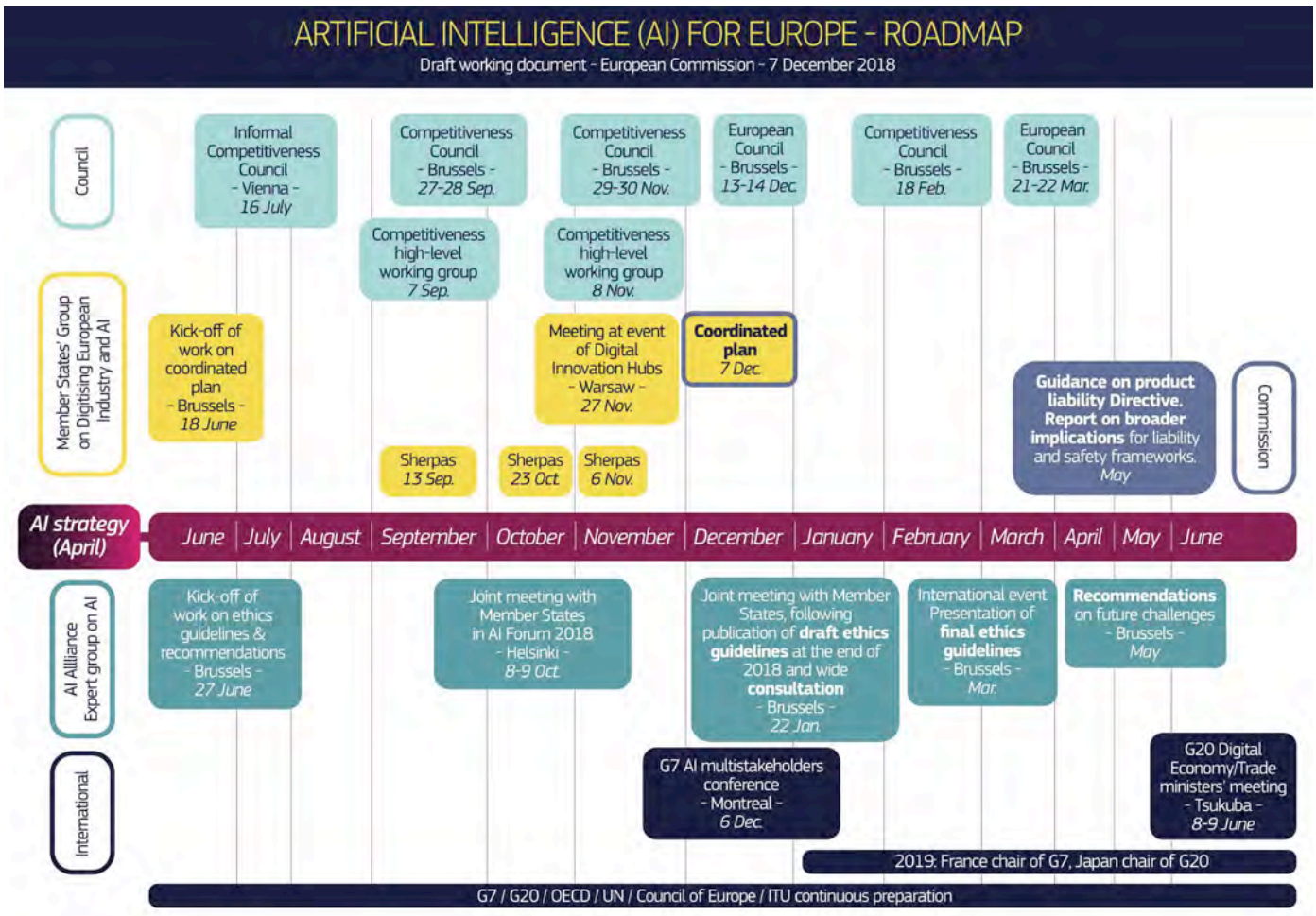
L'Intelligenza artificiale come abbiamo visto genera valore sia per i singoli individui che per l'intera società tuttavia non bisogna sottovalutare i rischi da gestire adeguatamente che si celano dietro di essa. Nel complesso l'attenta valutazione del gruppo di esperti suggerisce come ad oggi i benefici dell'IA superino i rischi ad essa associati e proprio per questo è necessario *"**un approccio antropocentrico all'AI**, che [ci] obblighi a tenere presente che lo sviluppo e l'utilizzo dell'IA non dovrebbe essere considerato come un obiettivo di per sé, ma come un **mezzo per aumentare il benessere umano".***

Il quadro descritto nell'elaborato finale presentato alla Commissione si suddivide in 3 capitoli:

1 Il capitolo I si riferisce alle modalità per garantire la finalità etica dell'AI, definendo i diritti, i principi e i valori fondamentali[16] che dovrebbe rispettare quali il rispetto per l'uomo, l'autonomia, la prevenzione del danno, equità e chiarezza.

2 Partendo da tali principi, nel capitolo II viene elaborata una guida relativa alla realizzazione di un'IA affidabile, tenendo conto sia della finalità etica che della robustezza tecnica. A tal fine vengono elencati i requisiti per un'IA affidabile e si fornisce una panoramica dei metodi tecnici e non tecnici che possono essere utilizzati per la sua implementazione.

3 Il capitolo III infine rende operativi tali requisiti, fornendo una lista non esaustiva di controlli concreti ma non per la valutazione dell'affidabilità dell'IA. Tale lista viene successivamente adattata a casi d'uso specifici.



- La prima delle tre parti definisce i principi etici e sociali per valutare i possibili effetti futuri dell'IA sugli esseri umani e sul bene comune. L'IA dovrebbe infatti essere sviluppata, distribuita e utilizzata con **"finalità etiche"** che riflettono i **diritti fondamentali, i valori sociali e i principi etici** su cui sono basate e di cui si accennava sopra, vale a dire i quattro **Imperativi Etici: rispetto e autonomia dell'essere umano, beneficenza (fare del bene) ovvero di non maleficenza (non nuocere), equità, autonomia, giustizia ed esplicabilità.**

- Il **Primo capitolo** quindi riassume tutti i **diritti fondamentali** che non possono essere tralasciati se si affronta l'IA responsabilmente e nel pieno rispetto della Carta EDU.

Il ***"Rispetto della dignità umana",*** l'idea che ogni essere umano possiede un *"valore intrinseco",* che non dovrebbe mai essere sminuito, compromesso o represso da altri - né da nuove tecnologie come i sistemi di intelligenza artificiale.

La ***"Libertà dell'individuo"*** che con in un contesto AI, richiede, ad esempio, la mitigazione della (in) diretta coercizione illegittima, delle minacce all'autonomia mentale e alla salute mentale, della sorveglianza ingiustificata, dell'inganno e della manipolazione ingiusta.

L' ***"Uguaglianza, la non discriminazione e la solidarietà"*** e cioè *necessita di focalizzare particolare attenzione anche alle situazioni che coinvolgono i gruppi più vulnerabili, come i bambini, le persone con disabilità o le minoranze, o a situazioni in cui si verificano asimmetrie di potere o di informazione, ad esempio tra datori di lavoro e lavoratori, o tra imprese e consumatori.*[17]

Il ***"Rispetto per la democrazia, la giustizia e lo stato di diritto",*** dove tutto il potere governativo delle democrazie costituzionali è legalmente lecito e limitato dalla legge. I sistemi di intelligenza artificiale infatti dovrebbero servire a mantenere e promuovere i processi democratici e rispettare la pluralità dei valori e i bilanci degli individui.

L'***esplicabilità*** che racchiude all'interno del proprio significato sia epistemologico di "intelligibilità" (come risposta alla domanda "come funziona?") sia etico di "responsabilità" (come risposta alla domanda: "chi è responsabile del modo in cui funziona?")

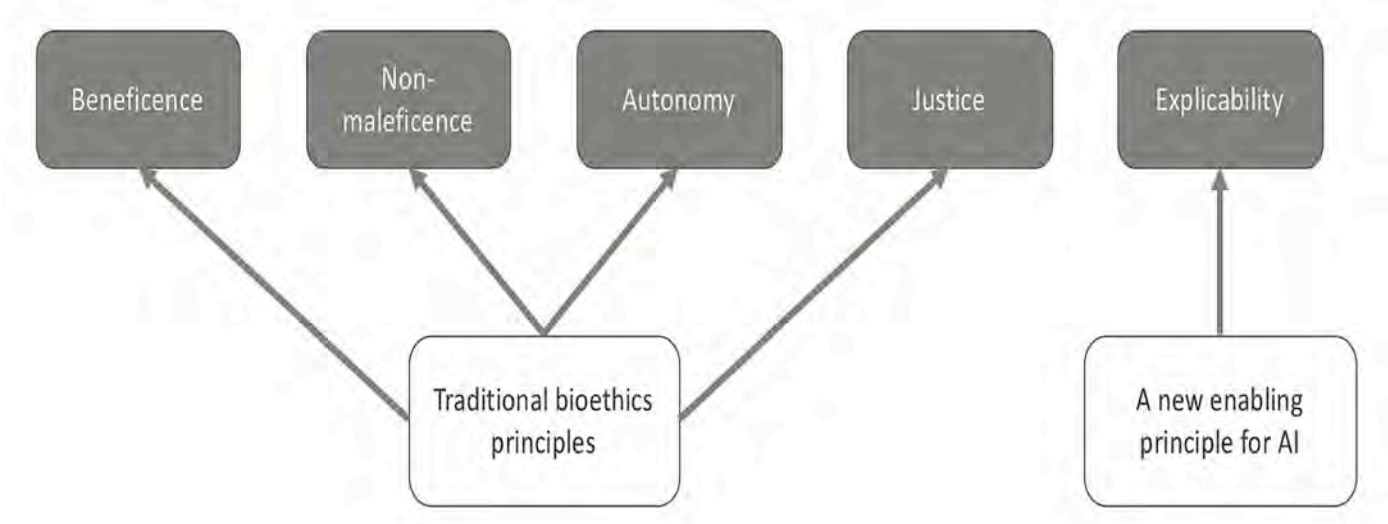
Riconoscere essere consapevoli del fatto che, pur apportando benefici sostanziali agli individui e alla società, l'IA può avere anche conseguenze negative. **È necessario mantenere alta la guardia anche per gli ambiti più critici.**

Oltre alle criticità individuate dal primo documento pubblicato, quello sintetico include anche tutti gli altri rischi che possono avere un impatto negativo, compresi gli impatti difficili da prevedere, identificare o misurare (ad esempio le ripercussioni che l'IA potrebbe avere sui sistemi giuridici democratici, sullo stato di diritto, sulla giustizia distributiva eche concerne la natura di una distribuzione di beni socialmente giusta) o addirittura sulla mente umana stessa.

- Il **Secondo capitolo** invece fornisce una guida su come l'IA attendibile può essere realizzata, elencando **sette requisiti generali che i sistemi di intelligenza artificiale dovrebbero soddisfare.** Gli esperti suggeriscono inoltre due differenti approcci uno tecnico e uno non-tecnico come possibili soluzioni per l'implementazione di tali requisiti.

I sette requisiti per una Intelligenza Artificiale Etica sono:

- **Supervisione umana:** i sistemi di intelligenza artificiale dovrebbero favorire lo sviluppo dell'equità sociale, sostenendo i diritti fondamentali, senza diminuire, limitare o fuorviare l'autonomia umana.
- **Robustezza e sicurezza:** la Trustworthy AI richiede algoritmi sicuri e sufficientemente robusti da contrastare gli errori e le inconsistenze durante l'intero ciclo di vita dei sistemi di Intelligenza Artificiale.
- **Privacy e data governance:** i cittadini dovrebbero avere pieno controllo sui propri dati, nella sicurezza che i



Framework per l'intelligenza artificiale, formato da quattro principi tradizionali e uno nuovo Immagine di AI4People

dati che li riguardano non possano essere utilizzati a loro danno o a fini discriminatori.

- **Trasparenza:** deve essere garantita la tracciabilità dei sistemi di Intelligenza Artificiale
- **Diversity, correttezza, assenza di discriminazione:** i sistemi di Intelligenza Artificiale dovrebbero prendere in considerazione tutte le capacità e le skill umane, garantendo a tutti l'accessibilità.
- **Benessere sociale e ambientale:** i sistemi di Intelligenza Artificiale dovrebbero essere utilizzati per sostenere cambiamenti positivi, migliorare la sostenibilità ambientale e la responsabilità ecologica.
- **Responsabilità:** devono essere adottati meccanismi che garantiscano la responsabilità sui sistemi di Intelligenza Artificiale e sui loro risultati.

Al termine del secondo capitolo, il documento riassume alcune best practice da applicare all'AI per rendere i sistemi più efficaci:

- **Promuovere la ricerca** e l'innovazione per aiutare a valutare i sistemi di intelligenza artificiale e favorire il conseguimento dei sette requisiti; **diffondere i risultati** e coinvolgere il pubblico creando sistematicamente nuovi contenuti da condividere.
- **Comunicare**, in modo **chiaro, proattivo e trasparente le informazioni** alle parti interessate in merito alle capacità e ai limiti del sistema di intelligenza artificiale, consentendo valutazioni e aspettative realistiche e comunicare le modalità con i quali tali requisiti sono implementati.
- Facilitare la tracciabilità e l'audit dei sistemi di IA, in particolare in contesti o situazioni critiche.
- **Coinvolgere le parti interessate** in tutto il ciclo di vita del sistema AI. Incoraggiare la formazione e l'istruzione in modo che tutti i soggetti siano consapevoli e addestrati nell'IA
- Non dimenticare che potrebbero esserci sbilanciamenti importanti tra diversi principi e requisiti. **Identificare, valutare, documentare e comunicare continuamente** questi trade-off e le loro soluzioni.

Ma non solo, il secondo capitolo cerca di riassumere gli strumenti che si possono effettivamente implementare e sviluppare in termini di AI. Gli approcci tecnici, non-tecnici invece si suddividono in diverse categorie. Di seguito un elenco riassuntivo:

"Strettamente" Tecnici:

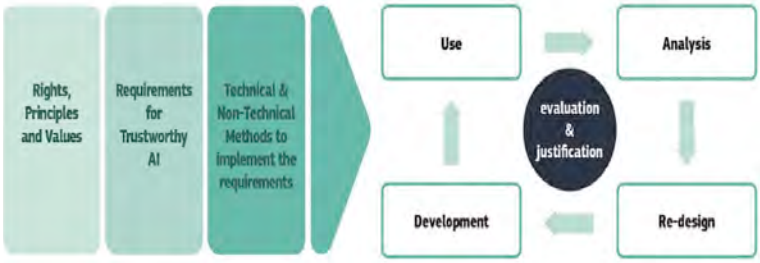
- Architetture per una Trustworthy IA
- Etica e diritto in base alla progettazione (X-by-design. Ad esempio privacy-by-design e security-by-design)
- Metodi e parametri di valutazione (chiamati Explainable AI - XAI)
- Test e convalide
- Indicatori della qualità del servizio

Non "strettamente" Tecnici

- Regolamenti
- Codici di condotta
- Standard e Certificazioni
- Governance e definizione di Ruoli e responsabilità
- Educazione e awareness per promuovere la mentalità etica
- Partecipazione delle parti interessate e il dialogo sociale
- Diversità e team di progettazione inclusivi.

- Il **Terzo capitolo** invece cerca di fornire una valutazione, non esaustiva, per rendere operativi i punti del secondo capitolo per l'applicazione del metodo tecnico – non tecnico di cui si accennava prima ed inoltre fornendo un questionario pilota sull'**Trustworthy Ai Assessment.**

- Adottare un **Risk Assessment approach** idoneo per la Trustworth AI durante lo sviluppo, l'implementazione o l'utilizzo di sistemi AI e adattarlo al caso d'uso specifico in cui viene applicato il sistema.
- Ricordare che l'elenco di valutazione non sarà mai esaustivo. Garantire un AI affidabile **non può essere un ticking box** di una checklist, ma una **identificazione e un'implementazione continua** dei requisiti, una valutazione delle soluzioni per una garanzia di risultato dell'intero ciclo di vita del sistema AI e il necessario coinvolgimento degli stakeholder nel processo.



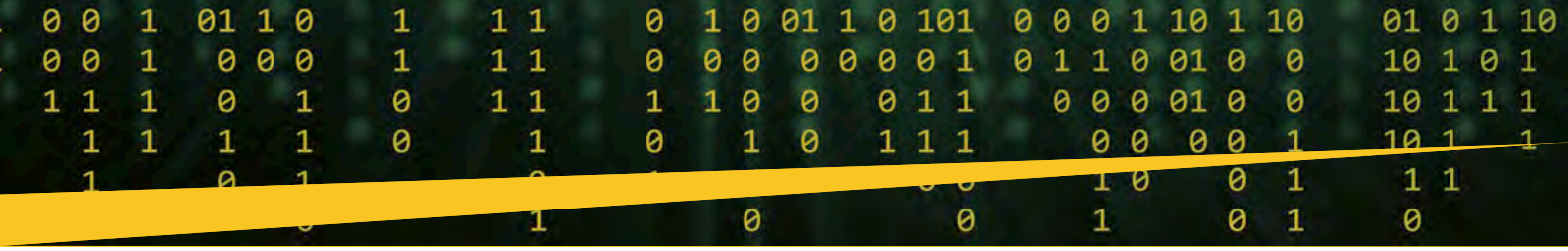
Realizzazione di un ciclo di vita del sistema del sistema di Trustworthy AI

Gli esperti, nelle proprie raccomandazioni, sottolineano come il documento rappresenti un punto di partenza per aprire un serio dibattito sull'etica e l'AI e le sue applicazioni. Il framework orizzontale definito con il presente documento non deve essere preso come uno "standard" né tantomeno tenta di sostituirsi ad alcuna forma di regolamentazione attuale o futura, bensì invita ad esplorare le verticalità che la stessa AI potrebbe avere nell'impiego pratico dei singoli settori.

Gli Use Cases delle Linee Guida

L'ultima parte delle Linee riportano degli importanti esempi di Use Cases dove l'IA ha trovato applicazione.

A titolo esemplificativo si cita uno dei tanti esempi che ben si sposa con i vari progetti che si sono interessati delle difficoltà nella formazione e nella ricerca delle risorse nei nuovi settori tecnologici[18]:



Uno degli use case riportati è ad esempio il **Quality education e digital transformation**.

"I nuovi cambiamenti tecnologici, economici e ambientali impongono alla società deve diventare più proattiva. I governi, i leader del settore, le istituzioni educative e i sindacati devono assumersi la responsabilità di accompagnare i cittadini nella nuova era digitale, assicurando che abbiano le giuste competenze per riempire i futuri posti di lavoro. Le tecnologie AI affidabili potrebbero aiutare a prevedere con maggiore precisione quali posti di lavoro e professioni saranno interrotti dalla tecnologia, quali nuovi ruoli saranno creati e quali competenze saranno necessarie. Ciò potrebbe aiutare governi, sindacati e industria a pianificare la (ri) qualificazione dei lavoratori. Potrebbe anche dare ai cittadini che temono la ridondanza un percorso di sviluppo in un nuovo ruolo. Inoltre, l'intelligenza artificiale può essere un ottimo strumento per combattere le disuguaglianze educative e creare programmi educativi personalizzati e adattabili che possano aiutare tutti ad acquisire nuove qualifiche, abilità e competenze in base alla propria capacità di apprendere[19]*. Potrebbe aumentare sia la velocità di apprendimento sia la qualità dell'istruzione, che va dalla scuola elementare all'università."*

Conclusioni

Horizon 2020 è sicuramente il progetto cardine che regge l'intera infrastruttura di investimenti europea per lo sviluppo tecnologico e che travolge trasversalmente una moltitudine di settori tra cui l'IA.

Fino ad ora il programma dell'UE ha finanziato più di 18.000 progetti di ricerca proprio sull'IA spendendo più di 30 miliardi di euro. Ha inoltre impegnato 1,5 miliardi di euro esclusivamente nella ricerca in ambito etico, aspettandosi che altri 2,5 miliardi arrivino da finanziamenti pubblici e privati. Sono invece previsti almeno 7 miliardi di investimenti tra i programmi di Horizon Europe (2021 – 2027) e Digital Europe[20].

Sembrerebbe necessario a questo punto dover operare paragoni. Tra nazioni più impegnate nello sviluppo di tecnologie di intelligenza artificiale la Cina rappresenta sicuramente la prima nel panorama mondiale con la sua rivale U.S.A. in termini di competitività tecnologica.

Per riportare al lettore dei dati significativi, nella sfera etica e IA, la Cina, ha previsto un investimento totale di 13 miliardi a cui verranno aggiunti gli investimenti dei privati.[21] L'intelligenza artificiale infatti è tra gli obiettivi politici del progetto madre *"Made in China 2025"* di Pechino che definisce l'ambizioso programma di condurre la Cina a diventare leader globale nel settore AI entro il 2030[22].

Il necessario dibattito che deve necessariamente instaurarsi tra Etica e Intelligenza Artificiale fa pensare molto al film di Isaac Asimov "I, robot" e alla contemporanea serie televisiva Westworld, dove le macchine, progettate per servire fedelmente l'uomo, si trasformano e si ritorcono proprio contro i propri creatori, punto che non dovrà essere mai raggiunto.

Concludendo *"la Trustworthy AI può migliorare la prosperità individuale e il benessere collettivo generando prosperità, creazione di valore e massimizzazione della ricchezza. Può contribuire al raggiungimento di una società equa, contribuendo ad aumentare la salute e il benessere dei cittadini in modi che favoriscano l'uguaglianza nella distribuzione delle opportunità economiche, sociali e politiche"* e che dovrà necessariamente tener conto dei potenziali rischi e pericoli che la stessa tecnologia potrà riverberare sull'uomo e sui sistemi innovativi. ■

Note:

1 https://ec.europa.eu/digital-single-market/en/artificial-intelligence
2 Le Linee Guida Ethicsguidelines for trustworthy AI sono state pubblicate su sito della Commissione Europea con il REPORT STUDY dell'8 Aprile 2019 - https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
3 Elenco dei paesi firmatari della dichiarazione: Austria, Belgio, Bulgaria, Repubblica Ceca, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito, Norvegia. - https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence
4 https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe
5 L'intelligenza artificiale è presente nell'"EU research and developmentframework" dal 2004 con un focus specifico sulla robotica. Gli investimenti stanziati sono aumentati fino a € 700 milioni per il periodo 2014-2020, investimento perfezionato dai € 2,1 miliardi di investimenti privati nel partenariato pubblico-privato sulla robotica. Questi sforzi hanno significativamente contribuito alla leadership mondiale dell'Europa nella robotica come il Progetto Sparchttps://eu-robotics.net/sparc/
6 In Europa sono presenti le 100 migliori istituzioni di ricerca in tema di intelligenza artificiale del mondo. 32 Istituti di ricerca sono nella top 100 globale per pubblicazioni in tema di AI contro le 30 dagli Stati Uniti e le 15 dalla Cina. Fonte: Atomico, State of EuropeanTech, 2017. È da annoverare tra queste il Centro di ricerca tedesco per l'intelligenza artificiale (DFKI) fondato nel 1988 che ad oggi è uno dei più grandi centri di ricerca al mondo nel campo dell'IA.
7 Ulteriori ambiti di applicazione menzionati sono: intelligence e sorveglianza umana, safety, privacy e gestione dei dati, trasparenza, diversità e non discriminazione, equità e benessere sociale e ambientale, responsabilità
8 Per un esempio concreto di Deepreinforcementlearning sul tema, Un computer di Google ha battuto il campione europeo di un complicatissimo gioco da tavolo, https://www.ilpost.it/2016/01/28/go-alphago-google-deep-mind-intelligenza-artificiale/
9 https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence
10 https://www.ai4eu.eu/
11 L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, EJMVayena (2018), "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations", Minds and Machines 28 (4): 689-707.
12 Non essendoci una traduzione ufficiale sono stati tradotti i seguenti principi dalla lingua inglese: Respect for human autonomy, Prevention of harm, Fairness, Explicability
13 L'elenco completo degli esperti è disponibile al seguente link: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence
14 Sintesi scaricabile gratuitamente dal sito della Commissione Europea: https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai
15 Le linee guida sono disponibili in versione Inglese al seguente link: https://ec.europa.eu/futurium/en/ai-alliance-consultation
16 I diritti fondamentali sono alla base del diritto internazionale e dell'UE in materia di diritti umani e sono alla base dei diritti giuridicamente vincolanti garantiti dai trattati dell'UE e dalla Carta dell'UE. Essendo giuridicamente vincolante, il rispetto dei diritti fondamentali rientra quindi nella prima componente dell'AI fidata (AI legittima). Tuttavia, i diritti fondamentali possono anche essere intesi come riflessi di speciali diritti morali di tutti gli individui che sorgono in virtù della loro umanità, indipendentemente dal loro status giuridicamente vincolante. In tal senso, quindi, fanno anche parte della seconda componente dell'AI affidabile (AI etica).
17 Si vedano gli articoli da 24 a 27 della Carta dei diritti fondamentali dell'UE (Carta UE), che tratta dei diritti del bambino e anziani, l'integrazione delle persone con disabilità e dei diritti dei lavoratori. Vedi anche l'articolo 38 relativo alla tutela del consumatore.
18 In tema si suggerisce lo studio della Fondazione GCSEC con l'Università di Oxford: POLICY INTERVENTIONS AND THE CYBER SECURITY SKILLSSHORTAGE nelle due versioni: quadro internazionale, "Mind the Gap:The Cyber Security SkillsShortage and Public Policy Interventions" e il quadro italiano: "Il fenomeno del Cyber Security SkillShortage italiano nel contesto internazionale", disponibili al seguente link: https://gcsec.org/it/policy-interventions-and-the-cyber-security-skills-shortage/
19 Esempio di tali progetti sono il progetto MaTHiSiS, volto a fornire una soluzione per un apprendimento affected-based e, comprendente dispositivi e algoritmi tecnologici di alto livello: (http://mathisis-project.eu/). Vedi anche la Watson Classroom di IBM o la piattaforma Century Tech.
20 UN Sustainable Development Goals, EU Agenda 2030, https://sustainabledevelopment.un.org/?menu=1300
21 Accenture, How Artificial Intelligence Can Drive China's Growth, 2017, https://www.accenture.com/_acnmedia/PDF-55/Accenture-How-Artificial-Intelligence-Can-Drive-Chinas-Growth.pdf
22 Attualmente la Cina già gode di un ampio vantaggio rispetto a molti altri paesi in termini di documenti accademici, brevetti e finanziamenti AI, sia transfrontalieri che globali)

Cybersecurity Act, un nuovo tassello nella strategia Cyber Sec dell'Unione Europea

Autore: Gianluca Bocci

Il Cybersecurity Act è il regolamento che, proposto dalla Commissione Europea, è stato recentemente approvato dal Parlamento Europeo per dare seguito alle diverse iniziative utili ad aggiornare e sviluppare la strategia di sicurezza cibernetica a livello comunitario; si tratta di un complesso di norme che, articolandosi in due parti, rinvigorisce il mandato dell'ENISA, l'Agenzia dell'Unione europea per la sicurezza informatica e definisce il quadro comune di riferimento europeo per la valutazione e la certificazione della sicurezza informatica di prodotti, processi e servizi di tecnologie dell'informazione e della comunicazione. La risoluzione legislativa, proposta dalla Commissione Europea, è stata votata il 12 Marzo 2019 dal Parlamento Europeo, con il voto favorevole di una larga maggioranza dei partecipanti ai lavori; successivamente, in data 9 Aprile, è stata ufficialmente adottata dal Consiglio Affari Generali del Consiglio Europeo ed entrerà in vigore decorsi 20 giorni dalla pubblicazione in Gazzetta Ufficiale avvenuta il 7 Giugno 2019. Il Parlamento Europeo, nella stessa seduta del 12 Marzo, ha colto l'occasione per manifestare grande preoccupazione per il continuo aumento della presenza di tecnologia cinese nel nostro continente, con particolare riferimento a quella impiegata per realizzare reti 5G; il timore è che possono essere introdotte *"backdoor"* con le quali accedere a dati personali e in generale favorire le intercettazioni. A tal proposito, il CyberSecurity Act[1] è una delle risposte a questa minaccia. L'Europa, con questi interventi legislativi, si pensi altresì alla direttiva NIS *(Network and Information Systems)* o al regolamento GDPR (General Data Protection Regulation), oltre a favorire la crescita della propria *"cyber resilience"*, intende ridurre la criminalità informatica, sviluppare politiche e capacità di *"cyber defense"* e realizzare proprie risorse industriali e tecnologiche per la sicurezza cibernetica, anche nell'ottica di creare le condizioni per disporre di una propria indipendenza rispetto a grandi *"player"*, come ad esempio gli Stati Uniti e la Cina, tra

l'altro sempre più in contrasto tra loro. Una indipendenza che, in un regime fortemente concorrenziale, consentirebbe di non escludere la possibilità di utilizzare forniture cinesi, a patto di una rispondenza a determinate specifiche di sicurezza, valutabili e certificabili in maniera oggettiva, in linea con i valori fondanti dell'UE.

ENISA - European union agency for network and information security

L'Agenzia, creata nel 2004, con questo nuovo regolamento assumerà un ruolo e una organizzazione a carattere permanente per sostenere in maniera energica gli Stati membri e le istituzioni nel miglioramento della sicurezza cibernetica, promuovendone in tal senso un elevato livello comune in tutta l'Unione. L'ENISA provvederà dunque a supportare lo sviluppo, la revisione

e l'attuazione delle politiche e della normativa dell'Unione in materia di *"cyber security"*; motivo questo, per cui tra i suoi obiettivi, vi rientra anche quello di assistere gli Stati membri nell'attuazione della direttiva (UE) 2016/1148 (precedentemente citata come direttiva NIS) attraverso pareri e orientamenti sullo sviluppo di strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi, la realizzazione di CSIRT nazionali, l'analisi del rischio, la gestione degli incidenti informatici e la condivisione delle informazioni[2]. Fondamentale sarà anche il contributo che fornirà al Gruppo di Cooperazione che, previsto nell'articolo 11 della direttiva NIS, sostiene e agevola la cooperazione strategica e lo scambio d'informazioni tra gli Stati membri. Non meno importante sarà il settore dell'identificazione e dei servizi fiduciari ai quali dovrà garantire servizi di consulenza, agevolando allo stesso tempo lo scambio delle migliori pratiche tra le autorità competenti; con il medesimo approccio promuoverà anche un livello di sicurezza più elevato delle comunicazioni elettroniche. Molti altri compiti dovrà svolgere l'Agenzia per migliorare il livello di protezione delle reti e dei sistemi informativi, anche attraverso lo sviluppo di un'efficace cooperazione operativa a livello di Unione; tra questi compiti ricordiamo, l'assistenza agli Stati Membri, le istituzioni e gli organismi dell'Unione stessa, in particolare i CSIRT nazionali e il CERT- UE, nello sviluppo delle capacità di prevenzione, rilevazione e analisi delle minacce e di risposta ad incidenti informatici, compresi quelli a carattere transfrontaliero, l'organizzazione di esercitazioni periodiche di cyber sicurezza (anche settoriali) su larga scala che interesseranno l'intera comunità europea, predisporre e rendere disponibile un'offerta di formazione specifica, ecc.. In generale, su richiesta, l'ENISA dovrà fornire anche assistenza agli Stati membri per valutare gli incidenti che determinano un impatto rilevante, condividendo tra gli stessi Stati sia informazioni, sia soluzioni tecniche. L'Agenzia, oltre ad impegnarsi nello sviluppo della cooperazione a livello europeo, provvederà ad operare per favorire la crescita dello sviluppo della cooperazione con paesi extra-UE e in generale di tutte le organizzazioni internazionali che trattano il tema della cyber security. D'interesse per l'ENISA, sarà anche l'opinione pubblica, per la quale, attraverso campagne ad hoc, ne promuove da sempre la sensibilizzazione e l'informazione in materia di sicurezza cibernetica (e.g. European Cyber Security Month[3]); al riguardo fornisce e continuerà a fornire agli stessi Stati membro il proprio contributo per avviare iniziative analoghe su scala nazionale. L'agenzia, attenta alle tecnologie emergenti in ambito cyber security, fornirà valutazioni sui possibili impatti derivanti dal suo utilizzo, secondo diversi punti di vista, quello sociale, giuridico, economico e normativo, fornendo anche pareri utili per orientare i programmi di ricerca e innovazione in materia di cyber security. In generale diversi temi di cyber security a cui abbiamo fatto finora riferimento, sono stati già indirizzati nei precedenti anni da ENISA; ne consegue che, quanto disposto con il nuovo regolamento, il

BIO

Gianluca Bocci, laureato in Ingegneria Elettrica presso l'Università La Sapienza di Roma ha conseguito un Master Universitario di 2° livello presso l'università Campus Bio-Medico di Roma in "Homeland Security - Sistemi, metodi e strumenti per la Security e il Crisis Management". Attualmente è Security Professional Master nella funzione Tutela delle Informazioni di Tutela Aziendale, nella direzione Corporate Affairs di Poste Italiane. Certificato CISM, CISA, Lead Auditor ISO/IEC 27001:2013, Lead Auditor ISO/IEC 22301:2012, CSA STAR Auditor e ITIL Foundation v3, supporta le attività del CERT e del Distretto Cyber Security di Poste Italiane; in tale ambito ha maturato una pluriennale esperienza nella sicurezza delle applicazioni mobili, anche attraverso attività di ricerca e sviluppo realizzate con il mondo accademico. Precedentemente, presso importanti multinazionali ICT, in qualità di Security Solution Architect, ha supportato le strutture commerciali nell'ingegneria dell'offerta tecnico-economica per Clienti di fascia enterprise, con particolare riferimento ad aspetti di Security Information and Event Management, Security Governance, Compliance e Risk Management.

Cybersecurity Act (ma anche con la Direttiva la NIS), permetterà all'Agenzia di dare continuità alle proprie attività, ma soprattutto di migliorarle grazie al nuovo assetto dell'Agenzia con la quale saranno disponibili un maggior numero di risorse economiche ed umane; tra le ipotesi, si prevede a regime una crescita del budget che dovrebbe passare dai circa 11 milioni di euro all'anno ai 23 milioni di euro; analogamente le risorse dovrebbero passare dalle circa 80 attuali a 125 a regime.

ENISA potrà altresì essere coinvolta, se richiesto, nella preparazione di una proposta di sistema o di rivedere un sistema europeo di certificazione per la sicurezza di prodotti, processi e servizi digitali che saranno commercializzati nell'Unione Europea, istituendo in tal senso un gruppo di lavoro ad hoc e comunque attraverso la stretta collaborazione delle autorità nazionali di certificazione dei diversi Stati Membro; almeno ogni cinque anni l'ENISA valuterà ogni sistema europeo di certificazione della cyber sicurezza adottato, tenendo conto del riscontro ricevuto dalle parti interessate. In sostanza, con questa nuova disposizione legislativa, si conferisce all'ENISA, nell'ambito di una trasformazione voluta e funzionale alle nuove esigenze della comunità europea, un ruolo sempre più operativo.

Sistema europeo per la certificazione di sicurezza di prodotti e servizi digitali

Con il nuovo mandato l'ENISA dovrà dunque sostenere e promuovere lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della sicurezza cibernetica di prodotti, servizi e processi relativi alle tecnologie dell'informazione e della comunicazione, anche attraverso il monitoraggio continuo degli sviluppi che caratterizzano i settori di normazione connessi, la valutazione dei sistemi europei di certificazione della cyber sicurezza già adottati e la predisposizione delle linee guida necessarie agli enti di certificazione per valutare e conferire la certificazione di sicurezza a chi ne farà richiesta; ciò non senza le preoccupazioni espresse, senza mezzi termini, da alcune importanti Agenzie Governative appartenenti ad alcuni importanti Stati membri[4]. Infatti, esistono già diversi schemi di certificazione nei paesi della Comunità Europea; uno degli obiettivi del CyberSecurity Act sarà proprio quello di favorire, attraverso la definizione di quelle linee guida già citate, un processo di convergenza che, per armonizzazione e uniformazione, consenta di riconoscere valida la certificazione di sicurezza in tutta la comunità europea, a prescindere dal paese in cui è stata acquisita. Ad esempio, in Italia lo schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione trova riscontro nell'Organismo di Certificazione della Sicurezza Informatica (OCSI) dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM)[5]. Per la gestione dell'Organismo di Certificazione, l'ISCOM si avvale della collaborazione della Fondazione Ugo Bordoni. Le valutazioni all'interno dello Schema nazionale vengono eseguite applicando i criteri europei ITSEC (Information Technology Security Evaluation Criteria) o quelli, denominati Common Criteria, che costituiscono lo standard internazionale ISO/IEC IS-15408. Analoghe considerazioni potremmo fare per il Centro di Valutazione (CE.VA.) della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal Segreto di Stato o di vietata divulgazione[6]. In ogni caso, tralasciando le precedenti osservazioni, l'ENISA per definire i criteri di certificazione dovrà prima consultare società e Stati membri. Tra i requisiti dei sistemi di certificazione, tutti orientati alla sicurezza, saranno valutati quelli per garantire la disponibilità, l'integrità e confidenzialità dei dati durante il loro ciclo di vita, la capacità di registrare l'accesso ai dati, da parte di chi, quando e che utilizzo se ne fa degli stessi, la verifica che non contengano vulnerabilità note e che comunque dispongono di meccanismi per effettuare aggiornamenti, in generale che siano progettati in linea con il principio della "security by design". Si tratta di requisiti che, tutti o in parte, dovranno essere valutati in funzione del livello di affidabilità che si intende certificare (di base, sostanziale o elevato) del prodotto, processo e\o servizio. Al riguardo il livello di affidabilità è proporzionale al rischio che interessa ciò che si certifica rispetto alla probabilità che la stessa possa essere interessato ed impattato da un incidente informatico. L'esame dei requisiti spetterà ai singoli Stati membro attraverso centri di valutazione che, realizzati ad hoc, saranno accreditati da Accredia, l'ente unico nazionale di accreditamento designato dal governo italiano, in applicazione del Regolamento europeo 765/2008. Proprio la procedura di accreditamento. L'accreditamento assicurerà che gli organismi di certificazione, ispezione e verifica, e i laboratori di prova e taratura, abbiano tutti i requisiti richiesti dalle norme per svolgere attività di valutazione della conformità. L'attuazione

del Cybersecurity Act ed in particolare la certificazione della sicurezza informatica di prodotti, processi e servizi digitali sarà comunque, almeno in una prima fase, rilasciata solo su base volontaria, anche se non è escluso che in un prossimo futuro la stessa sarà resa obbligatoria. Ne consegue che anche per l'applicazione della Direttiva NIS nei confronti degli operatori di servizi essenziali, la certificazione non sarà imposta per servizi e processi a carattere sistemico o comunque in generale ritenuti critici.

Conclusioni

Dalle precedenti considerazioni si evince come, attraverso un'articolata politica dell'Unione Europea avviata ormai da diversi anni, s'intende realizzare un sistema digitale sempre più resiliente, ridurre la criminalità informatica, sviluppare nuove e progressive capacità di difesa cibernetica e analogamente risorse e tecnologie per la cyber sicurezza. Obiettivi che

necessariamente richiedono sforzi da parte dei diversi Stati membro e da tutti gli organi istituzionali, nazionali e non, coinvolti in questa sfida. Sforzi che passano per la ricerca di figure professionali opportunamente preparate e motivate, a tutti i livelli, dagli operatori e analisti che conoscono le soluzioni e i linguaggi di programmazione orientati alla sicurezza e le metodologie di analisi degli eventi di sicurezza e dei malware, fino a chi

disegna procedure e processi, ad esempio quelli per la gestione degli incidenti di sicurezza informatica e progetta architetture cyber sec attraverso la conoscenza di best practice, standard di riferimento e normativa di settore. Altrettanto importanti, per il raggiungimento dei medesimi obiettivi, sono gli investimenti economici che, non solo dovrebbero essere incrementati nel tempo, ma anche allineati tra i diversi Stati membro, così da poter raggiungere, realmente, un elevato livello comune di sicurezza delle reti e dei sistemi informativi. Purtroppo, conoscere con esattezza tali investimenti non è cosa semplice e molte organizzazioni hanno difficoltà a quantificare questo dato, considerando che spesso non riescono a distinguerlo da quello più generale dell'IT. ■

1 https://eucyberact.org
2 Dettagli ulteriori sul il ruolo di ENISA nell'ambito della NIS, sono disponibili nell'articolo "La Direttiva NIS: un articolato quadro tecnico-normativo", disponibile, proprio sulla rivista Cyber Security Trends, al link https://www.cybertrends.it/la-direttiva-nis-un-articolato-quadro-tecnico-normativo/.
3 https://cybersecuritymonth.eu/
4 https://www.euractiv.com/section/cybersecurity/news/french-cybersecurity-chief-warns-against-step-back-into-the-past/
5 http://www.isticom.it/index.php/qualita-del-servizio/sicurezza-ocsi
6 http://www.isticom.it/index.php/qualita-del-servizio/sicurezza-ceva

Il futuro delle comunicazioni. 5G tra benefici e sfide della sicurezza informatica

Autore: **Virgilius Stanciulescu,**
Consiglere del Presidente per le questioni IT&C, ANCOM

Il futuro così come le abitudini quotidiane cambieranno sostanzialmente con lo sviluppo della tecnologia che collegherà tutto ciò che ci circonda. Con le reti 5G, le connessioni saranno più veloci e gli strumenti che quotidianamente utilizziamo saranno interconnessi apportando benefici ancora poco compresi e noti a ciascuno di noi.

La rete in fibra ottica, l'integrazione fisso-mobile e la necessità di trasportare ad alta velocità enormi quantità di dati con ritardi minimi (millisecondi) e un numero massiccio di dispositivi collegati, apriranno per gli operatori di reti di telecomunicazione la strada al 5G.

Tra breve, avremo tutti accesso ai servizi supportati da questa tecnologia e, in questo articolo, passerò brevemente in rassegna sia i benefici che le vulnerabilità che dovremo prendere in considerazione come specialisti della sicurezza IT & C.

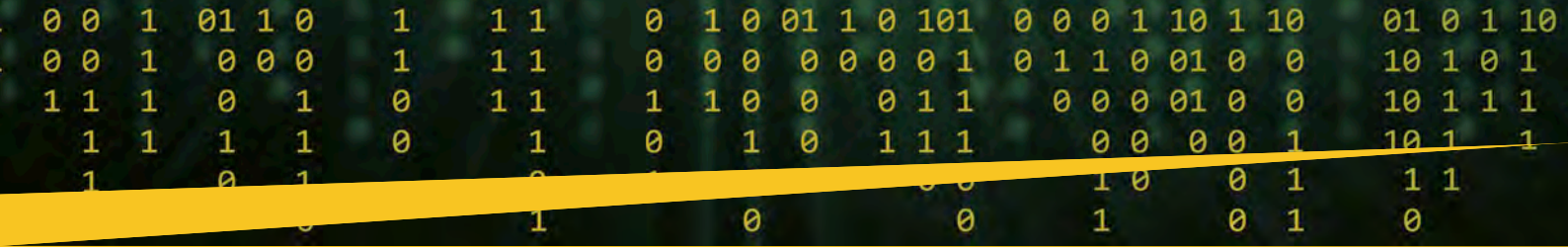
Informazioni sul background

Le seguenti bande di frequenze sono state individuate a **livello europeo** come bande prioritarie per la rapida introduzione dei sistemi di comunicazioni mobili 5G nell'Unione:

- **La banda di 700 MHz** (694-790 MHz) è molto importante per fornire una copertura estesa, specialmente in zone economicamente difficili, come le zone rurali, montane o altre zone remote. La banda è idonea a garantire una copertura efficiente su vaste aree e una migliore copertura interna, essendo sia adatta a migliorare la qualità dei servizi di comunicazione mobile già offerti dalle tecnologie 4G, sia alla diffusione delle tecnologie di comunicazione mobile di prossima generazione note come 5G o IMT-2020. Le frequenze nella banda 700 MHz amplieranno le risorse dello spettro al di sotto di 1 GHz, frequenze già utilizzate per la fornitura di servizi di comunicazioni mobili a banda larga attraverso la tecnologia LTE, e faciliteranno lo sviluppo di reti 5G e l'introduzione generalizzata di servizi digitali innovativi.

BIO

Con un'esperienza ventennale nel settore IT&C, osservatore costante delle sfide strategiche e tecniche imposte dall'evoluzione digitale, Virgilius è Consigliere IT&C del Presidente dell'ANCOM (Autorità Nazionale delle Comunicazioni della Romania), con spirito manageriale e analitico, cercando di guidare ANCOM sulla strada della trasformazione digitale.
La sua visione è quella di un ANCOM digitale, con sistemi IT distribuiti sicuri e interoperabili. Nel quadro stesso dell'ANCOM ci sono già sistemi avanzati che rappresentano da soli una base di sviluppo futuro.
Virgilius ha un Ph.D, Magna cum Laude, ha avuto collaborazioni didattiche con l'Università Politecnica, è certificato in hacking etico, esperto in competitive/ business intelligence, in sicurezza delle infrastrutture critiche e in gestione delle informazioni di sicurezza nazionale. Membro del National System for Fighting Against Cybercrime, si è occupato di cooperazione ed esercitazioni tecniche per l'individuazione, l'investigazione e la risposta agli incidenti informatici.



▸ La banda 3400-3800 MHz è considerata una banda primaria apposita per l'introduzione dei servizi 5G entro il 2020, in quanto offre un'ampia larghezza di banda dei canali radio e un buon equilibrio tra copertura e capacità. Garantendo una crescita significativa della capacità, supporta comunicazioni a banda larga avanzate, nonché applicazioni che richiedono bassa latenza e alta affidabilità, come le applicazioni *mission critical* (automazione industriale e robotica)

▸ La banda 26 GHz (24,25-27,5 GHz) è considerata una banda "pioniera" per l'armonizzazione dei primi 5G nell'UE entro il 2020, in quanto offre più di 3 GHz di spettro contiguo e consente di fornire reti ad altissima densità e ad altissima capacità su brevi distanze, nonché applicazioni e servizi 5G rivoluzionari, che comportano velocità di trasferimento dati molto elevate, maggiore capacità e latenza molto bassa.

Ecco le misure adottate o in corso di attuazione della prossima generazione di reti di comunicazione in Romania:

L'ANCOM (l'Autorità Nazionale Romena di Regolamentazione delle Telecomunicazioni) ha discusso e adottato, in una sessione del Consiglio consultivo insieme all'industria, il piano d'azione nazionale e il calendario per l'assegnazione della banda di frequenza 470-790 MHz e le relative opzioni normative, sotto forma di una programma nazionale per l'assegnazione e l'uso futuro della banda 470-790 MHz. *"Nella consultazione sulla banda dei 700 MHz, abbiamo concordato il calendario per la concessione dello spettro radio necessario per l'implementazione della tecnologia 5G in Romania. Completeremo l'intera documentazione di questa asta, compresi i prezzi di riserva, entro luglio 2019 e completeremo l'asta dello spettro entro dicembre 2019",* ha dichiarato Sorin Grindeanu, presidente dell'ANCOM *(cf. www.ancom.org.ro per la versione inglese).*

Calendario delle azioni relative all'assegnazione e all'uso futuro della banda 470-790 MHz

▸ Un primo passo essenziale è la tempestiva concessione di uno spettro radio adeguato per il futuro sviluppo dei sistemi mobili a banda larga. Affinché la banda di 700 MHz sia disponibile, l'ANCOM proporrà modifiche alla NTFA *(National Table of Radio Frequency Allocations)* e l'assegnazione della banda di 790 MHz al servizio mobile terrestre, in quanto la banda è attualmente assegnata ai servizi di televisione digitale terrestre.

▸ Entro la fine del 2018, l'ANCOM ha sviluppato ed adottato una posizione nazionale sull'assegnazione e sul futuro utilizzo delle frequenze radio disponibili nelle bande di frequenza 700 MHz, 800 MHz, 1500 MHz, 2600 MHz, 3400-3600 MHz e 26 GHz per i sistemi di comunicazioni elettroniche senza fili a banda larga.

▸ Un'altra azione che ha un impatto sull'attuazione delle tecnologie 5G è la conclusione di accordi bilaterali di coordinamento con i paesi vicini entro il 30 giugno 2019. Inoltre, ANCOM realizzerà una campagna di monitoraggio dello spettro radio delle bande di frequenza da mettere all'asta e metterà a disposizione degli offerenti una relazione sullo stato dei segnali radio individuati sul territorio della Romania e quelli provenienti dal altri stati.

▸ Entro il 31 luglio 2019, l'ANCOM adotterà la decisione sull'organizzazione della procedura di rilascio delle licenze, ovvero la definizione delle condizioni di assegnazione dei diritti d'uso delle frequenze e di altri atti normativi necessari.

▸ Secondo la proposta dell'Autorità e a seguito di dibattiti con i rappresentanti dell'industria, l'asta per l'assegnazione dei diritti d'uso delle frequenze nella banda 700 MHz e nelle altre bande di frequenza previste per la fornitura di comunicazioni fisse e mobili nell'ambito della tecnologia 5G, sarà completata entro il 15 dicembre 2019.

5G ci porterà benefici e opportunità

Gli esperti hanno annunciato prestazioni straordinarie:

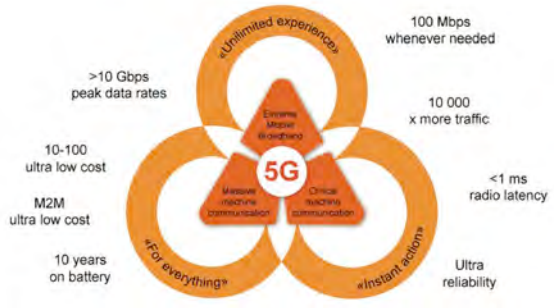
▸ Il numero di dispositivi interconnessi aumenterà rispetto ad oggi. Ciò è anche in concomitanza con l'adozione dell'IPv6;

▸ In futuro il volume dei dati trasmessi sarà esponenzialmente moltiplicato;

▸ Gli esperti stimano che aumenterà la velocità di elaborazione dati fino a 10Gbps o forse più;

▸ Latenza ridotta: la latenza, nota anche come "ritardo", è il tempo necessario affinché i dati arrivino dal trasmettitore al ricevitore. Ovviamente, più piccolo è, più veloce sarà la connessione. Per un utente abituale che utilizza un dispositivo connesso a Internet, i valori di questa funzione via 4G sono piuttosto difficili da percepire, ma per l'Internet degli Oggetti (IoT), una latenza inferiore è un aspetto molto importante. La latenza 5G dovrebbe essere di 1 millisecondo (ms), molto inferiore alla capacità percettiva umana, rispetto alla latenza 4G che invece è compresa tra 20 e 50 ms;

▸ Riduzione del consumo energetico.



Abbiamo tutti sentito parlare dei nuovi ed entusiasmanti servizi che porterà il 5G: dai veicoli interconnessi, alla produzione intelligente. Mentre alcuni servizi industriali avanzati impiegheranno da cinque a dieci anni per svilupparsi completamente, per altri il 5G offrirà un valore aggiunto a breve termine. Tuttavia, questo non è ben noto. Secondo un recente sondaggio di GSMA, i consumatori pensano che il 5G sia solo una versione più veloce del 4G mentre solo il 25% delle persone comprende il vero valore che può portare il 5G.

Applicazioni del 5G

Il 5G migliorerà notevolmente la *mobile experience* degli utenti. Permetterà di attivare nuovi servizi come la realtà virtuale basata sul cloud (niente più cuffie ingombranti), il cloud per mobile (offre al telefono le stesse capacità di elaborazione di un laptop) e video ad altissima definizione, ovunque ci si trovi.

Il 5G migliorerà l'efficienza nell'uso dello spettro radio, di dieci volte e la capacità di rete di 20-30 volte, consentendo agli operatori di fornire ai consumatori un servizio migliore a un prezzo inferiore. Ad oggi non c'è dubbio che la rete 5G stia già rappresentando un valore economico per i consumatori, gli operatori delle telecomunicazioni e le industrie verticali. Il 5G sarà distribuito in circa 110 mercati entro il 2025, secondo la previsione della GSMA (GSM Association).

Intrattenimento

Le caratteristiche tecniche precedentemente elencate permetteranno di accedere a Internet ad alta velocità da mobile anche in aree affollate senza subire limitazioni di velocità, interferenze o instabilità del segnale come a concerti, festival, eventi sportivi.

Il download di filmati con risoluzione 4K sarà una questione di secondi. Le trasmissioni televisive in diretta e gli eventi sportivi diventeranno vere e proprie esperienze visive anche per chi non parteciperà fisicamente, offrendo la possibilità di una partecipazione virtuale e sensoriale a eventi reali. Suona bene, vero? Esperimenti e dimostrazioni hanno dimostrato che ciò è possibile, e la penetrazione di queste esperienze nella vita quotidiana dipenderà anche dalla capacità di assimilazione e di consumo degli utenti finali. Nel periodo di prova, un operatore rumeno ha fatto un esperimento organizzando un concerto rock con un ologramma!

Nel novembre 2018, il più grande operatore BT/EE del Regno Unito ha trasmesso in diretta la finale della Wembley Cup in alta definizione su una rete commerciale 5G. Poiché il 5G è particolarmente veloce e con poca latenza nella trasmissione del segnale, BT è stata in grado di produrre effetti particolari che hanno reso il gioco ancor più interessante per gli spettatori, potendo nello stesso tempo realizzare tutta la produzione televisiva a distanza, senza dover installare attrezzature pesanti sul sito del torneo.

Oltre alla TV, le applicazioni di realtà virtuale (VR) 5G-enabled permetteranno anche agli appassionati di sport di guardare le partite come se fossero proprio i giocatori preferiti - o con una visuale della palla stessa. Questo cambierà completamente il modo in cui viviamo lo sport, aprendo al contempo nuovi introiti economici per gli operatori di telecomunicazioni e altre aziende lungo la catena del valore.

INTERNET DELLE COSE e INTERNET OF EYES

Il monitoraggio dinamico del traffico, la sua gestione e la pubblica sicurezza (il cosiddetto concetto di Internet of Eyes) sarà possibile ed esteso con il rilevamento e posizionamento degli oggetti in tempo reale. Assisteremo anche a un'esplosione di applicazioni e framework dedicati a smart city, smart home, smart building, perché il 5G sarà la spina dorsale dell'IoT (Internet of Things), collegando gli oggetti intorno a noi in modi che non avremmo mai ritenuto possibili.

Le tecnologie del futuro permetteranno ai veicoli indipendenti di interagire con i semafori, le infrastrutture, comunicare tra loro, sulla base di sistemi di intelligenza artificiale o aumentata. Inoltre, i sensori integrati nelle strade, nelle ferrovie e nelle rotte aeree, comunicheranno tra loro e con i veicoli intelligenti per migliorare il controllo delle infrastrutture e i servizi critici.

La rete 5G di nuova generazione produrrà un'altra rivoluzione nei processi aziendali. L'alta velocità e un breve tempo di risposta garantiranno la diffusione di massa dei robot e dell'Internet degli oggetti. Il business moderno è stato a lungo digitalizzato e ha bisogno di un nuovo ciclo di produttività e la rete 5G ha tutte le possibilità per farlo. Nonostante la massiccia campagna pubblicitaria sull'Internet degli oggetti, non è ancora possibile combinare oggetti wireless in un'unica rete poiché manca un unico standard dell'internet degli oggetti. I dispositivi indossabili funzionano tramite Bluetooth mentre le case intelligenti – via Wi-Fi – utilizzano diversi protocolli contemporaneamente.

Il 5G è particolarmente utile in quei segmenti IOT dove gli oggetti sono pesanti e distanti (ad esempio, in agricoltura) o dove è necessaria una reazione rapida (ad esempio, per i veicoli senza conducente). Ci sono anche applicazioni nel campo dell'agricoltura dove, sensori di umidità, distributori automatici di fertilizzanti, aziende di intelligenza artificiale specializzati in previsioni, interverranno per la regolazione, il controllo e la massimizzazione dei risultati.

I veicoli volanti in movimento, autonomi e telecomandati e la loro gestione del traffico saranno guidati anche da sistemi che scambieranno grandi quantità di dati, ma soprattutto lo faranno in tempo reale.

Possiamo dire che il 5G moltiplicherà i noti vantaggi dell'Internet degli Oggetti e ne favorirà la sua diffusione.

L'elevata velocità di trasferimento dati nelle reti 5G aumenterà il carico sull'infrastruttura. Ciò richiederà notevoli sforzi e investimenti da parte degli operatori di telefonia mobile. L'introduzione in massa degli oggetti IoT arricchirà i fornitori di tecnologie cloud: i dispositivi intelligenti produrranno enormi quantità di dati che dovranno essere conservati.

How 5G will change our lives

Sphere	Effect
Driverless vehicles	elimination of dangerous signal delay at high speed
Industry	speed of industrial robots and the unification of infrastructure
Agriculture	remote management of agricultural machinery, monitoring of fields and herds
Education	visual training through VR-translation of the process from the point of view of the master
Telemedicine	real time remote operations
Communication	interactive virtuality: users will be able to interact at a distance as they are nearby
Entertainment	fast wireless video transmission of ultra-high definition (4K, 8K), broadcast events with the VR effect
Computer games	multiplayer VR-games without signal delay

Medicina e istruzione

L'espansione del 5G potrebbe impattare anche test e applicazioni nel campo della robotica controllata dal cloud, più precisamente con il controllo di un robot da remoto.

Sono stati effettuati test di interventi medici ***internet touch-based***, combinati con le realtà virtuali, come quelli che hanno interessato la trasmissione remota e in tempo reale della sensazione tattile. I medici opereranno i pazienti a distanza. Utilizzeranno caschi di realtà virtuale e guanti speciali che daranno loro la sensazione di afferrare il paziente e allo stesso tempo gli consentiranno di poterlo operare.

Utilizzando la rete 5G, China Mobile, ha contribuito a trasformare le ambulanze in ospedali mobili. I medici della Zhejiang University School of Medicine in Cina possono infatti utilizzare apparecchiature ad ultrasuoni a distanza attraverso occhiali VR e attraverso un braccio robotizzato per esaminare i pazienti nelle ambulanze o in altri luoghi. Il 5G è fondamentale in questo caso in quanto qualsiasi ritardo nella trasmissione del segnale potrebbe essere disastroso per il paziente e la sua stabilità consentirebbe ai medici di eseguire a distanza procedure molto delicate.

Nel gennaio 2019, i medici della provincia cinese sudorientale del Fujian hanno eseguito la prima operazione remota al mondo utilizzando una trasmissione di rete 5G. L'operazione di successo (eseguita su un maiale) segna l'avvento della chirurgia a distanza 5G, ponendo le basi per una serie di nuove applicazioni cliniche innovative per il futuro.

Un giorno, le reti 5G collegheranno i pazienti in aree isolate con i medici di tutto il mondo. Le persone nel deserto del Gobi e nel Circolo Polare Artico avranno accesso alle stesse cure che potrebbero ricevere se fossero a Londra o Dubai.

Sono anche previsti progetti pilota 5G che mettano in contatto gli studenti delle regioni più povere, con alcuni dei migliori insegnanti del mondo. I video ad alta definizione e i VR non garantiscono affidabilità con l'utilizzo di reti 4G cosa che invece le connessioni 5G ad alta potenza potrebbero fare andando ad aiutare i bambini delle regioni sottosviluppate e dando agli studenti la possibilità di ricevere una buona istruzione.

Espansione del 5G

Si stima che entro il 2023, il 20% della popolazione mondiale avrà una copertura 5G e la tecnologia 5G genererà un giro di affari da 1.200 miliardi di dollari entro il 2026.

Debolezze del 5G

Parlando di vulnerabilità e rischi associati, ne identifico almeno due:

- una relativa al livello di applicazione, alle vulnerabilità associate e ai nuovi tipi di servizi e applicazioni
- uno relativo agli aspetti tecnici delle tecnologie stesse e ai moduli o protocolli di gestione.

Quanto, la prima categoria di vulnerabilità:

- Si possono facilmente elaborare proiezioni partendo dall'attuale situazione di infezione da malware di più dispositivi IP o reti e poi usati per attacchi DDoS (Distributed Denial of Service). L'aumento del numero di dispositivi interconnessi aumenterà la massa critica dei dispositivi potenziali rilevati in una rete Botnet per avviare attacchi più forti con una velocità forse migliaia di volte superiore! Da un punto di vista tecnologico, i dispositivi di contrattacco dovranno tenere il passo alle minacce, probabilmente utilizzando l'intelligenza artificiale, per avere una capacità di risposta adeguata.

- Il furto di informazioni può raggiungere livelli incalcolabili: se parliamo di estorsione di informazioni e furto di dati personali, intercettazioni di traffico per la decifrazione di password o informazioni riservate. Nel caso della rivoluzione industriale 4.0, che porta la prototipazione virtuale e l'invio del modello online direttamente sulla linea di produzione, un attacco man-in-the-middle potrebbe significare un importante danno (furto della proprietà intellettuale, spionaggio

industriale) o peggio, la distorsione del modello o la sua sostituzione proprio prima che inizi la realizzazione fisica. I risultati e gli effetti negativi possono essere veramente incalcolabili.

- L'intercettazione/modifica in tempo reale dei dati provenienti da sensori di traffico, edifici intelligenti, veicoli autonomi o controlli di volo porterebbe disastri, crimini, catastrofi o potrebbe compromette le infrastrutture critiche mettendo in pericolo molte vite umane.
- Gli effetti di una manomissione / intercettazione in tempo reale del traffico dati associato sono facilmente immaginabili. Data l'enorme velocità e i tempi di risposta vicini allo zero purtroppo tali operazioni sono molto facili da realizzare.

Quanto la seconda vulnerabilità:

L'ENISA ha reso pubblico lo studio *"Signalling Security in Telecom SS7/Diameter/5G"* [1] sul 5G che evidenza quanto segue:

- Gli attacchi SS7 possono essere complessi in quanto gli aggressori stanno acquisendo sempre più conoscenze e hanno avuto il tempo di sviluppare scenari di attacco efficaci. Una protezione base probabilmente contrasterà la maggior parte degli attacchi, ma lascerà spazio agli attacchi complessi o mirati che possono realmente causare danni a livello sociale, economico o politico (es. spionaggio, ecc.). In conclusione, possiamo ricordare che in termini di SS7 le misure minime di sicurezza sono adottate dalla maggioranza dei fornitori. Questa conclusione è rafforzata anche dall'industria, attraverso diversi documenti, risultati o altri materiali. Tuttavia, tali misure di sicurezza di base forniscono solo un primo livello di protezione. Inoltre, l'infrastruttura della SS7 è in alcuni casi piuttosto vecchia e non tutte le attrezzature supportano l'adozione di misure di sicurezza comprese quelle basilari. Ciò è confermato anche dai vincoli tecnici e di costo chiariti nello studio.

L'attenzione dell'industria sulla sicurezza Diameter è arrivata solo dopo quella degli SS7 e certamente non ha ancora raggiunto una sua maturità. Diameter deriva da RADIUS (Remote Authentication Dial-In User Service) e fornisce un protocollo di autenticazione, autorizzazione e accounting per le reti informatiche. In termini di design, ha preso in prestito molti concetti dall'SS7, comprese le sue vulnerabilità. Trattandosi di un protocollo puramente IP, il rischio che un intruso possa accedervi attraverso l'hacking aumenta. Maggiore è la conoscenza che l'aggressore ha sui protocolli correlati a Internet, maggiori sono le possibilità del suo successo. Queste caratteristiche rende questo protocollo, in teoria, più semplice da sfruttare rispetto all'SS7.

Alla luce di quanto sopra, si può concludere che occorre prestare particolare attenzione alla sicurezza 5G. Poiché la mobilità svolge un ruolo enorme nella nostra società digitale, assicurando la nostra infrastruttura digitale quotidiana a sostegno dell'economia stessa, la posta in gioco è alta. Le vecchie generazioni di telefonia mobile hanno dimostrato i loro svantaggi in termini di sicurezza e gli stessi approcci non possono più essere adottati. Poiché le vulnerabilità relative di Diameter stanno cominciando ad essere scoperte pubblicamente, l'uso futuro di questo protocollo o approcci simili dovrebbero essere evitati. I vettori tecnologici avranno bisogno di una nuova architettura di trasmissione in grado di affrontare: l'impatto dell'introduzione di miliardi di dispositivi statici e in roaming, il comportamento degli abbonati, i requisiti di larghezza di banda e le nuove applicazioni.

Le raccomandazioni dell'ENISA sono: *"mentre si sta lavorando per affrontare gli attacchi a SS7 e Diameter, solo una piccola parte dei protocolli è stata studiata. Si prevede la scoperta di nuove vulnerabilità. Inoltre, sono ora disponibili gratuitamente strumenti per la scansione e l'eventuale attacco alle reti mobili. Il 5G, la nuova generazione di telefonia mobile, è ancora in fase di sviluppo. Sono disponibili le prime versioni di alcuni produttori, ma gli standard sono ancora agli inizi. Tuttavia c'è il rischio di ripetere gli errori commessi. Visti i miglioramenti che il5G porterà (più utenti, più larghezza di banda, ecc.), i rischi per la sicurezza tuttavia rimarranno gli stessi e ciò porterà pericoli estremamente importanti".*

Sfide per la sicurezza in SDN e NFV

Un SDN (software-defined network) centralizza le piattaforme di controllo rete e consente la programmabilità delle reti di comunicazione. Queste due caratteristiche dirompenti, tuttavia, creano opportunità di cracking e hacking della rete stessa. Ad esempio, il controllo centralizzato sarà una scelta favorevole per gli attacchi DoS e l'esposizione non intenzionale delle interfacce di programmazione delle applicazioni critiche (API) a software può coinvolgere l'intera rete.

Il controller SDN modifica le regole *flow* nel percorso dei dati, quindi il traffico del controller può essere facilmente identificato. Questo trasforma il controllore in un'entità visibile nella rete, rendendolo la vittima preferita per gli attacchi DoS. La centralizzazione del controllo di rete può anche creare per il controller l'effetto collo di bottiglia per l'intera rete se soggetta ad attacchi di saturazione.

Anche se il VNF (Virtual Network Functions) è molto importante per le future reti di comunicazione anch'essa presenta sfide per la sicurezza come: la riservatezza, l'integrità, l'autenticità e la conformità alle norme di sicurezza e di non-ripudio.

Dal punto di vista dell'utilizzo nelle reti mobili, le odierne piattaforme di NFV (Network Functions Virtualization) non forniscono una sicurezza e un

isolamento adeguato ai servizi di telecomunicazione virtualizzati. Una delle principali sfide che persistono nell'uso di NFV nelle reti mobili è la natura dinamica delle funzioni di rete virtuale (VNF) che potrebbe portare a errori di configurazione e quindi alla perdita di sicurezza.

La sfida principale che richiede un'attenzione immediata, è che l'intera rete può essere compromessa se *l'hypervisor* viene dirottato.

Soluzioni di sicurezza per SDN e NFV

Grazie al piano di controllo centralizzato, visualizzato e programmato logicamente a livello di rete globale, l'SDN faciliterà la rapida identificazione delle minacce attraverso un ciclo di raccolta di informazioni dalle risorse di rete, dagli stati e da flows.

L'architettura SDN supporta sistemi di monitoraggio della sicurezza altamente reattivi e proattivi, sistemi di analisi del traffico e sistemi di risposta per facilitare l'analisi forense della rete, l'inalterazione delle politiche di sicurezza e l'inserimento di servizi di sicurezza.

Grazie alla visibilità globale della rete è possibile implementare criteri di sicurezza di rete coerenti in tutta la rete, mentre sistemi di sicurezza come Firewall e Intrusion Detection System (IDS) possono essere utilizzati per scopi specifici aggiornando le tabelle flow degli switch SDN.

La sicurezza delle VNF può essere migliorata attraverso un orchestrator platform in corrispondenza all'architettura che fornisce sicurezza non solo alle funzioni virtuali in un ambiente multi-tenant, ma anche alle entità fisiche di una rete di telecomunicazione. L'utilizzo di sistemi informatici affidabili, il controllo remoto della veridicità e integrità dei sistemi virtuali e degli hypervisor si prospetta essere una protezione basata su hardware alle informazioni private e di rilevare il software corrotto in ambienti virtualizzati.

Le sfide della sicurezza nei canali di comunicazione

Prima delle reti 5G, le reti mobili avevano canali di comunicazione dedicati basati su tunnel GTP e IPsec. Le interfacce di comunicazione, come X2, S1, S6, S6, S7, che vengono utilizzate solo nelle reti mobili, richiedono un significativo livello di competenza per attaccare queste interfacce.

Tuttavia, le reti 5G basate su SDN non avranno tali interfacce dedicate, ma piuttosto interfacce SDN comuni. L'apertura di queste interfacce aumenterà il numero possibile di aggressori. La comunicazione nelle reti mobili 5G basate su SDN può essere suddivisa in tre canali di comunicazione, canale dati, canale di controllo e canale inter-controllore.

Negli attuali sistemi SDN, questi canali sono protetti da sessioni TLS (Transport Layer Security)/ SSL (Secure Sockets Layer). Tuttavia, le sessioni TLS/SSL sono altamente vulnerabili; sono possibili attacchi a livello IP, attacchi agli scanner SDN e alla mancanza di meccanismi di strong authentication.

Soluzioni di sicurezza per i canali di comunicazione

Il 5G ha bisogno di una sicurezza adeguata del canale di comunicazione non solo per prevenire le minacce alla sicurezza identificate, ma anche per mantenere gli ulteriori vantaggi dell'SDN, come la gestione centralizzata dei criteri, la programmabilità e la visibilità globale dello stato della rete. L'IPsec è il protocollo di sicurezza più comunemente usato per proteggere i canali di comunicazione nelle attuali reti di telecomunicazione come il 4G-LTE. E' possibile utilizzare il *tunneling* IPsec, con lievi modifiche, per proteggere i canali di comunicazione 5G.

Inoltre, la sicurezza delle comunicazioni LTE (Long-Term Evolution) è garantita dall'integrazione di vari algoritmi che garantiscono l'autenticazione, il rispetto dell'integrità e la crittografia. Le principali sfide di questi sistemi di sicurezza, ad oggi esistenti, sono l'elevato consumo di risorse, le spese generali elevate e la mancanza di coordinamento. Pertanto, queste soluzioni non sono fattibili per la comunicazione con le infrastrutture critiche in 5G.

In questo modo sarà possibile ottenere un livello di sicurezza più elevato per le comunicazioni critiche proprio utilizzando nuovi meccanismi di sicurezza, come la sicurezza a livello fisico, adottando la **stampa a radiofrequenza (RF)**, utilizzando **schemi di sicurezza asimmetrici** e **modificando** dinamicamente **i parametri di sicurezza a seconda della** situazione.

Allo stesso modo, la **comunicazione utente end-to-end** può essere protetta utilizzando protocolli crittografici come HIP (Host Identity Protocol).

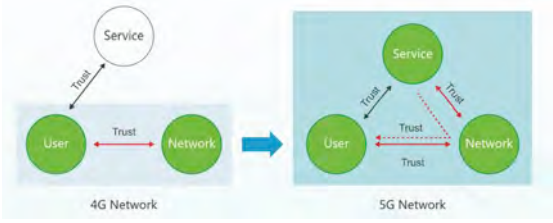
Ecco una tabella con le sfide della sicurezza nelle tecnologie 5G

Security Threat	Target Point/Network Element	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information data bases				✓	✓
TCP level attacks	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

Nuovo modello di trust e gestione dell'identità

Nelle reti di comunicazione mobile legacy, le reti "telco" sono responsabili dell'autenticazione di un utente per il solo accesso alla rete. Si crea un modello di fiducia tra due elementi, gli utenti e le reti. L'autenticazione tra utente e servizi non è coperta dalle reti.

Tuttavia, nelle reti 5G, al modello di fiducia appena descritto, si inserisce un nuovo soggetto ovvero il fornitore di servizi verticali. Le reti possono cooperare con i fornitori di servizi per una gestione dell'identità ancora più sicura ed efficiente.



Le sfide della gestione dell'autenticazione ibrida

Le reti 5G sono piattaforme aperte che offrono una moltitudine di servizi quali ad esempio smart transport, smart grid e IoT industriale. Sia le reti che i fornitori di servizi, devono affrontare sfide per rendere più semplice e meno costoso l'accesso e l'autenticazione ai servizi.

Sono 3 i possibili modelli di autenticazione che potrebbero coesistere nel 5G per rispondere alle esigenze aziendali.

▸ Autenticazione solo da parte delle reti

Dato che l'autenticazione comporta costi significativi per i fornitori di servizi, gli stessi potrebbero pagare le reti per la gestione dell'autenticazione in modo che gli utenti possano accedere a più servizi una volta completata un'unica autenticazione. Questo libera gli utenti dall'ingombrante compito di ottenere ripetutamente l'autorizzazione quando si accede a servizi diversi.

▸ Autenticazione solo da parte dei fornitori di servizi

Le reti possono contare sulle comprovate capacità di autenticazione delle industrie di settore ed esonerare i dispositivi dall'autenticazione dell'accesso alla rete (radio), operazione che può aiutare i sistemi di rete a ridurre i costi operativi.

▸ Autenticazione da parte di reti e fornitori di servizi

Per alcuni servizi potrebbe essere adottato un modello in cui le reti si dedicano all'accesso alla rete e i fornitori di servizi si occupano dell'accesso ai servizi.

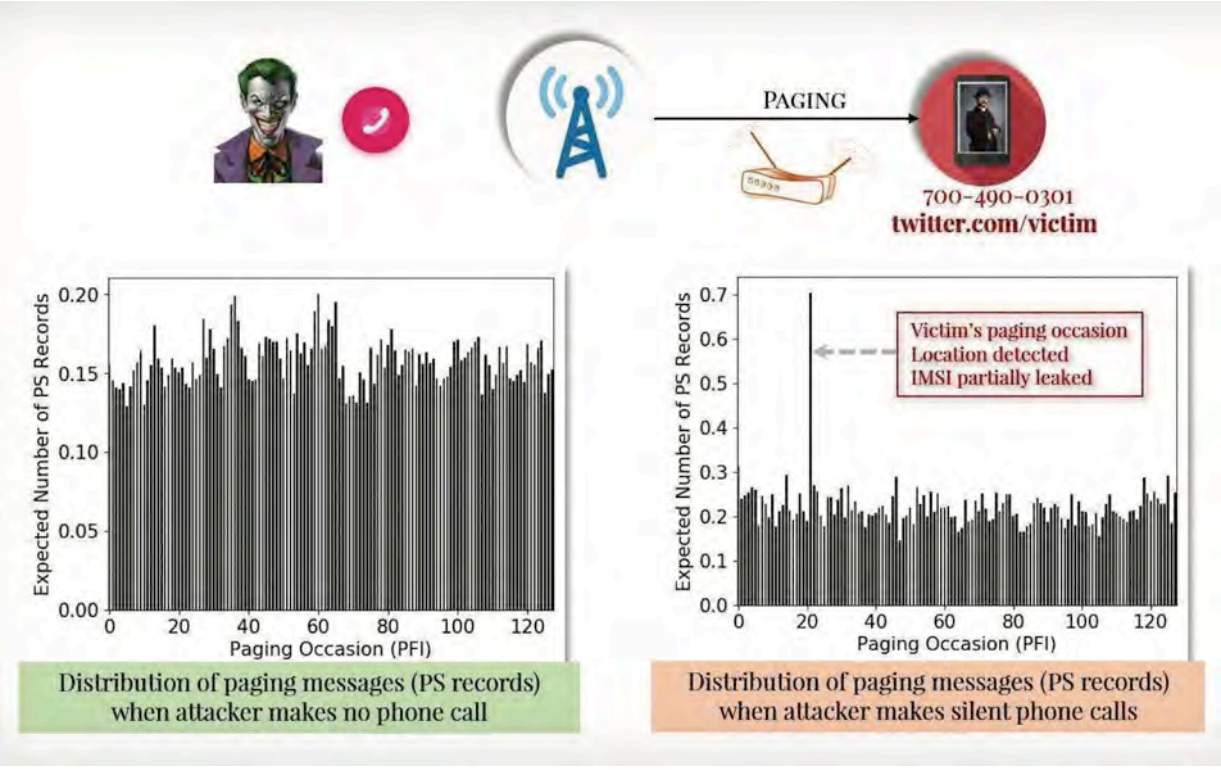
Nuove vulnerabilità 5G scoperte e rese pubbliche nel febbraio 2019

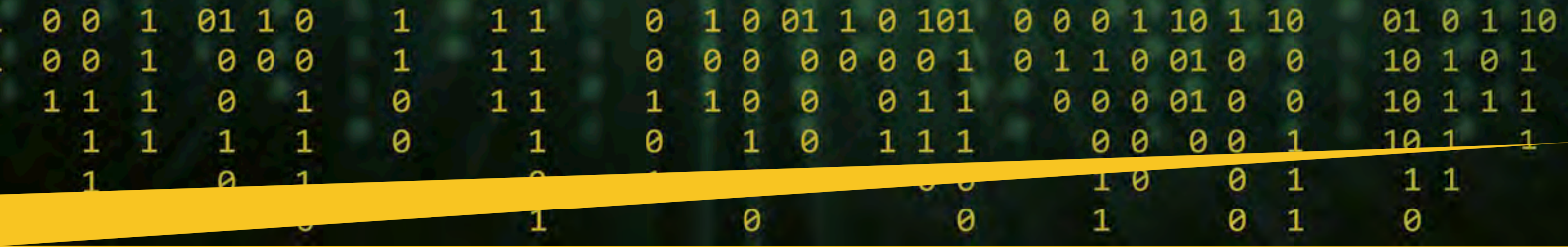
Un gruppo di ricercatori della Purdue University e dell'Università dell'Iowa ha presentato al Network and Distributed System Security Symposium di San Diego i risultati di uno studio da cui emergono alcune vulnerabilità del 5G. Gli stessi sottolineano che le loro scoperte, segnalate per la prima volta da TechCrunch, sono particolarmente preoccupanti in quanto lo standard 5G è stato sviluppato proprio per proteggere al meglio i sistemi da determinate tipologie di attacchi.

"Siamo rimasti davvero sorpresi che, sebbene il 5G prometta una maggiore sicurezza e privacy, non può garantire questo livello, perché eredita molte politiche di sicurezza e sottoprotocolli delle generazioni precedenti, che sono più soggette ad errori", dice Syed Rafiul Hussain di Purdue, uno degli autori del documento. *"Si apre la porta agli avversari che potranno sfruttare queste debolezze."*

I ricercatori, che lo scorso anno avevano scoperto anche alcune vulnerabilità nella rete 4G, descrivono una serie di nuove debolezze del protocollo 5G che potrebbero essere utilizzate in una varietà di attacchi. Alla base degli attacchi vi è un exploit che i ricercatori chiamano Torpedo; questo fa leva sui difetti del "protocollo di paging" utilizzato per notificare ai dispositivi le comunicazioni in entrata.

Un dispositivo quando non comunica attivamente, ricevendo o trasmettendo chiamate o sms, entra in modalità inattiva quindi non consuma batteria cosa che invece farebbe costantemente. I ricercatori hanno scoperto che tuttavia questa funzionalità può essere sfruttata. Se un aggressore decide di attaccare l'obiettivo selezionato che si trova nelle vicinanze, avvia una rapida serie di attacchi che si concretizzano in vere e proprie telefonate al dispositivo finalizzate allo "sniffing" del dispositivo stesso. In egual modo potrà condurre lo stesso attacco, oltre che per gli smartphone anche per i cercapersone. Sia la rete 4G che la rete 5G hanno protezioni integrate contro questo tipo attacco ma i ricercatori hanno





scoperto che gli sforzi di "offuscamento" sono insufficienti. Un aggressore può infatti inviare ugualmente messaggi di paging andando a rubare l'intero contenuto dei pacchetti inviati al ripetitore e mostrando allo stesso attaccante lo stato del dispositivo se attivo o spento nonché la sua posizione.

Gli attacchi Torpedo permettono ad un hacker di manipolare il cercapersone di un bersaglio con la conseguenza di aggiungere, cancellare o bloccare messaggi e chiamate. Un hacker potrebbe anche usare la tecnica per falsificare certi tipi di messaggi, come ad esempio i messaggi di AMBER (America's Missing: Broadcast Emergency Response) Alerts.

Ma un aggressore può usare Torpedo come trampolino di lancio in un *"IMSI-cracking attack"* che potrebbe consentire a un hacker di accertare il numero di "International Mobile Subscriber Identity" (IMSI) di una vittima. Il numero identificativo IMSI dello smartphone può essere utilizzato per tracciare un dispositivo in modo più preciso, o per monitorare le comunicazioni attraverso dispositivi illegali installati sui ripetitori di telefonia cellulare, spesso chiamati stingrays o "IMSI catcher". Tali strumenti sono ormai da anni una nota minaccia per la privacy e, prevalentemente presenti negli Stati Uniti, sono utilizzati sia dalle forze dell'ordine che da aggressori.

Per proteggere i dispositivi da tali attacchi, i numeri IMSI nelle reti 4G e 5G sono cifrati, ma i ricercatori hanno scoperto ancora una volta che le protezioni implementate non sono sufficienti. Hanno anche riscontrato un problema di implementazione della rete, chiamato Piercer, che potrebbe esporre i numeri IMSI sulla rete 4G in altro modo. Si presume che un operatore statunitense, che non è stato ancora reso pubblico, è attualmente vulnerabile agli attacchi di Piercer.

"Una volta che l'IMSI di un utente è esposto, un avversario può effettuare attacchi più sofisticati, tra cui il monitoraggio della posizione e l'intercettazione delle chiamate telefoniche e dei messaggi SMS dell'utente", dice Hussain di Purdue. "La privacy dei consumatori medi è a rischio ed è a disposizione di terzi malintenzionati che possono conoscere dati di geolocalizzazione e altre informazioni private".

Stante l'eccezione dei difetti Piercer, le vulnerabilità scoperte dai ricercatori non possono essere corrette dal singolo operatore ma dal GSMA, che supervisiona lo sviluppo degli standard per i dati mobili, tra cui 4G e 5G.

La GSMA è a conoscenza dei risultati di questa ricerca e sta valutando soluzioni per alcune delle vulnerabilità identificate contestando tuttavia la complessità degli attacchi.

Secondo la GSMA: "I risultati suggeriscono che un hacker potrebbe teoricamente prendere di mira l'IMSI di un abbonato o un identificatore unico su una rete 4G inviando più messaggi in rapida successione e quindi monitorando la rete per identificare l'aumento di traffico contro un abbonato specifico. Tuttavia, questo approccio in realtà dovrebbe essere eseguito in un determinato lasso di tempo ed essere basato su prove ed errori, il che, per avere successo, sarebbe un processo completo e dispendioso in termini di tempo. La GSMA sta lavorando con il 3GPP per valutare le opzioni di rilevamento degli attacchi, il livello di minaccia e se è possibile apportare modifiche agli standard".

La GSMA nella sua dichiarazione contesta inoltre che la rete 5G sarebbe vulnerabile agli attacchi indicati dai ricercatori poiché lo studio è stato condotto " su una versione iniziale dello standard che da allora è cambiata. Questo miglioramento della sicurezza dimostra come i livelli di sicurezza continuano ad evolvere e migliorare attraverso la standardizzazione".

I ricercatori affermano però che i miglioramenti non risolvono ancora il problema. "Abbiamo controllato le modifiche e sembra che anche il nuovo sistema sia vulnerabile all'attacco di Torpedo in 5G".

Tutto questo non vuol dire che lo standard 5G deve essere scartato. Ha ancora molti vantaggi, compresi quelli in termini di sicurezza, che rendono l'arrivo della rete 5G un elemento importante e produttivo. Ma i difetti di sicurezza negli standard telefonici devono essere presi sul serio e risolti. I difetti fondamentali del protocollo, come quelli dello storico standard SS7, sono rimasti irrisolti per decenni e hanno portato ad un aumento dei rischi per gli utenti finali.

Maggiore è la pressione esercitata sulle compagnie di telecomunicazioni per risolvere questi difetti, meglio è.

Bibliografia:

1. Sito ufficiale l ANCOM: www.ancom.org.ro
2. Virgilius Stanciulescu - Cybersecurity Forum: 5G beneficii si vulnerabilitati
3. Virgilius Stanciulescu - Congresso sulla sicurezza informatica, Sibiu & Porentruy, 2018: 5G vulnerabilità e nuove strategie di attacco e contromisure
4. Virgilius Stanciulescu - Congresso sulla sicurezza informatica, Firenze 2019: 5G vulnerabilità e nuove strategie di attacco e contromisure
5. 5G Sicurezza: Libro bianco di Huawei sul futuro
6. 5G Sicurezza: Analisi delle minacce e delle soluzioni
7. Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtovk, Centro per le comunicazioni wireless, Università di Oulu, Finlandia.
8. https://www.go4it.ro/telefoane-mobile/au-fost-descoperite-noi-vulnerabilitati-in-retelele-4g-si-5g.-toate-dispozitivele-pot-fi-accesate-de-catre-hackeri-17890274/
9. Forum Economico Mondiale: https://www.weforum.org/agenda/2019/01/here-s-how-5g-will-revolutionize-the-digital-world
10. Forum economico mondiale: https://www.weforum.org/agenda/2019/02/heres-what-5g-will-bring-in-2019/
11. Nuove tecnologie di linea: https://newline.tech/blog/what-will-the-era-of-5g-bring-us/
12. ENISA: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g
13. WIRED : https://www.wired.com/story/torpedo-4g-5g-network-attack-stingray/
14. TECNICRUNCH: https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/ ■

1 https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

In soli 5 anni, l'*homo sapiens sapiens* è diventato *homo smartphonicus schizophrenicus*

Autore: Laurent Chrzanovski

Ho intitolato provocatoriamente l'articolo *"homo smartphonus schizophrenicus"* perché l'atteggiamento e la percezione digitale travolgente delle persone è agli antipodi del loro comportamento fisico naturale e sociale nativo ... ma con più smartphone che abitanti e oltre l'80% dei dati a cui si accede attraverso questi strumenti non sicuri e invasivi, questo atteggiamento digitale, rapidamente, sta già cambiando i comportamenti fisici quotidiani e le relazioni sociali della maggior parte delle persone.

La decennale mancanza di educazione e cultura dedicata a far conoscere ai cittadini un *"ad minima"* della giungla digitale, sta causando quella che viene definita medicalmente *Schizophrenia*, cioè *"una grave malattia mentale caratterizzata da una disintegrazione del processo di pensiero, di contatto con la realtà e di risposta emotiva"* (Oxford Concise Medical Dictionary, 9th ed., 2015).

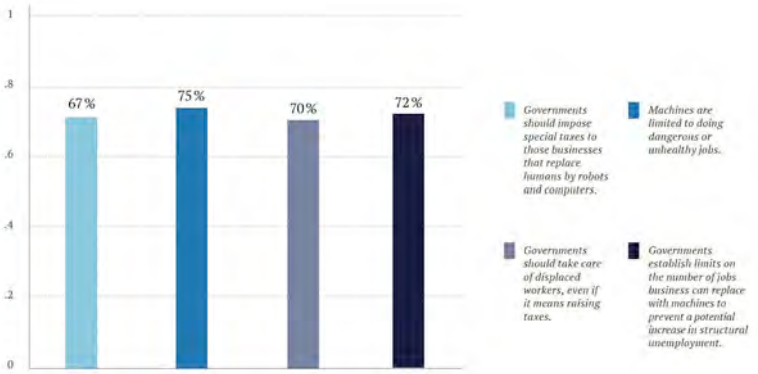
Swiss Luxury Clinics Time/Price costs for detox

Una recente ricerca sull'evoluzione delle Tecnologie e, soprattutto, dell'Intelligenza Artificiale (Rubio, Lastra 2019) evidenzia una schizofrenia totale.

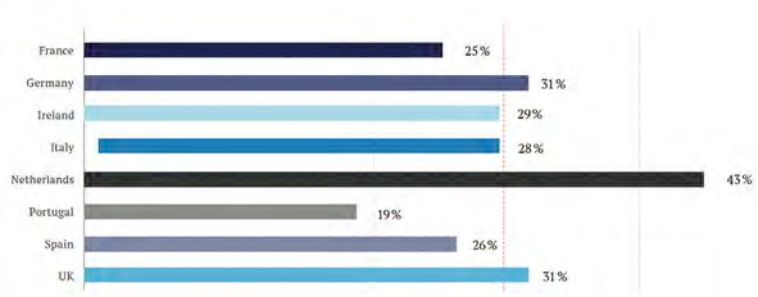
Da un lato, gli europei temono le nuove tecnologie, considerate una sfida enorme e da controllare: "il 67% degli europei ritiene che la governance delle nuove tecnologie sia, con i cambiamenti climatici, la più grande sfida che l'UE deve affrontare in questo momento; il 70% degli europei di tutte le età ritiene che, se non adeguatamente

controllate, le nuove tecnologie causeranno più danni che benefici alla società nel prossimo decennio."

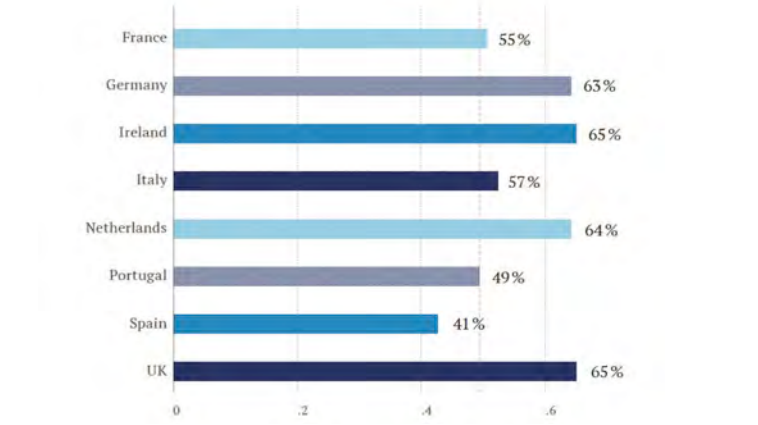
Inoltre, "il 40% degli europei ritiene che l'impresa per cui lavora scomparirà nei prossimi 10 anni se non si attuano cambiamenti rapidi e profondi" e "la maggior parte degli europei ritiene che i governi dovrebbero intervenire per limitare l'automazione e affrontare gli effetti negativi sulla società".



D'altra parte, in una sorta di *schizofrenia totale*, "circa il 25% degli europei è in qualche modo totalmente favorevole al fatto che un'intelligenza artificiale prenda decisioni importanti sulla gestione del proprio paese". In altre parole, l'intelligenza artificiale sarebbe di gran lunga il primo partito politico dei Paesi Bassi - il 43% dei cittadini olandesi è favorevole/non contrario all'opzione AI - ma anche in Germania, Italia o Spagna se si considerano le percentuali del primo partito politico in parlamento).



Peggio ancora, in un continente dove si vede uno smartphone in ogni mano, "il 68% degli europei è preoccupato o molto preoccupato che le persone socializzino digitalmente più che di persona"... quando poi sono i primi a comportarsi in questo modo.



BIO

Dottore di ricerca in Archeologia romana dell'Università di Losanna, Laurent ha poi ottenuto un diploma post-dottorale in Storia e Sociologia presso l'Accademia delle Scienze della Romania, l'abilitazione UE a dirigere Dottorati di ricerca nel campi della Storia e delle scienze affini. Oggi, Laurent è professore presso la Scuola dottorale e postdottorale dell'Universita' Statale di Sibiu. Tiene regolarmente corsi post-dottorato in Università di prestigio in diversi paesi dell'UE, in primis a Varsavia. E' autore/redattore di 31 libri, di oltre un centinaio di articoli scientifici e di altrettanti articoli destinati al grande pubblico.
Nel campo della cybersecurity, Laurent è membro e consulente contrattuale del gruppo di esperti dell'ITU. Ha fondato e gestisce ogni anno il trittico di congressi PPP "Cybersecurity Dialogues" (Romania, Svizzera, Italia) organizzati in collaborazione con un grande numero di istituzioni specializzate, internazionali e nazionali. Nello stesso spirito e con lo stesso spirito e con i stessi partner, è fondatore e redattore capo e redattore capo di Cybersecurity Trends, la prima rivista trimestrale di sensibilizzazione alla sicurezza informatica per adulti, pubblicata in quattro variante adattate ad altrettanti ecosistemi lingusitsici e culturali. Il suo campo di studio è focalizzato sulla relazione tra i comportamenti umani nel mondo digitale e il bisogno di trovare il giusto equilibrio tra la sicurezza e la privacy per l'utente finale, cioè "l'e-cittadino" che siamo tutti diventati.

Ma il più grande disprezzo storico, politico, democratico e sociale di tutto il nostro passato, da Atene alle Lumières, è che *"più del 50% degli europei ritiene che i contenuti politici e ideologici dovrebbero essere vietati dalle reti sociali per proteggere la democrazia"*.

In un'epoca in cui l'agorà, il luogo pubblico, i caffè letterari, i dibattiti filosofici e ideologici prendevano il loro posto "virtuale" nel mondo digitale, e soprattutto nei "social media", dove poteva essere espresso un "contenuto politico"? E, tra l'altro, che cos'è "politico" o "ideologico" se non qualche discorso fanatico in un periodo in cui tutti i partiti convenzionali negano da decenni la loro ragione d'essere (socialismo, liberalismo, conservatorismo) facendo le stesse false promesse e programmi utopici quando si avvicina un'elezione?

Le radici della malattia: una breve storia 2013-2019

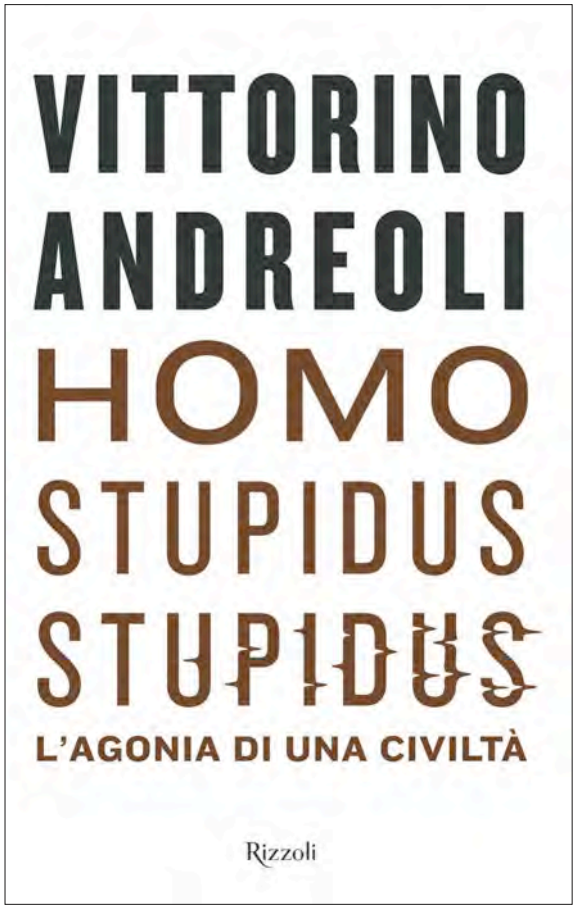
Vi ricordate che fino al 2013, i problemi e le ricerche si sono concentrati sulla limitazione dell'approccio BYOD, sull'uso dei computer portatili per accedere a contenuti

non professionali e ai fastidiosi sugli squilli sui telefoni dei colleghi di lavoro?

Ebbene, dall'invasione del 4G, tutto è cambiato, perché non abbiamo più un telefono ma un piccolo e potentissimo strumento multimediale BYOD - in qualche modo è possibile utilizzarlo anche come telefono, custodendo i nostri più profondi segreti personali e professionali e condividendoli con la moltitudine degli utenti presenti che usano hardware e software e delle applicazioni che abbiamo scelto. E tutto è cambiato. Viviamo l'inizio di uno slancio narcisistico ed egoistico di "me, ora, immediatamente", non importa se siamo al lavoro, a cena o addirittura ... a letto.

Questo nostro editoriale rappresenta l'opposto dell'obiettivo centrale che la rivista persegue, la sicurezza informatica, tuttavia, potrebbe essere quella base che se ignorata, senza uso di regole e sanzioni estremamente drastiche per qualsiasi strumento personale IT utilizzato nell'ambiente di lavoro, impedirà una possibile costruzione di una sicurezza completa.

Nel 2016, quando Jason Fried, il fondatore e CEO di Basecamp, intervenuto alla conferenza Lean Startup, ha chiesto alla folla "Chi qui ricorda di aver avuto mai 4 ore di lavoro continuo per sé stessi negli ultimi 5 anni? Il risultato: "Forse 20 o 30 persone hanno alzato la mano. Su 600 presenti. E' tragico. Un segnale di frattura in ogni dove. E sta peggiorando, non migliorando. Lo stato dell'arte è fottuto" (Fried 2016)



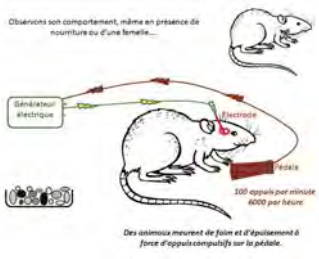
Oggi, considerando la transizione dal 4G al 5G , sempre più medici, psichiatri, specialisti comportamentali, ma anche esperti nel campo produttivo e nel team working, considerano l'uso e l'abuso degli smartphone come la radice di uno dei più importanti cambiamenti psicologici della storia umana e, dicono, che siamo solo all'inizio di questo nuovo passo dell'evoluzione dell'*"homo sapiens"*.

Nel suo ultimo capolavoro, *Homo Stupidus Stupidus Stupidus. L'agonia di una civiltà* (Milano 2018), lo psicopatologo di fama mondiale Vittorino Andreoli ha scritto senza equivoci: "Non stiamo più dando importanza ai principi con il risultato che stiamo progressivamente sprofondando nella barbarie. La civiltà non è una conclusione scontata, ma una conquista che passa attraverso la trasmissione di valori e comportamenti. Così, da sapiens sapiens, l'uomo di oggi corre il rischio di diventare uno "stupidus stupidus", *facile preda di una nuova solitudine e vittima di una malattia sempre più diffusa: l'autismo digitale"*.

Il concetto di un male ingegnosissimamente creato

Perché così tante persone diventano dipendenti dagli smartphone o in procinto di diventarlo? Ebbene, le ricette utilizzate da tutti i big di Internet GAFAM (Google, Apple, Facebook, Amazon, Microsoft) e dagli altri produttori di software, di strumenti e delle famose "app" si basano giusto su due fenomeni semplici e ben noti.

Las Vegas: centri di disintossicazione per il gioco d'azzardo (©LURC)



Esperimento di Olds e Miltner; disegno © Agace Berger

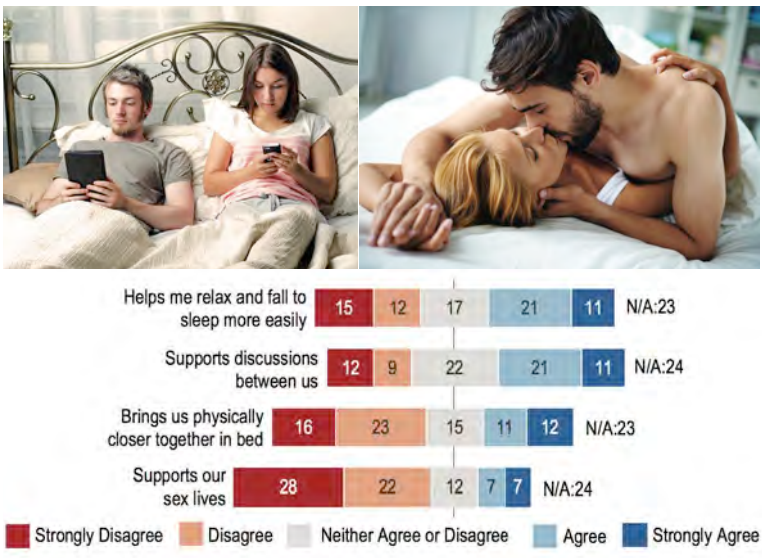
In primo luogo, l'attrattività di qualsiasi gioco, app o strumento informatico è stata ispirata dalla dipendenza da gioco di Las Vegas, un fenomeno studiato in modo approfondito da centinaia di specialisti. Il sapiente mix creato scientificamente di divertimento, di spettacoli gratuiti, del sentimento di essere in una città fiabesca lontana dall'ambiente domestico e dai problemi in aggiunta ad altri mezzi (luci, disegni, piccoli guadagni, atmosfera), portano il visitatore a fermarsi nel casinò fino a quando non ha speso l'ultimo centesimo.

La seconda fenomeno su cui si fonda l'intero successo dello smartphone, e la sua parte più oscura, si basa su una ricerca degli anni '50 sui ratti e sulla dopamina neuronale che viene rilasciata attraverso la stimolazione elettrica del cervello (Olds e Miltner 1952). Il risultato sui ratti maschi? Anche in presenza di cibo, acqua e femmine, i topi hanno premuto su un pedale che generava elettrostimolazione per ben 100 volte al minuto (6000 volte all'ora) solo per il piacere cerebrale ... fino a quando la maggior parte di loro è morta di esaurimento.

Conosciuto come *"drug, sex and rock and roll"* booster, la dopamina può essere creata dalle cellule cerebrali se si stimola opportunamente l'encefalo, come ad esempio succede nel caso dei numerosi e attraenti prodotti che già abbiamo o che possiamo scaricare sul nostro smartphone. (vedi Tank 2018 e, soprattutto, Parkin 2018, che prevede che l'Intelligenza Artificiale aumenterà in modo significativo la dipendenza da smartphone grazie all'anticipazione personalizzata e individuale dei desideri di ogni persona, opportunamente impostata all'interno del sistema operativo e in ogni app).

In grado di sconfiggere anche l'intimità della nostra camera da letto

Prima di parlare dell'impatto della dipendenza negli affari e nella democrazia e per dare un possibile esempio più rilevante di questa nuova dipendenza, un recente studio (Salmela, Colley, Häkkkilä 2019) mostra la nuova dipendenza dalle *"droghe intelligenti"* anche nella camera da letto. Le ragioni dell'utilizzo di questi strumenti informatici "sotto le coperte", sintetizzate nel grafico sottostante, sono assurde se pensiamo alla nostra vita prima dell'esistenza di questo fenomeno: dormire più facilmente e sostenere le discussioni tra i due partner, a discapito ... della tenerezza e della vita sessuale.

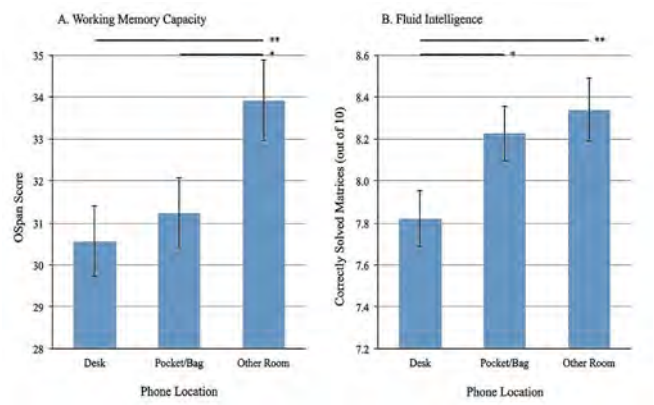


Sondaggio: motivi per l'uso di smartphone e tablet insieme nel letto © Salmela, Colley, Häkkkilä 2019, Fig. 4

Rendici così dipendenti che perdiamo memoria e intelligenza solo guardandoli

Una delle ricerche più pertinenti è stata condotta da un team dell'università di Chicago. L'esperimento consisteva nel portare alcune centinaia di studenti e persone non laureate in tre grandi aule dove sono stati indiscriminatamente distribuiti test identici che richiedevano una certa intelligenza di base con problemi di aritmetica / memoria e domande di cultura generale.

I partecipanti erano suddivisi in tre gruppi. Il primo gruppo aveva losmartphone ad un metro, con divieto di poterlo prendere. il secondo lo aveva in tasca o in borsa, sempre con divieto di afferrarlo, e il terzo era in una stanza con lo smartphone lasciato a un custode esterno. La grafica che segue ci lascia basiti e non ha bisogno di commenti: all'interno dei partecipanti del primo gruppo, la sola semplice visione dello smartphone, raddoppiata dall'impossibilità di afferrarlo, ha abbassato di quasi 1/2 la loro capacità mnemonica e di 1/3 la loro "fluid intelligence" rispetto ai partecipanti nella stanza senza telefono.



Ward, Duke, Gneezy, Bos 2017, figura 1. Esperimento 1: effetto della posizione – tratta a sorte – del telefonino sulla capacità di memoria di lavoro disponibile (OSpan Score, pannello A) e sull'Intelligenza fluida funzionale. I partecipanti che avevano lo smartphone sulla scrivania hanno mostrato la più bassa capacità cognitiva disponibile; quelli che avevano lo smartphone in un'altra stanza (e già semplicemente nella borsa/tasca) hanno mostrato la più alta capacità cognitiva disponibile.

Un disastro in termini di prestazioni aziendali

La tolleranza sul lavoro rispetto alla disponibilità dei dipendenti a essere raggiunti al di fuori dell'orario di lavoro si è trasformata in un grave errore. Recentemente, alcune delle più rinomate riviste di settore hanno dedicato una serie di articoli sulle perdite aziendali causate del tempo trascorso dai dipendenti sul proprio smartphone - fino a 4 ore al giorno su 8 ore lavorative! (si veda ad esempio Akhtar 2019).

La comunità scientifica ha riproposto una vecchia teoria: educare i dipendenti a dedicare speciali fasce orarie *("Zeitgebers")* nell'organizzazione della propria vita personale e professionale (Montag, Kannen, Lachmann, Sariyska, Duke, Reuter, Markowetz 2015). Questo metodo, tuttavia, nell'individualismo e nella mancanza di bioritmo e di igiene disciplinare, non sembra offrire risultati quantitativi di successo e ulteriori passi avanti per combattere la dipendenza dei dipendenti dagli strumenti intelligenti.

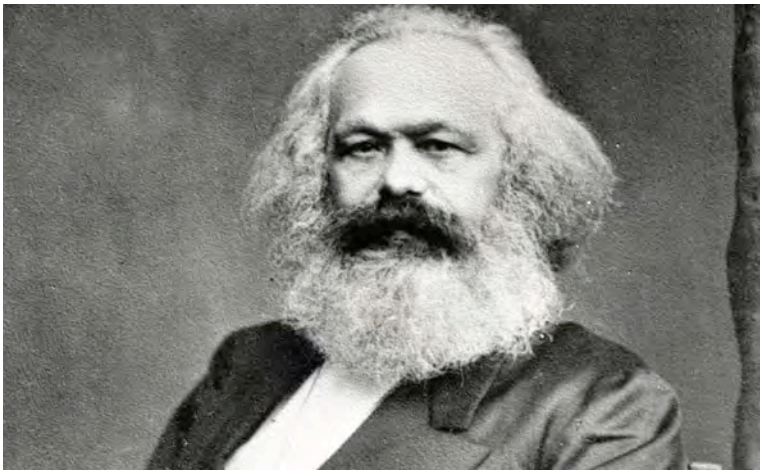
Inoltre, recenti studi condotti su dipendenti e leader del domani mostrano un costante degrado dovuto a una crescente dipendenza dagli smartphone (Arefin, Islam, Mustafi, Islam 2017; Mosalanejad, Nikbakht, Abdollahifrad, Kalani 2019) e lo sviluppo di effetti molto pericolosi sugli individui: cambiamenti di personalità, aumento costante dello stress e dell'isolamento/solitudine. Quest'ultimo fenomeno è molto più radicato negli adulti già inseriti nel mercato del lavoro (Ellie, Mazmanian 2013) dove il "flusso di notizie" dello smartphone scelto da ognuno può portare a conflitti con i propri colleghi a causa delle posizioni radicali assunte grazie all'alimentazione da fonti "info" scelte e dalle proprie conoscenze sui social network.

Vale la pena di notare che diversi articoli hanno indicato che le argomentazioni fatte su questo tipo di dipendenza fino a pochi anni fa erano molto limitate e contrastanti poiché la maggior parte delle ricerche venivano fatte su autovalutazioni dei dipendenti (vedi Duke, Montag 2017) o su campioni statistici, alcuni dei quali condotti per un lungo periodo di tempo (al contrario del capolavoro di Tossell, Kortum, Shepard, Rahmati, Zhong 2015).

Ora sono stati stabiliti nuovi standard di studio (Li, Lin 2019) grazie a un'università coreana che, avendo avuto accesso diretto in PPP (Point-to-Point Protocol) a banche dati governative e applicando tecniche di studio sul data mining, ha estrapolato statistiche di successo come ad esempio sull'utilizzo delle applicazioni e su tempo speso su ciascuna di esse (Lee, Han, Pak 2018).

Conclusioni

Amore e paura delle tecnologie non comprese, totale mancanza di cultura generale e di educazione digitale, tweet o false notizie ed erette come verità, individualismo intorno a "amici virtuali che condividono le stesse idee e opinioni", totale dipendenza da uno strumento telefonico spiato ... mettere al sicuro tutto questo, se non si spiega cosa sta accadendo, se non si definiscono le regole e le si impongono attraverso un consenso raggiunto con il dialogo, non può essere considerato una sfida ma solo un semplice sogno.



L'alternativa è accendere una candela a Santa Rita, patrona delle cause perse ...

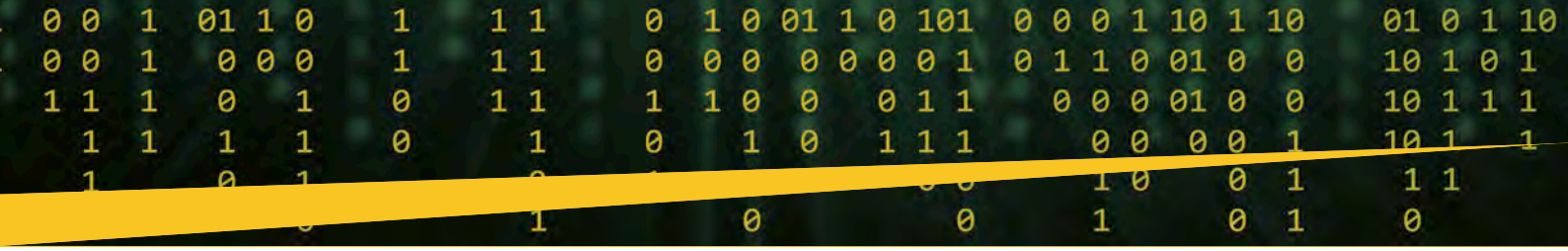
Potremmo non concludere mai, ma parafrasando – *sul ciò che la maggior parte degli europei vorrebbe proibire nel mondo virtuale* – riportiamo uno dei dibattiti politici e ideologici più interessanti sulla riforma del diritto e sulle allusioni a Dio, il *"Per la critica della filosofia del diritto di Hegel. Introduzione"* (del 1844) di Karl Marx, noto in tutto il mondo non per il suo contenuto affascinante ma per la frase *"La religione è l'oppio del popolo"*. Abbiamo quindi cambiato il temine "religione" mondiale con il termine **"mondo digitale"** nella versione inglese corretta del testo tedesco di Matthew Carmody nel 2009 e da noi tradotta.

(I *corsivi* sono mantenuti come nel testo tedesco, come le parti che Marx ha voluto sottolineare.)

*"L'uomo fa **Il mondo digitale**, e non **Il mondo digitale** l'uomo.* Infatti, ***il mondo digitale*** è la coscienza di sé e il sentimento di sé dell'uomo che non ha ancora conquistato o ha già di nuovo perduto se stesso. Ma l'uomo non è un essere astratto, posto fuori del mondo. *L'uomo è il mondo dell'uomo*, Stato, società. Questo Stato, questa società producono ***il mondo digitale***, *una coscienza capovolta del mondo*, poiché essi sono un mondo capovolto. ***Il mondo digitale*** è la teoria generale di questo mondo, il suo compendio enciclopedico, la sua logica in forma popolare, il *suo point d'honneur spiritualistico*, il suo entusiasmo, la sua sanzione morale, il suo solenne compimento, il suo universale fondamento di consolazione e di giustificazione. Essa è la *realizzazione fantastica* dell'essenza umana, poiché l'essenza umana non possiede una realtà vera. La lotta contro ***il mondo digitale*** è dunque mediatamente *la lotta contro quel mondo*, del quale ***il mondo digitale*** è l'aroma spirituale.

La miseria digitale è insieme l'espressione della miseria reale e la protesta contro la miseria reale. ***Il mondo digitale*** è il sospiro della creatura oppressa, il sentimento di un mondo senza cuore, così come è lo spirito di una condizione senza spirito. Essa è *l'oppio del popolo*. (…)

La critica ha strappato dalla catena i fiori immaginari, non perché l'uomo porti la catena spoglia e sconfortante, ma affinché egli getti via la catena e colga i fiori vivi. La critica **del *mondo digitale*** disinganna l'uomo affinché egli pensi, operi, configuri la sua realtà come un uomo disincantato e giunto alla ragione, affinché egli si muova intorno a se stesso e perciò, intorno al suo sole reale. ***Il mondo digitale*** è soltanto il sole illusorio che si muove intorno all'uomo, fino a che questi non si muove intorno a se stesso."



Bibliografia

▸ Akhtar 2019 = Allana Akhtar, Smartphone habits that are getting in the way of your success, in BusinessInsider Apr. 21, 2019 (https://www.businessinsider.com/smartphone-habits-that-are-ruining-your-productivity-2018-7)

▸ Arefin, Islam, Mustafi, Islam 2017= Afrin Shamsul Arefin, Rafiqul Islam, Sharmina Afrin, Mohitul Ameen Ahmed Mustafi, Nazrul Islam, impact of smartphone addiction on academic performance of business students: a case study, in: Independent Journal of Management & Production (IJM&P), v. 8:3, 2017 (www.ijmp.jor.br/index.php/ijmp/article/view/629/726)

▸ Duke, Montag 2017 = Éilish Duke, Christian Montag, Smartphone addiction, daily interruptions and self-reported productivity, in: Addictive Behaviors Reports 2017:6, pp. 90-95 (https://www.sciencedirect.com/science/article/pii/S2352853217300159)

▸ Ellie, Mazmanian 2013 = Harmon Ellie, Melissa Mazmanian, Stories of the Smartphone in Everyday Discourse: Conflict, Tension and Instability, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York: ACM, 2013 (https://ellieharmon.com/docs/HarmonMazmanian-SmartphoneStories-CHI2013.pdf)

▸ Fried 2016 = Jason Fried, What's an hour? When 15 + 15 + 15 + 15 does not equal 60, December 14, 2016 (https://m.signalvnoise.com/whats-an-hour/)

▸ Lee, Han, Pak 2018 = MyungSuk Lee, MuMoungCho Han and JuGeon Pak, Analysis of Behavioral Characteristics of Smartphone Addiction Using Data Mining, in Applied Sciences 2018: 8 (https://www.mdpi.com/2076-3417/8/7/1191/htm)

▸ Li, Lin 2019 = Li Li, Trisha T. C. Lin, Smartphones at Work: A Qualitative Exploration of Psychological Antecedents and Impacts of Work-Related Smartphone Dependency, in: International Journal of Qualitative Methods Volume 18: 1–12 (2019) (https://www.researchgate.net/publication/330572104_Smartphones_at_Work_A_Qualitative_Exploration_of_Psychological_Antecedents_and_Impacts_of_Work-Related_Smartphone_Dependency)

▸ Montag, Kannen, Lachmann, Sariyska, Duke, Reuter, Markowetz 2015 = Christian Montag, Christopher Kannen, Bernd Lachmann, Rayna Sariyska, Éilish Duke, Martin Reuter, Alexander Markowetz , The importance of analogue zeitgebers to reduce digital addictive tendencies in the 21st century, in: Addictive Behaviors Reports 2 (2015) 23–27 (https://www.sciencedirect.com/science/article/pii/S2352853215000140)

▸ Mosalanejad, Nikbakht, Abdollahifrad, Kalani 2019 = Leili Mosalanejad, Ghazale Nikbakht, Saead Abdollahifrad, Navid Kalani, The Prevalence of Smartphone Addiction and its Relationship with Personality Traits, Loneliness and Daily Stress of Students, in Jahrom University of Medical Sciences in 2014: A Cross-sectional Analytical Study, in: Journal of Research in Medical and Dental Science 2019, Volume 7, Issue 2, Page No: 131-136 (https://www.researchgate.net/publication/332548885_The_Prevalence_of_Smartphone_Addiction_and_its_Relationship_with_Personality_Traits_Loneliness_and_Daily_Stress_of_Students_in_Jahrom_University_of_Medical_Sciences_in_2014_A_Cross-sectional_Analytica)

▸ Olds, Miltner 1955 = J. Olds, P. Miltner, Positive reinforcement produced by electrical stimulation of septal area and other regions of rat brain, in Journal of Comparative and Physiological Psychology 47:6, 1955, pp. 419-427

▸ Parkin 2018 = Simon Parkin , Has dopamine got us hooked on tech?, in The Guardian, 4th of March 2018 (https://www.theguardian.com/technology/2018/mar/04/has-dopamine-got-us-hooked-on-tech-facebook-apps-addiction)

▸ Rubio, Lastra 2019 = Diego Rubio and Carlos Lastra, European Tech Insights 2019. Mapping European Attitudes to Technological Change and its Governance, Madrid: Center for the Governance of Change, 2019 (de citit pe: www.ie.edu/cgc; download: http://docs.ie.edu/cgc/European-Tech-Insights-2019.pdf)

▸ Salmela, Colley, Häkkilä 2019 = Tarja Salmela, Ashley Colley, Jonna Häkkilä, Together in Bed? Couples' Mobile Technology Use in Bed, in Proceedings of the International Conference on Human Factors in Computing Systems (CHI), (Glasgow, May 2019), New York: ACM, 2019 (https://www.researchgate.net/publication/332060502_Together_in_Bed_Couples%27_Mobile_Technology_Use_in_Bed)

▸ Tank 2018 = Aytekin Tank. Why productivity isn't the only thing your smartphone is stealing from you, in JotForm May 24, 2018 (https://www.jotform.com/blog/productivity-and-smartphone/)

▸ Tossell, Kortum, Shepard, Rahmati, Zhong 2015 =Chad Tossell, Philip Kortum, Clayton Shepard, Ahmad Rahmati, Lin Zhong, Exploring Smartphone Addiction: Insights from Long-Term Telemetric Behavioral Measures, in International Journal of Interactive Mobile Technologies Volume 9: 2 (2015), pp. 37-45 (https://online-journals.org/index.php/i-jim/article/view/4300)

▸ Ward, Duke, Gneezy, Bos 2017 = Adrian F. Ward, Kristen Duke, Ayelet Gneezy, and Maarten W. Bos, Brain Drain: The Mere Presence of One's Own Smartphone Reduces Available Cognitive, in: Journal of the Association for Consumer Research (University of Chicago), Volume 2: 2 (April 2017), "The consumer in a connected world" (https://www.journals.uchicago.edu/doi/full/10.1086/691462) ■

La Romania e la presidenza dell'UE: uno stato sotto assedio. Sei mesi di attacchi, non un secondo di indisponibilità dei sistemi e delle reti.

Intervista esclusiva al Generale Sorin Vasilca, Direttore Generale del Servizio di Telecomunicazioni Speciali.

Autore: Laurent Chrzanovski

Alla data in cui leggerete questo numero di Cybersecurity Trends, la Romania avrà appena concluso il suo semestre di presidenza dell'Unione europea. In questo contesto, un ruolo centrale è stato svolto con successo dal Servizio di Telecomunicazioni Speciali (STS), l'organismo specializzato dello Stato centrale rumeno incaricato di sviluppare, organizzare, condurre, svolgere, controllare e coordinare tutte le attività nel campo delle telecomunicazioni speciali ad uso delle autorità pubbliche in Romania. In questa intervista, il Direttore Generale dell'Istituzione, il Lt.-Generale Ing. Sorin Vasilca, *"summus artifex et custos"* di tutti i servizi e sistemi comunicazioni di Stato del semestre di presidenza rumena dell'Unione Europea (1 gennaio- 30 giugno), ci svela i dettagli delle misure di contrasto preventive e reattive alle diverse tipologie di attacchi subite durante questo periodo. Queste rivelazioni rappresentano una première dopo la presidenza estone (2° semestre del 2017), poiché tali dati sono, nella maggior parte dei casi, confidenziali o comunque lo restano per almeno sei mesi o un anno in funzione dei paesi che hanno assunto questa carica.

Lt.-Generale Vasilca, la sua Istituzione ha una struttura militare e fa parte del sistema di difesa nazionale. Quali sono i principali compiti che ha dovuto svolgere per la presidenza rumena dell'UE, oltre a quelli svolti dal Suo Servizio in un anno "normale"?

Lt.-Generale Vasilca: in primo luogo, ben prima del 1 gennaio 2019, l'intera direzione del STS è stata coinvolta nel Comitato interministeriale per la sicurezza *"ROMANIA-EU 2019"*, costituito dagli dirigenti di tutti gli attori statali attivi nel settore della difesa, ossia il Ministero della Difesa, il Ministero dell'Interno, i Servizi di intelligence interna ed esterna (SRI e SIE) e il Servizio di Protezione e Guardia (SPP). Nell'ambito di questo gruppo di lavoro permanente, al STS è stata affidata la responsabilità di due compiti primari.

Il primo quello principale, sotto la direzione del Ministero degli Affari Esteri, è stato quello di sviluppare, implementare e mantenere la continuità del perfetto funzionamento 24/7 di tutti i sistemi e servizi di comunicazione specificamente progettati per la presidenza dell'UE.

Infatti, a parte le comunicazioni *stricto sensu*, il sito web e le app connesse *Romania2019.eu*, sono state progettate con un user end dedicato per il visitatore con tutte le informazioni necessarie su ogni evento, mentre il *back end* è stato ideato ed implementato con requisiti di sicurezza elevata per il Ministero degli Affari Esteri al fine di fornire tutti i flussi di informazioni e dati ufficiali ed anche, in collaborazione con il Servizio di Protezione e Guardia, per gestire ogni singolo accreditamento ad ogni evento.

Il secondo, anch'esso vitale, è stato quello di garantire il trasporto e il buon funzionamento della trasmissione ufficiale ad opera della televisione pubblica nazionale (TVR), di tutti gli eventi della presidenza dell'UE.

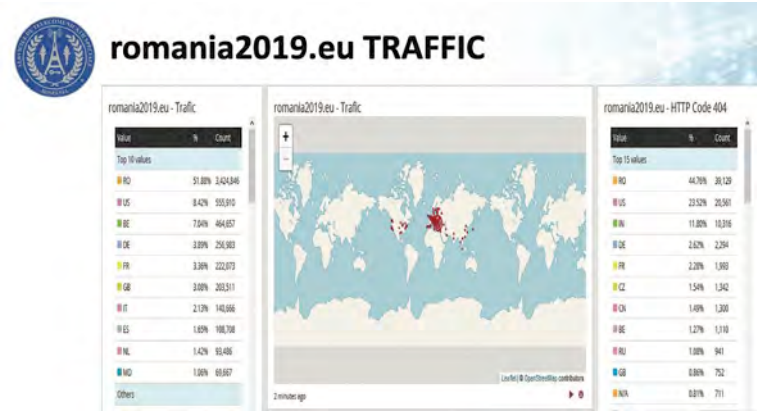
Allora, cos'è successo a partire dal 1 gennaio?

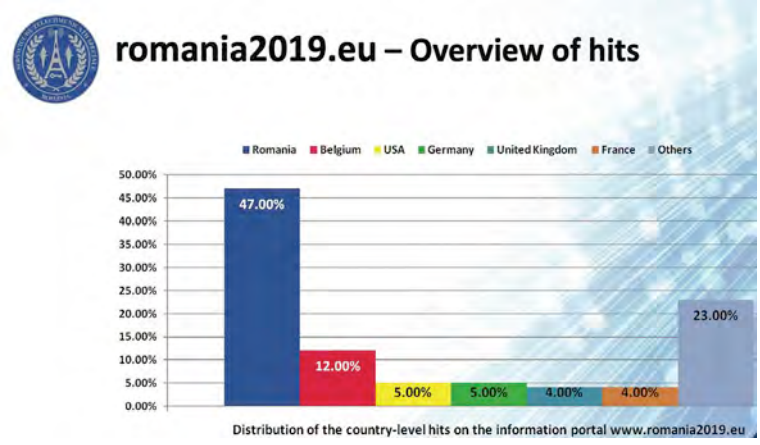
Lt.-Generale Vasilca: abbiamo dovuto assicurare e garantire una comunicazione perfetta per più di 300 eventi, tra i quali solo un terzo si è svolto nella capitale, Bucarest. Per questo, abbiamo elaborato una scala di importanza suddivisa in 5 gruppi: il primo, il più alto, per la riunione di tutti i capi di Stato dell'Unione europea, tenutasi a Sibiu il 9 maggio scorso. Al secondo posto troviamo le 23 riunioni dell'UE di livello ministeriale e, dal terzo al quinto posto in ordine di importanza strategica, i restanti 275+ eventi (riunioni interministeriali / tecniche).

Inoltre, l'STS ha avuto il ruolo primario nel fornire e garantire 24/7 tutti i servizi Internet e di comunicazione in tre punti principali: il Palazzo del Parlamento - sede della Presidenza Europea –, la Biblioteca Nazionale – sede dei grandi meeting – e la Banca Nazionale – sede dei gruppi di lavoro in materia di finanze. Un compito questo, che siamo stati in grado di raggiungere grazie a potenti gruppi di server situati a Bucarest e vicino a Brasov, una delocalizzazione parziale decisa nei fini di aumentare l'efficienza dei servizi disponibili a livello di tutto il territorio nazionale.

Su quest'ultimo aspetto, suppongo che lei sia stato particolarmente scrupoloso per quanto riguarda la quantità di dati, mantenendo al contempo la sicurezza totale di tutte le comunicazioni.

Lt.-Generale Vasilca: Esattamente. Immaginate che il portale ufficiale *"Romania2019.eu"* ha avuto una media di 2,23 milioni di visite al mese, culminante con quasi il triplo, più di 6 milioni di visite, durante il mese di maggio, quando tutti i capi di Stato si sono riuniti a Sibiu.





> *L'uso massiccio di della tecnica di code injection ha supera di gran lunga il ricorso alla Brute Force e ella File Inclusion.*

Per quanto riguarda la nostra capacità di traffico, abbiamo avuto un feedback costante da parte dei nostri colleghi bulgari e austriaci, che ci hanno aiutato molto a stimare la quantità e il numero di download e upload. Questo dato si è rivelato particolarmente importante durante gli eventi principali, in cui tutti i delegati dell'UE e i media di tutto il mondo scaricavano materiali o caricavano contenuti video da inviare in patria. Con 3 connessioni Tier 1, siamo riusciti ad offrire una velocità media di trasmissione dati fino a 30 Gb/secondo. Abbiamo anche potuto vedere statisticamente da quali paesi abbiamo avuto i più alti numeri in termini di visite e quantità di dati: la Romania e il Belgio (cioè la sede centrale dell'UE) che hanno raggiunto quasi il 60% dei flussi di dati.

E l'aspetto "cibernetico"? Come hai fatto a proteggere tutti quei servizi?

Lt.-Generale Vasilca: Per quanto riguarda la sicurezza informatica, abbiamo operato dal nostro Centro CORIS *(Centrul national pentru raspuns la incidente de Securitate/ Centro nazionale di risposta agli incidenti di sicurezza), fondato nel 2008, in collaborazione con il CertMil (Esercito)*, il Cert-RO (Ministero delle Telecomunicazioni) e il Centro Cyberint (Servizio Interiore di Intelligence - SRI). Devo sottolineare che, grazie al duro lavoro svolto nel corso degli anni, non solo il CORIS ha ottenuto un tasso di fiducia molto alto - è accreditato da Trusted Introducer dal 2011 - ma gode di un team CERT molto stabile, molti colleghi vi lavorano sin dall'apertura del centro, più di dieci anni fa'. Ciò ha permesso di monitorare 24 ore su 24 e 7 giorni su 7 tutti i sistemi direttamente o indirettamente collegati alla presidenza dell'UE e di fornire un helpdesk 24 ore su 24, 7 giorni su 7, dedicato a tutte le istituzioni statali che necessitavano servizi o competenze.

A pochi giorni dalla fine della Presidenza rumena, quali circostanze ci può svelare?

Lt.-Generale Vasilca: prima di tutto un dato statistico: su mille "click" sul sito ufficiale, 4 erano classificati

"anormali" o *"errori"*, cioè un rapporto estremamente ridotto. Ora, se guardiamo più in dettaglio, abbiamo osservato una crescita significativa di un nuovo tipo di incidente informatico. Questo semestre è stato infatti caratterizzato dall'uso massiccio di della tecnica di code injection, superando di gran lunga due tecniche criminali "convenzionali" ben note e utilizzate negli ultimi anni, cioè la *Brute Force* e la *File Inclusion*.

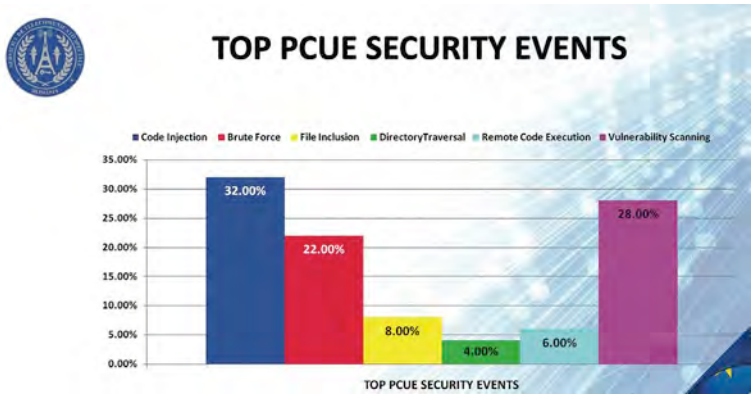
Durante il *"Grande Giorno"*, cioè l'incontro di tutti i Capi di Stato a Sibiu, abbiamo raggiunto un picco di attacchi che comprendevano statisticamente un 75% di malware + 18% di tentativi di spam.

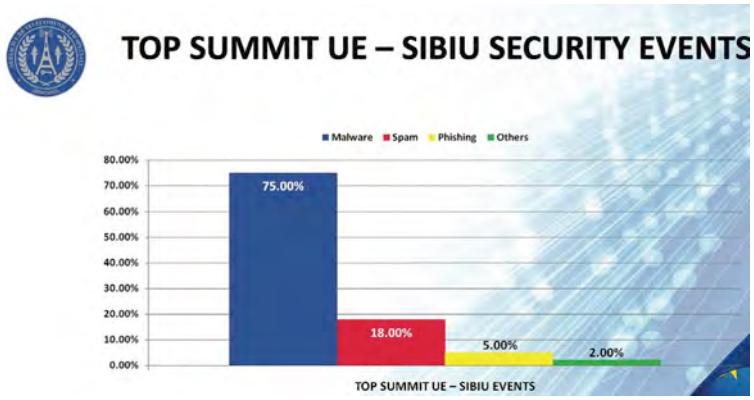
Come è riuscito a gestire con successo una tale quantità di tentativi illegali?

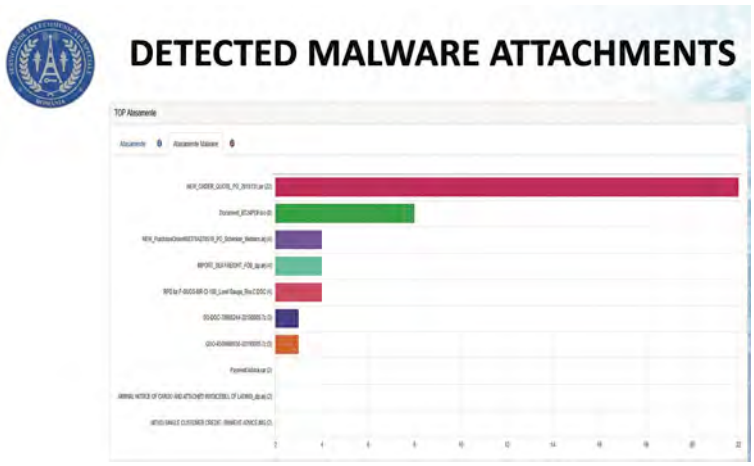
Lt.-Generale Vasilca: in primo luogo, abbiamo creato una sandbox all'avanguardia, in totale collaborazione con Bitdefender. Grazie a questo nuovo ed unico tipo di sandbox, che filtrava i malware, li quantificava e li classificava neutralizzandoli, abbiamo potuto concentrare tutta la nostra attenzione nel monitoraggio del sito e dei suoi sottodomini e della sicurezza delle web app. Naturalmente, dovevamo garantire anche la disponibilità del servizio 24/7.

Tutto questo è stato reso possibile grazie ad una serie di strumenti costruiti *"in house"* dal nostro team anno dopo anno, come contromisure ai tentativi di "defacement". Tutti questi strumenti hanno permesso di vedere "in diretta" all'interno di una precisa classificazione, sia i livelli di compromesso che i potenziali compromessi del sito e delle app, e prendere quindi le misure necessarie al caso. Inoltre, ci ha permesso di bloccare immediatamente qualsiasi tentativo illecito di modifica dei contenuti e, naturalmente, di contrastare gli attacchi volti a provocare l'indisponibilità dei servizi da noi forniti.

Quali sono le sue principali conclusioni di questo successo di resilienza mentre è sotto costante e reale attacco a un livello che il paese non ha mai saputo finora?





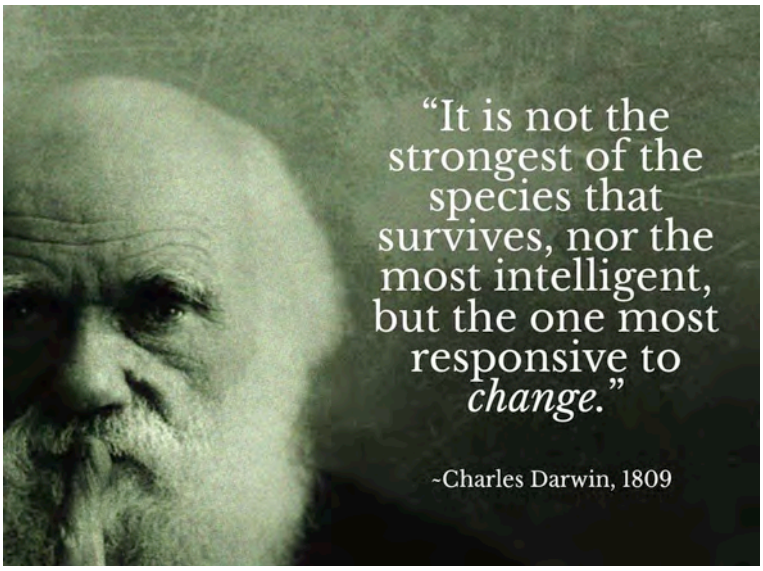


Lt.-Generale Vasilca: dal punto di vista delle STS, sono tre i punti chiave per una buona difesa. Il primo e la base degli altri due punti è quello di avere un team qualificato e compatto, con eccezionali capacità tecnologiche e umane. Questo permette di raggiungere un secondo punto: non dipendere mai soltanto da soluzioni già pronte, ma sviluppare in continuazione i propri strumenti, unici e su misura, adatti alla sicurezza delle particolarità di ciò che si deve difendere. E poi, naturalmente, aldilà dei due punti precedenti, non si dovrebbe mai affrontare da soli una risposta agli incidenti di sicurezza. La collaborazione perfettamente oliata con tutti gli altri enti di sicurezza è l'unica possibilità per migliorare tutte le vostre capacità.

Un'ultima domanda. Molti cittadini sono spaventati e affascinati, allo stesso tempo, dall'arrivo di 5G e dai continui miglioramenti e implementazioni dell'AI e dell'internet of Things. Cosa possiamo dire allora?

Lt.-Generale Vasilca: Abbiamo imparato molto familiarizzando con l'AI, il Deep Learning, il Machine Learning. Da queste esperienze abbiamo cercato di capire perfettamente come queste tecniche funzionano e come, molto probabilmente, evolveranno a breve termine. Siamo quindi stati in grado di progettare e di costruire i nostri propri prodotti, adatti ai nostri bisogni e perfettamente funzionali.

Il cambiamento principale che abbiamo di fronte già ora, senza tralasciare il 5G, è il cambiamento simmetrico e il rapporto tra i dati caricati e quelli scaricati *(upload vs. download)*. A differenza di una stabile e massiccia



evoluzione dei download e di una lunga e lenta evoluzione degli upload, nell'ultimo anno abbiamo visto un'evoluzione esponenziale degli upload mese dopo mese. La quantità di dati caricati sta già superando la quantità di dati scaricati. Questo è il risultato dell'uso sempre più massiccio dei dispositivi dell'Internet of Things e, in generale, di tutti gli strumenti di nuova generazione, i cui sistemi di base hanno bisogno di un'alimentazione costante di dati da ogni singolo misuratore.

Il punto quindi non è tanto il cambio di modalità di trasmissione (da 4G a 5G) ma il modo in cui ogni utente si comporterà e sarà consapevole nell'utilizzare l'infinità di strumenti messi a sua disposizione, in un modo sicuro e protetto.

Come aneddoto, durante tutti gli eventi che dovevamo gestire, raccogliendo le esigenze, dai 1000 ai 5000 partecipanti, NESSUNO ha desiderato collegarsi via cavo - una delle soluzioni da noi proposta - e tutti hanno utilizzato sistematicamente il sistema wireless criptato, anch'esso da noi fornito. Questo dimostra come il 5G verrà ampiamente utilizzato fin dal suo principio. E' inevitabile e dovremmo essere tutti pronti a prenderne atto.

Per quanto riguarda l'altra parte della sua domanda, il dialogo tra macchine esiste già quasi ovunque. La vera differenza sta e rimarrà nella misura dell'intervento umano che ogni utente o entità vorrà o richiederà, dal poter intervenire di propria iniziativa ed in ogni momento sino, all'opposto, ad essere chiamati solo quando deve essere presa una decisione finale.

Anche in questo caso, tutti possono beneficiare dei vantaggi di un uso responsabile e basato sulla conoscenza di qualsivoglia nuova tecnologia disponibile o presto disponibile, ma la sicurezza, più che mai, può essere realizzata solo comprendendo perfettamente l'ambiente digitale in continua evoluzione in cui viviamo.

Poi, scegliendo correttamente gli strumenti e le soluzioni da utilizzare in base alle specificità della propria vita quotidiana (professionale e privata), sarà facile metterle in sicurezza. Ogni essere umano, Stato, azienda è quindi chiamata a dover decidere il proprio livello di resilienza. Non c'è nessun aspetto del futuro prossimo che sia più inevitabile di quanti ce ne siano già oggi.

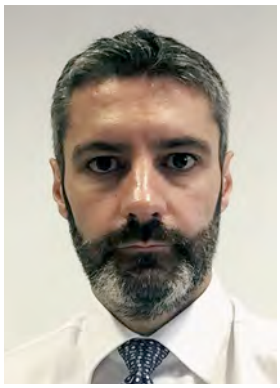
Come conclusione, senza una conoscenza di base che sia al passo con le novità tecnologiche e quelle di sicurezza, senza un dialogo ampio e aperto ed una collaborazione tra utenti ed esperti, nonché tra enti statali e aziende private, ogni nuova implementazione tecnologica potrà portare – e porterà – naturalmente nuovi pericoli; è proprio qui che c'è il grande cambiamento e cioè che questi pericoli ci raggiungeranno molto, molto più velocemente rispetto al passato e a livello globale.

Nota dell'editore: la sfida che il STS ha dovuto affrontare è stata ancora più grande di quanto riportato in questa intervista, poiché oltre alla presidenza rumena dell'UE, il Servizio speciale ha dovuto assicurare, il 26 maggio anche la giornata di votazioni nazionali che ha portato i cittadini alle urne non solo per le elezioni europarlamentari ma anche per due referendum nazionali sulla giustizia, tema questo, estremamente importante agli occhi della popolazione negli ultimi quattro anni. Infine, vi sono stati 3 giorni di visita (1), a Bucarest ed in Provincia, di Papa Francesco (dal 31 maggio al 2 giugno), prima visita pontificale da ben vent'anni.

(1) https://www.sts.ro/en/press-releases/inter-ministerial-committee-for-security-pope-francis-visit-2019

Sito ufficiale: https://www.sts.ro/en ■

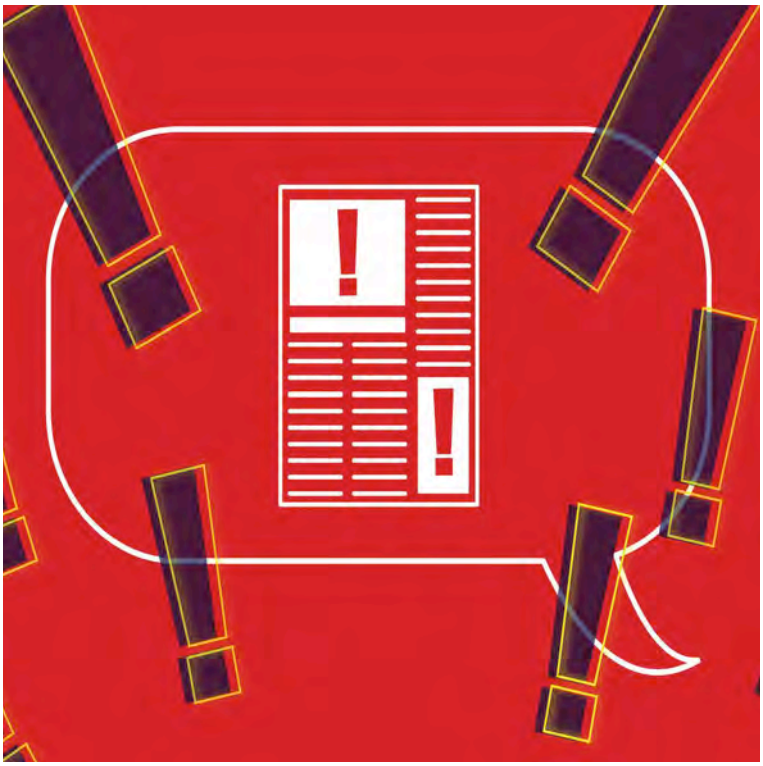
Furto di dati e impatto sul valore azionario



Autori: Massimo Cappelli e Marika Mazza

Nel 2017, sul terzo numero della rivista Cybersecurity Trends Italia, avevo scritto un articolo relativo all'impatto della disinformazione sul valore azionario.

Citai un esempio relativo alle elezioni presidenziali americane del novembre 2016: *"A metà novembre 2016 viene riportata da un blog di conservatori statunitensi una intervista al CEO dell'azienda produttrice della bevanda, in cui avrebbe dichiarato (condizione d'obbligo) – CEO Tells Trump Supporters to Take Their Business Elsewhere -. … Il giorno stesso della notizia riportata, il punteggio del gradimento nei confronti dell'azienda sembrerebbe crollato di circa il 35%. Il prezzo dell'azione lo stesso giorno è crollato del 3,75% e per la restante parte del mese è sceso di oltre il 5%. Le due cose potrebbero non essere associate ma è stato comunque un caso discusso dagli analisti di brand reputation e*



BIO

Massimo Cappelli è operations planning manager presso la Fondazione GCSEC, oltre che responsabile delle attività di Early Warning, Brand Protection, Information Sharing e Cyber Threat Intelligence nella struttura CERT di Poste Italiane. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz &Company nella practice Risk, Relisience and Assurance.

BIO

Marika Mazza, studentessa magistrale di Analisi Economica presso l'Università degli Studi di Roma "La Sapienza". Approfondisce le sue conoscenze in ambito finanziario attraverso un'attiva ricerca nel campo dell'EMH (Efficient Market Hypothesis) affinando le tecniche di analisi econometrica a tal fine. Ha lavorato su un'analisi in collaborazione con GCSEC per verificare gli effetti sui mercati finanziari degli eventi di violazione della sicurezza informatica.

comunicazione". Oltre a questo caso citai altri, come esempio, anche i casi legati alla tecnica "Pump & Dump" cioè pompare e scaricare.

La disinformazione è uno strumento molto potente e difficile da arginare, se non anticipandola con una strategia di comunicazione pervasiva e trasparente. Da qui, sono nate altre considerazioni relative all'impatto sul valore azionario, non solo della disinformazione, ma anche di un attacco cyber nei confronti di un'azienda. La domanda che ci siamo posti è: "Un attacco cyber, con furti di dati, ha impatto sul valore azionario di un'azienda?".

Marika, studentessa di Analisi Economica all'Università La Sapienza, sta effettuando approfondimenti sulla tematica di Efficient Market Hypothesis e durante il periodo di stage presso la Fondazione GCSEC ha analizzato il fenomeno sopra citato sulla base della sua esperienza e delle indicazioni fornitele.

L'analisi si è focalizzata sull'individuazione degli effetti degli attacchi informatici in merito all'andamento dei titoli azionari. Gli attacchi presi in considerazione sono di tipo esterno; in particolare sono stati aggregati: la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.; la divulgazione di dati personali). L'etichetta che è stata associata è: data breach. Non è stata necessaria alcuna distinzione tra essi, in quanto, dall'analisi l'impatto è risultato essere identico.

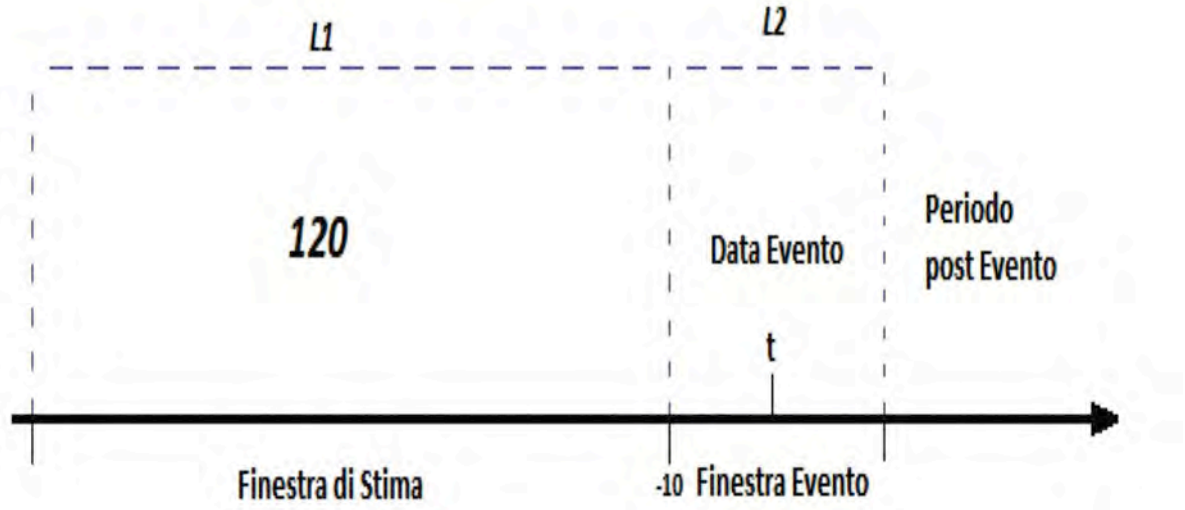
I dati presentati sono relativi a 37 attacchi significativi[1] dal 2016-2019. Le aziende selezionate sono state divise in base alla borsa di quotazione. Gli Aggregati sono 3: New York Stock Exchange (18 aziende), NASDAQ (11 aziende) e Altro (Tokyo, Oslo, Londra ecc. 8 aziende). Gli stati più attaccati e le cui informazioni erano maggiormente disponibili sono quelli dell'America del Nord, motivo per cui è stata effettuata questa divisione. Le 37 aziende sono: 27 statunitensi, 3 britanniche, 2 canadesi, 2 cinesi, 2 tedesche e una norvegese.

Lo studio si basa sulla letteratura finanziaria degli Event Study, metodo di analisi che studia il comportamento di una serie storica in corrispondenza di un dato avvenimento. L'approccio di Event Study più comune prevede in linea generale tre passaggi:

1. Il calcolo dei parametri nell'*estimation period* prescelto;
2. La valutazione del risultato aggregato per l'insieme delle imprese e, contestualmente, la considerazione dell'effetto medio;
3. La stima degli Abnormal Returns in modo tale che sia possibile isolare quelle caratteristiche rilevanti del titolo che si pensa possano influenzare l'impatto della pubblicazione dell'evento.

L'Abnormal Return dell'azione, è ottenuto come differenza tra il rendimento normale e atteso in assenza del verificarsi dell'evento e il rendimento attuale calcolato nel periodo dell'evento. Per procedere alla stima del rendimento normale di ogni impresa, in relazione al rendimento del portafoglio di mercato, viene adottato il *market model*. Il confronto è invece effettuato con l'indice di mercato corrispondente ovvero IXIC per Nasdaq, GPSC per New York Stock Exchange e un indice generale per i restanti mercati.

Il periodo per la stima del rendimento atteso del titolo è effettuato nella finestra di stima di 120 giorni, la quale si interrompe 10 giorni prima dell'evento così da ottenere



valori non distorti. Si sottolinea, infatti, che il Data Breach non viene annunciato quasi mai tempestivamente. Dunque, per evitare che i suoi effetti possano distorcere il valore azionario nel periodo precedente all'annuncio, questo non è considerato nella previsione. La finestra evento, invece, inizia nel periodo subito successivo (-10, +10) ed è quella usata nell'analisi effettiva. E' stato dunque considerato il breve periodo e non il lungo periodo.

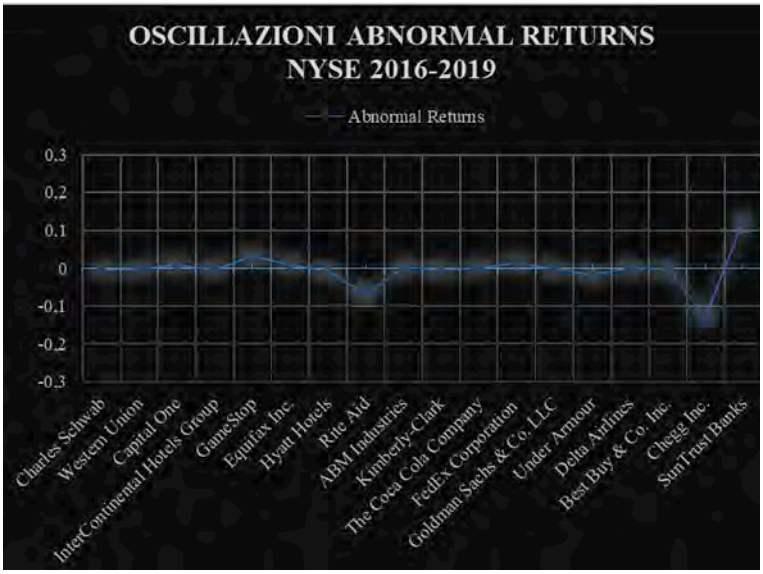
Le event windows selezionate per la stima dei Cumulative Abnormal Returns sono centrate sulla report date (data evento) di 3 giorni (-1, +1), è stata poi possibile calcolare la risposta media nell'intero campione (Cumulative Average Abnormal Return, CAAR) e sottoposto a verifica statistica che questa fosse diversa da 0.

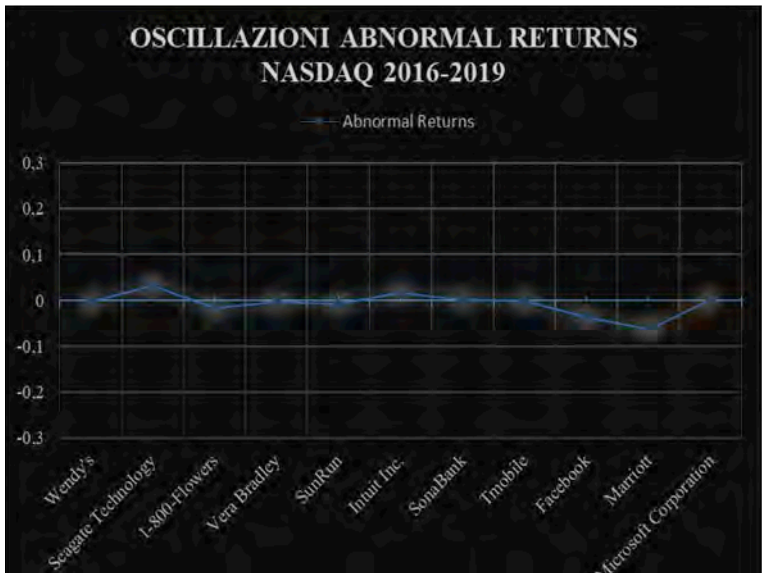
Di seguito riportiamo i risultati ottenuti dall'analisi:

- ***New York Stock Exchange (NYSE)***

Sui casi delle 18 aziende attaccate, si mostra di seguito un grafico contenente le oscillazioni dei *Rendimenti Anormali*. L'impatto dell'annuncio è diverso da zero, talvolta discostandosi da esso di poco e talvolta risulta addirittura positivo. Il valore azionario e il volume di scambio delle azioni è mutato nella giornata di contrattazione, ma questo non si discosta dal rendimento normale atteso previsto. Le oscillazioni presenti all'interno del grafico, possono rappresentare eventi di diversa natura che nella stima sono stati tralasciati, eventi probabilmente correlati all'azienda in sé e non al mercato (gli eventi relativi al mercato sono stati inglobati nella stima dei rendimenti normali attraverso l'indice ^GPSC).

Attraverso l'uso del CAAR, l'indagine ha voluto catturare un effetto che potesse dare risposta universale per le aziende esaminate. L'impatto sul valore azionario del titolo causato dall'evento è dunque -0,0226%, negativo e molto piccolo, dunque è davvero difficile che un investitore decida modificare posizioni su un titolo in seguito a eventi di questo genere, se lo facesse, sarebbe comunque limitata nel brevissimo periodo, se non addirittura giornaliera.





NASDAQ

Anche sul NASDAQ l'impatto è minimo, maggiore rispetto al NYSE, ma comunque molto basso. Complessivamente è pari a -0,0762%. Nel secondo grafico (pagina precedente) è riportato l'andamento dei Rendimenti Anormali giornalieri, la trama è la medesima. Inoltre, gli assestamenti avvengono nella giornata subito successiva all'annuncio. L'evento non si propaga. Quando è di piccola portata, esso è impercettibile sul mercato finanziario.

Altri mercati

Anche sui restanti mercati l'impatto è minimo, esso sembra essere talvolta nullo, infatti, il valore catturato in questa analisi è pari a -0,0086%.

Conclusione

Rispetto ad altri fenomeni, sembra che l'impatto di un attacco cyber, con furto di dati, incida minimamente sul rendimento azionario di un'azienda. Questo ci permette di fare alcune considerazioni. La prima è che questa tipologia di attacco non è utile per premeditare una eventuale scalata per acquisire maggiori quote azionarie. Inoltre, mette in evidenza il fatto, che la perdita di informazioni è qualcosa che colpisce più a livello di conformità e sanzioni invece che sulla propensione all'acquisto del titolo.

Si sottolinea, per giunta, che tali attacchi, per le sanzioni ad essi correlate, talvolta vengono taciuti dalle imprese stesse, è dunque raro che l'annuncio avvenga contestualmente al verificarsi dell'evento stesso, ciò causa perdita di effetto del fenomeno sui mercati.

Nel mercato azionario i prezzi riflettono il comportamento di agenti che per la teoria economica sono razionali, ma per i nuovi filoni della finanza questa è un'ipotesi non sufficiente; gli agenti non si muovono solo in base a rischio e rendimento, infatti, la percezione di un fenomeno funge da perno nelle decisioni e se la disinformazione dilaga, gli effetti sono sedati.

In futuro, con la massiva digitalizzazione dei servizi, qualcosa potrebbe cambiare, ma allo stato attuale i risultati del campione analizzato hanno portato alla considerazione di non approfondire o ampliare questa analisi per comprendere gli effetti dell'impatto. Di tutt'altra natura è il discorso della disinformazione che meriterebbe un approfondimento. Sulla base anche dei casi riscontrati di disinformazione o di ampliamento della diffusione di notizie attraverso bot, durante le campagne europee, si dovrebbe studiare quale sia la portata dell'impatto della disinformazione sugli investimenti o sui titoli delle aziende nei Paesi interessati dalle elezioni stesse. ■

1 Significatività riferita alla quantità di dati rubati, il parametro di selezione è "almeno 5000 per tipologia di dato"(almeno 5000 account, almeno 5000 profili di carte di credito, almeno 5000$ in riferimento alle perdite), il criterio di selezione è stato utile per evitare di considerare impatti troppo insignificanti la cui rilevazione avrebbe generato outlier.

Il 2° congresso "Cybersecurity-Mediterranean": temi maggiori e lezioni da trarne

Autore: Marc-André Ryter

NdR: *Il 9 e 10 maggio si è tenuta a Firenze la 2a edizione del congresso "Cybersecurity-Mediterranean", organizzata dalla Swiss Webacademy con Thales Italia e il sostegno della Fondazione GCSEC oltre che della IATA e della Polizia di Stato di Ginevra. L'evento ha visto partecipi i settori pubblici e privati sotto il patrocinio della Regione Toscana, del Comune di Firenze, di Confindustria Toscana, di Federmanager Toscana e del Cispel Toscana.*

Il programma creato su misura ha permesso l'ottima riuscita dell'evento e ha visto protagonisti 165 partecipanti, dalle Piccole e Medie Imprese ai Manager aziendali il tutto organizzato all'interno della bellissima cornice della sede delle Murate IdeaPark di Firenze.

Il primo giorno è stato dedicato alla formazione dei dirigenti con una master class sulla sicurezza informatica proposta da Pascal Buchner (CIO, IATA) e una serie di demo e corsi a cura dell'AIIC, della Fondazione GCSEC, di One Step Beyond e di Active Change Management. Durante tutto il pomeriggio del primo giorno si è tenuta una tavola rotonda tra 20 specialisti del settore che avevano come chiave comune delle loro attività la complessità della sicurezza nei settori trasversali di trasporti, logistica, infrastrutture critiche, organi di Law Enforcement.

Nel secondo giorno, invece, si è entrati nel cuore dell'evento con il saluto istituzionale del Sindaco di Firenze e dell'Assessore in carica di Sistemi Informativi, Privacy e Sicurezza della Regione Toscana. Successivamente la cerimonia di inaugurazione hanno preso parte 15 speaker di 8 differenti paesi che sono riusciti a coprire a 360° i principali rischi della sicurezza. Sono stati affrontati temi legati ai possibili scenari presenti e futuri, le contromisure tecniche, umane ed del sistema educativo che si possono mettere in campo in questo delicato periodo di evoluzione tecnologica guidata dal 5G, dalla "quarta rivoluzione industriale" e dal "4.0".

Proponiamo a seguito, in esclusiva, la sintesi dei temi più interessanti nonché degli insegnamenti tratti dai dibattiti, redatta dal Col. Marc-André Ryter, un documento gentilmente fornito dallo Stato Maggiore dell'Esercito svizzero.

L'inaugurazione del Congresso: a destra, il Sindaco di Firenze Dario Nardella e, a sinistra, l'Assessore della Regione Toscana Vittorio Bugli.

BIO

Colonnello, diplomato in Studi di politica di sicurezza e laureato in Scienze Politiche, Marc-André Ryter collabora con lo Stato Maggiore dell'Esercito svizzero per tutto ciò che riguarda la dottrina militare. Segue gli sviluppi tecnologici per le Forze Armate e gli scenari d'intervento in particolar modo per ciò che concerne la dottrina militare.
Marc-André Ryter può essere contattato all'indirizzo: marcandre.ryter@vtg.admin.ch

Il fattore umano

Il fattore umano è l'elemento che sta diventando sempre più importante nella sicurezza informatica; la formazione e la sensibilizzazione del personale sono indispensabili per migliorare il livello di sicurezza aziendale. L'investimento nella formazione è fondamentale almeno quanto l'investimento tecnico.

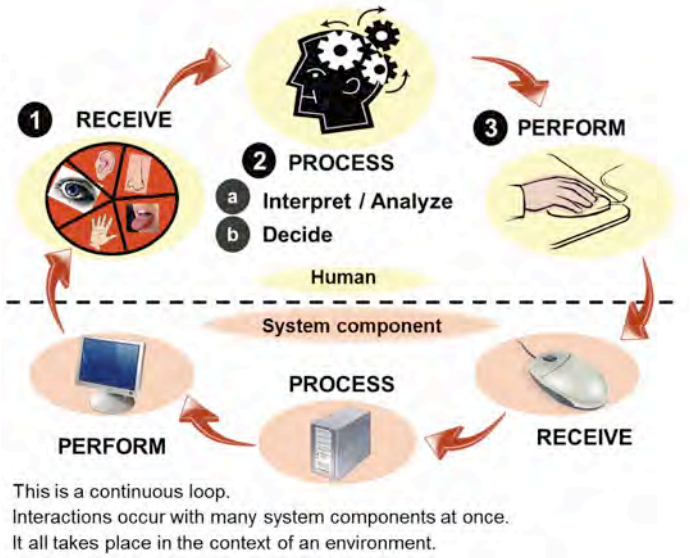
Il *profiling* degli utenti e il monitoraggio delle attività *(scanning)* con l'aiuto dell'intelligenza artificiale diventeranno sempre più importanti e il modo più efficace per individuare tempestivamente i problemi di sicurezza. Attualmente, ad esempio, *"Darktrace"* è in grado di stabilire un profilo affidabile entro 10 giorni.

> *"Darktrace Enterprise utilizza una componente di Machine Learning e algoritmi propri di intelligenza artificiale per analizzare passivamente il traffico grezzo e per costituire una comprensione di ciò che è "normale" per ogni utente, dispositivo e sottorete dell'organizzazione. Senza presupporre in anticipo quali attività siano dannose o meno, Darktrace Enterprise impara autonomamente a rilevare le discrepanze; il sistema avverte immediatamente l'organizzazione delle minacce emergenti, dagli attacchi interni scaltri, discreti e lenti ai virus automatizzati come i ransomware".*
>
> (fonte: sito web Darktrace, www.darktrace.com/fr)

La facile violazione e diffusione delle password o delle informazioni relative alla sicurezza della rete rimangono ancora le principali sfide da affrontare, pertanto le persone e le loro attività sono spesso considerate il punto più vulnerabile delle infrastrutture.

L'utente deve adottare tutte le misure possibili per proteggere i suoi dati, anche privati, ed essere sicuro che siano protetti da chi li conserva.

L'aumento dei rischi legati al fattore umano dipende dal fatto che gli esseri umani interagiscono tra loro nella vista quotidiana principalmente tramite Internet. Questo lascia tracce e genera dati che creano nuove vulnerabilità (uso dannoso). Inoltre, quando la pressione sul lavoro è troppo elevata, le persone tendono a sacrificare la sicurezza a favore della produttività.



Il fattore umano ©Tufts (Human Factors and Ergonomics Blog)

Cybersecurity nel settore della logistica e dei trasporti

Lo scambio di informazioni lungo tutta la supply chain è essenziale; per migliorare l'efficienza è necessaria una forte connettività tra gli attori coinvolti. Al tempo stesso però, l'interazione tra attori e oggetti aumenta anche la superficie di attacco (esseri umani, robot, veicoli, sistemi GPS) esponendo a nuove vulnerabilità. In questo ambito qualsiasi modifica indesiderata (sabotaggio) può causare gravi danni. I rischi legati all'uomo sono riconducibili principalmente alla condotta e al processo decisionale.

C'è troppo poco interesse per la sicurezza informatica nel mondo della logistica. I rischi informatici non sono sufficientemente integrati e sono visti come un problema tecnico strettamente di competenza dei responsabili tecnici.

La protezione delle infrastrutture critiche (porti, aeroporti in particolare) deve tener conto anche degli aspetti di logistica per cui deve essere sviluppata la cooperazione. Tutti gli attori legati alla logistica e ai trasporti sono raggruppabili in un gruppo di stakeholder con i medesimi interessi. L'integrazione di tutti questi

attori è una sfida importante, poiché ad oggi non esiste una *"security by design"* per la maggior di loro e nelle interazioni tra di loro. C'è ancora poca percezione del reale valore della sicurezza informatica in questo settore.

I porti rappresentano infrastrutture privilegiate per l'utilizzo delle nuove tecnologie come il 5G. Nelle grandi infrastrutture critiche, la sicurezza informatica deve essere introdotta fin dalla fase di progettazione per garantire, ad esempio, uno scambio di dati sicuro, scambio per cui ad oggi non è stata ancora sviluppata una specifica certificazione, che potrebbe definire anche diversi livelli di sicurezza. La governance è pertanto necessaria per garantire un quadro di riferimento e dei "best practice in sicurezza informatica". Più le informazioni sono diffuse e condivise, più devono essere protette.

Il settore della logistica elabora una quantità di dati molto elevata ma la sicurezza informatica è considerata ancora una questione supplementare e sottovalutata.

Possono esserci interessi terroristici nel furto di dati, ad esempio per conoscere i passeggeri di un volo, di una crociera o per conoscere il contenuto di aerei, navi o trasporti su strada. L'ambiente in cui si trova un sistema è di per sé critico. La natura di questo ambiente cambierà la natura del rischio. In qualsiasi sistema, il livello di sicurezza di tutti gli attori può essere migliorato solo elevando il livello di ogni singolo attore. Un difetto in-house di un attore mette a rischio tutti gli altri soggetti coinvolti. Abbiamo quindi bisogno di un quadro di riferimento comune ma spesso gli attori e i sistemi hanno le loro specificità (vincoli).

Fortunatamente nelle infrastrutture critiche è possibile riconoscere pattern di comportamento anomali. Attraverso l'uso di piattaforme innovative multidimensionali è possibile identificare istantaneamente gli attacchi riconoscendone le caratteristiche principali (pattern). Ad esempio è possibile identificare gli scambi con macchine che non fanno parte del sistema e che tentano di introdurre o esfiltrare dati.

Le norme per la supply chain sono le nuove sfide. La frammentazione delle informazioni potrebbe essere una possibile soluzione di sicurezza, poiché rende più difficile attaccare l'intero sistema o i singoli attori, ma il problema principale è l'assoluta necessità per i diversi attori di comunicare tra loro. Conoscere i partner, come lavorano, contribuisce alla sicurezza. Sapere chi ha bisogno di accedere a determinate informazioni o chi ha accesso a determinate informazioni contribuisce ad elevare il livello di segretezza.

È sempre difficile attirare investimenti nel campo della sicurezza informatica. Il finanziamento della sicurezza deve essere integrato nei prodotti (hardware e software) o separatamente come servizio aggiuntivo? Probabilmente il consumatore per avere un livello di sicurezza più elevato dovrà accettare di pagare un prezzo più alto, ma finché ci saranno prodotti ideati secondo logiche di vendita e senza garanzia di sicurezza, il sistema sarà a rischio. Una soluzione potrebbe essere quella di applicare il principio di "security by design".

Sicurezza informatica nel settore delle infrastrutture critiche

Gli sforzi normativi nell'ambito del programma NICE forniscono l'impulso allo sviluppo della sicurezza informatica.

> *"Il Cybersecurity Framework o Framework for Improving Critical Infrastructure Cybersecurity (attualmente versione 1.1) è un framework voluto, composto da standard, linee guida e best practices per gestire il rischio legato alla sicurezza informatica [il come e cosa della sicurezza informatica]. Il NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (vedi domanda sopra) descrive e categorizza ruoli e funzioni [il who of cybersecurity]".*
>
> (fonte: Sito web dell'Istituto nazionale di norme e tecnologia (NIST), U.S. Department of Commerce, www.nist.gov/itl/applied-cybersecurity/nice).

Tale approccio risulta necessario anche per le infrastrutture idriche ed elettriche particolarmente vulnerabili.

Le opportunità di digitalizzazione in questo campo sono notevoli e necessarie, ma espongono a ulteriori vulnerabilità creando nuovi punti di

accesso ai sistemi. La tecnologia *"Smart Metering"* (contatori comunicanti) ad esempio è molto sensibile. I prodotti attualmente disponibili sul mercato, rispondono più o meno alle esigenze di sicurezza ma devono ancora essere perfezionati.

La sicurezza informatica nell'Healt Care, compresa l'assistenza domiciliare, diventerà una questione sempre più rilevante sia per l'invecchiamento della popolazione sia per l'aumento dei servizi somministrati via Internet. Dato che questo settore si sta sviluppando già da ora, è fondamentale agire immediatamente per garantire che la sicurezza sia integrata fin dalla fase di progettazione degli strumenti in particolate per la sicurezza dei dati e la privacy che assumono un importante ruolo in questo ambito.

Una criticità è rappresentata dalla mancanza di consapevolezza del top management delle infrastrutture critiche sui problemi di sicurezza informatica. In questo settore, è essenziale essere in grado di lavorare in modo connesso e scambiare informazioni per poter svolgere al meglio i propri compiti.

In parallelo, i service provider raccolgono molti dati sui cittadini e hanno gli stessi vincoli delle pubbliche amministrazioni. Sono in aumento anche le interazioni su Internet tra i cittadini e i loro fornitori, nonché con le autorità. In contrasto, molte aziende con sempre meno risorse devono svolgere una moltitudine di operazioni in più. Spesso si corre così il rischio di sacrificare la sicurezza al vantaggio della cosiddetta efficienza, mentre ci si dimentica che le possibilità offerte da Internet possono generare nuove necessità proprio di sicurezza.

I requisiti di sicurezza possono essere in conflitto con i requisiti di trasparenza. Sono spesso due facce della stessa medaglia. Ciò che è esposto, visibile e trasmesso non deve contenere dati protetti.

È necessario trovare risposte alle seguenti domande:

NICE National Institute for Health and Care Excellence

- Qual è il livello di miglioramento necessario agli stakeholder delle infrastrutture critiche per consentire loro di cooperare in conformità alle linee guida NICE.
- Qual è il grado necessario di condivisione dei dati e delle soluzioni tra gli attori al fine di creare un ambiente informatico sicuro?

Sicurezza informatica nel settore delle forze dell'ordine

Per uno Stato, l'obiettivo principale è quello di evitare il cyberspeaking (furto di informazioni strategiche), il cyber crime (motivato dal guadagno economico) e il cyber terrorismo (propaganda, notizie false, ricatti, furti di dati per la preparazione di attacchi). Il modo migliore per prevenirli è di iniziare un processo di sensibilizzazione oltre che di formazione a livello universitario.

Per sviluppare efficaci capacità di difesa è importante promuovere centri di difesa informatica, campus e altre iniziative di formazione. La cooperazione tra i vari centri consente di comprendere la reale necessità di condividere le informazioni. Le forze di polizia regionali e nazionali stanno, infatti, sviluppando strumenti di cooperazione. La via da seguire è la condivisione internazionale delle informazioni.

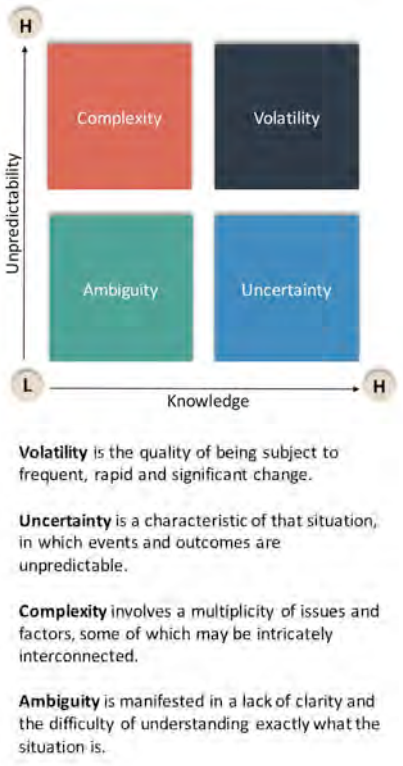
Le organizzazioni civili e le agenzie governative dovranno affrontare gli stessi rischi e porsi le stesse fondamentali domande sulla loro sicurezza informatica: in che misura siamo minacciati nel ciberspazio, quali sono i nostri interessi e come possiamo difenderli, quali opzioni abbiamo e come possiamo garantire la resilienza dei sistemi? Inevitabilmente l'uso del cyberspazio andrà via via aumentando perché garantisce sia una migliore qualità e rapidità del processo decisionale sia del controllo che della gestione delle informazioni e di enormi quantità di dati. Per l'esercito in particolare, si tratterà di adottare tutte le misure possibili per limitare i rischi e quindi di gestirli costantemente. Si dovrà affrontare uno scenario complesso caratterizzato da opportunità, rischi e vulnerabilità.

La sicurezza informatica e la minaccia in evoluzione

La minaccia diventa sempre più complessa. Più oggetti sono collegati tra loro, sempre più ci sono obiettivi da proteggere. Bisogna abituarsi agli ambienti VUCA (Volatility, Uncertainty, Complexity and Ambiguity), volatili, incerti, complessi e ambigui come mai prima d'ora.

Il 5G porterà ad un'evoluzione globale e non solo perché la Cina attualmente è al primo posto nel suo sviluppo. È molto più potente e può essere destinato a molti usi, per queste due ragioni sarà un problema per le forze dell'ordine. Inoltre, è preoccupante che i problemi del 2G, 3G e 4G non sono stati ancora risolti e saranno trasferiti al 5G.

Bisogna poi potersi fidare del sistema altrimenti partire da una fiducia zero significherebbe aspettarsi di poter essere attaccati in qualsiasi momento.



Caratteristiche di un ambiente Vuca e delle sue componenti (© www.acceleration-lab.com)

Alcuni pensieri aggiuntivi

È importante garantire la sicurezza delle reti rafforzando le attività continua di monitoraggio e analisi. La resilienza si ottiene attraverso il monitoraggio delle attività. Possiamo applicare metaforicamente il modello di organizzazione di un formicaio con 4 livelli :

- attività specifiche (compiti e ruoli codificati)
- allerta
- identificazione di attività anomale
- misurazioni

Il corretto funzionamento delle future smart city si baserà su una grande quantità di dati che dovranno essere raccolti ed elaborati, ma anche protetti. Il modo migliore per garantirne la sicurezza e organizzare i dati in moduli separati è quello di utilizzare un sistema multidimensionale ma dovrà essere istituito un sistema automatico o semiautomatico di audit, valutazione, revisione e misurazione. ■

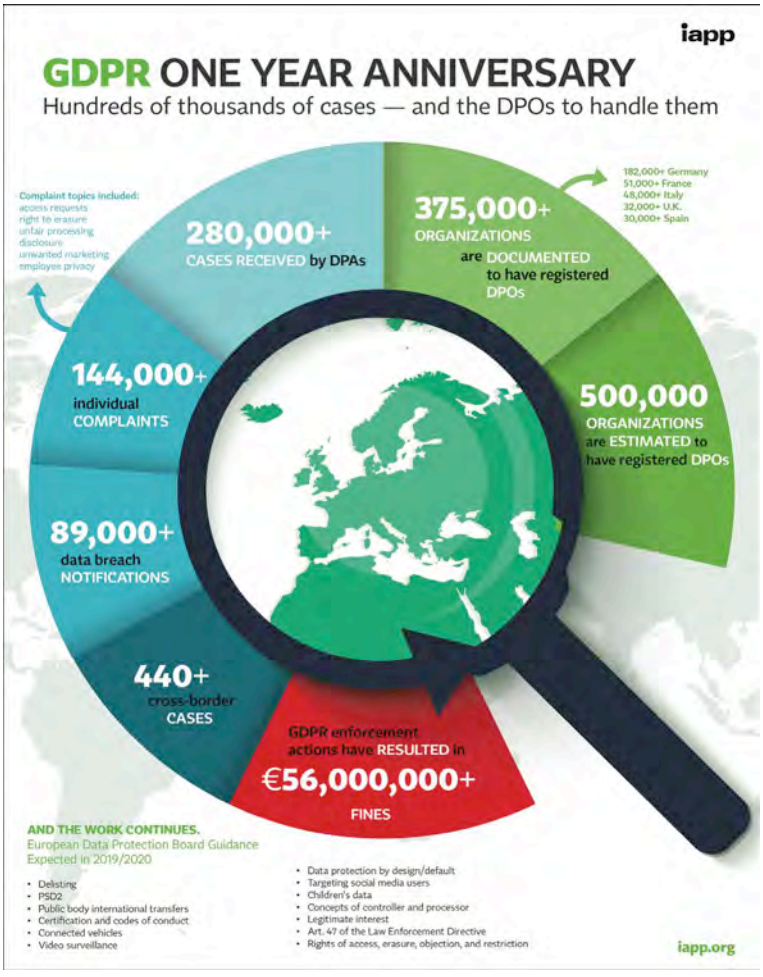
Il futuro dell'Identity and Access Management

Autore: **Sergio Sironi,**
Sales Director Southern Europe, Gemalto

La tecnologia è spesso definita la grande livellatrice: consente a tutte le organizzazioni, grandi e piccole, così come ai consumatori, di fare praticamente qualsiasi cosa, da qualsiasi luogo, in qualsiasi momento. Tuttavia, man mano che aumenta il nostro affidamento su di essa, di pari passo crescono le possibilità per gli hacker di sfruttarne le vulnerabilità per attaccarci. Anzi, grazie alle crescenti capacità del cloud e alle tecnologie mobile, la superficie d'attacco delle aziende si è ampliata rapidamente, e non è più ristretta alle reti locali.

Fortunatamente, anche l'industria della sicurezza continua ad adattarsi a queste minacce crescenti, diventando sempre più proattiva e innovativa nelle tecniche che sviluppa per contrastare i piani degli attaccanti. Come se non bastasse, con l'entrata in vigore lo scorso anno del General Data Protection Regulation (GDPR) e i potenziali danni che verrebbero causati da un data breach, la protezione dei dati e i rischi, finanziari e d'immagine, a essa correlati sono diventati uno dei temi centrali per le organizzazioni.

Un'area su cui ci si sta concentrando particolarmente, in seguito a una serie di attacchi basati sull'uso di credenziali rubate, è l'Identity and Access Management (IAM). Formate da due elementi, le tecnologie IAM sono fondamentali per le aziende nella definizione e gestione dei profili



BIO

Sergio Sironi è Responsabile della strategia di vendita ed espansione della divisione Gemalto Enterprise & Cybersecurity (ex Safenet) in Sud Europa per le regioni Italia, Malta, Spagna, Portogallo, Israele e Cipro.
Nato a Monza nel 1967, entra in Safenet nel 2014 come Country Manager con il compito di guidare la crescita dell'azienda nella regione, organizzare la distribuzione e i partner Cyber Security in Italia e Malta. Sironi ha maturato oltre 20 anni di esperienza con ruoli di crescente responsabilità nelle vendite e nel business sia in ambito italiano che internazionale principalmente nel settore Sicurezza, Enterprise Software, Hardware ed Embedded. Ha una vasta conoscenza del mercato europeo grazie a vari incarichi svolti in aziende multinazionali americane come Wind River, The MathWorks e OSIsoft dove ha ricoperto ruoli di District Sales Manager e Sales Manager per Italia, Grecia e Malta.

personali di accesso alle risorse e per garantire che a tali profili e ai loro accessi si applichino adeguati livelli di sicurezza. Ad esempio, quando un nuovo impiegato entra in azienda, il processo di identity management gli creerà un profilo digitale da aggiungere al sistema, fornendogli la password e definendo di quali applicativi avrà bisogno per svolgere il suo lavoro. Dopodiché, il sistema di access management validerà le credenziali dell'utente che entra nell'applicativo, e garantirà che sono applicate le corrette policy d'accesso.

Ma, di fronte a cyber attacchi sempre più sofisticati, e a tecniche d'attacco che possono ricorrere a tecnologie nuove e dirompenti, quali l'Intelligenza Artificiale, cosa si prospetta nel futuro dell'Identity and Access Management?

Password: il sogno di ogni hacker

Dal Single Sign On (SSO) alle tecniche biometriche all'Intelligenza Artificiale e la tokenizzazione, l'industria della sicurezza continua a sviluppare nuovi modi per migliorare la gestione degli accessi, ma l cuore di gran parte delle misure di sicurezza adottate dalle aziende rimangono sempre gli username e le password. Ad oggi, i consumatori hanno una media 90 account online e, per semplificarsi la vita, quasi tutti (89%) utilizzano una o due password per tutto.

Questo diventa fonte di grande preoccupazione, se si pensa che nella prima metà del 2018 sono stati compromessi 3,3 miliardi di dati online. Quelle credenziali, molte delle quali comprendevano indirizzi email e password, hanno fornito agli hacker un ricco bottino da cui attingere per attaccare le aziende. Una volta che gli hacker entrano in possesso della combinazione email+password, possono programmare dei bot per forzare l'accesso potenzialmente a decine di migliaia di account online e aziendali.

E, mentre le tecnologie come il SSO e l'autenticazione a due fattori stanno riducendo le capacità di successo di questo tipo di attacchi, le nuove tecnologie rappresentano un rischio. Fra non molto, gli hacker saranno capaci di creare dei bot machine-learning, che potranno imitare i comportamenti dell'utente, rendendo più difficile ai professionisti della sicurezza riuscire a distinguere fra tentativi di log-in ai sistemi aziendali legittimi e quelli invece condotti da bot malevoli. Inoltre, quando arriveranno le tecnologie quantistiche, la crittografia tradizionale non basterà più allo scopo, ed è per questo che l'access management deve essere al centro delle strategie di sicurezza di qualsiasi azienda, al fine di proteggere i dati contenuti nel suo perimetro.

La risposta è nel machine-learning?

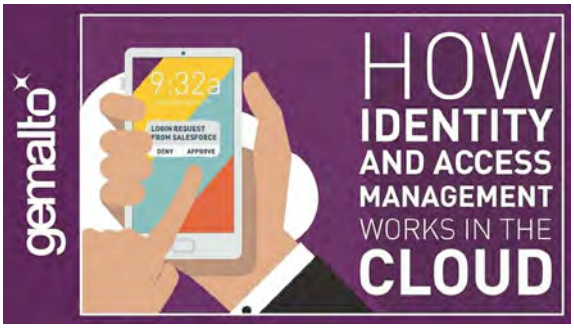
Fortunatamente, l'industria della sicurezza sta utilizzando le stesse tecnologie machine-learning per tenersi al passo con le minacce emergenti. Poiché i bot diventano capaci di imitare il comportamento umano, è necessario trovare delle soluzioni per validare l'utente che superino i meri dati di log-in: devono essere adattive.

Storicamente, l'autenticazione è una decisione one-time-only basata sulle credenziali inserite dall'utente. Ma mentre questo è sufficiente a proteggere le reti dalla maggior parte degli attuali attacchi malevoli, il machine-learning potrebbe invece consentire un furto di account più facile senza essere rilevati. Al giorno d'oggi, le tecnologie di access management devono essere in grado di tracciare il comportamento dell'utente, al fine di fornire autenticazione e autorizzazione continuative.

Per stabilire se un utente è chi dichiara di essere, il sito o il sistema devono saper leggere i segnali provenienti dall'interazione dell'utente, dalle attività contestuali e di navigazione al fine di capire cosa costituisca un comportamento "normale" per un determinato utente. In questo modo, è possibile individuare e lanciare un alert di fronte a qualsiasi comportamento si discosti dall'ordinario. In parole semplici: se un utente effettua log in da Londra, e digita in una certa maniera, un tentativo di log in dall'Ucraina con uno stile di digitazione meccanico nasconderà probabilmente un attacco malevolo, anche se le credenziali sono corrette. Se il comportamento indica una frode, il sistema di controllo accessi dovrebbe interrompere la sessione e richiedere ulteriori livelli di autenticazione da parte dell'utente.

Mentre la corsa all'Intelligenza Artificiale continua, con fini sia protettivi sia d'attacco, è diventato evidente come le tecnologie di controllo accessi siano centrali per mantenere al sicuro le aziende. E il rafforzamento non passa solo per l'AI: i controlli biometrici sono d'aiuto nelle industrie altamente regolamentate, quali quelle che operano nel settore della difesa o collaborano con il governo.

Le innovazioni nella cybersecurity si tradurranno in innovazione per le tecnologie di access management e per la sicurezza delle reti. Le aziende che costruiscono un framework d'accesso forte non solo migliorano il proprio

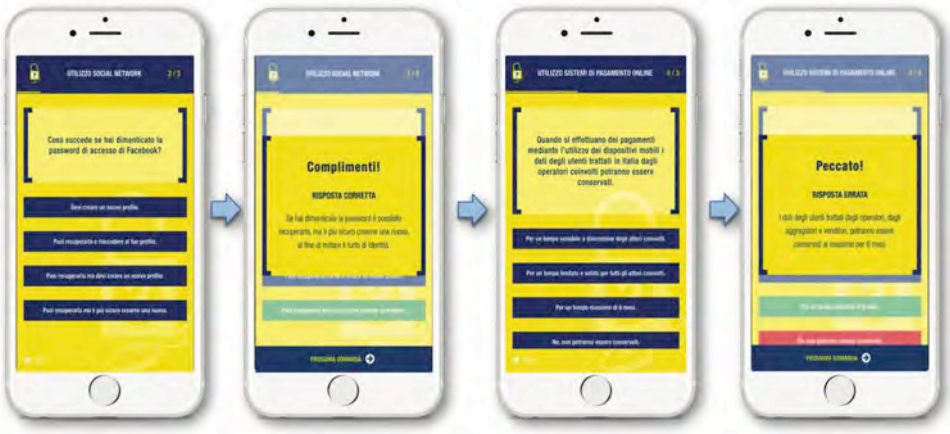


livello di sicurezza, ma in ultima istanza creano un futuro in cui la sicurezza potrà essere invisibile. Con le tecnologie di access management adattive, gli utenti non saranno frenati dalla sicurezza: il processo di log-in sarà basato sull'assessment, enforcement e monitoraggio delle politiche di accesso e offrirà all'utente un'esperienza sicura e priva di fastidi. ■

CyberSecQuiz

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

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



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

Giancarlo Butti, Maria Roberta Perugini, 2019, Franco Angeli

AUDIT E GDPR – MANUALE PER LE ATTIVITÀ DI VERIFICA E SORVEGLIANZA DEL TITOLARE E DEL DPO

Le attività di **verifica ed audit**, oltre a costituire un obbligo per i DPO, sono uno strumento di **accountability per tutti i titolari e responsabili del trattamento.**

Il volume affronta il tema delle verifiche in ambito privacy evidenziando le peculiarità determinate da una normativa particolarmente articolata, vasta, trasversale, in continua evoluzione e nella quale i pochi requisiti di conformità definiti in modo puntuale (ad esempio, il contenuto obbligatorio dell'informativa) coesistono con i molti la cui valutazione è lasciata alla responsabilità del Titolare (ad esempio, le misure di sicurezza).

Il volume descrive dunque il processo di audit nel suo complesso: la stesura di un piano di audit, la definizione di una metodologia di descrizione delle non conformità, la loro valutazione secondo diverse metodologie (quali ad esempio modelli di maturità), la stesura di un audit report e la relativa valutazione complessiva.

Dopo una presentazione delle caratteristiche dell'attività di audit e dei relativi standard e buone pratiche, il **volume propone metodologie per effettuare un assessment iniziale utile a individuare le aree a maggiore rischio di non conformità e a definire il conseguente piano di audit.**

Vengono proposte metodologie di verifica dei requisiti di conformità attraverso check list precostituite, ma anche suggerimenti su come **costruire check list personalizzate** ed altri strumenti utili nei documenti realizzati da Enti, Agenzie e Autorità Garanti, quali esempi di buone pratiche.

Vengono descritti sia **i punti di controllo di carattere generale**, che caratterizzano una normativa che impone ai titolari di essere in grado di dimostrare in ogni momento la propria conformità, sia quelli specifici di ogni macro argomento trattato.

Gli obiettivi del libro sono molteplici:

- consentire sia ad "auditor" professionisti, sia a soggetti che conoscono la normativa privacy ma che hanno poca dimestichezza con le attività di verifica di:
  - svolgere un assessment in ambito privacy
  - definire un piano di audit
  - definire un programma di audit
  - creare check list
  - raccogliere evidenze
  - valutare le risultanze dell'audit
  - stilare un verbale di audit

  al fine di verificare il livello di conformità della organizzazione sottoposta a verifica.
- consentire a Titolari e Responsabili di valutare:
  - quali tipi di verifica meglio siano rispondenti alle loro esigenze
  - le offerte su attività di verifica, distinguendo in particolare fra quelle che si limitano a considerare gli aspetti formali (verifiche di impianto) da quelle che effettuano un riscontro oggettivo su come opera l'organizzazione (di funzionamento).
- fornire, anche se limitatamente ai casi trattati, dettagli sulle implementazioni richieste per garantire la conformità alla normativa.

Un breve capitolo analizza anche le varie figure coinvolte: chi può svolgere un'attività di verifica, le qualifiche che deve avere, le certificazioni esistenti per dimostrare le proprie competenze. ■

The GCSEC is proud to be among the Institutional partners of the 3rd "Cybersecurity-Switzerland Congress", to be held on December 2nd and 3rd with the support of the IATA at its European Headquarters, at Geneva Airport. KEEP THE DATES! More info on: www.cybersecurity-dialogues.ch

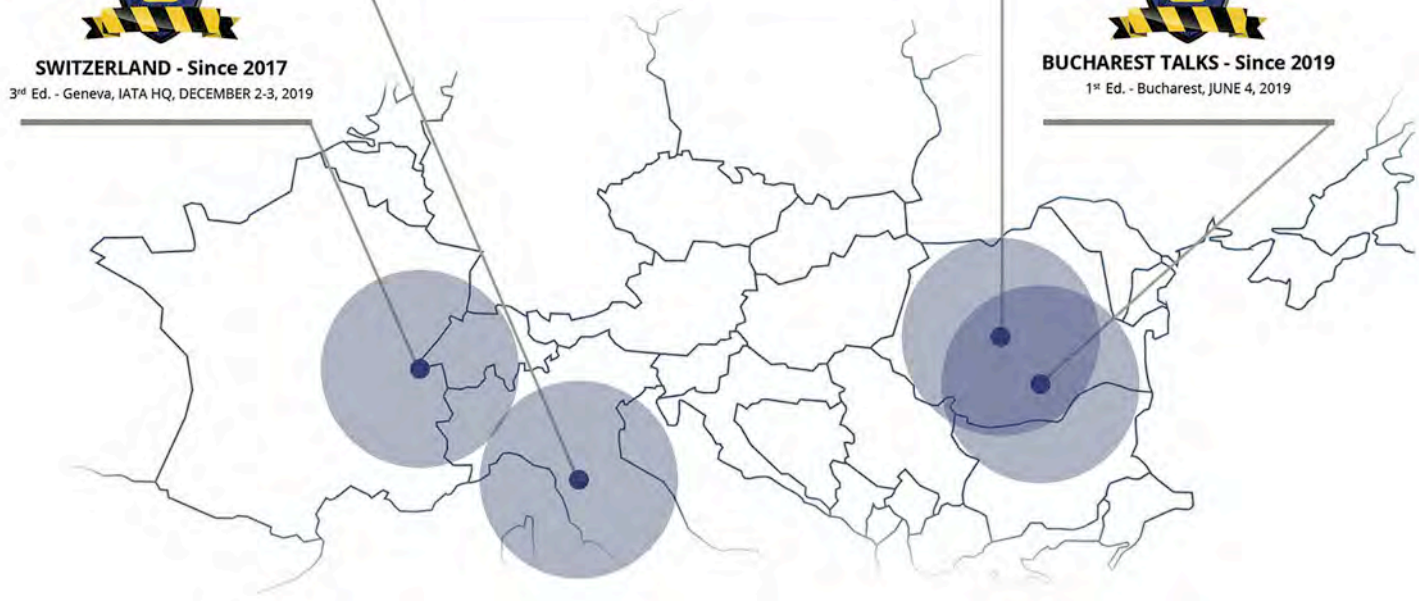
web for your business
swiss webacademy

MEDITERRANEAN - Since 2018
2rd Ed. - Florence, MAY 9-10, 2019

ROMANIA - Since 2013
7th Ed. - Sibiu, SEPTEMBER 12-13, 2019

SWITZERLAND - Since 2017
3rd Ed. - Geneva, IATA HQ, DECEMBER 2-3, 2019

BUCHAREST TALKS - Since 2019
1st Ed. - Bucharest, JUNE 4, 2019



www.cybersecurity-dialogues.org

Roberto Panzarani, Viaggio nell'innovazione, ed. Guerini e Associati

IL PRIMO "VIAGGIO" PER COSTRUIRE UN'ITALIA DIVERSA DEVE COMINCIARE DENTRO DI NOI

Autore: Massimiliano Cannata

L'innovazione è un termine complesso, che presenta mille sfaccettature e una molteplicità di definizioni. Roberto Panzarani, docente di *innovation management* e presidente dello ***Studio Panzarani e Associati***, che segue da molti anni questo tema, lo sa molto bene, proprio per questo nel suo ultimo brillante saggio (*Viaggio nell'innovazione*, ed. Guerini e Associati) parte dai fondamentali, evitando etichette alla moda. Il suo viaggio prende le mosse da alcune esperienze concrete, da cui il lettore può trarre stimolo oltre che insegnamento. "L'innovazione – spiega l'autore fin dalle prime pagine - non è mai stata così al centro dell'attenzione. Dalla tecnologia al marketing, alla definizione dei piani di business, nulla si potrebbe evolvere in assenza di questo motore, che si è di fatto aggiunto ai tradizionali fattori della produzione, perché la rende possibile".

Saremmo però fuori strada se pensassimo, magari condizionati dalle mirabolanti scoperte della scienza, che l'innovazione si possa risolvere in un mero fatto tecnico. E' lo stato d'animo, che informa uomini e organizzazioni che accende la scintilla e che fa la differenza. Questo aspetto quasi impalpabile dell'innovazione, perché legato alla forma mentis e alla sensibilità di ciascun individuo è spesso colpevolmente trascurato, lo dimostra il caso Italia. Abbiamo molta capacità di innovazione di prodotto, siamo spesso pronti a ripensare e riadattare il modello di business, dimostriamo però una palese difficoltà a sviluppare e diffondere una cultura dell'innovazione. I riflessi di questo *vulnus*, visibile da tempo nel nostro tessuto industriale e produttivo, sono percepibili non solo a livello degli assetti organizzativi, ma anche nella scarsa propensione a mettersi in discussione e ad aggiornare le competenze. Come superare l'*impasse*?

Bisogna lasciare le zone di confort

La risposta è prima di tutto di metodo, che vuol dire creare una sorta di "mobilitazione all'innovazione" all'interno delle aziende. Con questa finalità da molti anni lo Studio Panzarani ha sperimentato lo strumento del *learning tour*, per sollecitare imprenditori e manager a visitare i luoghi dell'innovazione, per trarne idee, suggerimenti, ma soprattutto per creare lo spirito giusto, che è il segreto che sta a monte di ogni iniziativa di successo. "Quando – confessa Panzarani – a valle di un corso di formazione o di un confronto in aula, un'azienda (la cosa capita più spesso di quanto si possa pensare n.d.r.) decide di creare una direzione dell'innovazione, penso tra me e me: meglio di niente, anche se non è questa la soluzione auspicabile. L'innovazione non può, infatti, essere confinata in un solo ambito, ma deve trasversalmente contagiare tutte le fasi del processo produttivo e tutte le risorse che operano in una struttura organizzativa". E' molto importante, insomma, che si crei un *mood* positivo, perché nella società della conoscenza vince chi sa mettere in comune idee che moltiplicano il valore, contribuendo a creare quella dimensione dell'intelligenza collettiva che, come ci ha insegnato Pierre Levy, è la condizione di sistema giusta per far crescere la ricchezza di un Paese a qualsiasi latitudine.

Per comprendere ancora meglio il messaggio di fondo che proviene da questo lavoro non bisogna, però, dimenticare che nella contemporaneità innovazione, tecnologie e globalizzazione sono termini inscindibili. Per creare un "ecosistema del cambiamento", altro termine chiave della ricerca, bisogna dunque porsi il problema dell'*execution*, altro punto debole del sistema Italia. "Silicon valley, Istraele, Bengalore, sono luoghi che proponiamo ai manager di visitare per dimostrare che le buone idee e le intuizioni brillanti, non devono rimanere confinate nel regno dell'utopia. In molti contesti le soluzioni innovative sono già da tempo divenute realtà, con un vantaggio misurabile da tutto il corpo sociale. Questo significa che bisogna, a tutti i livelli, uscire dalle zone di "confort", per valutare bene le potenzialità che nazioni come l'Italia hanno, ma che troppo spesso rimangono inespresse".

La tecnologia ha ampliato lo spazio delle possibilità

La tecnologia ha dilatato lo spazio della possibilità, adesso siamo chiamati a sfruttare il nuovo orizzonte del digitale. Non solo l'Italia ma anche la vecchia Europa hanno molto da imparare in questo momento di evidente declino. "Nazioni come il Brasile pur scontando enormi difficoltà di carattere storico politico stanno crescendo non solo in virtù di una maggiore presenza dei giovani, ma anche per la capacità di usare reti sociali dinamiche, aperte alla promozione del cambiamento". Ci vuole un alto tasso di energia positiva per seguire certi esempi, come è noto purtroppo l'Europa non parte da una posizione di vantaggio in quanto i giovani latitano. Questo complica la situazione anche se non conta solo l'anagrafe,

occorre lavorare di più sulla mentalità, liberarsi da vecchi schemi mentali per ritrovare quello spirito pionieristico che ha fatto dell'Occidente la culla della civiltà. L'atteggiamento positivo alimentato dalla cultura è, infatti, un importante requisito, anche se da solo non basta.

Sarebbe ora che si facesse sentire una capacità progettuale delle classi dirigenti, orientata a individuare le strade della ripresa che devono necessariamente passare attraverso un rafforzamento degli investimenti in formazione. "I dati che abbiamo a disposizione sono purtroppo sconfortanti: solo il 20% della forza lavoro è impegnata in percorsi di aggiornamento del know-how, mentre nell'ultimo anno 50mila giovani hanno lasciato il nostro paese. Un'emorragia di intelligenze che non possiamo più permetterci – commenta Panzarani – perché di questo passo usciremo definitivamente dal novero dei paesi che contano nello scacchiere internazionale".

Sembra quasi che l'Italia in questi anni abbia scelto la strada della rimozione. Invece di saper cogliere le opportunità legate a un cambiamento d'epoca senza precedenti che sta letteralmente trasformando industria e società, ha deciso di mettere la testa sotto la sabbia, pensando che "passata la nottata" tutto sarebbe tornato come prima. Ma il vento del divenire non aspetta, i giovani parlano linguaggi che i vecchi sistemi di potere non riescono più a comprendere, basti pensare che il 40% dei bambini che frequentano la scuola stanno studiando per un lavoro che dovrà essere ancora inventato. Serviranno giovani preparati, capaci di incarnare nuove leadership in grado di gestire la conoscenza e la massa crescente di dati e informazioni che la rivoluzione digitale ci mette a disposizione.

Per concludere, ritornando al caso Italia, sarà fondamentale recuperare l'energia e la forza dei talenti che abbiamo lasciato scappare via. Ecco perché il viaggio deve partire da noi, per rimuovere scorie e pregiudizi. Creare il profilo dell'Italia che verrà, in un'Europa anch'essa rinnovata, capace di recuperare una vera unità sul terreno dei valori, scavalcando il freddo schema dei parametri di stabilità e la gabbia della burocrazia è l'obiettivo che una classe dirigente avvertita dovrà porsi, senza sconti né rimandi. Il tempo dell'incertezza e dell'irresolutezza è infatti ormai scaduto da un pezzo. ■

Realizzata per essere esposta nel 2013 all'ITU (l'Unione Internazionale delle Telecomunicazioni), premiata dall'ITU e quindi tradotta ed esposta consecutivamente in 28 città di Romania, Polonia e Svizzera, la mostra è stata tradotta in italiano per le Poste Italiane, col patrocinio della Polizia Nazionale. E stata presentata in anteprima nel 2016 presso la "MakerFaire – European Edition" di Roma (dove ha superato i 130.000 visitatori). In 30 pannelli, l'esposizione illustra l'evoluzione delle tecniche di comunicazione e di manipolazione delle informazioni dai tempi più antichi ai social media usati oggi da tutti. Consente senza essere moralizzatrice di educare giovani ed adulti ad una fruizione consapevole e protetta di Internet.
La mostra è integralmente visitabile sul sito del Distretto di Cyber Security delle Poste Italiane, dove l'esposizione reale è allestita in modo permanente: https://www.distrettocybersecurity.it/mostra-2/

Una pubblicazione

web for business
swiss webacademy

A cura del

Global Cyber Security Center

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

ISSN 2559 - 1797
ISSN-L 2559 - 1797

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

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

CERT STAR

Programma

Il CERT STAR è un programma di incontri a porte chiuse dedicato ai CERT e ai SOC italiani volto ad alimentare le competenze, promuovere la cooperazione e la condivisione di esperienze. Nel corso degli incontri sono analizzate a livello tecnico operativo le principali tematiche "core" dei team di security

28 febbraio

APT e Cyber Range

04 aprile

Dark Web Intelligence

10 luglio

Cyber Threat Intelligence

19 settembre

Application Security

07 novembre

End Point Security

03 dicembre

Incontro Executive

GLOBAL CYBER SECURITY CENTER

FORTINET · INTSIGHTS Defend Forward · Carbon Black. · XM CYBER · brinthesis · f5

Hotel Radisson Blue – Via Filippo Turati, 171 Roma
Per maggiori informazioni scrivere a info@gcsec.org

web for your business
swiss webacademy

Presents:

CYBERSECURITY ROMANIA CONGRESS
7th Edition

7th Central European Cybersecurity Congress

A Public-Private-User Dialogue Platform
September 12-13, 2019, Sibiu, Romania
www.cybersecurity-dialogues.ro

Under the aegis :

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

With the support of :

POLICE GENÈVE

GLOBAL CYBER SECURITY CENTER

In partnership with :

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EUCACS

EUROPEAN CENTER FOR ADVANCED CYBER SECURITY

CHARENTE-MARITIME CYBER SÉCURITÉ
CMCS 2019

ULBS
Universitatea "Lucian Blaga" din Sibiu

C.fas
Club Francophone d'Affaires de Sibiu

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

ROMANIA SRI Patria a priori SERVICIUL ROMÂN DE INFORMAȚII

ROMANIA CENTRUL NAȚIONAL CYBERINT SERVICIUL ROMÂN DE INFORMAȚII

IGPR POLIȚIA ROMÂNĂ

DIRECȚIA DE COMBATERE A CRIMINALITĂȚII ORGANIZATE I.G.P.R.

CERT-RO