ETTORE GALLUCCIO

Bachelor of

Computer Science

Digital Transformation & Cybersecurity

La grande opportunità per il Sistema Italia

Roma, 30/11/2019

Ettore Galluccio

Con la presente dichiaro di essere l'unico autore di questo progetto/tesi e che il suo contenuto è solo il risultato delle letture fatte e delle ricerche svolte.

Sommario

Acronimi

Atm: Automated Teller Machine o sportello automatico, è un'apparecchiatura per il prelievo in modalità self di denaro contante che viene addebitato direttamente sul rapporto bancario. Inoltre, permette anche la fruizione di altri servizi previo riconoscimento del cliente.

Big Data: In statistica e informatica il termine big data, o mega dati, indica genericamente una raccolta di dati così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza.

Bitcoin: Bitcoin è una criptovaluta (Il vocabolo criptovaluta è l'italianizzazione dell'inglese cryptocurrency e si riferisce ad una rappresentazione digitale di valore basata sulla crittografia) e un sistema di pagamento mondiale creato nel 2009 da un anonimo inventore, noto con lo pseudonimo di Satoshi Nakamoto, che sviluppò un'idea da lui stesso presentata su Internet a fine 2008.

Business Continuity: Per Business Continuity si intende la capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente.

Chatbot: Chat bot, chatbot o chatterbot, è un software progettato per simulare una conversazione con un essere umano.

CyberCrime: È un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica sia hardware che software, per la commissione di uno o più crimini

Cyberwarfare: Con il nome di cyberwar si identificano tutte quelle attività tese a procurare danni a sistemi informatici di ogni tipo. A differenza dei “normali” attacchi informatici, si tratta di azioni compiute con precisi scopi politico-militari da speciali apparati militari o da organizzazioni di cyber criminali finanziate, comunque, da entità governative.

Data Analytics: Nell'ambito della scienza dei dati l'analisi dei dati è un processo di ispezione, pulizia, trasformazione e modellazione di dati con il fine di evidenziare informazioni che suggeriscano conclusioni e supportino le decisioni strategiche aziendali.

data breach: Con il termine data breach si intende un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito **a:**

- perdita accidentale: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
- furto: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
- infedeltà aziendale: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
- accesso abusivo: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

Disaster Recovery: Con disaster recovery (brevemente DR, in italiano: Recupero dal Disastro), in informatica ed in particolare nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.

Fake-news: Il termine inglese fake news (letteralmente in italiano notizie false) indica articoli redatti con informazioni inventate, ingannevoli o distorte, resi pubblici con il deliberato intento di disinformare attraverso i mezzi di informazione. Tradizionalmente a veicolare le

fake news sono i grandi media, ovvero le televisioni e le più importanti testate giornalistiche. Tuttavia con l'avvento di Internet, soprattutto con la condivisione dei media sociali, è aumentata grandemente anche la diffusione di notizie false.

ICS/SCADA: Nell'ambito dei controlli automatici, l'acronimo SCADA (dall'inglese "Supervisory Control And Data Acquisition", cioè "controllo di supervisione e acquisizione dati") indica un sistema informatico distribuito per il monitoraggio e la supervisione di sistemi fisici. Si tratta di una tecnologia in essere da oltre 30 anni e che si è costantemente evoluta grazie al progresso dell'elettronica, dell'informatica e delle reti di telecomunicazioni, principalmente utilizzata in ambito industriale e infrastrutturale.

IoT: I**nternet of Things (IoT)** è un neologismo utilizzato in telecomunicazioni, un termine di nuovo conio nato dall'esigenza di dare un nome agli oggetti reali connessi ad internet. Il significato di IoT si esprime bene con degli esempi: IoT è ad esempio un frigorifero che ordina il latte quando "si accorge" che è finito. IoT è una casa che accende i riscaldamenti appena ti sente arrivare. Questi sono esempi di IoT, ovvero di oggetti che, collegati alla rete, permettono di unire mondo reale e virtuale.

Matrix: Matrix (The Matrix) è un film di fantascienza del 1999 scritto e diretto dai fratelli Andy e Larry Wachowski. Il film, che ha vinto numerosi premi, tra cui 4 Oscar, ha avuto un forte impatto culturale e vi sono state numerose opere che vi fanno riferimento. Nel 2012 è stato scelto per la conservazione nel National Film Registry della Biblioteca del Congresso degli Stati Uniti.

P2P: Peer-to-peer (espressione della lingua inglese, abbreviato anche P2P ovvero rete paritaria/paritetica) nelle telecomunicazioni indica un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi ('clienti' e 'serventi'), ma anche sotto forma di nodi equivalenti o 'paritari' (peer), potendo fungere al contempo da client e server verso gli altri nodi terminali (host) della rete. Mediante

questa configurazione, qualsiasi nodo è in grado di avviare o completare una transazione. I nodi equivalenti possono differire nella configurazione locale, velocità di elaborazione, ampiezza di banda e quantità di dati memorizzati. Esempio tipico di P2P è la rete per la condivisione di file (file sharing).

RPA: La Robotic Process Automation (RPA) afferisce a tutte le tecnologie, prodotti e processi coinvolti nell'automazione dei processi lavorativi e utilizza software "intelligenti" (i cosiddetti "software robot") che possono eseguire in modo automatico le attività ripetitive degli operatori, imitandone il comportamento e interagendo con gli applicativi informatici nello stesso modo dell'operatore stesso.

Smart: Il termine "smart" (in italiano Intelligente) è il prefisso che usiamo per tutti quei dispositivi che hanno capacità di calcolo e comunicazione nel senso che possono raccogliere, usare e comunicare dati.

Terminator: Terminator (The Terminator) è un film del 1984 diretto da James Cameron. La trama fantascientifica, scritta da Cameron con Gale Anne Hurd, è incentrata sul personaggio del titolo, un cyborg assassino (interpretato da Arnold Schwarzenegger) inviato indietro nel tempo dal 2029 al 1984 per uccidere Sarah Connor (Linda Hamilton), il cui figlio un giorno diventerà un salvatore contro le macchine in un futuro post apocalittico. Michael Biehn interpreta Kyle Reese, un soldato del futuro inviato anch'egli indietro nel tempo per proteggere Connor. I produttori esecutivi John Daly e Derek Gibson della Hemdale Film Corporation furono strumentali nel finanziamento e nella produzione del film.

Lista delle figure

Introduzione

La digitalizzazione è un processo di conversione ormai alla base dello sviluppo della nostra società e della nostra economia. Nel mondo di oggi persone, dispositivi e macchine sono collegati in rete tramite mezzi cablati o wireless. Se dovessimo definire la nostra era geologica probabilmente la definiremmo "**l'era di Internet e dei dispositivi mobili intelligenti**". Internet ha toccato ogni essere umano e ha cambiato il modo con cui svolgiamo le nostre attività quotidiane come lavorare, giocare, fare shopping, vedere film e sport, parlare al telefono, ascoltare la nostra musica preferita, ordinare cibo, pagare le bollette, fare amicizia e salutare i nostri amici e parenti nelle occasioni speciali.

Oggi quasi tutti gli strumenti di uso quotidiano sono comparabili a computer.

Computer connessi in rete. Gli ATM che consentono di prelevare contatti sono computer. Il frigorifero, la lavatrice ed il robot da cucina ormai (negli USA non sono più commercializzati elettrodomestici "non-smart") esplicano le loro mansioni mediante computer. Il funzionamento di un'automobile viene determinato da decine di sistemi computerizzati che sovrintendono i dispositivi necessari al suo moto (dal controllo dell'impianto frenante a quello del motore). I telefonini (il primo smartphone risale al 2007) sono diventati computer potentissimi nei quali gli uomini hanno immesso sia la propria vita privata che quella lavorativa. Il termine "smart" è ormai un suffisso applicato a qualunque tipologia di prodotto. Sono smart la televisione, gli orologi e gli strumenti di fitness. Sono smart anche tanti dispositivi medici (pensiamo i moderni pacemakers e pompe di insulina). Sono smart i giocattoli per i nostri animali domestici, le penne, le apparecchiature per il caffè e le tazze del caffè stesso. Sono smart i sex-toys, i sensori per la casa ed i caschi dei motociclisti. Sono smart i bulbi per le lampadine, i meccanismi per il controllo delle toilette e per le chiusure delle porte di casa. E ormai l'uomo si sta abituando a far interagire questi oggetti smart con altri oggetti altrettanto smart come "Alexa" o "Google Assistant".

Negli ambienti lavorativi le cose non vanno diversamente. I dispositivi “smart”, come telecamere e sensori di movimento, sono collegati fra loro per rispondere ad esigenze di sicurezza e controllo dei locali in cui si opera. I sistemi “Smart” negli edifici consentono di godere di un'illuminazione più efficiente, di ottimizzare il funzionamento di un ascensore, di governare e controllare al meglio le condizioni climatiche interne e tanto altro.

Tante città hanno da tempo iniziato a introdurre nel loro tessuto oggetti “smart” utilizzati in strade, lampioni, piazze e marciapiedi. Oggetti smart sono collegati ad altri dispositivi smart a supporto di reti energetiche e di trasporto intelligenti. Studi avanzati di sistemi di automobili intelligenti senza conducente ottimizzeranno gli spostamenti sia umani che di beni al fine di ridurre al minimo l'utilizzo dei veicoli, tutto a beneficio del risparmio energetico e della tutela dell’ambiente. I sensori e i controlli informatici sulle strade ridurranno i tempi di risposta di polizia o di medici in caso di incidenti con segnalazione automatica di situazioni di pericolo. Detti esempi, modesti rispetto a quelli che effettivamente ci prospetta questo sorprendente mix di tecnologia, sono sufficienti a far intendere quanto l’uomo è e sarà sempre di più dipendente dagli sviluppi della scienza del digitale.

Ed il processo è irreversibile.

Di questa dipendenza e cardinalità dei sistemi digitali non ne siamo totalmente consapevoli ed abbiamo la falsa convinzione che questi riescano ad essere sicuri nel loro utilizzo, totalmente affidabili e rispettosi della privacy di ciascuno di noi.

Quanto ci sbagliamo. E quanto siamo distanti dalla realtà!

Infatti, le minacce collegate alla Digital Transformation, e più in generale al cyberspace, sono in crescita esponenziale. Il world Economic forum, nel suo report annuale “Global Risk Report 2019”, ha individuato al 4° e 5° posto, come rischi globali, rispettivamente l’accesso non autorizzato ai dati e gli attacchi cibernetici. Aziende, organizzazioni e governi stanno

cercando, con estrema fatica, di organizzarsi per gestire al meglio questo rischio che è, per buona pace di tutti, intrinseco ed inevitabile. I paesi che riusciranno a garantire un'adeguata protezione del cyberspace avranno la capacità sia di crescere a ritmi incalzanti, rispetto ai paesi meno preparati (infondendo fiducia e facendo da volano per nuovi servizi), e sia di attrarre investimenti senza precedenti perché, anche se i dati sono il nuovo petrolio, questi non dipendono da un territorio ma da una corretta macchina di protezione e garanzia.

Questo studio cercherà di ripercorrere la "Digital Run" degli ultimi anni, di razionalizzare gli sforzi regolatori di istituzioni e governi per regolare e proteggere il cyberspace e di motivare, con forza, le ragioni che dovrebbero spingerci a diventare un paese ad alto tasso di resilienza Cyber.

Capitolo 1 - Digital Transformation

Cyberspace e Digital Transformation. Evoluzione inarrestabile

È innegabile che nell'ultimo ventennio, con un'accelerazione senza precedenti nell'ultima decade, una grande trasformazione sociale ed economica è stata trainata dall'evoluzione tecnologica e dal settore telecomunicazioni. Un'evoluzione che ha colpito (non solo metaforicamente) il mondo delle aziende private (praticamente in ogni settore), organizzazioni ed enti pubblici e noi stessi come uomini e cittadini.

E siamo solo all'inizio.

I prossimi 10 anni saranno talmente concentrati di innovazioni e rivoluzioni digitali che, ripensando a quello che si sta vivendo ora (momento in cui questo documento viene redatto), si avrà l'impressione di tornare indietro ere geologiche.

Ma andiamo con ordine cercando di capire, da un punto di vista business e meno sociologico, cosa effettivamente rappresenta l'onnipresente concetto di "Digital Transformation".

Cominciamo dalle immancabili definizioni. Per ***Digital Transformation*** si intende l'evoluzione dei processi, tradizionalmente effettuati manualmente, per iscritto oppure tramite azioni fisiche o processi analogici, verso il mondo digitale o cyberspace, termine ormai di uso comune molto più affascinante e d'effetto. Con cyberspace, seppur con qualche declinazione differente in base al contesto che si sceglie di prendere a modello, si individua uno spazio interattivo composto da reti digitali che raccolgono, archiviano e manipolano informazioni per facilitare diverse forme di comunicazione; pertanto il cyberspazio include

Commentato [EG1]: Definire il cyberspace

Internet e una serie di sistemi che supportano i servizi, l'infrastruttura e le persone che vi partecipano[1].

Questo tipo di trasformazione porta con sé efficacia ed efficienza incredibili che si possono tradurre, per semplicità, in un risparmio notevole in termini di tempo e di lavoro. Non è dunque un caso o semplice passione se sempre più aziende scelgono di avvalersi di modelli di erogazione di servizi e di processi basati su tecnologie digitali.

L'uso di tecnologie e flussi di lavoro automatizzati implica, nella maggior parte dei casi, un notevole miglioramento dell'efficienza all'interno dei meccanismi del Business, con un conseguente incremento della produttività e quindi di ricavi e utili.

È chiaro che il concetto stesso di trasformazione digitale implica l'utilizzo di tecnologie digitali per ridisegnare i processi al fine di renderli allo stesso tempo più efficienti ed efficaci. L'idea fondante non è solo quella di utilizzare la tecnologia per replicare un servizio (o processo) esistente, trasformandolo in forma digitale, ma anche quella di introdurre un miglioramento significativo dei processi al fine di ottenere molteplici vantaggi. Si prevede che la Digital Transformation possa portare ad importanti incrementi di fatturato delle aziende grazie al potenziamento sia in termini di efficienza che di volume di servizi erogati. Il dato di fatto è che mentre prima senza di essa venivano raggiunti solo bacini di utenti "territoriali" ora la platea di riferimento è praticamente mondiale.

L'interesse delle aziende per questo nuovo tipo di trasformazione è, perciò, sempre più preponderante nelle decisioni prese a livello direzionale, con il conseguente rinnovamento profondo dei modelli di Business.

1 (Hunter & Huntert, 2003; Kohl, 2015)

Per dare un'idea della vastità della tendenza alla digitalizzazione globale basta considerare il numero di dispositivi elettronici impiegati nei processi digitali e connessi alla rete.

All'alba dei tempi della rete Internet e del concetto di connettività, stagione dei primi grandi ed ingombranti Computer (utilizzati esclusivamente in contesti militari, accademici, e successivamente aziendali) si stima che di questi ne esistessero all'incirca diecimila.

La crescita dei dispositivi, da quel momento in poi, ha seguito negli anni un andamento esponenziale, complici le grandi innovazioni e l'accessibilità ai componenti elettronici sempre più miniaturizzati, performanti ed economici. Nel 2003, ad esempio, già con l'ampia diffusione del Personal Computer, l'ordine di grandezza sul numero dei dispositivi interconnessi raggiunse i cinquecento milioni. Questo numero, con la successiva affermazione dello Smartphone, arrivò a toccare i due miliardi e mezzo, e pochi anni dopo, nel 2014, addirittura i dieci miliardi, **superando così il numero degli abitanti terrestri**. Tale exploit rappresenta in modo evidente il segnale dell'utilizzo esteso di tali tecnologie, oramai alla portata di tutti, con sempre più spesso la presenza di un alto numero di dispositivi adoperati per singolo individuo: tutto per soddisfare le molteplici esigenze delle informazioni e dei servizi disponibili sulla rete Internet. Questo è ipotizzabile essere solo l'inizio di un futuro inimmaginabile.

E' prevista che la diffusione dell'Internet of Things (vale a dire qualsiasi tipo di dispositivo a cui è stata fornita la funzionalità di accedere alla rete Internet e conservare e condividere dati) porterà, nel giro di pochi anni, ad un numero multimiliardario di utilizzazioni con tendenza di crescita annuale a due cifre.

Un'idea immediata nel tempo della crescita esponenziale dei dispositivi digitali è data dall'infografica seguente:

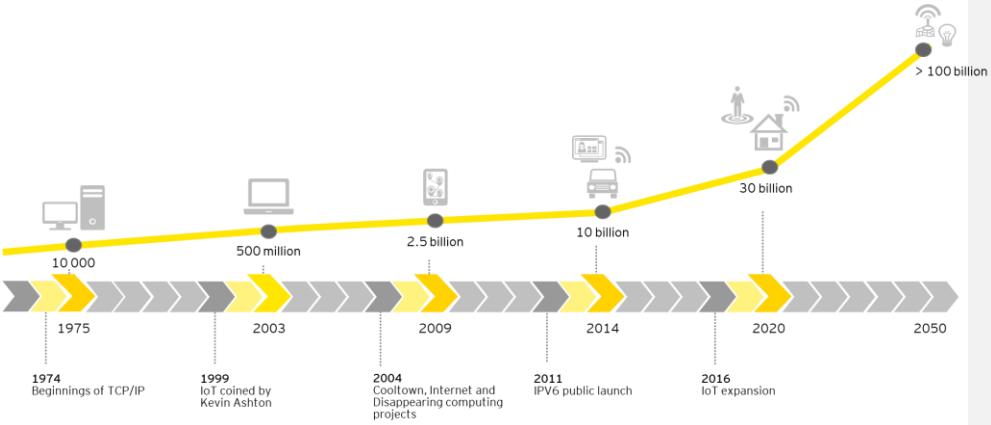


Figura 1 Evoluzione dei dispositivi connessi

Il grafico mostra la curva esponenziale degli apparati digitali connessi alla rete, dispositivi che sono destinati, secondo le previsioni, entro pochi anni, a raggiungere i 100 miliardi.

La crescita dei detti dispositivi testimonia una precisa volontà dell'uomo di fare affidamento sulle nuove tecnologie e sul grande potere che esse comportano, abilitando, tramite la connettività, la collaborazione diffusa e la condivisione delle informazioni in tempo reale; i frutti si manifestano in una sempre più profonda accelerazione dell'economia globale accompagnata da una semplificazione dei processi e della gestione degli stessi.

Evoluzione e accelerazione digitale

Naturalmente questa grande evoluzione non è solo collegata ai dispositivi digitali. Allora per sviscerare meglio il fenomeno occorre dare una risposta a questa domanda: *"Quali sono le innovazioni che stanno segnando e segneranno sempre più il prossimo futuro?"*.

La risposta certo non è né immediata e né tantomeno banale (troppe sono infatti le innovazioni tecnologiche); tuttavia è possibile dare qualche spiegazione nell'identificare dei "pillar" di base su cui la Digital Transformation cresce e si evolve.

Le principali innovazioni sono riassumibili in tre filoni fondamentali, strettamente correlati fra loro, in una modalità di interdipendenza:

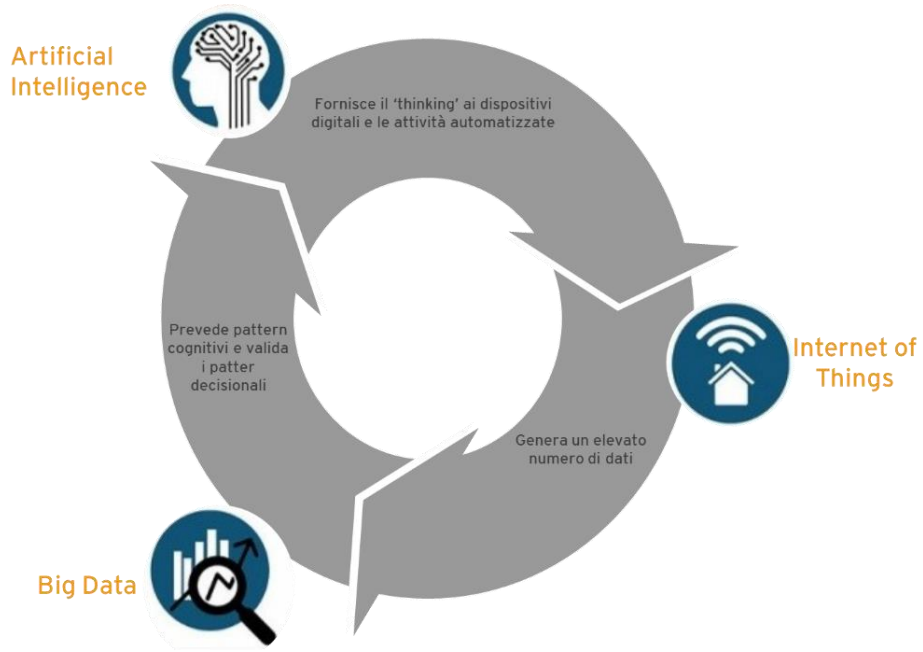


Figura 2 Il collegamento tra Big Data, Intelligenza Artificiale e Internet of Things

L'Internet of Things (IoT), menzionato precedentemente ed immaginabile come una grande quantità di dispositivi eterogenei connessi a Internet e distribuiti in tutti gli angoli del globo con le funzioni più diverse, è in grado di produrre una quantità notevole di dati tramite sensori, rilevatori e qualsiasi dispositivo deputato all'acquisizione di dati quantitativi e misurabili. Questi dati, per essere compresi e tradotti in un valore pratico, necessitano di essere elaborati; per ottenere questo occorre l'introduzione di un altro concetto fondamentale ovvero quello di Big Data, che riguarda la produzione, l'immagazzinamento, il processamento e il calcolo statistico di quantità di dati ingenti, eterogenei e destinati progressivamente a crescere.

Il discorso sui Big Data è strettamente legato a doppio filo ai dispositivi IoT poiché l'utilizzo e la gestione delle moli di dati prodotti devono essere accompagnati da tecniche avanzate, anche per quanto riguarda l'immagazzinamento, che stanno spingendo alla creazione di nuovi modelli computazionali ottimizzati.

Infine, il concetto di Artificiale Intelligence, vale a dire l'insieme di quei meccanismi che permettono a Software e Programmi di processare informazioni autonomamente, simulando una forma rudimentale di ragionamento, pone le basi nella soluzione per l'automazione della gestione delle informazioni.

Sulla base della mole di informazioni prodotte tali Software possono catalogare i dati in autonomia, rilevando eventuali pattern e correlazioni, permettendo comprensioni complesse impossibili da raggiungere esclusivamente tramite l'intervento umano.

Ovviamente queste informazioni particolarmente qualificate verranno utilizzate per migliorare le prestazioni e l'efficacia degli stessi dispositivi IoT, i quali potrebbero per-processare i dati già in fase di raccolta ottimizzando così i successivi passaggi.

In tal modo i principali fattori di crescita ed innovazione si alimentano a vicenda in un processo che oggi pochi riescono a comprendere appieno le possibili evoluzioni. Non molti anni fa film come Matrix, Terminator ed altri hanno fatto ipotizzare realizzazioni di sistemi che, da buoni propositi, si sono trasformati in dispositivi distruttivi per lo stesso uomo. Di sicuro visioni apocalittiche che comunque la ricerca attuale non può non tenere a conto soprattutto se si immagina che certe frontiere sono ostacoli di poco conto e non occorre molto per superarli.

Queste innovazioni hanno portato ad una consistente accelerazione della trasformazione digitale, con numerose implicazioni sul mondo della produttività e dell'uso in generale della tecnologia nella vita di ogni giorno. Per dare un'idea si riportano alcuni dati interessanti:

- Oggi il numero di utenti in rete è stimato essere di 3.8 miliardi di persone, vale a dire circa la metà della popolazione mondiale contro i 2 miliardi del 2015.
- Secondo questo andamento si stimano 6 miliardi di persone connesse nel 2022, fino ai 7 miliardi e mezzo nel 2030, con un andamento che si avvicina in numeri sempre di più al totale delle persone sul pianeta Terra.
- Ciò influenza altri dati interessanti, quali il numero di linee di codice sviluppato annualmente per far fronte ai nuovi bisogni di un Cyberspazio in espansione (ad oggi circa 1.2 miliardi di siti Web).
- Si prevede infatti un incremento notevole di dati disponibili online (nel 2020 ci si aspetta un volume di 50 volte superiore rispetto ad oggi), complice anche il numero sempre maggiore di dispositivi IoT connessi ad Internet.

Di seguito riportiamo un'infografica riassuntiva, per mostrare l'effettiva entità dei cambiamenti del mondo digitale in termini di numeri:

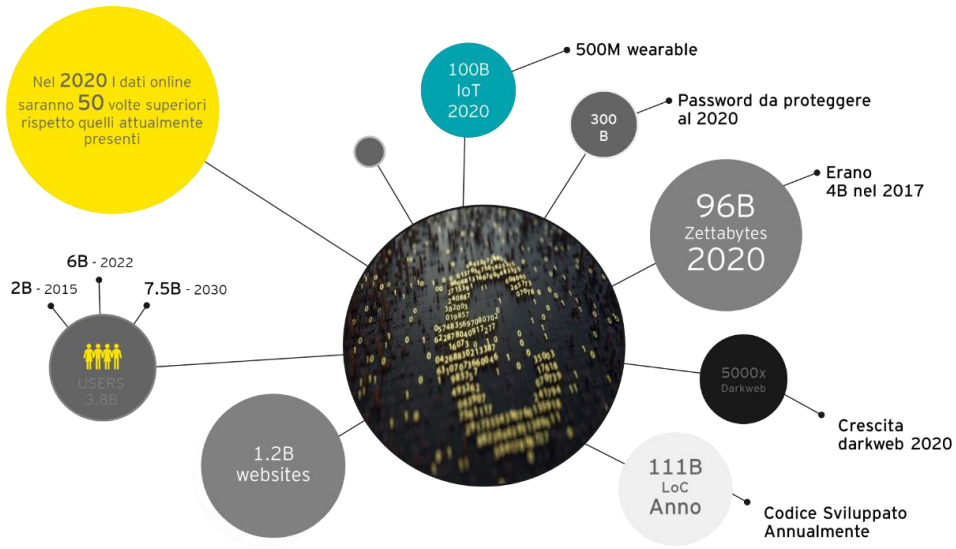


Figura 3 - Dati sintomatici della Digital Transformation

Il nuovo volto della trasformazione digitale

L'innovazione portata da un uso molto più estensivo delle nuove tecnologie sta assumendo aspetti sempre più evidenti nei processi quotidiani. I nuovi trend coprono numerose aree tecnologiche e, in virtù dei vantaggi portati in termini di produttività, attirano sempre di più l'attenzione del mondo Enterprise.

Il Cloud Computing, che consiste nel superamento dei sistemi fisicamente presenti nelle aziende e nella fornitura di soluzioni dislocate geograficamente grazie agli avanzamenti nella tecnologia di comunicazione remota, sta diventando sempre più prevalente in questo mondo. Il modello rappresentato dai sistemi on-premise, che richiedono l'uso di potenti calcolatori spesso legati a vecchie tecnologie, come i sistemi "Legacy", viene progressivamente abbandonato: questi sistemi Legacy sono infatti spesso sostituiti per i significativi vantaggi che offre in termini di prestazioni dal modello Cloud.

L’uso di sistemi utilizzati “as a Service” presenta meno problemi sia in termini di scalabilità che di aggiornamento e le tipiche problematiche complesse da affrontare nei modelli on-premis - come la Business Continuity e Disaster Recovery (ovvero la garanzia della disponibilità dei sistemi) - sono brillantemente affrontate e (parzialmente) risolte da un modello distante geograficamente e quasi sempre replicato dal fornitore che si occupa della gestione fisica dei sistemi.

L’uso estensivo dei Big Data oggi è sempre più preponderante. Per questo motivo sono richieste sempre più risorse da investire in Data Analytics - vale a dire in quelle attività deputate al processamento di una grande mole di informazioni in modo simultaneo, fornendo accesso in tempo reale alle informazioni raccolte - allo scopo di effettuare calcoli statistici e di valutare eventuali soluzioni ottimali per rispondere alle più eterogenee e complesse necessità del Business.

Un’ altra tendenza attuale si esplica nell’automazione dei processi, fisici e non, avvalendosi degli avanzamenti nel campo dell’Intelligenza Artificiale e del Machine Learning. In tal modo si consente ad un Software di “ragionare”, sulla base delle informazioni raccolte e di opportuni input specifici, in modo concettualmente analogo al pensiero umano. Stiamo parlando di RPA - Robotic Process Automation - che integra questo nuovo approccio all’automazione nella gestione dei processi, coinvolgendo anche macchine autonome (Robot).

I driver che portano le grandi organizzazioni a convergere su questi temi sono essenzialmente riconducibili a concetti ben definiti, che rappresentano un filo conduttore comune a questa nuova ondata di progresso tecnico e tecnologico. Prima di discutere brevemente questi concetti è utile elencare i benefici che questi sistemi comportano:

- Capacità di trasformare i modelli di business
- Possibilità di offrire un’esperienza sempre più immersiva e coinvolgente ai clienti

- Opportunità di rivedere i modelli operativi per ottimizzarli ed adeguarli ad un mercato sempre più veloce nei suoi tempi di trasformazione.

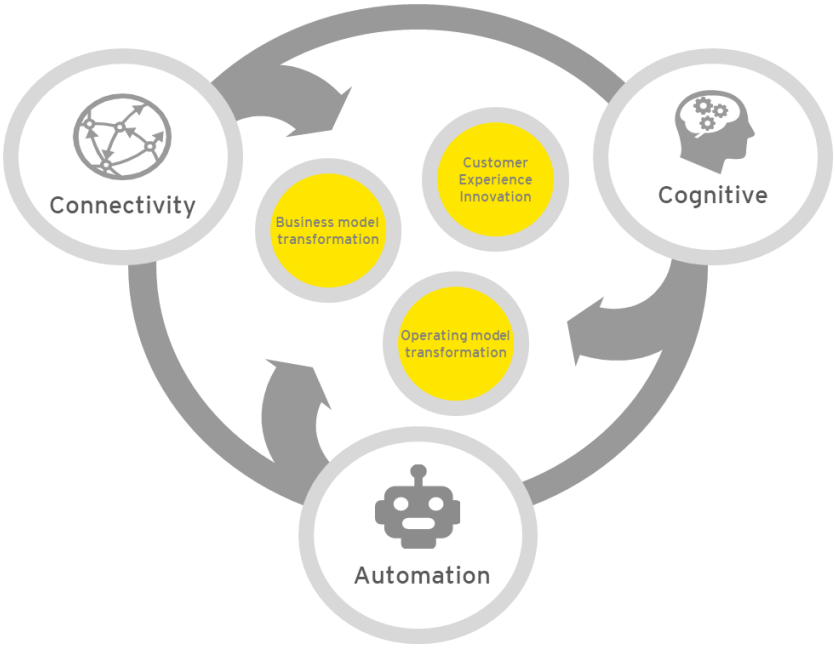


Figura 4 – Concetti "portanti" della digital transformation

Il primo punto fondamentale è rappresentato dalla connettività e dagli avanzamenti nel campo delle telecomunicazioni. La fusione di dati, piattaforme tecnologiche e dispositivi fisici eterogenei, accomunati da un sistema condiviso di interconnessione in tempo reale e quasi del tutto indipendente da confini geografici, sta sbloccando approcci completamente nuovi che prevedono sempre più collegamenti remoti senza l'effettiva necessità di trovarsi fisicamente all'interno di un ufficio. Su questo aspetto stiamo per assistere ad una vera e propria rivoluzione epocale con l'avvento del 5G. Per completezza di informazione il **termine 5G** significa **fifth generation**, quinta generazione, e sta ad indicare il nuovo modello di telecomunicazioni mobili che sostituirà l'attuale 4G. La rete usa una banda senza fili a

frequenza decisamente più alta, dal nome **millimeter wave**, che permette ai dati di viaggiare in modo più rapido. Sono diverse le stime riguardo all'effettiva **velocità della tecnologia 5G**. Secondo Verizon essa viaggerà 200 volte più rapidamente della 4G. Altri la reputano più bassa, sostenendo che essa sarà raddoppiata o triplicata rispetto all'attuale. Comunque, la International Telecommunication Union ha dichiarato che il **5G sarà capace di trasmettere 20 gigabyte per secondo**. I principali vantaggi offerti dalla ***rete 5G*** saranno

- **maggiore velocità,**
- **minore latenza**
- **la possibilità di gestire più dispositivi in contemporanea**.

I dati saranno trasmessi in modo **più veloce** a causa della più altra frequenza utilizzata. L'affidabilità dei dispositivi sarà perfezionata con all'abbassamento della latenza. Svariate funzionalità ed usi legati agli Internet of Things saranno sviluppabili grazie alla capacità di gestione "in contemporanea" di dispositivi eterogenei.

Il 5G sarà effettivamente il "brodo primordiale" dal quale nascerà una nuova civiltà che, solo qualche anno addietro, era immaginabile esclusivamente leggendo libri di fantascienza.

Un altro aspetto fondamentale è la tendenza a delegare l'aspetto cognitivo a computers o automi in generale. L'aumento di macchine artificialmente intelligenti sta guidando rapidi progressi nel calcolo cognitivo, dai chatbot (vale a dire software che rispondono ad un utente in una chat, imitando l'interazione con un essere umano) che semplificano le esperienze dei clienti, fino all'analisi avanzata, al riconoscimento delle immagini e all'apprendimento automatico introdotti dalle moderne tecniche di Intelligenza Artificiale e Machine Learning. E queste non sono tecnologie future ma già presenti da qualche anno e con un tasso di maturità in crescita esponenziale anno dopo anno. Era il lontano 2015 (nel mondo digitale quattro anni possono rappresentare davvero un lungo tempo) quando Ashley Madison, popolare sito di incontri hot, subì un databreach di oltre 60Gb di dati aziendali, comprensivi

di informazioni dettagliate degli utenti del sito. Queste informazioni finirono su vari siti di scambi dati o reti P2P. Alla gravità del databreach, che ha portato ad una class action del valore di $567 milioni, si aggiunse la notizia scioccante per la società puritana americana che Annalee Newitz, Editor-in-Chief di Gizmodo, durante l'analisi del databreach di Ashley Madison aveva rilevato che erano attivi sul sito circa 70000 chatboat femminili che inviavano messaggi ammiccanti ad utenti del sesso forte. E nessuno se ne era mai accorto. Se questo succedeva nel 2015 non è difficile presagire che oggi queste attività sono, oltre che in crescita, anche supportate con video, immagini o audio. Con questi presupposti occorre di questi tempi prestare particolari attenzioni alle fake-news che fanno spesso presa sugli utenti della rete con notizie che stravisano la realtà con conseguenze inimmaginabili per i singoli od intere comunità.

Associamo ora a questa innovazione l'altra che cammina parallelamente all'intelligenza artificiale ovvero l'automatizzazione dei processi. L'automazione delle operazioni, effettuate nei servizi in rete sia lato front-end (ovvero nell'interazione con l'utente) che back-end (ovvero dove avviene il normalmente il calcolo o processo vero e proprio, con l'interrogazione di dati sui Server) insieme agli incredibili sviluppi nell'interfaccia uomo-macchina, ha drasticamente trasformato le aspettative ed i bisogni dello stesso cliente sia rispetto la modalità di interazione con il servizio sia rispetto il servizio stesso. E questa trasformazione, guidata da intelligenza artificiale ed automatica, ha inevitabilmente costretto a ripensare e ridisegnare i processi aziendali incidendo in modo radicale sul modo con cui i servizi vengono erogati, sempre alla ricerca costante di diminuzione dei costi e miglioramento in efficienza. È un circolo autoalimentato che potremmo chiamare il vortice della "Digital transformation".

Tutto ciò ha ovviamente una potente incidenza sulla vita di ogni giorno dell'uomo.

Un saggio lo abbiamo già quando si ha a che fare con Smartphone e Smart Device in generale, apparecchi sempre connessi alla rete con un potere immenso in termini di accesso ad informazioni e servizi real-time. I benefici prodotti consistono nel risparmiare tempo e ridurre le energie applicate; con tale sistema è facile proiettare tutte queste innovazioni anche nell'ambiente nel quale si vive e si opera. Sempre più diffuso infatti è il tema "Smart Cities" ovvero intere città che si avvalgono dell'Internet of Things per fornire un miglioramento della vita degli abitanti, offrendo loro qualsivoglia tipo di servizio accessibile digitalmente.

Proviamo ad immaginare (ma spesso è già realtà in alcuni casi) una città composta di apparecchiature sempre interconnesse che riescono a ottimizzare la gestione dell'ambiente attraverso, ad esempio:

- sensori di inquinamento
- monitoraggio delle aree verdi
- smaltimento rifiuti
- stazioni metereologiche
- Connettività con strutture pubbliche e private
- Servizi di illuminazione e di fornitura idrica
- Trasporto urbano.

È facile ipotizzare quale rivoluzione può comportare un tale scenario. Con un accesso totale ai servizi è facile prevedere l'ottimizzazione delle politiche abitative e dei trasporti, il miglioramento delle relazioni tra le persone stesse e una totale trasparenza dei metodi di amministrazione della città. Da questo punto di vista, in una breve parentesi, alcuni problemi particolarmente complessi come la salvaguardia ambientale ed il controllo del clima potranno trovare soluzione grazie all'applicazione delle tecnologie precedentemente interpretate (avendo sempre presente di non cadere nelle apocalittiche conclusioni del

genero umano come previsto dalle già richiamate scene dei film futuristici di qualche anno fa).

Pur non potendo in questa ricerca focalizzarsi sulle smart cities, è comunque utile visualizzarne graficamente un probabile sviluppo:

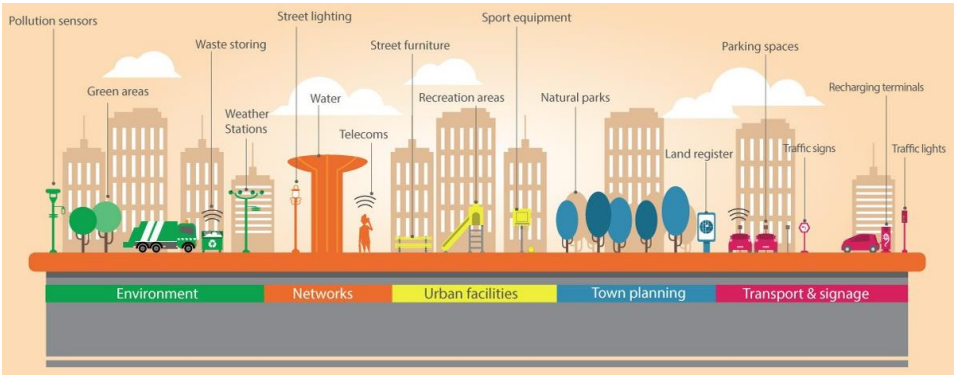


Figura 5 - Un esempio di "Smart City"

Guardando l'infografica della figura 5 si ha l'immediata sensazione che le possibilità e gli scenari che si apriranno con queste innovazioni "disruptive" sono ad oggi insondabili ed inimmaginabili.

Naturalmente quanto analizzato brevemente sinora è solo un esiguo set di esempi che, almeno per la sensibilità dell'autore che sta affrontando questa ricerca, sono più che sufficienti per far sperare in un futuro radioso piuttosto che in un mondo dominato da Matrix o Terminator.

Pur tuttavia occorre rimanere sempre vigili ed affrontare il tema della trasformazione digitale con grande serietà e, soprattutto, consapevolezza. La tecnologia porta in sé un concetto di vulnerabilità, che verrà approfondito più avanti, e dunque un'esposizione a possibili rischi.

Tecnologia e nuovi Driver – Scelte e scommesse

A questo punto dovrebbe essere abbastanza ovvia la determinazione che l'investimento in nuove tecnologie rappresenta certamente un'opportunità per migliorare la vita delle persone e potenziare le capacità delle aziende nel produrre fatturato e trarre profitto. Però, come è facilmente intuibile, l'utilizzo di queste incredibili tecnologie sottopone l'umanità ad altrettanti incredibili rischi.

Ritorniamo all'esempio delle Smart Cities. Immaginiamo che tutti quei dispositivi che si occupano di gestire traffico, segnali, sensori e servizi siano connessi alla rete. Come la cronaca ci insegna, esistono sempre agenti malevoli disposti ad attaccare un'organizzazione o anche una città, come dimostrato dagli assalti degli anni scorsi contro, come esempio, il colosso della grande distribuzione Target o Sony, o al Ransomware che ha tenuto interamente sotto scacco la città di Baltimora (Maryland, USA). La presenza di dispositivi con accesso continuo alla rete Internet potrebbe quindi rappresentare un grande rischio, specialmente se i costruttori insistono nel non applicare le Best Practice di sicurezza nei dispositivi IoT e nello sviluppo ed erogazione dei servizi.

Rischio al momento molto concreto visto che per troppo tempo la sicurezza è stata vista come una scelta a perdere, un investimento che non porta guadagno, quando invece è sufficiente capovolgere il discorso e rispondere ad una semplice domanda: ***"quanti danni economici può portare una sottovalutazione del rischio cyber? ".***

Se si presta la dovuta attenzione alla domanda precedente, è facile intendere che l'investimento "a perdere" diventa un investimento necessario per preservare tutte le attività aziendali con uno scudo informatico pronto a rintuzzare qualunque attacco o evento avverso. Le aziende che per prime hanno scommesso sulla sicurezza, al di là dell'efficienza e della produttività, sono quelle che si sono dimostrate tra le più vincenti in assoluto (ad esempio Google e Amazon hanno sempre prestato un occhio di riguardo per la sicurezza

informatica). Questo modo di affrontare la realtà aziendale sta sempre più convincendo le aziende stesse ad investire in sicurezza, riconoscendo la dovuta importanza all'aspetto del cyber security. L'esigenza di rendere cyber-sicuri i propri servizi o prodotti ha inciso notevolmente sulle priorità strategiche delle aziende (quantomeno le più strutturate). L'infografica seguente, estrapolata da un report EY del 2018, mostra chiaramente come si è spostato l'interesse delle organizzazioni negli ultimi due anni.

Figura 6 - Top 10 delle priorità strategiche 2018, con riferimento alla Top 10 2017

Il grafico evidenzia che l'anno passato Il tema della valorizzazione Cyber e della Data Security è salita al primo posto tra le prime dieci priorità strategiche aziendali, ancor prima dei piani di implementazione della Digital Transformation. Chiaro segnale di una consapevolezza crescente del ruolo abilitate ed imprescindibile della Sicurezza nella trasformazione Digitale. L'attenzione al tema cyber è particolarmente imprescindibile per la grande eterogeneità e complessità dei moderni ecosistemi che, per queste ragioni, sono sempre più difficili da governare comportando la complessità rischi crescenti.

Proteggere il futuro – il ruolo della Cybersecurity

Il grande interesse (ed impegno) da parte di aziende e governi per il tema Cyber Security non è quindi casuale ma nasce da dati sempre più preoccupanti, anche alla luce della recente cronaca. Il numero di attacchi informatici è destinato a crescere nel tempo cosi come chiaramente di mostra il grafico seguente.

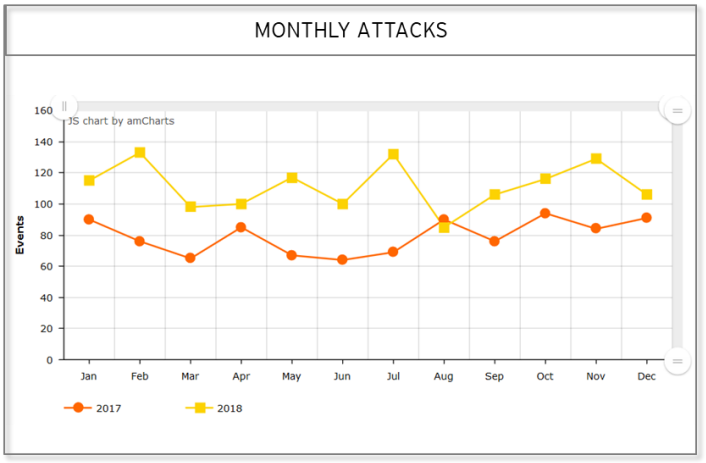


Figura 7 - Attacchi informatici per ogni mese, con riferimento al 2018 e al 2017 Fonte: hackmageddon.com

Mettendo a confronto infatti i dati degli ultimi anni (2017 e 2018) si registra un incremento degli attacchi informatici su ognuno dei dodici mesi dell'anno rispetto ai precedenti. I dati sottolineano anche un particolare aumento degli attacchi legati al Cyber Crime, finalizzati spesso all'estorsione di denaro o al sabotaggio di gruppi di aziende.

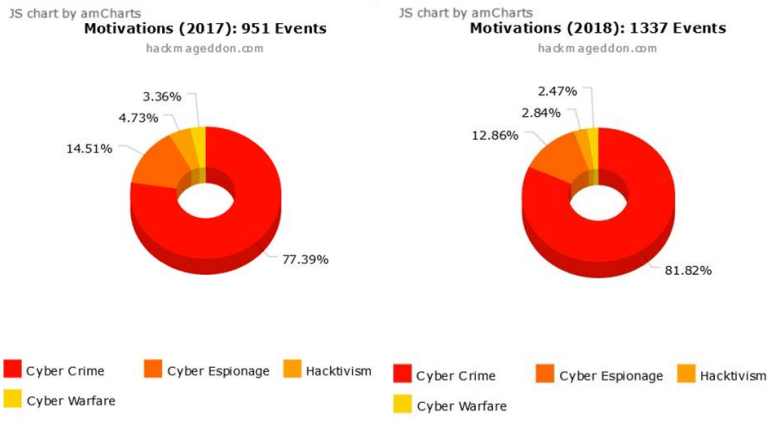


Figura 8 - Moventi degli attacchi informatici: 2017 e 2018. Fonte: hackmageddon.com

Un'altra grande preoccupazione deriva dal coinvolgimento di stati sovrani in azioni offensive, che testimonia una vera e propria guerra planetaria combattuta tramite attacchi hacker. Per questo negli ultimi anni si parla di "Cyber Warfare", che consiste in azioni di sabotaggio e spionaggio a danno dell'economia o dell'influenza di paesi nemici da parte di stati nazionali.

In alcuni casi il Cyber Crime e il Cyber Warfare possono anche essere strettamente collegati: si pensa infatti che dietro ad alcune azioni di Cyber Crimine, come la diffusione di alcuni Ransomware (vedi box più avanti) si celi in realtà la volontà distruttrice di superpotenze o stati cosiddetti "canaglia".

Un ransomware è una tipologia di malware che normalmente cifra informazioni sul nostro pc e non permette alcune funzionalità del computer infettato richiedendo un riscatto (dal termine "ransom", in inglese riscatto, e "ware", diminutivo di malware) richiesto (tipicamente in

BitCoin) per poter rimuovere il blocco delle funzionalità del pc o ripristinare i dati crittografati.

Oltre all'incremento di attacchi informatici è importante tenere presente le tipologie di attacco più diffuse nel mondo che potrebbero minacciare l'evoluzione tecnologica nel futuro. Il tipo di attacco più diffuso riguarda l'uso di Malware, vale a dire software malevolo, come nel caso dei Ransomware citati in precedenza. La diffusione di un Malware all'interno di una rete aziendale, o addirittura all'interno degli uffici di intere città rappresenta una gravissima minaccia in grado di paralizzare le funzionalità degli ambienti di lavoro, portando danni economici immensi specialmente vista la tendenza a digitalizzare massivamente i processi. Famoso l'attacco individuato lo scorso maggio alla città americana di Baltimora divenuta ostaggio di un attacco hacker sferrato tramite ransomware che ha paralizzato il funzionamento di sistemi It e di alcuni dei servizi erogati dall'amministrazione pubblica. Gli hacker chiedevano 3 Bitcoin per sbloccare un singolo sistema infettato o 13 Bitcoin per sbloccarli tutti. Come noto, il prezzo della valuta digitale è altamente fluttuante. Al momento dell'attacco il riscatto valeva 75.000 dollari.

Il grafico seguente chiaramente rappresenta la distribuzione degli attacchi dell'ultimo anno (2018):

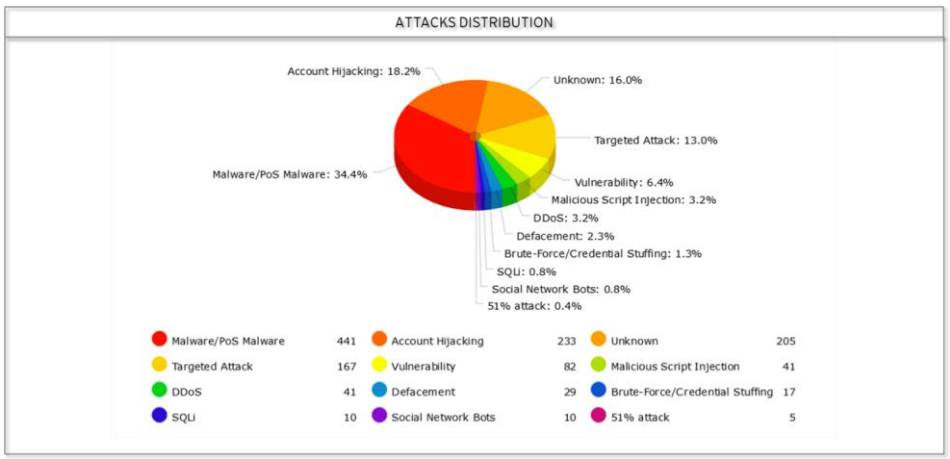


Figura 9 - Tipologie di attacco recentemente riscontrate. Fonte: hackmageddon.com

Se infatti in passato gli attacchi informatici rappresentavano fenomeni non solo sporadici, ma soprattutto legati ad ambienti di nicchia ed ad opera soprattutto di individui isolati che sfruttavano le vulnerabilità di un World Wide Web con ridotte misure di sicurezza, sia per tornaconto personale, attivismo informatico (Hacktivism) o semplicemente divertimento, l'escalation della minaccia in fenomeni di Cyber Crimine e di azioni "State-sponsored" ha implicato nel corso degli anni un aumento del rischio legato alle problematiche di Cyber Security. Gli attacchi sono diventati massivi, le esfiltrazioni di dati (Data Breach) e le frodi via mezzo informatico sono nel tempo diventate minacce sempre più probabili, con impatti notevoli e universalmente presenti. La corsa alla Digital Transformation significa infatti un drastico aumento dell'impatto distruttivo di azioni legate ad attacchi informatici, vista la diffusione e l'importanza centrale delle tecnologie non solo IT, legate quindi ai servizi telematici, ma anche OT (Operational Technology) come ad esempio la gestione dei controlli automatici all'interno di una centrale elettrica (anche nucleare) delegata a sistemi specifici, che costituiscono un potenziale bersaglio di eventuali azioni di sabotaggio. Ricordiamo il celebre attacco Malware per sistemi SCADA (Supervisory Control And Data

Acquisition, strettamente legati al mondo OT) noto come “Stuxnet”, contro gli impianti di energia nucleare iraniani, attribuito all’azione degli Stati Uniti d’America e presumibilmente atto a compromettere il programma nucleare. L’impatto di un attacco informatico può quindi raggiungere livelli critici anche per quanto riguarda l’erogazione di servizi essenziali.

Il compito della Cyber Security diventa quindi quello di proteggere tutto ciò che è alla base dell’evoluzione tecnologica. L’ affidabilità dei sistemi virtuali e automatizzati tende a fornire un’illusione di intangibilità e inattaccabilità, e le persone non sono in generale completamente al corrente delle reali problematiche di sicurezza legate, ad esempio, all’uso di Internet ogni giorno, o di come vengano portate a termine frode online tramite E-mail, o semplicemente dell’importanza di utilizzare Password sicure. Il Cyber Crimine non fa distinzione tra privati cittadini e aziende, pertanto chiunque è potenziale bersaglio di tentativi di attacco. L’illusione dell’intangibilità degli ambienti digitali si infrange contro il muro della realtà, in quanto la distinzione tra “virtuale” e reale sta assumendo contorni sempre più sfumati, in cui ciò che avviene nel Cyberspazio si ripercuote sulle nostre vite pian piano che la Digital Transformation avanza e cambia le nostre vite.

Probabilmente la miglior rappresentazione dei concetti su espressi ci è fornita dall’organizzazione ISF (Internet Security Forum) che, nel suo report “Threat Horizon 2020”, parla di “Digital Illusion Shatters” individua i tre principali pericoli rappresentati nell’infografica seguente:

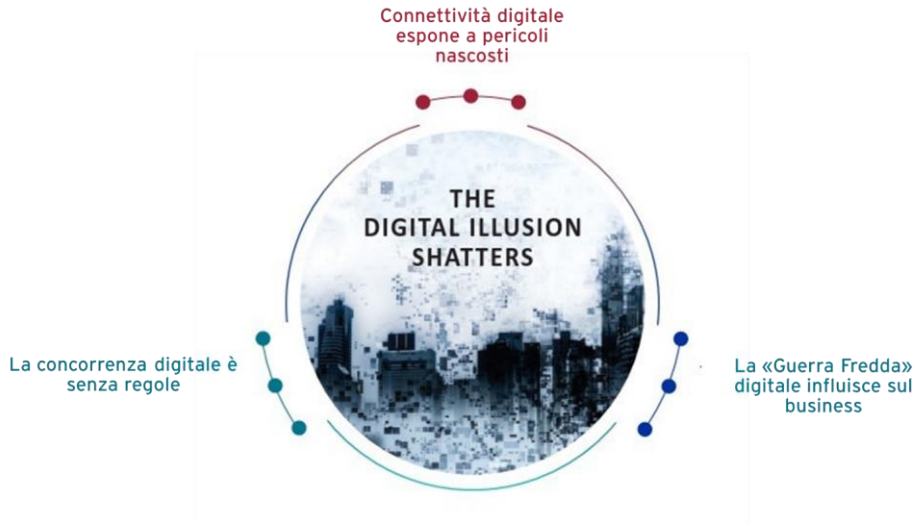


Figura 10 - La "bolla" dell'illusione di intangibilità del digitale e le minacce alla sicurezza digitale

Investire nella Cyber Security significa proteggersi contro i pericoli legati al Cyber Crimine, al Cyber Warfare e, nel caso delle aziende, da azioni di spionaggio industriale e sabotaggio da parte di aziende rivali che potrebbero agire nell'ombra. Se quindi vogliamo che l'evoluzione digitale continui, è necessario portare di pari passo un discorso di potenziamento in termini di Difesa Cyber. Anche se è stato fatto tanto in questi anni, ciò non sarà sicuramente sufficiente in futuro, foriero di moltiplicazioni delle minacce in termini non solo di numero ma anche di intensità.

Capito 2 Opportunità e Rischi. Gli interventi regolatori

Digital Transformation tra vantaggi e pericoli

Nonostante i grandi rischi legati al potenziamento del lato digitale delle nostre vite, la Digital Transformation comporta vantaggi troppo grandi per far sì che a causa dei rischi si fermi l'avanzamento della tecnologia e della digitalizzazione. Dell'innegabile vantaggio e della diffusione pressoché totale delle tecnologie digitali in ogni settore della nostra vita sembrano ormai convinti i vertici aziendali, i governi e le istituzioni internazionali.

Come ogni cosa, dunque, la Digital Transformation ha i suoi lati positivi e negativi. Da un lato l'incremento della produzione, dell'efficienza e dell'efficacia dei servizi offerti dalle nuove tecnologie (sia in termini privati che di Business) rappresenta un notevole incentivo ad adottare con facilità innovazioni e nuovi paradigmi. Dall'altro lato ci espone a grossi pericoli dovuti soprattutto ad un approccio che tende a potenziare le capacità tecnologiche senza di pari passo aumentare il livello di guardia rispetto alle minacce informatiche, sempre presenti e destinate a crescere con l'aumento del livello delle soluzioni tecnologiche e, in generale, della potenza computazionale e di connettività e trasmissione di dati. È evidente come l'impatto di qualsiasi azione malevola con mezzi telematici sia amplificato in un mondo tecno-dipendente, iperconnesso e scarsamente consapevole dei rischi che si corrono.

Per questo motivo, allo scopo di cogliere i frutti del progresso tecnologico in modo ottimale, è necessario mitigare il più possibile i pericoli. Pericoli che nei prossimi tre anni, con la diffusione del 5G, intelligenza artificiale e l'imminente commercializzazione di computer quantistici, sono destinati a crescere prepotentemente.

Quest'ultimo tema (quello relativo ai computer quantistici) potrebbe effettivamente rappresentare un momento critico visto che uno degli strumenti di cyber defense moderno,

ovvero la crittografia, perderebbe di colpo la sua efficace a causa dell'incredibile potenza di calcolo di questa nuova classe di calcolatori.

A fronte dell'evoluzione tecnologica è quindi necessario potenziare di pari passo gli aspetti relativi alla sicurezza in un discorso interamente parallelo, sia dal lato di soluzioni tecnologiche, know-how, standard e leggi.

Di certo non si possono fare previsioni precise del futuro e di quel che potrebbe accadere, però con una cyber security all'altezza del suo compito si può certamente affrontare il futuro con un lucido ottimismo e con la capacità di fare scelte informate, ponderate e consapevoli.

Il business dell'insicurezza

È chiaro che, alla luce di quanto detto sinora, il tema debba essere affrontato in modo organico con importanti interventi regolatori ed una presa di coscienza assoluta sul pericolo che corriamo e sulle azioni da realizzare a tutti i livelli ovvero Governo – Aziende – Cittadini. Ma prima di addentrarci nel riepilogo degli ultimi (importanti) sforzi regolatori, che prenderanno in considerazione esclusivamente lo scenario comunitario e nazionale, è utile fare delle considerazioni su un concetto particolarmente importante, espresso da Shoshana Zuboff nel 2014, ovvero il "**surveillance capitalism**". Il termine "**surveillance capitalism**" descrive un processo guidato dal mercato in cui la merce in vendita sono i dati personali e l'acquisizione e produzione di questi dati si basa sulla sorveglianza di massa di Internet. Questa attività viene spesso svolta da aziende che ci forniscono servizi online gratuiti, come motori di ricerca (Google) e piattaforme di social media (Facebook).

Queste aziende raccolgono e controllano i nostri comportamenti online (Like, commenti ed orientamenti, ricerche, social network, acquisti) per produrre dati che possono essere ulteriormente utilizzati a fini commerciali. Ed è spesso fatto senza che noi comprendiamo la portata della sorveglianza. Non bisogna essere un esperto conoscitore delle dinamiche digitali o essere un esperto di sicurezza per capire che le più grandi Corporation hanno

manipolato il network per i propri fini personali. E sono normalmente quelle stesse corporation che offrono le soluzioni più sicure sul mercato tranne poi acquisire ogni tipo di informazione a loro utili o monitorare qualsivoglia azione compiuta dagli utenti. L'insicurezza, in fin dei conti, è un grosso business ed un preciso interesse di svariati soggetti. E tutte le Big lottano per diventare "centrali" ed "essenziali" nel controllo del nostro mondo digitale ed è molto probabile che nei prossimi anni assisteremo a feroci battaglie fra titani (in realtà già in corso) per il controllo degli utenti e, quindi, dei clienti.

Ma su questo tema non bisogna commettere l'errore di imputarlo esclusivamente al mondo privato. L'insicurezza è anche un interesse Governativo (o meglio di alcuni governi). Ovviamente per motivazioni diverse dal mondo privato che ha, nel mero profitto, l'interesse principale. Per molti governi governare l'insicurezza è un interesse per poter effettuare azioni di "Law enforcement", controllo sociale e spionaggio. E abbiamo già molte prove ed esempi di questo interesse. Il Messico, e sono informazioni di dominio pubblico, ha acquistato software per monitorare giornalisti, dissidenti ed operatori politici.

Un importante Spyware governativo, FinFisher, è usato da governi come la Bosnia, l'Egitto, l'Indonesia, la Giordania, il Venezuela, la Turchia e tanti altri.

Esistono ormai aziende ultra-specializzate nella produzione di sistemi di sorveglianza di massa che possono contare su un mercato a grande crescita (Famoso il caso dell'azienda italiana HackingTeam).

Pensiamo inoltre all'eclatante caso "Cinese" con il progetto 2020 con il quale avvierà un "social credit system" con il quale verrà attribuito uno score "digitale" ad ogni cittadino. Score basato su inquietanti meccanismi di sorveglianza.

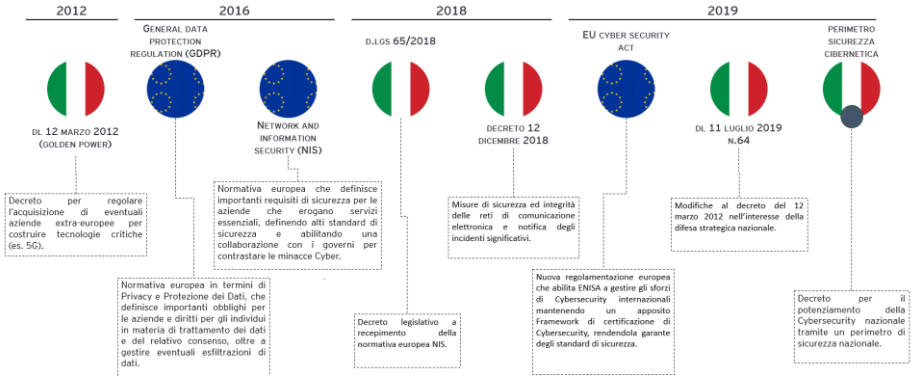
È vero che parliamo di Governi "particolari", che possono contare sulla collaborazione di Telco, di Produttori di Hardware e Software e di grandi Corporate Digitali, ma gli scenari su

descritti esistono diffusamente e rappresentano una seria minaccia alla nostra libertà personale e minano il concetto stesso di democrazia. Per fortuna siamo però in Europa che, seppur conta qualche caso accomunabile a qualcuno di quelli descritti, è un continente in cui le libertà personali e la democrazia rappresentano dei beni che si ritengono necessari ad essere difesi. E questa difesa, perlomeno sul campo di guerra cyber, è attuata attraverso importanti interventi regolatori.

Interventi regolatori in Europa ed Italia

Gli ultimi anni sono stati particolarmente intensi sul fronte dell'azione regolatoria, comunitaria e Nazionale, sui temi di Cybersecurity. Ovviamente con qualche anno di ritardo rispetto i nostri buoni amici americani ma, come dice il detto, meglio tardi che mai.

Gli sforzi sono chiaramente visibili nell'infografica seguente che rappresenta i più importanti interventi regolatori degli ultimi dieci anni:



È assolutamente doveroso, seppur non è possibile approfondire in questa ricerca ciascun elemento, ricordare brevemente cosa comportano gli interventi indicati nell'infografica.

Decreto 15 Marzo 2012 – Golden Power

Non è un decreto strettamente legato al contesto Cyber ma ha assunto poi, nell'ultimo periodo, una rilevanza particolare per il mondo IT. Il decreto originale nasce con lo scopo di salvaguardare gli assetti proprietari delle società operanti in settori reputati strategici e di interesse nazionale conferendo al governo poteri speciali. Si tratta, in particolare, di poteri esercitabili nei settori della **difesa** e della **sicurezza nazionale,** nonché di taluni ambiti di attività definiti di rilevanza strategica nei settori dell'**energia,** dei **trasporti** e delle **comunicazioni.** Per **poteri speciali (golden power)** si intendono, tra gli altri, la facoltà di dettare specifiche condizioni all'acquisito di partecipazioni, di porre il veto all'adozione di determinate delibere societarie e di opporsi all'acquisto di partecipazioni societarie.

General Data Protection Regulation

Emanato il 27 aprile 2016, il Regolamento UE 2016/679 o GDPR (General Data Protection Regulation) è definitivamente in vigore dal 25 maggio 2018 in tutti gli stati membri dell'Unione Europea e regola la gestione dei dati personali (privacy) senza necessità di leggi nazionali di recepimento. Con questa nuova normativa il legislatore europeo ha voluto rendere più forte e più omogenea la protezione dei dati personali sia dei cittadini europei sia di coloro che risiedono nell'Unione Europea, all'interno o all'esterno dei confini dell'Unione europea (UE). Il GDPR è un nuovo insieme di regole per la tutela della privacy a livello europeo, nato per effetto della globalizzazione e della diffusione delle tecnologie digitali degli ultimi decenni, che hanno portato ad un continuo aumento dello scambio quotidiano di dati in rete. Nell'evoluzione storica degli eventi relativi alla privacy, il GDPR rappresenta un evento che segna il prima e il dopo o meglio l'inizio di una nuova epoca in tema di diritto ad esercitare un controllo sulle informazioni che si rilasciano e che riguardano la persona fisica. Il GDPR cambia l'approccio alla gestione dei dati personali: da una visione puramente giuridica si è passati ad una prospettiva strategica per una nuova economia dei dati. Nasce

per essere Statuto della Data Economy e definisce le regole per usare i dati legalmente e dare avvio a innovazione di prodotti e servizi, creando una prospettiva di nuovi fatturati e maggiore lavoro.

Network and Information Security (Direttiva NIS)

Il 6 luglio 2016 il Parlamento Europeo ha adottato la direttiva sulla sicurezza dei sistemi delle reti e dell'informazione comunemente conosciuta come direttiva NIS. Essa rappresenta il primo insieme di regole sulla sicurezza informatica univoco a livello dell'Unione Europea. L'obiettivo della direttiva è raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti i Paesi membri dell'UE.

I tre punti chiave della direttiva NIS sono:

- Migliorare le capacità di cyber security dei singoli Stati dell'Unione;
- Aumentare il livello di cooperazione tra gli Stati dell'Unione;
- Obbligo di gestione dei rischi e di riportare gli incidenti di una certa entità da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali.

Relativamente al miglioramento delle capacità dei singoli Stati dell'Unione, la direttiva NIS sottolinea alcuni principi necessari per rispettare i criteri adottati. Ogni Stato infatti dovrà dotarsi, qualora già non l'avesse, di una strategia nazionale di cyber security che definisca gli obiettivi strategici, le politiche adeguate e le misure di regolamentazione. Tra gli aspetti che una strategia nazionale dovrebbe includere vengono citati gli obiettivi strategici, le priorità nazionali, la governance, l'individuazione di misure proattive, di risposta e di recovery; sensibilizzazione, formazione ed istruzione; incentivazione della cooperazione tra settore pubblico e settore privato; lista degli attori coinvolti nella attuazione della strategia. La direttiva NIS richiede agli Stati di designare una o più autorità competenti per il controllo dell'applicazione della direttiva stessa a livello nazionale. Un singolo punto di contatto dovrà essere designato da ognuno degli Stati membri, con il compito di assicurare la cooperazione

internazionale e di collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati della direttiva stessa. Ogni Stato dovrà infine designare uno o più **CSIRT** (Computer Security Incident Response Team) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti. La cooperazione tra i vari enti dei singoli Stati membri è un punto veramente fondamentale della direttiva NIS. Proprio per questo è stato stabilito un gruppo di cooperazione che faciliti i rapporti tra gli Stati membri e che aumenti la fiducia. L'ultimo dei punti principali della direttiva riguarda gli operatori dei servizi essenziali per la Nazione e i fornitori di servizi digitali. Gli operatori di servizi essenziali sono aziende pubbliche o private che hanno un ruolo importante per la società e l'economia, quelli che comunemente vengono chiamate "infrastrutture critiche".

La direttiva NIS obbligherà queste entità a dotarsi di misure di sicurezza appropriate e di notificare all'autorità nazionale competente gravi incidenti di sicurezza secondo parametri di numero di utenti coinvolti, durata dell'incidente e diffusione geografica. Le misure di sicurezza richieste comprendono: prevenzione dei rischi; garantire la sicurezza dei sistemi, delle reti e delle informazioni; capacità di gestire gli incidenti. Queste entità verranno identificate direttamente da ogni Stato membro, all'interno dei seguenti ambiti: energia, trasporti, banche e società finanziarie, salute, acqua ed infrastrutture digitali.

Anche i fornitori di servizi digitali saranno tenuti, secondo la direttiva NIS, ad attuare misure di sicurezza appropriate e a notificare incidenti rilevanti. Oltre alle misure già previste per gli operatori di servizi essenziali, le misure di sicurezza relative ai fornitori di servizi digitali prevedono alcuni fattori specifici, come ad esempio la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i test e la conformità a norme internazionali.

Decreto-legge 65/2018

Decreto di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS). Il decreto legislativo, che recepisce la Direttiva NIS, prevede l'adozione di misure tecnico-organizzative per ridurre il rischio e limitare l'impatto di incidenti informatici e l'obbligo di notifica di incidenti con impatto rilevante sulla fornitura dei servizi. Parallelamente, individua le Autorità competenti NIS (il Ministero dello sviluppo economico, il Ministero delle infrastrutture e trasporti, il Ministero dell'economia e finanza, il Ministero della salute e il Ministero dell'ambiente) e i rispettivi compiti svolti in cooperazione con le omologhe Autorità degli Stati Membri dell'UE. Si istituisce, inoltre, il CSIRT (Computer Security Incident Response Team) italiano con compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici svolti in cooperazione con gli altri CSIRT europei e il Punto di contatto unico, organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea.

Decreto-legge 12/12/2018

Il DM 12 dicembre 2018 "Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi" ha lo scopo di individuare le "adeguate misure di natura tecnico-organizzativa" necessarie a prevenire e limitare l'impatto degli incidenti che potrebbero "pregiudicare la sicurezza per gli utenti e per le reti interconnesse".

Vengono stabiliti i campi di applicazione: servizi di comunicazione con accesso alla rete fissa o mobile da postazione fissa e accesso alla rete fissa o mobile da terminale mobile, fornitori di reti e servizi di comunicazione elettronica "che servono un numero di utenti effettivo pari o superiore all'1% della base di utenti nazionale".

Il Decreto indica i parametri che definiscono la “significatività” di un incidente. I criteri da tenere in considerazione sono la durata del disservizio e la percentuale degli utenti colpiti rispetto al totale degli utenti nazionali.

Infine, il DM stabilisce che “entro novanta giorni” dall'entrata in vigore del decreto i fornitori di reti e servizi devono trasmettere all’Istituto superiore delle comunicazioni e delle tecnologie dell'informazione del Mise (Iscti) l’elenco degli asset critici.

EU Cybersecurity ACT

Il Cybersecurity Act costituisce una parte fondamentale della nuova strategia dell’UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell’Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali. Lo strumento normativo in questione si affianca, ed è in parte complementare, alla prima normativa in materia di sicurezza cibernetica introdotta a livello dell’Unione, ossia la Direttiva NIS. **Il Cybersecurity Act si compone di due parti**: nella prima vengono specificati il ruolo e il mandato dell’Enisa, mentre nella seconda viene introdotto un sistema europeo per la certificazione della sicurezza informatica dei dispositivi connessi ad Internet e di altri prodotti e servizi digitali. Trattandosi di un Regolamento, una volta entrato in vigore, il Cybersecurity Act sarà immediatamente applicabile in tutti gli Stati membri, senza che vi sia necessità di interventi attuativi da parte dei legislatori nazionali, salvo per quanta riguarda alcune limitate disposizioni, ad esempio in materia di sanzioni. Un primo punto chiave del Cybersecurity Act riguarda il rafforzamento del ruolo dell’Agenzia dell’Unione europea per la sicurezza delle reti e dell’informazione (ENISA). Un altro punto chiave del Cybersecurity Act riguarda l’introduzione di un **sistema europeo di certificazione della sicurezza informatica dei prodotti e dei servizi digitali**. Ciò anche al fine di **facilitare lo scambio degli stessi**

all'interno dell'Unione europea e di accrescere la fiducia dei consumatori nei medesimi.

Decreto n° 65 11 Luglio 2014 – Golden Power 5G

Delibera di poteri dei poteri speciali – a norma dell'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21 – in relazione all'**acquisto di beni e servizi legati al 5G** da parte di **Linkem, Vodafone, Tim, Wind Tre e Fastweb**. E i provvedimenti ricadono indirettamente anche su **Huawei e Zte.** Il nuovo golden power impone alle aziende di telecomunicazioni di notificare gli acquisti da aziende extra-europee per costruire le reti di 5G. Il governo ha l'ultima parola sui contratti: può accettarli in toto, bloccarli o imporre condizioni o prescrizioni. Come ha fatto, in questo caso, con Vodafone e Wind Tre, per esempio. Di fatto, l'obiettivo dello scudo è di monitorare tecnologie critiche come quelle di comunicazione, specie per il 5G, prima che siano installate.

Decreto-legge 21 Settembre 2019

Il Dl 21 settembre 2019, n. 105. – "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" introduce disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. Il decreto mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

Inoltre, il testo integra e adegua il quadro normativo in materia di esercizio dei poteri speciali da parte del Governo, con particolare riferimento a quanto previsto dal decreto-legge 15 marzo 2012, n. 21, in modo da coordinare l'attuazione del Regolamento (UE) 2019/452, sul

controllo degli investimenti esteri, e apprestare idonee misure di tutela di infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione del decreto-legge 15 marzo 2012, n. 21.

Le nuove norme, tra l'altro:

- definiscono le finalità del perimetro e le modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica;
- prevedono il coinvolgimento del Comitato interministeriale per la sicurezza della Repubblica (CISR) nella fase attuativa;
- Istituiscono un meccanismo teso ad assicurare un procurement più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi di information and communication technology (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti;
- Prevedono che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa e, con riferimento alle autorizzazioni già rilasciate ai sensi del decreto-legge 15 marzo 2012, n. 21, la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi standard.

Capito 3 Opportunità per il sistema paese Italia

Guardando i dati del Paese si rileva che la nostra è un'economia in fase di stallo (crescita stimata del PIL 2019: +0,2%; crescita annua '14-'18 del PIL: +1,1%) e che, nel quadro di riferimento internazionale, mostra performance inferiori anche rispetto a quelle economie meno virtuose (che hanno risentito maggiormente della crisi) ma che oggi mostrano segnali di maggiore vitalità (crescita annua '14-'18: Spagna +3,1%; Portogallo +2,1%; Grecia +0,7%, ma con crescita prevista nel 2019 del 2,2%).

Al Paese vengono internazionalmente riconosciuti fattori di assoluta distintività ed attrattività tra cui, senza pretese di esaustività, possiamo citare i settori Fashion&Luxury, Turismo, Agrifood, Manifattura. A questi elementi di distintività, si associano fondamentali solidi come un risparmio privato tra i più grandi al mondo, un modello sanitario universalistico tra i più evoluti, una popolazione lavorativa con elevatissimo grado di specializzazione, un posizionamento geografico strategico.

A fronte di questi elementi, però, l'**Italia**:

- **Fatica ad attrarre investimenti stranieri**, i cd. *FDI-Foreign Direct Investments*, soprattutto se comparata rispetto ai peers internazionali (FDI inflow pari all'1,1% del PIL, vs Olanda 7.0%, Svizzera 5.7%, Inghilterra 3,9%)
- **Presenta poche imprese "champion" internazionali** (solo 6 aziende nella lista *Fortune Top 500*, vs 28 Francia, 20 Germania, 20 UK)
- **Vede la crescita di alcuni settori chiave al di sotto del potenziale** (ad esempio il Turismo che cresce meno dei peers, con una crescita media annua '14-'18 +3,8%, vs UK 4,6% e Spagna 4,7%)

Bisogna necessariamente intraprendere una serie di azioni tese a risolvere fattivamente questa situazione di stallo e lavorare affinché nuove iniziative possano dare uno nuovo slancio alla crescita del Paese.

Una delle azioni chiave per il rilancio consiste sicuramente nel concretizzare una “messa in sicurezza” del Paese, facendone un elemento caratterizzante di quei settori chiave che oggi, pur avendo fondamentali forti, fanno fatica ad attirare investitori (sia nazionali che esteri) e a far crescere le aziende che vi operano.

La messa in sicurezza del Paese oggi ha molteplici significati ciascuno dei quali con pesi specifici importanti:

- nell’opinione pubblica
- nel mondo del business
- nelle agende politiche

Come largamente trattato nei paragrafi precedenti, assistiamo a Cyberattacchi quotidiani sempre più sofisticati e letali e cresce dunque la necessità della riqualificazione e sviluppo di infrastrutture adeguate a questi nuovi scenari.

È fondamentale l’adozione di misure di sicurezza adeguate a protezione del cyber spazio ormai divenuto elemento essenziale dell’economia e della stessa società, con buona parte delle attività economiche che già oggi sono, in una o più fasi, intermediate da infrastrutture e servizi digitali. Gli sforzi normativi accennati nel capitolo precedente sono un ottimo inizio ma non sufficiente e soprattutto generico.

La digitalizzazione avanza a ritmi vertiginosi guidata da importanti innovazioni tecnologiche e dalla necessità delle organizzazioni (pubbliche e private) di rivedere ed innovare i propri processi di business. È un processo irreversibile che vedrà, nei prossimi mesi, una spinta propulsiva senza precedenti con l’introduzione del 5G e dei nuovi computer quantici.

Digitalizzazione ed iperconnettività, pur creando un senso di stabilità ed affidabilità, in realtà espongono ogni attività a nuove vulnerabilità e, dunque, a possibili cyber-attacchi. Ecco allora che la cyber security assume oggi un ruolo fondamentale a garanzia del mantenimento della “digital society” e “digital economy” e, ancor di più, per la sua evoluzione.

La cybersecurity è essenziale sia per la nostra prosperità che per la nostra sicurezza.

Da qui la necessità forte di individuare ed implementare modelli di cyber-security per:

- **Proteggere gli operatori e le imprese** che lavorano in Italia, anche in modo da rendere più attrattivo il sistema Paese per gli investimenti esteri (FDI), puntando a far sì che gli investitori possano identificare l’Italia come un Paese pioniere del cyber security, (in grado quindi di proteggere al meglio le loro attività di business)
- **Proteggere gli utilizzatori** (sia privati cittadini, che piccole-medie imprese) dei prodotti/ servizi digitali
- **Garantire** adeguati livelli di **fiducia** nei sistemi digitali per sostenerne la crescita

Molto è stato fatto negli ultimi anni sia a livello comunitario che a livello Italiano.

Su questo fronte il Governo e le Agenzie mostrano forte attenzione ed hanno già compiuto passi significativi. In Italia è stata individuato nel Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio DIS la responsabilità di coordinare la prevenzione e gestione delle crisi cibernetiche mediante il Nucleo per la sicurezza cibernetica (NSC) e con il recente D.lgs 65/2018, in attuazione della direttiva NIS, si istituisce uno CSIRT (Computer Security Incident Response Team) pubblico nazionale, si attribuisce al DIS il ruolo di punto di contatto con le istituzioni dell’Unione e si individuano le autorità responsabili dell’attuazione delle misure previste dalla direttiva per i settori economici considerati

strategici (Energia – Trasporto – Sanità -Strutture finanziarie – Sistema bancario – Acqua potabile – Infrastrutture Digitali – Servizi Digitali).

Nonostante gli sforzi fatti, vista la complessità e vastità della materia, il nostro livello di esposizione è ancora troppo alto e soffriamo nell'implementazione diretta degli strumenti ad oggi a nostra disposizione.

Le agenzie responsabili della cybersecurity, infatti, soffrono di una organica insufficienza di risorse umane ed economiche con un inevitabile rallentamento nella capacità di azione.

La governance della cybersecurity è fortemente frammentata e le competenze, a livello pubblico e privato, scarseggiano come confermato dall'ultimo report dell'istituto ISC2 che evidenzia, al 2022, la mancanza di 350.000 professionisti della cybersecurity in EU.

Manca ancora la giusta consapevolezza sia a livello pubblico che privato ed alcuni settori non percepiscono adeguatamente il problema rischiando di perdere competitività internazionale.

Delicata è la situazione delle PMI (modello produttivo primario per il nostro sistema paese) che, per l'incapacità di investire e la mancanza di giuste competenze, rischiano oggi di rappresentare l'anello debole del sistema (proprio la "supply chain" è oggi il veicolo principale per l'esecuzione di attacchi cibernetici alle strutture strategiche) e perdere significative quote di mercato. Interi settori commerciali, senza le giuste contromisure, potrebbero essere fortemente penalizzati. Per dare un esempio concreto, secondo il world economic forum, la competitività dei sistemi turistici nazionali è correlata a 14 pillar due dei quali si riferiscono a 'safety and security' (Pillar 3) e 'ICT infrastructure' (Pillar 9).

Il sistema paese deve necessariamente essere capace di rispondere alle nuove sfide non subendole ma trasformandole in grandi opportunità di crescita economica e posizionamento internazionale.

Bisogna accelerare e dare forza alle iniziative. Serve una governance forte ed un piano operativo accelerato per mettere in sicurezza il paese ed il suo tessuto produttivo e dare spinta alla ripresa economica. Oggi si ritiene necessario curare la realizzazione della sicurezza informatica mediante l'approfondimento dei punti successivi:

- La definizione di un piano di spinta evolutiva sulla cybersecurity, da intersecare con quanto già previsto dal Piano Nazionale e sul relativo stato di avanzamento, in termini di "normazione" di regole, procedure e infrastrutture. L'obiettivo è quello di creare le condizioni per la cyber security lavorando su cinque macro-ambiti di attività:
    - Identificazione e sistematizzazione di un **modello di governance forte** e dei meccanismi di controllo, in termini di ruoli, responsabilità, processi necessari per il funzionamento della macchina organizzativa ed operativa
    - Definizione di **modelli concreti di cooperazione e sviluppo** come:
        - Distretti: focalizzati a ricerca e sviluppo sulla cyber, collegati a università e centri produttivi
        - La costituzione o individuazione di un ente che si occupi di rendere operativa la partnership pubblico privato ed università (PPP)
        - Rafforzamento dell'ecosistema per una difesa "sistemica"
        - Creazione di servizi cyber sostenibili per piccole medie aziende
        - Definizione delle **modalità di intervento diretto**, ad esempio tramite l'ingresso nel capitale delle aziende strategiche, il funding e l'indirizzo di startup dedicate, defiscalizzazione investimenti cyber
        - Disegno ed implementazione di **campagne di formazione\sensibilizzazione**, sia dedicate alle aziende che alla popolazione (ad esempio con formazione scolastica sin dalle scuole

primarie e programmi di scambio con paesi ad alto tasso di sviluppo sulla tematica)

- Definizione di un **modello di cooperazione internazionale**, tramite ad esempio l'incremento e il rafforzamento della partecipazione ai tavoli congiunti comunità EU-NATO e partnership internazionali pubblico-private (US-ISR)

Declinazione per settore del modello di cybersecurity, partendo da quelli individuati dalla direttiva NIS e allargando su quelli più rilevanti/ distintivi per il nostro Paese, su cui iniziare ad implementare le attività identificate, tenendo in considerazione alcune variabili sulla base delle quali "personalizzare" approccio e modelli:

- Livello di esposizione alla digitalizzazione
- Livello di internazionalizzazione

In via di sperimentazione si dovrebbe puntare sulla messa in sicurezza dei settori altamente strategici per il nostro sistema economico come il Turismo, Alimentare, Manufatturiero e Cantieristico (tema che parzialmente è stato indirizzato con il decreto-legge 21-settembre-2019)

È necessario comprendere che, secondo gli indirizzi comunitari, le nostre aziende, per sopravvivere e crescere nel mercato internazionale, dovranno necessariamente intraprendere un percorso virtuoso per poter dimostrare la loro maturità rispetto al tema cybersecurity. E le aziende saranno più forti se l'ecosistema su cui poggiano fornisce le giuste garanzie di resilienza ed affidabilità di servizi ed infrastrutture.

È fondamentale, per il nostro Paese, agire tempestivamente e diventare un punto di riferimento, non solo comunitario, per le aziende. Non possiamo perdere quest'ulteriore opportunità!

Bibliography

- World Economic Forum – Global Risk Report 2019
- ISF – Threat Horizon Report
- Rapporto Clusit sulla sicurezza informatica 2019
- The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power
- Finfisher : https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
- The Chinese Social-Credit System Experience: A National Reputation System In The Making
- hackmageddon.com - Information Security Timelines and Statistics
- Bruce Snider : Click Here to Kill Everybody
- Marilyn Wolf · Dimitrios Serpanos : Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems
- Cyber Security and Global Information Assurance Threat Analysis and Response Solutions